Dell™ AppAssure™

Guia do usuário

5.4.3 Revisão B

© 2015 Dell Inc.
TODOS OS DIREITOS RESERVADOS.

Este guia contém informações proprietárias protegidas por direitos autorais. O software descrito neste guia é fornecido com uma licença de software ou um acordo de não divulgação. Este software pode ser usado ou copiado somente segundo os termos do acordo aplicável. Nenhuma parte deste guia pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópias e gravações para qualquer outro fim que não o uso pessoal do comprador sem permissão por escrito da Dell Inc.

As informações contidas neste documento são fornecidas em conjunto com os produtos da Dell. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a quaisquer direitos de propriedade intelectual é concedida por este documento ou em conexão com a venda dos produtos da Dell. EXCETO CONFORME DEFINIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO ACORDO DE LICENÇA DESTE PRODUTO, A DELL NÃO ASSUME NENHUMA RESPONSABILIDADE E RENUNCIA QUALQUER GARANTIA EXPRESSA, IMPLÍCITA OU ESTABELECIDA POR LEI RELACIONADA A SEUS PRODUTOS INCLUINDO, MAS NÃO LIMITADO A, GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA OU NÃO VIOLAÇÃO. EM NENHUMA CIRSCUSTÂNCIA A DELL SERÁ RESPONSÁVEL POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENCIAIS, PUNITIVOS, ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) RESULTANTES DO USO OU DA INCAPACIDADE DE USAR ESTE DOCUMENTO, MESMO SE A DELL TIVER SIDO NOTIFICADA A RESPEITO DA POSSIBILIDADE DE TAIS DANOS. A Dell não faz representações ou garantias com relação à precisão ou integridade do conteúdo deste documento e se reserva o direito de fazer alterações em especificações e descrições de produtos a qualquer momento e sem aviso. A Dell não faz nenhum compromisso em atualizar as informações contidas neste documento.

Se você tem quaisquer dúvidas ou perguntas sobre seu potencial uso deste material, entre em contato com:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Consulte o nosso website (software.dell.com/br-pt) para obter informações de contato de escritórios regionais e internacionais.

O software Dell AppAssure faz uso da biblioteca de links dinâmicos (DLL) Emit Mapper v. 1.0.0, licenciada nos termos da Licença Pública Geral de Biblioteca GNU (LGPL) versão 2.1, de fevereiro de 1999. O aviso de direitos autorais do Emit Mapper é: “Copyright © 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 EUA. Todos têm permissão para copiar e distribuir cópias idênticas deste documento de licença, porém não é permitido alterá-lo.”

Os usuários poderão visualizar o texto completo da licença LGPL quando for publicada como um acordo de licença de terceiros em http://www.software.dell.com/legal/license-agreements.aspx. O código fonte do Emit Mapper poderá ser localizado em http://opensource.dell.com/.

Marcas registradas

Dell, o logotipo da Dell e AppAssure são marcas registradas da Dell Inc. e/ou seus afiliados. Outras marcas registradas e nomes comerciais poderão ser usados neste documento para se referir às entidades proprietárias das marcas e nomes ou a seus produtos. A Dell renuncia qualquer interesse de propriedade nas marcas e nomes de terceiros.

Legendas

CUIDADO: o ícone de CUIDADO indica a possibilidade de danos ao hardware ou perda de dados caso as instruções não sejam seguidas.

AVISO: o ícone de AVISO indica a possibilidade de danos à propriedade, ferimentos pessoais ou morte.

NOTA IMPORTANTE, **NOTA**, **DICA**, **MÓVEL** ou **VÍDEO:** o ícone de informações indica uma informação extra/de apoio.

Dell AppAssure Guia do usuário
Atualizado - Abril de 2015
Versão de software - 5.4.3 Revisão B

Conteúdo

Introdução ao AppAssure 13
Principais tecnologias do AppAssure 14
Live Recovery 14
Verified Recovery 14
Universal Recovery 14
True Global Deduplication 14
Recursos do produto do AppAssure 15
Repositório 15
True Global Deduplication 15
Criptografia 16
Replicação 17
Recovery-as-a-Service (RaaS) 18
Retenção e arquivamento 18
Virtualização e nuvem 19
Gerenciamento de eventos e alertas 19
Portal de licenças 19
Console da Web 19
APIs de gerenciamento de serviço 20
Atribuição de marca branca 20
Assistentes AppAssure 20

Noções básicas sobre o AppAssure Core Console 22
Navegar no Core Console 26
Visualizar a guia Início 26
Visualizar a guia Replicação 28
Visualizar a guia Standby virtual 31
Visualizar a guia Eventos 32
Visualizar a guia Ferramentas 34
Visualizar a guia Configuração 35
Usar a caixa de diálogo Erro 36
Noções básicas sobre o Guia de início rápido 37
Início do Guia de início rápido 39
Ocultação do Guia de início rápido 39
Visualizar o menu de máquinas protegidas 40
Visualizar a guia Máquinas de uma máquina protegida 41
Visualizar a guia Resumo 44
Visualizar a guia Pontos de recuperação 46
Visualizar a guia Eventos de uma máquina protegida 47
Visualizar a guia Ferramentas de uma máquina protegida 48
Visualizar a guia Configuração de uma máquina protegida 49
Visualizar o painel Máquinas replicadas 50
Visualizar o menu Apenas pontos de recuperação 50
Visualizar o menu Grupos personalizados 51

Configurar o AppAssure Core 52
Noções básicas sobre repositórios 53
Gerenciar um repositório 54
Criar um repositório 54
Visualizar detalhes de um repositório 57
Modificar definições de repositório 58
Abrir um repositório existente 58
Adicionar um local de armazenamento a um repositório existente 59
Verificar um repositório 61
Excluir um repositório 61
Sobre o trabalho de verificação de integridade do repositório 61
Executar o trabalho de verificação de integridade em um repositório 62
Noções básicas sobre grupos personalizados 63
Criar grupos personalizados 64
Modificar nomes de grupos personalizados 64
Remover grupos personalizados 65
Realizar ações de grupo 65
Visualizar todas as máquinas de um grupo personalizado em uma página 66
Realizar cópia de segurança e restauração da configuração do Core 66
Realizar cópia de segurança da configuração do Core 66
Restaurar uma cópia de segurança da configuração do Core 67

Gerenciar as definições do AppAssure Core 68
Noções básicas sobre informações do sistema 73
Visualizar informações do sistema 73
Configurar as definições gerais do Core 74
Configuração das definições de atualização 74
Noções básicas sobre trabalhos noturnos 75
Configurar trabalhos noturnos para o Core 76
Modificar definições de fila de transferência 77
Ajustar definições de tempo limite do cliente 77
Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento . . .78
Configurar definições de cache de deduplicação 79
Configurar as definições do mecanismo Replay 80
Configurar as definições do implantação 81
Configurar definições de conexão de banco de dados 82
Gerenciar licenças 83
Alterar uma licença 84
Contatar o servidor do Portal de licenças do Dell AppAssure 85
Criar cópia de segurança e restaurar definições do Core 85
Configurar as definições de trabalhos do Core 87
Editar as definições de trabalhos do Core 87
Adicionar trabalhos ao Core 88
Acessar os diagnósticos do Core 88
Baixar os logs do Core 89
Visualizar os logs do Core 89
Carregar logs 89

Noções básicas sobre chaves de criptografia 90
Aplicar ou remover criptografia de uma máquina protegida 91
Associar uma chave de criptografia a uma máquina protegida 91
Aplicar uma chave de criptografia na guia Máquinas 92
Desassociar uma chave de criptografia de uma máquina protegida 93
Gerenciar chaves de criptografia 94
Adicionar uma chave de criptografia 95
Importar uma chave de criptografia 96
Bloquear ou desbloquear uma chave de criptografia 97
Editar uma chave de criptografia 99
Alterar a frase de acesso de uma chave de criptografia 99
Exportar uma chave de criptografia 100
Remover uma chave de criptografia 100
Alterar o status da chave de criptografia 100

Proteger máquinas usando o AppAssure Core 102
Limitações de suporte para volumes dinâmicos e básicos 102
Sobre o Agent Installer 103
Download do Agent Installer 103
Implantação do Agent (instalação por push) 103
Modificar definições de implantação 104
Noções básicas sobre implantação em massa 104
Implantar em várias máquinas 105
Implantar em máquinas de um domínio Active Directory 105
Implantar em máquinas de um host virtual VMware vCenter/ESX(i) 107
Implantar nas máquinas de qualquer outro host 108
Confirmar a implantação em várias máquinas 109
Noções básicas sobre programações de proteção 109
Proteger uma máquina 110
Criar programações de proteção personalizadas 115
Modificar programações de proteção 117
Pausar e retomar a proteção 118
Proteger várias máquinas 120
Monitorar a proteção de várias máquinas 125

Gerenciar servidores Microsoft Exchange e SQL 126
Configurar definições de Exchange e SQL Server 127
Definir credenciais para uma máquina Exchange Server 127
Definir credenciais para uma máquina SQL Server 127
Noções básicas sobre indicadores de status de ponto de recuperação 128
Modificar as definições do Exchange Server 129
Modificar as definições do SQL Server 129
Gerenciar a capacidade de anexação do SQL e o truncamento de log 130
Configurar as definições de capacidade de anexação do SQL 131
Configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log em todas as máquinas protegidas 132
Forçar uma verificação de capacidade de anexação do SQL Server 132
Forçar truncamento de log para uma máquina SQL 133

Gerenciar verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log 133
Configurar verificações noturnas de soma de verificação do banco de dados do Exchange e truncamento de log 134
Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange 134
Forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server 135
Forçar o truncamento de log para uma máquina Exchange 135

Proteger clusters do servidor 136
Aplicativos e tipos de cluster suportados 137
Suporte limitado para volumes compartilhados de cluster 137
Proteger um cluster 138
Proteger nós em um cluster 139
Modificar definições de nó de cluster 140
Configurar definições de cluster 140
Modificar definições de cluster 140
Configurar as notificações de eventos de cluster 141
Modificar a política de retenção do cluster 142
Modificar programações de proteção de cluster 143
Modificar definições de transferência de cluster 143
Converter um nó de cluster protegido em uma máquina protegida 143
Visualizar informações de cluster do servidor 144
Visualizar informações de sistema de cluster 144
Visualizar tarefas, eventos e alertas de cluster 144
Visualizar informações de resumo 144
Trabalhar com pontos de recuperação de cluster 145
Gerenciar os snapshots de um cluster 145
Forçar um snapshot de um cluster 146
Pausar e retomar snapshots de cluster 146
Realizar uma restauração de clusters e nós de cluster 146
Realizar uma restauração de clusters CCR e DAG (Exchange) 146
Realizar uma restauração de clusters SCC (Exchange, SQL) 147
Replicar dados de cluster 147
Remover um cluster da proteção 147
Remover nós de cluster da proteção 148
Remover todos os nós de um cluster da proteção 148
Visualizar um relatório de cluster ou nó 148

Exportar dados protegidos de máquinas Windows para máquinas virtuais 150
Gerenciar exportações 151
Exportar dados para uma máquina virtual baseada em Windows 152
Exportar dados para uma máquina virtual ESXi 153
Realizar uma exportação única para ESXi 153
Realizar uma exportação contínua (Standby virtual) para ESXi 154
Exportar dados para uma máquina virtual VMWare Workstation 156
Realizar uma exportação única para VMware Workstation 156

Realizar uma exportação contínua (Standby virtual) para VMware Workstation 157
Exportar dados para uma máquina virtual Hyper-V 159
Realizar uma exportação única de Hyper-V 159
Realizar uma exportação contínua (Standby virtual) para Hyper-V 161
Exportar dados para uma máquina virtual VirtualBox 163
Realizar uma exportação única de VirtualBox 163
Realizar uma exportação contínua de VirtualBox (Standby virtual) 164

Gerenciar máquinas protegidas 166
Configurar as definições da máquina 167
Visualizar e modificar as definições de configuração 167
Visualizar informações do sistema de uma máquina 168
Configurar grupos de notificação para eventos do sistema 168
Editar grupos de notificação para eventos do sistema 170
Modificar definições de transferência 172
Personalizar trabalhos noturnos para uma máquina protegida 174
Acessar o diagnóstico de máquinas protegidas 175
Baixar logs de máquina 175
Visualizar logs de máquina 175
Visualizar o status da máquina e outros detalhes 176
Gerenciar máquinas 177
Remover uma máquina 177
Cancelar operações em uma máquina 178
Visualizar informações de licença em uma máquina 178
Gerenciar snapshots e pontos de recuperação 178
Visualizar pontos de recuperação 179
Visualizar um ponto de recuperação específico 179
Montar um ponto de recuperação 181
Desmontar pontos de recuperação 182
Forçar um snapshot 182
Remover pontos de recuperação 183
Excluir uma cadeia de pontos de recuperação órfãos 183
Migrar pontos de recuperação para um repositório diferente 184

Noções básicas sobre replicação 185
Noções básicas sobre unidades de propagação 190
Noções básicas sobre ativação pós-falha e reativação pós-falha no AppAssure 191
Considerações sobre desempenho para transferência de dados replicados 191
Sobre replicação e pontos de recuperação criptografados 192
Sobre políticas de retenção para replicação 192
Configurar a replicação 192
Replicar para um Core de destino autogerenciado 193
Replicar para um Core de destino de terceiros 196
Enviar uma solicitação de replicação para um provedor de serviços terceirizado . . . 197
Revisar uma solicitação de replicação de um cliente 199
Aprovar uma solicitação de replicação 200
Negar uma solicitação de replicação 200
Ignorar uma solicitação de replicação de um cliente 201

Adicionar uma máquina a uma replicação existente 201
Consumir a unidade de propagação em um Core de destino 203
Abandonar uma unidade de propagação 204
Gerenciar definições de replicação 205
Programar a replicação 205
Usar a função Copiar para criar uma unidade de propagação 206
Monitorar a replicação 208
Pausar e retomar a replicação 209
Forçar a replicação 210
Gerenciar definições para replicação de saída 210
Alterar as definições do Core de destino 211
Definir a prioridade de replicação de uma máquina protegida 211
Remoção da replicação 211
Remover uma máquina protegida da replicação no Core de origem 212
Remover uma máquina protegida no Core de destino 212
Remover um Core de destino da replicação 212
Remover um Core de origem da replicação 212
Recuperar dados replicados 213
Noções básicas sobre ativação pós-falha e reativação pós-falha 213
Definir um ambiente de ativação pós-falha 213
Realizar ativação pós-falha no Core de destino 214
Realizar reativação pós-falha 214

Gerenciar eventos 216
Visualizar tarefas, alertas e eventos 216
Visualizar tarefas 217
Visualizar alertas 218
Visualizar todos os eventos 218
Noções básicas sobre notificações por e-mail 219
Configurar um servidor de e-mail 219
Configurar um modelo de e-mail de notificação 220
Configurar grupos de notificação 221
Configurar redução de repetição 223
Configurar retenção de eventos 224

Gerar e visualizar relatórios 225
Usar a barra de ferramentas de relatórios 226
Noções básicas sobre relatórios de conformidade 226
Noções básicas sobre relatórios de falha 227
Noções básicas sobre o relatório resumido 227
Resumo de repositórios 227
Resumo de agentes 228
Gerar um relatório sobre um Core ou agente 228
Noções básicas sobre os relatórios do Central Management Console no Core 229
Gerar um relatório no Central Management Console 229

Restaurar dados 230
Restaurar dados de pontos de recuperação 230

Restaurar volumes a partir de um ponto de recuperação 231
Restaurar um diretório ou arquivo usando o Windows Explorer 234
Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer 234

Noções básicas sobre bare metal restores em máquinas Windows 236
Realizar uma bare metal restore em máquinas Windows 237
Pré-requisitos para realizar uma bare metal restore em uma máquina Windows . . . 238
Gerenciar uma imagem de inicialização do Windows 239
Criar uma imagem ISO de um CD de inicialização para Windows 239
Definir os parâmetros da imagem ISO do CD de inicialização 240
Nomear o arquivo do CD de inicialização e definir o caminho 240
Criar conexões 240
Especificar um ambiente de recuperação 241
Injetar drivers em um CD de inicialização 241
Criar a imagem ISO do CD de inicialização 242
Visualizar o progresso da criação da imagem ISO 242
Acessar a imagem ISO 242
Transferir a imagem ISO do CD de inicialização para a mídia 243
Carregar o CD de inicialização e inicializar a máquina de destino 243
Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina 244
Iniciar uma bare metal restore para Windows 247
Selecionar um ponto de recuperação e iniciar a BMR 247
Mapear volumes para uma bare metal restore 248
Carregar drivers usando o Universal Recovery Console 249
Injetar drivers no servidor de destino 250
Verificar uma bare metal restore 250
Visualizar o progresso da recuperação 251
Inicializar um servidor de destino restaurado 251
Solucionar problemas de conexão com o Universal Recovery Console 251
Reparar problemas de inicialização 252

Retenção e arquivamento 253
Gerenciar políticas de retenção 253
Configurar as definições da política de retenção padrão do Core 253
Noções básicas sobre arquivos 257
Criar um arquivo 257
Definir um arquivo programado 259
Pausar ou retomar um arquivo programado 261
Editar um arquivo programado 261
Verificar um arquivo 263
Importar um arquivo 263
Arquivar na nuvem 264

Gerenciar contas de nuvem 265
Adicionar uma conta de nuvem 265

Editar uma conta de nuvem 266
Configurar as definições da conta de nuvem 266
Remover uma conta de nuvem 267

Trabalhar com máquinas Linux 268
Trabalhar com pontos de recuperação do Linux 268
Montar um volume de ponto de recuperação em máquina Linux 268
Desmontar um ponto de recuperação em uma máquina Linux 270
Exportar dados para uma máquina virtual VirtualBox baseada em Linux 270
Realizar uma exportação única de VirtualBox 271
Realizar uma exportação contínua de VirtualBox (Standby virtual) 272
Restaurar volumes em uma máquina Linux usando a linha de comando 273
Realizar uma bare metal restore em máquinas Linux 275
Pré-requisitos para realizar uma bare metal restore em máquinas Linux 276
Gerenciar uma imagem de inicialização do Linux 276
Baixar uma imagem ISO de inicialização para Linux 277
Transferir a imagem ISO do Live DVD para a mídia 277
Carregar o Live DVD e iniciar a máquina de destino 278
Gerenciar partições Linux 278
Criar partições na unidade de destino 279
Formatar partições na unidade de destino 280
Montar partições a partir da linha de comando 281
Iniciar uma bare metal restore para Linux 281
Iniciar o utilitário Screen 282
Realizar uma bare metal restore em uma máquina Linux usando a linha de comando 282
Confirmar a bare metal restore na linha de comando 284
Realizar uma verificação do sistema de arquivos no volume restaurado 284
Usar a linha de comando para tornar uma máquina Linux restaurada inicializável . . 285

Noções básicas do Local Mount Utility 288
Baixar o Local Mount Utility 288
Baixar o LMU do AppAssure Core Console 288
Baixar o LMU do Portal de licenças do Dell AppAssure 289
Instalar o Local Mount Utility 289
Usando o Local Mount Utility 290
Adicionar uma máquina Core ao Local Mount Utility 291
Montar um ponto de recuperação usando o Local Mount Utility 291
Usar o Local Mount Utility para explorar um ponto de recuperação montado 292
Usar o Local Mount Utility para desmontar um ponto de recuperação 293
Usar o menu de bandeja do Local Mount Utility 293
Usar opções do AppAssure Core e de máquina protegida 294
Acessar opções de localhost 294
Acesso às opções de Core remoto 294
Acessar opções de máquina protegida 294

Noções básicas do utilitário AppAssure Command Line Management 295
Comandos 296

Archive 296
CancelActiveJobs 298
CreateRepository 299
Dismount 300
Force 301
ForceAttach 302
ForceChecksum 302
ForceLogTruncation 303
ForceMount 304
ForceReplication 305
ForceRollup 306
Help 306
List 307
Mount 309
Pause [snapshot | vmexport | replication] 311
Protect 312
ProtectCluster 313
RemoveAgent 314
RemovePoints 315
RestoreArchive 316
Resume [snapshot | vmexport | replication] 317
StartExport 318
UpdateRepository 320
Version 321
Localização 321

Noções básicas do módulo AppAssure PowerShell 322
Pré-requisitos para usar o PowerShell 323
powershell.exe.config 323
Iniciar o PowerShell e importar o módulo 323
Trabalhar com comandos e cmdlets 324
Obter ajuda e exemplos de cmdlet 324
Cmdlets do módulo AppAssure PowerShell 324
Get-ActiveJobs 325
Get-Clusters 327
Get-CompletedJobs 327
Get-ExchangeMailStores 328
Get-Failed 329
Get-FailedJobs 330
Get-Mounts 331
Get-Passed 332
Get-ProtectedServers 333
Get-ProtectionGroups 333
Get-RecoveryPoints 334
Get-ReplicatedServers 335
Get-Repositories 336
Get-SqlDatabases 336
Get-UnprotectedVolumes 337

Get-VirtualizedServers . . . 338
Get-Volumes . . . 338
New-Base . . . 339
New-Mount . . . 340
New-Repository . . . 341
New-Snapshot . . . 342
Push-Replication . . . 343
Push-Rollup . . . 344
Remove-Mount . . . 344
Remove-Mounts . . . 345
Resume-Replication . . . 346
Resume-Snapshot . . . 347
Resume-VMExport . . . 347
Start-Archive . . . 348
Start-AttachabilityCheck . . . 349
Start-EsxiExport . . . 350
Start-HypervExport . . . 351
Start-LogTruncation . . . 353
Start-MountabilityCheck . . . 354
Start-Protect . . . 354
Start-ProtectCluster . . . 355
Start-RestoreArchive . . . 356
Start-VBExport . . . 357
Start-VMExport . . . 359
Suspend-Replication . . . 360
Stop-ActiveJobs . . . 361
Suspend-Snapshot . . . 362
Suspend-VMExport . . . 363
Update-Repository . . . 364
Localização . . . 365
Qualificadores . . . 365

Estender trabalhos do AppAssure usando scripts . . . 366
Usar scripts PowerShell no AppAssure . . . 366
Pré-requisitos para PowerShell Scripting . . . 367
Teste dos scripts do PowerShell . . . 367
Localização . . . 367
Qualificadores . . . 368
Parâmetros de entrada do PowerShell Scripting . . . 368
Exemplos de scripts PowerShell . . . 380
PreTransferScript.ps1 . . . 380
PostTransferScript.ps1 . . . 381
PreExportScript.ps1 . . . 381
PostExportScript.ps1 . . . 382
PreNightlyJobScript.ps1 . . . 382
PostNightlyJobScript.ps1 . . . 385
Usar scripts Bourne Shell no AppAssure . . . 387
Pré-requisitos para scripts do Bourne Shell . . . 388

Testar os scripts do Bourne Shell . . . 388
Parâmetros de entrada para scripts do Bourne Shell . . . 388
Exemplos de scripts do Bourne Shell . . . 390
PreTransferScript.sh . . . 390
PostTransferScript.sh . . . 390
PostExportScript.sh . . . 391

Noções básicas das APIs do AppAssure . . . 392
Público-alvo . . . 392
Leitura adicional recomendada . . . 392
Trabalhar com APIs REST do AppAssure . . . 392
Usar a API do AppAssure Core . . . 393
IAgentDiagnosticsManagement . . . 396
IAgentsGroupsManagement . . . 397
IAgentsManagement . . . 398
IApplianceEventsManagement . . . 405
IApplicationIdManagement . . . 405
IAutoUpdateManagement . . . 406
IBackgroundJobManagement . . . 407
IBackupManagement . . . 408
IBootCdBuilderManagement . . . 411
ICloudManagement . . . 412
IClustersManagement . . . 414
ICoreBackupRestoreManagement . . . 415
ICoreCallbackManagement . . . 416
ICoreDiagnosticsManagement . . . 416
ICoreMetadataManagement . . . 418
ICoreSettingsManagement . . . 419
IDatabaseStorageManagement . . . 420
IDiagnosticsManagement . . . 421
IEmailsManagement . . . 422
IEncryptionKeyManagement . . . 422
IEventsManagement . . . 425
IExchangeManagement . . . 428
IExportQueueManagement . . . 431
IExportSchedulerManagement . . . 432
IHyperVAgentManagement . . . 436
IIsoDatabaseManagement . . . 439
ILicenseManagement . . . 439
ILocalizationManagement . . . 441
ILocalMountManagement . . . 442
ILoggingManagement . . . 443
ILogTruncationManagement . . . 444
INightlyJobsManagement . . . 444
IProtectedItemsManagement . . . 446
IPushInstallCommunication . . . 446
IPushInstallManagement . . . 447
IRecoveryPointsManagement . . . 448

IRemoteMountManagement 453
IReplayEngineManagement 454
IReplicationCommunication 455
IReplicationManagement 466
IReportingManagement 473
IRepositoryManagement 474
IRollbackManagement 480
IRollupManagement 482
ISeedDriveManagement 483
IServiceHostManagement 484
ISqlManagement 485
IStatusSummaryManagement 486
ITransferQueueManagement 488
ITransferSchedulerManagement 489
IUtilitiesManagement 492
IVirtualDiskManagement 492
IWhiteLabelingManagement 495
Uso da API AppAssure Agent 495
IAgentMetadataManagement 496
IAgentPairManagement 497
IAgentServiceHostManagement 498
IAgentSettingsManagement 499
IAgentUpdateManagement 499
IApplicationIdManagement 499
IDiagnosticsManagement 500
IDriverChangeLogsManagement 501
IExchangeManagement 502
IExchangeServerManagement 502
IHyperVAgentManagement 503
IPowerShellManagement 506
IRollbackManagement 506
IRrcRollbackManagement 508
IServiceHostManagement 508
IShadowCopyManagement 509
ITransferManagement 509
IVirtualDiskManagement 511
IWhiteLabelingManagement 514

Glossário 515

Sobre o Dell 522
Contatos da Dell 522
Recursos do suporte técnico 522

1

Introdução ao AppAssure

Este capítulo fornece uma introdução e uma visão geral do Dell AppAssure. Ele descreve os recursos, a funcionalidade e a arquitetura, e consiste nos seguintes tópicos:

- Principais tecnologias do AppAssure
- Recursos do produto do AppAssure

O AppAssure estabelece um novo padrão de proteção de dados unificada, combinando backup, replicação e recuperação em uma única solução, projetada para ser o backup mais rápido e confiável para a proteção de máquinas virtuais (VM), ambientes físicos e de nuvem.

O AppAssure combina backup e replicação em um produto de proteção de dados integrada e unificada, que também fornece reconhecimento do aplicativo para garantir uma recuperação confiável de dados de aplicativo a partir dos backups. O AppAssure se baseia na nova arquitetura True Scale™ (patente pendente), que proporciona o desempenho de cópia de segurança mais rápido com objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) muito agressivos, próximos de zero.

O AppAssure combina várias tecnologias exclusivas, inovadoras e avançadas:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Essas tecnologias são projetadas com integração segura para a recuperação após desastres na nuvem e proporcionam uma recuperação rápida e confiável. Com seu armazenamento escalável de objetos, o AppAssure tem uma capacidade exclusiva de processar petabytes de dados muito rapidamente, com eliminação da duplicação de dados global embutida, compactação, criptografia e replicação para qualquer infraestrutura de nuvem pública ou privada. Aplicativos e dados de servidor podem ser recuperados em minutos, para fins de retenção de dados e conformidade.

As ferramentas de cópia de segurança legadas atuais e as ferramentas de cópia de segurança com VM da primeira geração são ineficientes e ineficazes. As ferramentas de backup desatualizadas não têm capacidade de trabalhar com dados em grande escala e não oferecem o nível de desempenho e confiabilidade necessário para proteger aplicativos críticos para os negócios. A combinação dessas características com ambientes de TI complexos e mistos representa um desafio administrativo para os profissionais de TI e vulnerabilidades para os dados do sistema.

O AppAssure enfrenta essa complexidade e ineficiência com a nossa tecnologia de core e suporte de ambientes com vários hypervisors, incluindo os que executam em VMware vSphere e Microsoft Hyper-V, que englobam nuvens públicas e privadas. O AppAssure oferece esses avanços tecnológicos e, ao mesmo tempo, reduz drasticamente os custos de gerenciamento de TI e armazenamento.

Principais tecnologias do AppAssure

Detalhes sobre as principais tecnologias do AppAssure são descritos nos tópicos a seguir.

Live Recovery

Live Recovery é uma tecnologia de recuperação instantânea para VMs ou servidores. Oferece acesso quase contínuo a volumes de dados em servidores virtuais ou físicos. É possível recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

A tecnologia de cópia de segurança e replicação do AppAssure registra snapshots simultâneos de várias VMs ou servidores, proporcionando proteção quase instantânea de dados e do sistema. É possível retomar o uso do servidor diretamente do arquivo de backup, sem esperar uma recuperação completa para o armazenamento de produção. Os usuários mantêm a produtividade e os departamentos de TI reduzem as janelas de recuperação para cumprir os contratos de nível de serviço atuais de RTO e RPO, cada vez mais exigentes.

Verified Recovery

O Verified Recovery permite realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Ele inclui, entre outros, os sistemas de arquivo: Microsoft Exchange Server 2007, 2010 e 2013 e Microsoft SQL Server 2005, 2008, 2008 R2, 2012 e 2014. O Verified Recovery fornece capacidade de recuperação de aplicativos e cópias de segurança em ambientes virtuais e físicos e oferece um algoritmo abrangente de verificação de integridade baseado em chaves de SHA de 256 bits que verificam a correção de cada bloco do disco na cópia de segurança durante as operações de arquivamento, replicação e propagação de dados. Isso garante a identificação precoce da corrupção de dados e impede que os blocos de dados corrompidos sejam mantidos ou transferidos durante o processo de cópia de segurança.

Universal Recovery

A tecnologia Universal Recovery oferece uma flexibilidade ilimitada de restauração de máquinas. É possível restaurar suas cópias de segurança de um meio físico para virtual, de virtual para virtual, de virtual para físico ou de físico para físico. Também é possível realizar bare metal restores para hardware distinto; por exemplo, P2V, V2V, V2P, P2P, P2C, V2C, C2P e C2V.

Também acelera as movimentações entre plataformas entre máquinas virtuais, por exemplo: mover de VMware para Hyper-V ou de Hyper-V para VMware. Baseia-se na recuperação no nível de aplicativo, nível do item e nível do objeto: arquivos individuais, pastas, email, itens de calendário, bancos de dados e aplicativos. Com o AppAssure, também é possível recuperar ou exportar de físico para a nuvem ou do virtual para a nuvem.

True Global Deduplication

O AppAssure fornece a true global deduplication, que reduz drasticamente os requisitos de capacidade do disco físico, oferecendo taxas de redução de espaço que passam de 50:1 e, mesmo assim, atendem aos requisitos de armazenamento de dados. A compactação embutida no nível do bloco da arquitetura True Scale e a deduplicação com desempenho com velocidade de linha, juntamente com a verificação de integridade embutida, impede que a corrupção dos dados afete a qualidade dos processos de backup e arquivamento.

Recursos do produto do AppAssure

Usando o AppAssure, você pode gerenciar todos os aspectos de proteção e recuperação de dados críticos por meio dos seguintes recursos e funcionalidades. Eles incluem:

- Repositório
- True Global Deduplication
- Criptografia
- Replicação
- Recovery-as-a-Service (RaaS)
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de eventos e alertas
- Portal de licenças
- Console da Web
- APIs de gerenciamento de serviço
- Atribuição de marca branca
- Assistentes AppAssure

Repositório

O repositório do AppAssure usa o gerenciador de volume para deduplicação (DVM) para implementar um gerenciador de volumes que oferece suporte a vários volumes, sendo que cada um deles pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS), armazenamento conectado à rede (NAS) ou armazenamento na nuvem. Cada volume consiste em um armazenamento escalável de objetos com deduplicação. O armazenamento escalável de objetos se comporta como um sistema de arquivos baseado em registros, em que a unidade de alocação de armazenamento é um bloco de dados com tamanho fixo, conhecido como registro. Esta arquitetura permite configurar o suporte do tamanho do bloco para compactação e deduplicação. As operações de rollup são reduzidas a operações de metadados a partir de operações com uso intenso do disco, porque o rollup não movimenta mais os dados, movimenta apenas os registros.

O DVM pode combinar um conjunto de armazenamentos de objetos em um volume, e eles podem ser expandidos pela criação de sistemas de arquivos adicionais. Os arquivos do armazenamento de objetos são pré-alocados e podem ser adicionados sob demanda conforme os requisitos de armazenamento mudam. É possível criar até 255 repositórios independentes em um único AppAssure Core e aumentar mais o tamanho de um repositório adicionando novas extensões de arquivo. Um repositório estendido pode conter até 4.096 extensões que abrangem diversas tecnologias de armazenamento. O tamanho máximo dos repositórios é 32 Exabytes. Um único core pode ter vários repositórios.

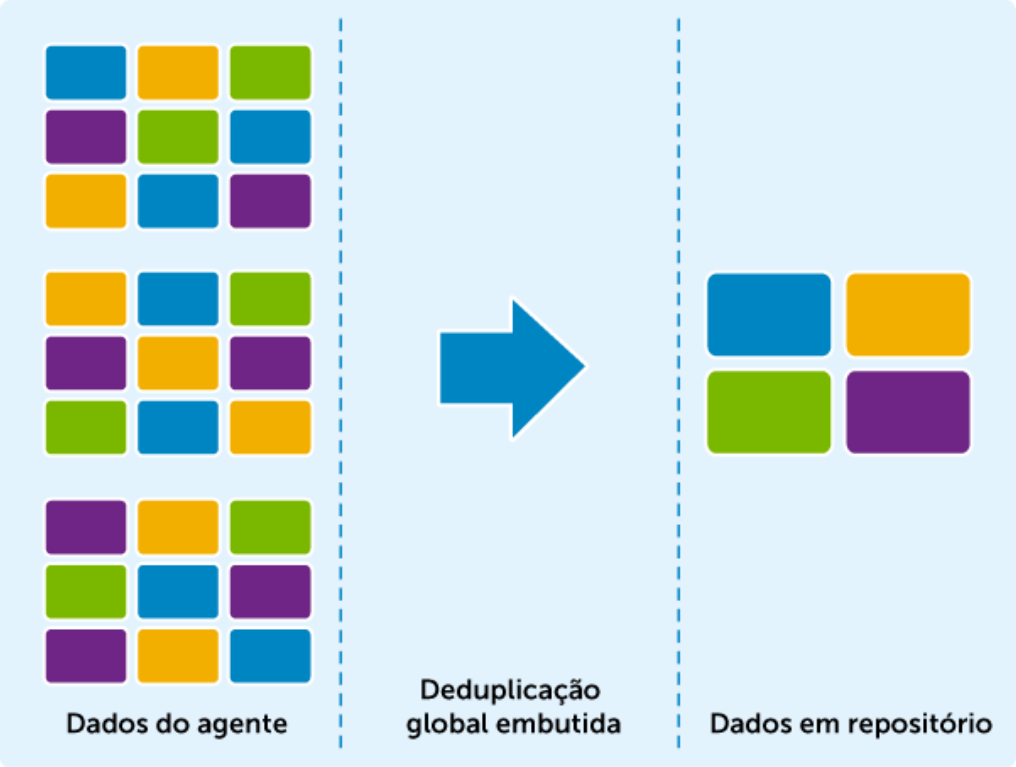
True Global Deduplication

O True Global Deduplication é um método efetivo de redução das necessidades de armazenamento de cópia de segurança, eliminando dados redundantes ou duplicados. A deduplicação é efetiva porque somente uma instância dos dados em vários backups é armazenada no repositório. Os dados redundantes são armazenados, mas não fisicamente; eles são simplesmente substituídos por um indicador que aponta para a instância única dos dados no repositório.

Os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas semanalmente, mas o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco.

O layout de disco típico de um servidor é constituído pelo sistema operacional, aplicativos e dados. Na maioria dos ambientes, os administradores frequentemente usam um tipo em comum de sistema operacional de desktop e server em vários sistemas, para que a implementação e o gerenciamento sejam efetivos. Quando o AppAssure faz uma cópia de segurança no nível do bloco em várias máquinas ao mesmo tempo, ele fornece uma visualização mais detalhada daquilo que está (e do que não está) na cópia de segurança, independentemente da origem. Esses dados incluem o sistema operacional, os aplicativos e os dados de aplicativo de todo o ambiente.

Figura 1. True Global Deduplication



O AppAssure realiza a deduplicação de dados embutida baseada no destino. Esse método transmite os dados de snapshot para o core antes de serem deduplicados. Deduplicação de dados embutida significa simplesmente que a duplicação dos dados é eliminada antes da confirmação no disco. Isso é muito diferente da deduplicação na origem ou após o processo, na qual a duplicação dos dados é eliminada na origem antes da transmissão; no pós-processo, os dados são enviados em forma bruta para o destino, onde são analisados e a duplicação é eliminada depois da confirmação dos dados no disco. A deduplicação de dados na origem consome recursos preciosos do sistema na máquina, ao passo que a abordagem de eliminação da duplicação de dados pós-processo requer que todos os dados necessários estejam no disco (uma sobrecarga maior de capacidade inicial) antes de começar o processo de deduplicação. Por outro lado, a deduplicação de dados embutida não requer capacidade de disco adicional e ciclos de CPU na origem nem no Core para o processo de deduplicação. Para concluir, os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas toda semana, enquanto que o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco, com uma proporção de redução de até 80:1.

Criptografia

O AppAssure fornece criptografia integrada para proteger cópias de segurança e dados em repouso contra o uso e acesso sem autorização, garantindo a privacidade dos dados. O AppAssure fornece criptografia forte. Ao fazer isso, os backups de computadores protegidos ficam inacessíveis. Somente o usuário que tem a chave de criptografia pode acessar e descriptografar os dados. Não há limite para o número de chaves de criptografia que podem ser criadas e armazenadas em um sistema. O DVM usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. A criptografia é realizada de forma

embutida nos dados de snapshot, a velocidades de linha, sem afetar o desempenho. Isso acontece porque a implementação do DVM é multiprocessamento e usa a aceleração de hardware específica para o processador no qual ele está implementado.

A criptografia está preparada para a multilocação. A deduplicação foi limitada especificamente aos registros que foram criptografados com a mesma chave; dois registros idênticos que foram criptografados com chaves diferentes não terão a deduplicação. Essa decisão de projeto impede que a deduplicação seja usada para vazar dados entre domínios de criptografia diferentes. Isso beneficia os provedores de serviços gerenciados, já que os backups replicados de vários locatários (clientes) podem ser armazenados em um único core, sem que um locatário possa ver ou acessar os dados de outros locatários. Cada chave de criptografia de um locatário ativo cria um domínio de criptografia dentro do repositório, no qual somente o proprietário das chaves pode ver, acessar ou usar os dados. Em um cenário de multilocação, os dados são particionados e deduplicados dentro dos domínios de criptografia.

Nos cenários de replicação, o AppAssure usa o SSL 3.0 para proteger as conexões entre os dois cores em uma topologia de replicação para impedir espionagem e adulteração.

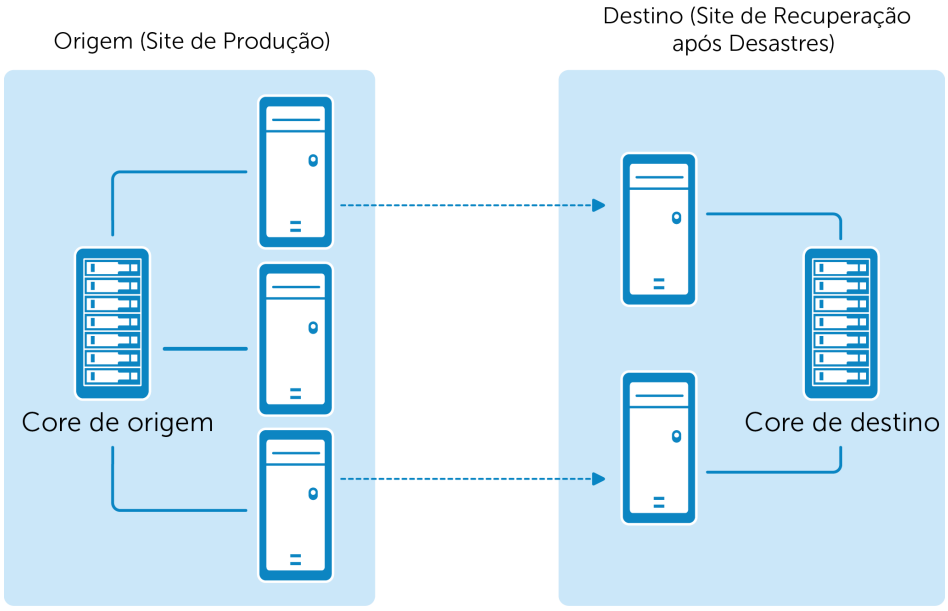
Replicação

Replicação é o processo de copiar pontos de recuperação de um core AppAssure e transmiti-los a outro core AppAssure em um local separado para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais cores.

Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para um site de recuperação após desastres remoto (ou seja, um core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um core de origem pode ser configurada para replicar em um core de destino.

Figura 2. Replicação



A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Na replicação RMW, o serviço de replicação de origem e destino faz a correspondência das chaves antes de transferir dados e, em seguida, replica somente os dados compactados, criptografados e de deduplicação pela WAN. Ao fazer isso, reduz em 10x os requisitos de largura de banda.

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas. Normalmente, isso é útil para grandes conjuntos de dados ou sites com links lentos. Os dados do arquivo de propagação são compactados e criptografados e a duplicação é eliminada. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Durante o processo de propagação, os pontos de recuperação incremental são replicados no site de destino. Depois que o core de destino consome o arquivo de propagação, os pontos de recuperação incremental recém-replicados são sincronizados automaticamente.

Recovery-as-a-Service (RaaS)

Os provedores de serviços gerenciados (MSPs) podem utilizar o AppAssure como uma plataforma para oferecer a recuperação como serviço (RaaS). A RaaS facilita a recuperação completa na nuvem replicando os servidores físicos e virtuais do cliente, juntamente com seus dados, para a nuvem do provedor de serviços como máquinas virtuais para suportar o teste de recuperação ou operações reais de recuperação. Os clientes que desejam realizar recuperação na nuvem podem configurar a replicação nas máquinas protegidas nos cores locais para um provedor de serviços do AppAssure. Em caso de desastre, os MSPs podem realizar instantaneamente o provisionamento das máquinas virtuais para o cliente.

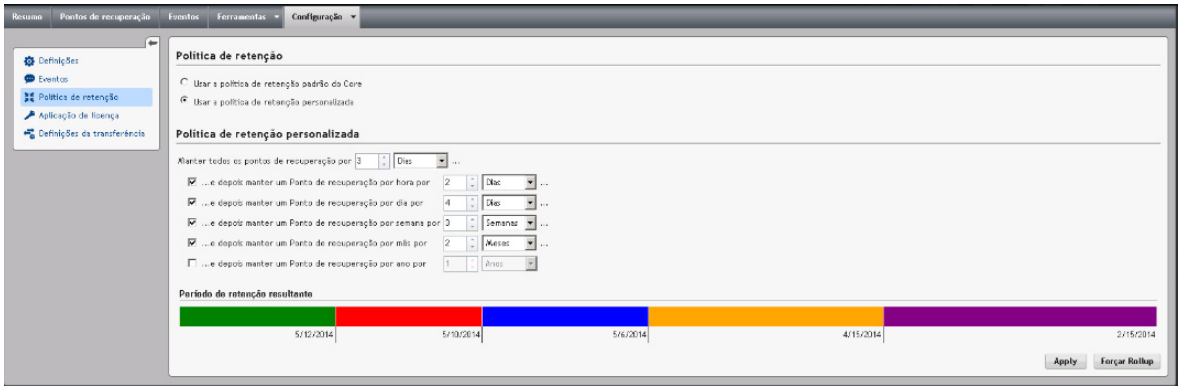
Os MSPs podem implementar uma infraestrutura de RaaS com multilocação baseada em AppAssure que pode hospedar várias organizações ou unidades de negócios separadas (os locatários), que normalmente não compartilham segurança ou dados em um único servidor ou um grupo de servidores. Os dados de cada locatário são isolados e protegidos de outros locatários e do provedor de serviço.

Retenção e arquivamento

O AppAssure oferece políticas flexíveis de cópia de segurança e retenção fáceis de configurar. A capacidade de ajustar as políticas de retenção às necessidades de uma organização não só ajuda a preencher os requisitos de conformidade, mas também faz isso sem comprometer os objetivos de tempo de recuperação (RTO).

As políticas de retenção impõem períodos de tempo em que os backups são armazenados em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada desses backups, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivamento suporta retenções prolongadas para dados de conformidade e não conformidade, além de ser usado para propagar dados de replicação para um core de destino.

Figura 3. Política de retenção



No AppAssure, as políticas de retenção podem ser personalizadas para especificar por quanto tempo um ponto de recuperação de cópia de segurança será mantido. Conforme o fim do período de retenção dos pontos de retenção se aproxima, eles vencem e são removidos do grupo de retenção. Normalmente, esse processo se

torna ineficiente e acaba falhando, já que a quantidade de dados e o período de retenção começam a aumentar rapidamente. O AppAssure resolve o problema do big data gerenciando a retenção de grandes quantidades de dados com políticas de retenção complexas e realizando operações de rollup para dados que estão vencendo, por meio de operações eficientes de metadados.

É possível realizar backups com um intervalo de poucos minutos, e esses backups vencem em dias, meses e anos. As políticas de retenção gerenciam o vencimento e a exclusão de backups antigos. Um método simples em cascata define o processo de vencimento. Os níveis dentro da cascata são definidos em minutos, horas e dias; semanas, meses e anos. A política de retenção é imposta pelo processo noturno de rollup.

Para arquivamento de longo prazo, o AppAssure permite criar um arquivo do Core de origem ou de destino em qualquer mídia removível. O arquivo é otimizado internamente, e todos os dados do arquivo são compactados, criptografados e têm deduplicação. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo ocupará vários dispositivos com base no espaço disponível nas mídias. A recuperação a partir de um arquivo não requer um novo core; qualquer core pode ingerir o arquivo e recuperar dados se o administrador tiver a senha e as chaves de criptografia.

Virtualização e nuvem

O AppAssure Core está preparado para a nuvem, permitindo que você utilize a capacidade computacional da nuvem para a recuperação e para o arquivamento.

O AppAssure pode exportar qualquer máquina protegida ou replicada para uma máquina virtual (VM), como uma versão licenciada do VMware ou Hyper-V. É possível realizar uma exportação virtual única ou criar uma máquina virtual em modo de standby virtual estabelecendo uma exportação virtual contínua. Nas exportações contínuas, a máquina virtual é atualizada de forma incremental depois de cada snapshot. As atualizações adicionais são rápidas e fornecem clones em estado de espera prontos para serem acionados com um clique em um botão. Tipos de exportação de VM suportados incluem: VMware Workstation e VMWare Server em uma pasta; exportação direta para um host do vSphere ou VMware ESX(i); exportação para o Oracle VirtualBox; e exportação para o Microsoft Hyper-V Server no Windows Server 2008 (x64), 2008 R2, 2012 (x64) e 2012 R2 (incluindo suporte para as máquinas virtuais Hyper-V geração 2).

Além disso, é possível arquivar seus dados do repositório na nuvem utilizando o Microsoft Azure, Amazon S3, Rackspace Cloud Files ou outros serviços de nuvem baseados em OpenStack.

Gerenciamento de eventos e alertas

Além das APIs de REST HTTP, o AppAssure também inclui um conjunto amplo de recursos para a criação de logs e a notificação de eventos usando e-mail, syslog ou o Log de eventos do Windows. As notificações por email podem ser usadas para informar os usuários ou grupos sobre o funcionamento ou o status de diversos eventos em resposta a um alerta. Os métodos do syslog e do Log de Eventos do Windows são usados para a criação de logs centralizada em um repositório, em ambientes com vários sistemas operacionais; por outro lado, em ambientes que só têm Windows, apenas o Log de Eventos do Windows é usado.

Portal de licenças

O Portal de licenças do Dell AppAssure fornece ferramentas fáceis de usar para gerenciar os direitos de licença. É possível fazer download, ativar, ver e gerenciar chaves de licença e criar um perfil de empresa para rastrear os ativos de licença. Além disso, o portal permite que os provedores de serviços e revendedores rastreiem e gerenciem as licenças de cliente.

Console da Web

O AppAssure tem um console central baseado na Web que gerencia cores distribuídos do AppAssure a partir de um local central. Os provedores de serviços gerenciados (MSPs) e clientes corporativos com vários cores distribuídos podem implementar esse console para obter uma visualização unificada para um gerenciamento centralizado. O AppAssure Central Management Console permite organizar os cores gerenciados em unidades

organizacionais hierárquicas. Essas unidades organizacionais podem representar unidades de negócios, locais ou clientes para os MSPs com acesso baseado em função. Usando o console central, você também pode executar relatórios em todos os cores gerenciados.

APIs de gerenciamento de serviço

O AppAssure vem com um conjunto de APIs de gerenciamento de serviços e fornece acesso programático a todas as funcionalidades disponíveis por meio do AppAssure Central Management Console. A API de gerenciamento de serviços é uma API de REST. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3. O serviço de gerenciamento pode ser acessado de dentro do ambiente ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar e receber solicitações e respostas de HTTPS. A abordagem facilita a integração fácil a qualquer aplicativo da Web, como ferramentas de metodologia de gerenciamento de relacionamentos (RMM) ou sistemas de faturação. Um cliente de SDK para PowerShell scripting também está incluído no AppAssure.

Atribuição de marca branca

O AppAssure pode ter a marca alterada ou ser comercializado sem marca para parceiros corporativos e de OEM selecionados, de acordo com o programa de provedor de serviços Platinum. Com o programa de provedor de serviços Platinum, os parceiros podem usar seu nome, logotipo e cores no AppAssure e fornecer o produto ou serviço com sua própria marca e visual para os clientes.

Como parceiro do AppAssure, você pode ajustar o software para que ele atenda aos seus requisitos de negócios. Para saber mais sobre a forma de uso da sua marca no AppAssure visando a suprir as suas necessidades de negócios, entre em contato com o Departamento de Vendas Dell AppAssure pelo e-mail sales@software.dell.com para obter mais informações.

Assistentes AppAssure

O assistente é um conjunto de etapas guiadas apresentadas ao usuário em uma janela pop-up para automatizar uma tarefa complexa ou mais. Por definição, os assistentes contêm duas páginas de informações (ou mais) para o usuário preencher. (Um pop-up de janela única é considerado simplesmente como uma caixa de diálogo). Os assistentes usam diversas convenções gráficas bastante conhecidas para coletar informações, como caixas de texto, botões de opções, caixas de seleção e menus suspensos.

Quando um assistente é iniciado, uma janela se abre acima da interface do usuário e o orienta em uma série de opções necessárias para realizar a tarefa. Você segue as informações apresentadas em cada página do assistente, conforme os seus requisitos, navegando pelas páginas do assistente por meio dos botões **Avançar** e **Voltar**. Ao terminar, você clica em um botão de enviar (para confirmar suas opções e realizar a tarefa) ou no botão **Cancelar** (para cancelar sem fazer alterações e voltar à UI na qual você abriu o assistente).

O AppAssure oferece vários assistentes, que podem ser divididos em duas categorias.

Primeiramente, há assistentes para instalar, atualizar ou remover o software AppAssure e os componentes relacionados. Normalmente, eles são iniciados ao clicar duas vezes em um programa executável de instalador de software. Os instaladores podem ser acessados ao baixar componentes específicos do Portal de licenças do Dell AppAssure.

Em segundo lugar, os assistentes estão disponíveis na interface de usuário do AppAssure Core Console. Normalmente, eles são lançados ao clicar em um botão ou link rotulado com a função ou o resultado do assistente. Os assistentes dessa categoria são listados a seguir.

Tabela 1. Assistentes disponíveis no AppAssure Core Console

Nome do assistente	Iniciado por	Descrição
Guia de início rápido	Opção Guia de início rápido (menu Ajuda)	Unifica vários fluxos de trabalho para simplificar tarefas comuns do AppAssure. Guia o usuário no processo de proteger máquinas, configurar a replicação em novos agentes, exportar dados protegidos para máquinas virtuais, criptografar dados pontuais de recuperação, configurar grupos de notificação por email e configurar uma política de retenção.
Assistente de proteção de máquina	Botão Proteger máquina (barra de botões)	Configura a proteção em uma máquina que você especifica. Permite dar um nome à máquina para ser exibido no console do Core. Se o software Agent já estiver instalado, ele permite selecionar volumes para a proteção. Caso contrário, o assistente instalará o software e protegerá todos os volumes. Configura uma programação padrão de proteção ou permite configurar uma programação personalizada. Nas configurações avançadas, é possível escolher (ou criar) um repositório e estabelecer a criptografia para os dados protegidos.
Assistente de proteção de diversas máquinas	Botão Proteção em massa (guia Inicial)	Configura a proteção em várias máquinas que você especifica, a partir de um servidor de domínio do Active Directory do Windows, um host virtual do VMware vCenter Server/ESX(i) ou manualmente (inserindo uma lista em um formato especificado).
Assistente de replicação	Link Adicionar core de destino (guia Replicação)	Configura a replicação a partir de um core primário (ou de origem) para que uma cópia dos dados protegidos esteja sempre disponível em um core de destino separado.
Assistente de restauração de máquinas	Botão Restaurar (barra de botões)	Orienta você durante o processo de restaurar dados a partir de um ponto de recuperação no Core para uma máquina protegida, ou ao iniciar uma bare metal restore.
Assistente de exportação	Botão Exportar (barra de botões), link Adicionar (guia Modo de espera virtual)	Exporta dados do ponto de recuperação de uma máquina protegida para uma máquina virtual em qualquer formato de VM suportado. É possível realizar uma exportação única ou configurar o modo de espera virtual para a exportação contínua.

Normalmente, os assistentes instalam ou configuram recursos no AppAssure, mas é possível modificar posteriormente a maioria desses aspectos no Core Console.

2

Noções básicas sobre o AppAssure Core Console

Este capítulo descreve os diferentes elementos da interface de usuário do AppAssure Core Console. Os seguintes tópicos estão incluídos:

- Navegar no Core Console
- Usar a caixa de diálogo Erro
- Noções básicas sobre o Guia de início rápido
- Visualizar o menu de máquinas protegidas
- Visualizar o painel Máquinas replicadas
- Visualizar o menu Apenas pontos de recuperação
- Visualizar o menu Grupos personalizados

O Core Console é a principal interface de usuário (UI) através da qual os usuários interagem com o AppAssure. Ao efetuar login no AppAssure Core Console, você vê os seguintes elementos na UI.

Tabela 2. Elementos de UI incluídos no Core Console

Elemento de UI	Descrição
Área de imagem corporativa	Na maioria dos ambientes, o AppAssure Core Console possui a imagem corporativa do Dell AppAssure. Quando você clica na área de imagem corporativa, uma nova guia é aberta no navegador da web, exibindo a documentação do produto no site de suporte.
Barra de botões	A barra de botões contém botões acessíveis de qualquer lugar no Core Console. Esses botões iniciam assistentes para realizar tarefas comuns, como proteger uma máquina, executar uma restauração a partir de um ponto de recuperação ou exportar dados para uma máquina virtual. Os botões incluem:
	O botão **Proteger** inicia o assistente de proteção de máquina, no qual você pode proteger uma única máquina no AppAssure Core. Para ver outras opções de proteção, acesse o menu suspenso ao lado desse botão. • A opção **Proteger máquina** é outro método para iniciar o assistente de proteção de máquina para proteger uma única máquina. • A opção **Proteger cluster** permite que você se conecte a um cluster de servidor. • A opção **Proteção em massa** abre o assistente de proteção de diversas máquinas para permitir que você proteja duas ou mais máquinas ao mesmo tempo.
	O botão **Restaurar** abre o assistente Restaurar máquina, que permite restaurar dados a partir de pontos de recuperação salvos de uma máquina protegida.

Tabela 2. Elementos de UI incluídos no Core Console

Elemento de UI	Descrição
	O botão **Exportar** abre o assistente Exportar. Nesse assistente, você pode criar uma máquina virtual a partir de pontos de recuperação salvos no AppAssure Core. Você pode criar uma exportação única ou definir parâmetros para uma VM que é continuamente atualizada após cada snapshot de uma máquina protegida.
Contagem de tarefas em execução	Mostra quantos trabalhos estão em execução no momento. Esse valor é dinâmico, com base no estado do sistema. Ao clicar no menu suspenso, você vê um resumo do status de todos os trabalhos em execução. Clicando no X de um trabalho, é possível selecionar o cancelamento desse trabalho.
Menu suspenso de Ajuda	O menu Ajuda inclui as seguintes opções: • **Ajuda**. Contém links para a documentação técnica do AppAssure no site de suporte do Dell. • **Suporte.** Contém links para o site de suporte do Dell, fornecendo acesso ao Live Chat, tutoriais em vídeo, artigos da base de conhecimento do AppAssure, perguntas frequentes etc. • **Guia de início rápido.** O Guia de início rápido é um fluxo guiado de tarefas sugeridas para configurar e usar o AppAssure. O guia é aberto automaticamente cada vez que você efetua login no Core Console, a menos que você desabilite essa função. Também é possível abrir o Guia de início rápido no menu Ajuda. Para obter mais informações sobre o Guia de início rápido, consulte Navegar no Core Console. • **Sobre**. Abre a caixa de diálogo Sobre o AppAssure Core, que inclui informações sobre a versão e uma descrição do software.
Data e hora do servidor	A hora e a data atuais da máquina que executa o serviço do AppAssure Core aparecem no canto superior direito do Core Console. Esse é o horário registrado pelo sistema para eventos como registro em log, programação e geração de relatórios. Por exemplo, ao aplicar as programações de proteção, o horário exibido no Core Console é usado. Isso é verdadeiro mesmo que o fuso horário seja diferente no server de banco de dados ou na máquina cliente onde o navegador está sendo executado.
Área de navegação esquerda	A área de navegação esquerda aparece abaixo da área de imagem corporativa, no lado esquerdo da interface de usuário. Ela contém a barra de ícones e o menu Máquinas protegidas. Se você adicionou replicação a esse Core, esta área contém um menu Máquinas replicadas. Se há máquinas que foram removidas da proteção, mas cujos pontos de recuperação foram salvos, esta área contém um menu Apenas pontos de recuperação. Se você adicionou grupos personalizados, esta área contém um menu Grupo personalizado. Você pode ativar ou desativar a exibição da área de navegação esquerda. Isso é útil quando é preciso ver mais conteúdo na área de navegação principal da UI. Para ocultar esta seção, clique na borda cinza entre as áreas de navegação esquerda e de navegação principal. Para mostrar este elemento de UI novamente, clique na borda cinza outra vez.
Barra de ícones	A barra de ícones inclui uma representação gráfica de cada guia do Core Console. Quando você clica em um item, é conduzido para a seção correspondente da interface de usuário, onde pode gerenciar aquela função. Os ícones da barra de ícones são:
Barra de ícones	**Início.** Clique no ícone Início para navegar até a guia Início do Core.

Tabela 2. Elementos de UI incluídos no Core Console

Elemento de UI	Descrição
	Replicação. Clique no ícone Replicação para visualizar ou gerenciar a replicação de entrada ou de saída.
	Standby virtual. Clique no ícone Standby virtual para exportar informações de um ponto de recuperação para uma máquina virtual inicializável.
	Eventos. Clique no ícone Eventos para visualizar um log de todos os eventos do sistema relacionados ao AppAssure Core.
	Ferramentas. Clique no ícone Ferramentas para visualizar ou gerenciar informações do sistema, CDs de inicialização, montagens, implementação em massa, downloads, arquivos, contas de nuvem, diagnósticos ou relatórios.
	Configuração (definições). Clique no ícone Configuração para visualizar ou gerenciar as opções de configuração do AppAssure Core, incluindo repositórios; chaves de criptografia; grupos de notificação ou definições de servidor de e-mail para notificações; política de retenção do Core; capacidade de anexação do SQL Server; detalhes da licença do AppAssure, limitações, informações sobre o conjunto de licenças e o servidor de licença; funcionalidade de cópia de segurança e restauração das definições do Core; e definições de trabalhos do Core.
Menu Máquinas protegidas	O menu Máquinas protegidas aparece na área de navegação esquerda da UI. O ícone representa uma única máquina. Neste menu, você pode ver as máquinas protegidas, clusters protegidos ou máquinas replicadas configurados no Core. Se houver grupos protegidos ou máquinas apenas com pontos de recuperação, eles também aparecerão neste menu. Para expandir ou retrair a exibição de algum desses objetos no Core, clique na seta no lado esquerdo dessas categorias. Nesse menu é possível executar todas as ações antes acessíveis apenas na guia Máquinas. Quando você clica no menu Máquinas protegidas, a guia Máquinas aparece, mostrando todas as máquinas protegidas neste Core no painel Máquinas protegidas. Para obter mais informações, consulte Visualizar o menu de máquinas protegidas.
Menu Máquinas replicadas	Ao replicar máquinas de outro AppAssure Core, o nome desse Core aparece como um menu separado no menu Máquinas protegidas. O ícone representa a replicação de uma para várias máquinas. Esse menu mostra uma lista das máquinas replicadas. Para expandir ou retrair a exibição de algum desses objetos no Core, clique na seta no lado esquerdo dessas categorias. No menu Máquinas replicadas, você pode executar ações em todas as máquinas replicadas. Quando você clica no menu Máquinas replicadas, a guia Máquinas aparece, mostrando todas as máquinas replicadas neste Core no painel Máquinas replicadas. Para obter mais informações, consulte Visualizar o painel Máquinas replicadas.

Tabela 2. Elementos de UI incluídos no Core Console

Elemento de UI	Descrição
Menu Apenas pontos de recuperação	Se alguma máquina que estava protegida anteriormente no Core tiver sido removida da proteção sem que seus pontos de recuperação tenham sido excluídos, o menu Apenas pontos de recuperação aparecerá. O ícone representa uma única máquina. Para expandir ou retrair a exibição de algum desses objetos no Core, clique na seta no lado esquerdo dessas categorias. No menu Apenas pontos de recuperação, você pode remover os pontos de recuperação de todas as máquinas que têm apenas pontos de recuperação neste Core. Quando você clica no menu Apenas pontos de recuperação, a guia Máquinas aparece, mostrando as máquinas cujos pontos de recuperação foram salvos. Para obter mais informações, consulte Visualizar o menu Apenas pontos de recuperação.
Menu Grupos personalizados	Se o Core inclui algum grupo personalizado, a área de navegação esquerda inclui um menu Grupo personalizado. Este ícone representa um rótulo, que é a propriedade usada para dar nome a um grupo personalizado. Para expandir ou retrair a exibição de algum desses objetos no Core, clique na seta no lado esquerdo dessas categorias. No menu Grupos personalizados, você pode executar ações com itens semelhantes no grupo. Quando você clica no menu Grupos personalizados, a guia Máquinas aparece, mostrando um painel para cada objeto do AppAssure que aparece no grupo: máquinas protegidas, máquinas replicadas e máquinas apenas com pontos de recuperação. Para obter mais informações, consulte Visualizar o menu Grupos personalizados.
Ajuda sensível ao contexto	No AppAssure Core Console, cada vez que você clica no ícone **Ajuda** (um ponto de interrogação azul), uma janela de navegador redimensionável é aberta com dois frames. O frame esquerdo contém uma árvore de navegação mostrando os tópicos do *Guia do usuário do Dell AppAssure*. O frame direito exibe o conteúdo para o tópico de ajuda selecionado. A qualquer momento, a árvore de navegação de ajuda se expande para exibir a localização do tópico selecionado em sua hierarquia. É possível procurar em todos os tópicos do Guia do usuário utilizando esse recurso de ajuda sensível ao contexto. Feche o navegador quando você terminar de pesquisar tópicos. Também é possível abrir a ajuda com a opção Ajuda no menu Ajuda.

Conclua as etapas a seguir para acessar o AppAssure Core Console.

Para acessar o AppAssure Core Console

- Execute um dos seguintes para acessar o AppAssure Core Console:
  a. Efetue login localmente no seu servidor do AppAssure Core e clique duas vezes no ícone **Core Console**.
  b. Ou digite uma das seguintes URLs no seu navegador da Web:
     - https://<yourCoreServerName>:8006/apprecovery/admin/ ou
     - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/

> **NOTA:** Como a interface de usuário do AppAssure Core Console depende de JavaScript, o navegador da Web usado para acessar o Core Console deve ter JavaScript ativado.
>
> Se você alterou a porta padrão do serviço AppAssure, altere a porta conforme necessário na URL acima.

Navegar no Core Console

Ao efetuar o login no Core Console, e ao clicar no ícone ou na guia Início a qualquer momento, a guia Início aparecerá e será automaticamente selecionada. É possível navegar para qualquer outra guia clicando no nome dela ou no ícone correspondente.

As outras guias acessíveis no Core incluem Replicação, Standby virtual, Eventos, Ferramentas e Configuração.

Quando você seleciona uma máquina protegida ou replicada, o foco do Core Console muda para exibir informações apenas sobre a máquina selecionada, e não sobre o Core.

As guias que podem ser acessadas a partir de um agente protegido ou replicado são Resumo (substituindo a guia Início), Pontos de recuperação, Eventos, Ferramentas e Configuração.

Para voltar a visualizar informações sobre o Core, incluindo exibições de várias máquinas protegidas ou replicadas, clique no ícone Início no canto superior esquerdo da UI.

NOTA: Quando você vê a guia Início, está visualizando informações sobre o Core. Quando vê uma guia Resumo, está visualizando informações sobre uma única máquina protegida pelo Core ou replicada nele. Quando você vê uma guia Máquinas, está visualizando informações sobre todas as máquinas protegidas pelo AppAssure Core ou replicadas nele. Quando você vê uma guia Pontos de recuperação, está visualizando informações sobre uma máquina apenas com pontos de recuperação no Core.

Para obter informações sobre os recursos e funções disponíveis em cada guia, consulte a seção apropriada a seguir.

Para obter mais informações sobre a visualização de máquinas protegidas, consulte Visualizar o menu de máquinas protegidas. Para obter mais informações sobre o gerenciamento de máquinas protegidas, consulte Gerenciar máquinas protegidas.

Para obter mais informações sobre a visualização de máquinas replicadas, consulte Monitorar a replicação.

Visualizar a guia Início

A guia Início aplica-se apenas ao Core. Ela exibe todas as máquinas que o Core protege, além de todos os repositórios e alertas associados a essas máquinas. Para acessar a guia Início, clique na guia ou no ícone de casa acima da coluna de máquinas no lado esquerdo da página. A tabela a seguir descreve os vários elementos da guia Início.

Tabela 3. Opções da guia Início

Elemento de UI	Descrição
Máquinas protegidas	O menu Máquinas protegidas mostra uma lista das máquinas que este Core protege. • Quando você clica no menu Máquinas protegidas, a guia Máquinas aparece, mostrando o painel Máquinas protegidas. Para obter mais informações sobre o que você pode realizar na guia Máquinas, consulte Visualizar a guia Máquinas de uma máquina protegida. • Quando você clica em uma máquina específica no menu Máquinas protegidas, a guia Resumo aparece, mostrando informações resumidas sobre essa máquina. Para obter mais informações sobre o que você pode realizar na guia Resumo, consulte Visualizar a guia Resumo.
Máquinas replicadas	Se aparecer o nome de outro AppAssure Core no menu Máquinas protegidas, esse é o menu Máquinas replicadas. Esse menu mostra uma lista das máquinas que este Core protege por meio de replicação, o que significa que este é o Core de destino das máquinas protegidas listadas. A seção inclui as seguintes informações sobre cada máquina replicada: • Quando você clica no menu Máquinas replicadas, a guia Máquinas aparece, mostrando o painel Máquinas replicadas. Para obter mais informações sobre o que você pode realizar na guia Máquinas, consulte Visualizar a guia Máquinas de uma máquina protegida. • Quando você clica em uma máquina replicada específica no menu Máquinas replicadas, a guia Resumo aparece, mostrando informações resumidas sobre essa máquina. Para obter mais informações sobre o que você pode realizar na guia Resumo, consulte Visualizar a guia Resumo. Para obter mais informações sobre replicação, consulte Noções básicas sobre replicação.
Apenas pontos de recuperação	Máquinas apenas com pontos de recuperação são máquinas que você não protege mais com um AppAssure Core, mas cujos pontos de recuperação você continua a armazenar. Se você remover uma máquina da proteção mas optar por manter os pontos de recuperação, a máquina aparecerá em Apenas pontos de recuperação. Esses pontos de recuperação podem ser usado para recuperação em nível de arquivo, mas não para bare metal restore, restauração de volumes inteiros ou adição de dados de snapshot. A seção inclui as seguintes informações sobre cada máquina apenas com pontos de recuperação: • **Status.** Não há indicador de status para máquinas apenas com pontos de recuperação, pois não há conexão com a máquina. • **Nome da máquina.** O nome de exibição da máquina cujos pontos de recuperação você manteve. • **Repositório.** O nome do repositório onde os pontos de recuperação da máquina estão armazenados. • **Último snapshot.** O horário em que o AppAssure criou o ponto de recuperação mais recente da máquina. • **Pontos de recuperação.** O número de pontos de recuperação da máquina armazenados no repositório. • **Espaço total protegido.** A quantidade de espaço que os pontos de recuperação dessa máquina consomem no repositório.

Tabela 3. Opções da guia Início

Elemento de UI	Descrição
Repositórios	Esta seção mostra uma lista de todos os repositórios que esse Core usa para armazenar pontos de recuperação. São incluídas as seguintes informações sobre cada repositório: • **Status.** Círculos coloridos na coluna Status mostram se o repositório está montado e se pode aceitar transferências de pontos de recuperação. • **Nome do repositório.** O nome de exibição do repositório. • **Tamanho total.** A quantidade total de espaço no repositório. • **Espaço livre.** A quantidade de espaço disponível no repositório. • **Dados protegidos.** A quantidade de espaço usado no repositório. • **Máquinas.** O número de máquinas cujos pontos de recuperação o repositório armazena. • **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório. • **Taxa de compressão.** A taxa com que o repositório comprime os dados protegidos para economizar espaço. Para obter mais informações, consulte Noções básicas sobre repositórios.
Alertas	Esta seção mostra os alertas do Core e de todas as máquinas que ele protege. A seção inclui as seguintes informações: • **Ícones.** A coluna de ícones indica a natureza do alerta. • **Data.** Exibe a data e a hora em que o AppAssure gerou o alerta. • **Mensagem.** Descreve o alerta. Você também pode ver esses detalhes na guia Eventos do Core. Para obter mais informações, consulte Visualizar tarefas, alertas e eventos.

Visualizar a guia Replicação

A guia Replicação permite visualizar e alterar detalhes dos Cores que estão configurados para transferir dados replicados com o Core atual. Você também pode visualizar e alterar os detalhes das máquinas que estão sendo replicadas. O layout da guia é o mesmo independentemente de ser um Core de origem ou de destino; portanto, há seções designadas para as duas situações.

Para acessar a guia Replicação, clique na guia ou no ícone Replicação, semelhante a um monitor de computador partido, acima da coluna de máquinas no lado esquerdo da página. A tabela a seguir contém descrições das seções e dos recursos disponíveis na guia Replicação.

Tabela 4. Opções da guia Replicação

Elemento de UI	Descrição
Replicação de saída	A seção exibe o Core ou os Cores que estão replicando dados para um Core de destino remoto. As informações exibidas incluem: • **Nome do Core de destino.** O nome do Core para o qual o Core de origem atual está replicando dados. • **Estado.** O estado do emparelhamento de replicação; por exemplo, Estabelecido indica um emparelhamento bem-sucedido entre os Cores de origem e de destino, de modo que a transferência pode ser realizada. • **Máquinas.** Esta coluna mostra o número de máquinas protegidas ou agentes que estão sendo replicados para o Core de destino. • **Progresso.** Quando um trabalho de replicação ocorre, essa coluna exibe uma barra que permite monitorar o progresso do trabalho.
Replicação de entrada	A seção exibe o Core ou os Cores dos quais o Core atual está recebendo dados replicados (por exemplo, quando você está no Core Console de um Core de destino). As informações exibidas incluem: • **Nome do Core de destino.** O nome do Core do qual o Core de origem atual está recebendo dados replicados. • **Estado.** O estado do emparelhamento de replicação; por exemplo, Estabelecido indica um emparelhamento bem-sucedido entre os Cores de origem e de destino, de modo que a transferência pode ser realizada. • **Máquinas.** Esta coluna mostra o número de agentes ou máquinas protegidas que o Core atual está replicando. • **Progresso.** Quando um trabalho de replicação ocorre, essa coluna exibe uma barra que permite monitorar o progresso do trabalho.
Adicionar Core de destino	Use esse botão para adicionar um Core de destino para o qual replicar. Para obter mais informações, consulte Configurar a replicação. **NOTA:** Não é possível adicionar um Core de origem a partir de um Core de destino.
Definições	Use este botão para alterar as definições de todas as replicações de entrada ou de saída. Para obter mais informações, consulte Gerenciar definições de replicação.
> (Core)	O botão de expansão ao lado do nome de um Core exibe os agentes ou máquinas protegidas que estão sendo replicados. Os seguintes detalhes são incluídos: • **Nome do agente.** Nome da máquina protegida. • **Estado.** Estado do emparelhamento entre essa máquina e o Core de destino; por exemplo, o estado Estabelecido indica um emparelhamento bem-sucedido, no qual pode ocorrer transferência. • **Status.** Esta coluna está presente apenas para agentes que aparecem em Cores de destino e indica se a máquina "Não foi replicada ainda" ou foi "Sincronizada a partir de [data e hora]". • **Progresso.** Quando um trabalho de replicação ocorre, essa coluna exibe uma barra que permite monitorar o progresso do trabalho.
> (Agente)	Este colchete aparece apenas ao lado de agentes listados em um Core de destino. Ele expande uma lista dos pontos de recuperação que foram replicados dessa máquina. Para obter mais informações, consulte Etapa 2 em Visualizar pontos de recuperação.

Tabela 4. Opções da guia Replicação

Elemento de UI	Descrição
Menu suspenso Core (em Replicação de saída)	O menu suspenso (ícone de engrenagem) ao lado do nome de um Core de destino inclui as seguintes funções: • **Detalhes.** Mostra o ID do cliente, URL, nome de exibição, estado, ID do Core, endereço de e-mail e comentários associados a esse Core. Para obter mais informações, consulte Monitorar a replicação. • **Alterar definições.** Permite editar o host e a porta desse Core. Para obter mais informações, consulte Alterar as definições do Core de destino. • **Excluir.** Remove o Core da replicação. Para obter mais informações, consulte Remover um Core de destino da replicação. • **Programar.** Permite designar horários específicos para a realização da replicação. Para obter mais informações, consulte Programar a replicação. • **Adicionar máquinas.** Permite adicionar a esse Core de destino máquinas protegidas para serem replicadas.
Menu suspenso Core (em Replicação de entrada)	O menu suspenso (ícone de engrenagem) ao lado do nome de um Core de origem inclui as seguintes funções: • **Detalhes.** Mostra o ID do cliente, URL, nome de exibição, estado, ID do Core, endereço de e-mail e comentários associados a esse Core. Para obter mais informações, consulte Monitorar a replicação. • **Consumir.** Adiciona uma unidade de propagação de uma máquina protegida ao repositório do Core de destino para estabelecer a base de um agente replicado. Para obter mais informações, consulte Consumir a unidade de propagação em um Core de destino. • **Excluir.** Remove o Core da replicação. Para obter mais informações, consulte Remover um Core de origem da replicação.
Menu suspenso Agente (linha de cabeçalho da tabela)	O menu suspenso (ícone de engrenagem) na linha de cabeçalho se aplica a máquinas protegidas ou agentes selecionados na tabela. Inclui as seguintes funções: • **Forçar.** Força uma transferência de dados replicados. • **Pausar.** Pausa a replicação e impede que o trabalho ocorra até ser retomado. • **Retomar.** Retira a replicação do estado de pausa • **Copiar.** Cria uma unidade de propagação da máquina protegida. Para obter mais informações, consulte Noções básicas sobre unidades de propagação e Usar a função Copiar para criar uma unidade de propagação. • **Excluir.** Remove os agentes selecionados da replicação. Para obter mais informações sobre essas funções, consulte Gerenciar definições de replicação e Remoção da replicação.
Forçar atualização	Há um botão Forçar atualização após as seções Replicação de saída e Replicação de entrada. Em cada seção, esse botão circular estabelece comunicação sob demanda entre os Cores para atualizar dados que possam ter sido alterados desde a última transferência programada.

Tabela 4. Opções da guia Replicação

Elemento de UI	Descrição
Menu suspenso Agente (agentes individuais em Replicação de saída)	O menu suspenso (ícone de engrenagem) ao lado de uma máquina protegida ou agente individual oferece funções que se aplicam apenas a essa máquina. Inclui as seguintes funções: • **Definições.** Permite definir a prioridade de replicação desse agente. Para obter mais informações, consulte Definir a prioridade de replicação de uma máquina protegida. • **Forçar.** Força uma transferência de dados replicados. Forçar a replicação. • **Excluir.** Remove o agente da replicação. Para obter mais informações, consulte Remover uma máquina protegida da replicação no Core de origem.
Menu suspenso Agente (agentes individuais em Replicação de entrada)	O menu suspenso (ícone de engrenagem) ao lado de uma máquina protegida ou agente individual oferece funções que se aplicam apenas a essa máquina. Inclui as seguintes funções: • **Definições.** Permite definir a prioridade de replicação desse agente. Para obter mais informações, consulte Definir a prioridade de replicação de uma máquina protegida. • **Ativação pós-falha.** Caso ocorra uma situação de recuperação após um desastre, essa função permite realizar ativação pós-falha da máquina replicada até que a máquina original seja reparada. Para obter mais informações, consulte Noções básicas sobre ativação pós-falha e reativação pós-falha. • **Excluir.** Remove o agente da replicação. Para obter mais informações, consulte Remover uma máquina protegida no Core de destino.

Visualizar a guia Standby virtual

A guia Standby virtual permite iniciar e gerenciar a exportação contínua de uma máquina protegida para um de vários tipos de host de máquina virtual (VM). Os tipos de VM disponíveis são:

- ESXi
- VMware Workstation
- Hyper-V
- VirtualBox

A barra de menus no cabeçalho Standby virtual inclui ações que você pode aplicar a qualquer máquina Virtual Standby selecionada. A tabela a seguir contém descrições dos vários elementos e recursos da guia Standby virtual.

Tabela 5. Opções da guia Standby virtual

Elemento de UI	Descrição
Adicionar	Cria uma máquina Virtual Standby exportando um ponto de recuperação para um destino virtual.
Force	Realiza uma transferência sob demanda dos últimos pontos de recuperação da máquina protegida original para a máquina Virtual Standby.
Pause	Pausa a transferência de dados do Core para a máquina virtual.
Resume	Retoma a transferência de dados após a pausa.
Remover	Encerra a conexão entre o Core e a máquina virtual.
Exibir fila de exportação (nº)	Revela a ordem da transferência programada de dados para várias máquinas virtuais.

No Core Console, a tabela abaixo da barra de menus mostra as máquinas virtuais às quais o Core está conectado. A tabela a seguir define os detalhes que a guia exibe para cada máquina.

Tabela 6. Tabela da guia Standby virtual

Elemento de UI	Descrição
Status	O estado atual da transferência de dados, como, por exemplo, pausado.
Nome da máquina	O nome da máquina Virtual Standby.
Destino	O nome da máquina para a qual o Core exporta os pontos de recuperação.
Tipo de exportação	O tipo do software host da máquina virtual.
Última exportação	Data e hora da última exportação.

Visualizar a guia Eventos

Na guia Eventos, você pode visualizar os trabalhos que ocorreram ou que estão em progresso no Core. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que o AppAssure precisa realizar para operar com êxito.
- **Alertas.** Uma notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Eventos.** Uma combinação de todas as tarefas e alertas do Core.

A tabela a seguir contém descrições de cada elemento da guia Eventos.

Tabela 7. Opções da guia Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa.
Ícones de status	Cada ícone representa um status diferente do trabalho. Quando você clica em um dos ícones, a lista é filtrada por esse status, gerando um relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.** Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.** Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Noções básicas sobre replicação.) • **Concluído.** Um trabalho que o Core concluiu com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status. Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.

Tabela 7. Opções da guia Eventos

Elemento de UI	Descrição
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Ela inclui os seguintes formatos: • PDF • XLS • XLSX • RTF • CSV
Ícone Exportar	Converte o relatório de eventos para o formato selecionado.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e setas na parte inferior da guia Eventos permitem navegar pelas páginas adicionais do relatório.

A guia Eventos exibe todos os eventos em uma tabela. A tabela inclui as seguintes informações sobre cada item.

Tabela 8. Informações da tabela da guia Eventos

Elemento de UI	Descrição
>	O colchete expande o trabalho para revelar os seguintes detalhes: • **Hora inicial.** Quando o trabalho começou. • **Hora de término.** Quando o trabalho terminou. • **Tempo decorrido.** O período de tempo durante o qual o trabalho esteve ativo. • **Taxa.** A taxa em que o Core transfere os dados. • **Progresso.** Quando um trabalho está em progresso, mostra em tempo real a proporção concluída pelo Core. Quando o trabalho está concluído, mostra o quanto do trabalho o Core concluiu. • **Fase.** Quando um trabalho está em progresso, esse detalhe mostra qual é o estágio atual de progresso (por exemplo, Transferindo). • **Cancelar.** Quando um trabalho está em progresso, um link aqui permite cancelá-lo. • **Trabalho total.** Quando um trabalho está concluído, mostra o quanto do trabalho o Core concluiu. • **Tarefa subordinada.** Mostra as subtarefas associadas a esse trabalho.
Trabalho	O tipo de trabalho que o Core realizou, como transferência de volumes, manutenção de repositório ou rollup em execução.
Status	O status do trabalho, como Bem-sucedido no caso de um trabalho concluído com êxito ou Erro no caso de um trabalho que falhou devido a erros.
Hora inicial	O dia e hora em que o trabalho foi iniciado.
Hora final	O dia e hora em que o trabalho terminou.
Detalhes	Abre a janela Monitorar tarefa ativa. Inclui os detalhes exibidos quando você expande o trabalho, além dos seguintes detalhes sobre trabalhos subordinados: • Hora inicial • Hora final • Tempo decorrido • Taxa • Progresso • Trabalho total

Visualizar a guia Ferramentas

A guia Ferramentas mostra informações do sistema por padrão e permite acessar ferramentas que ajudam a gerenciar o Core. Para acessar essas ferramentas, selecione uma opção no menu Ferramentas à esquerda ou no menu suspenso da guia Ferramentas. Essas ferramentas são descritas na tabela a seguir.

Tabela 9. Informações sobre as ferramentas acessíveis ao Core

Elemento de UI	Descrição
Informações do sistema	Mostra informações sobre o AppAssure Core, incluindo informações do sistema, volumes locais e montados e conexões do mecanismo Replay. Para obter mais informações, consulte Modificar definições de fila de transferência.
CDs de inicialização	No painel CDs de inicialização, você pode gerenciar (criar ou excluir) imagens ISO de CD de inicialização, necessárias para realizar uma bare metal restore (BMR). As informações sobre qualquer imagem de CD de inicialização exibidas são o caminho da imagem ISO, o ambiente de recuperação para o qual ela foi criada e a data de criação da imagem. Para obter informações sobre o gerenciamento de imagens de CD de inicialização, consulte Gerenciar uma imagem de inicialização do Windows ou Gerenciar uma imagem de inicialização do Linux, respectivamente.
Montagens	No painel Montagens locais, você pode visualizar ou desmontar volumes montados localmente. No painel Montagens remotas, você pode visualizar ou desmontar volumes montados usando o Local Mount Utility. Para obter informações sobre a desmontagem de volumes, consulte Desmontar pontos de recuperação. Para obter mais informações sobre a montagem local de um ponto de recuperação, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Implantação em massa	No painel Implantar Agent em máquinas, você pode implantar o software Agent do Core em várias máquinas Windows simultaneamente. Para obter mais informações sobre como fazer isso, consulte Noções básicas sobre implantação em massa.
Downloads	A página Downloads inclui três seções: Agente, Local Mount Utility e Outros arquivos. Cada seção inclui um link para baixar e instalar os arquivos relevantes. Por exemplo: • A seção Agente inclui um link para baixar o instalador da web do software AppAssure Agent (e também um link para o Portal de licença). • O Local Mount Utility inclui um link para baixar o instalador da web do LMU. • A seção Outros arquivos inclui um link para baixar o arquivo SNMP MIB.
Arquivo	Na página Arquivo, você pode gerenciar arquivos programados e montados. O menu Arquivo oferece as seguintes opções: • **Programado.** Esta opção leva à página Arquivos programados principal. • **Criar.** Permite criar um arquivo de pontos de recuperação. • **Verificar arquivo.** Abre a janela Verificar arquivo e permite procurar, em um arquivo, arquivos de índice mapeando deslocamentos, integridade de estrutura e integridade de soma de verificação. • **Importar.** Use essa opção para importar um arquivo de pontos de recuperação com o objetivo de procurar no arquivo e restaurar dados arquivados. Para obter mais informações, consulte Noções básicas sobre arquivos.

Tabela 9. Informações sobre as ferramentas acessíveis ao Core

Elemento de UI	Descrição
Nuvens	A página Nuvens permite adicionar suas contas de provedor de nuvem ao AppAssure Core Console para poder usá-las como destino de arquivos. Para obter mais informações, consulte Arquivar na nuvem. Para gerenciar contas de nuvem, consulte Gerenciar contas de nuvem.
Diagnóstico	A página Diagnóstico é para sua conveniência, caso você encontre um problema para o qual queira solicitar assistência do Suporte do AppAssure. Aqui você pode usar as opções de menu Download e Upload para baixar ou carregar um log do Core. Para obter mais informações, consulte Baixar os logs do Core e Carregar logs.
Relatórios	A página Relatórios permite gerar relatórios sobre a atividade do Core e exportá-los em diversos formatos. As opções de relatórios são: • **Conformidade.** Fornece o status de trabalhos realizados pelo Core. • **Resumo.** Fornece informações sobre os repositórios associados ao Core. • **Falha.** Um subconjunto do relatório Conformidade que mostra apenas os trabalhos com falha que o Core tentou realizar. Para obter mais informações, consulte Gerar e visualizar relatórios.

Visualizar a guia Configuração

A guia Configuração mostra definições e opções de configuração que permitem ajustar e personalizar a proteção do AppAssure de acordo com as necessidades de sua empresa. Para acessar essas opções, selecione uma opção no menu da página Configuração ou no menu suspenso da guia Configuração. Essas opções são descritas na tabela a seguir.

Tabela 10. Opções da guia Configuração

Elemento de UI	Descrição
Repositórios	A guia Repositórios permite adicionar, editar e remover repositórios e locais de armazenamento. Para obter mais informações, consulte Noções básicas sobre repositórios.
Segurança	Na guia Segurança, você pode adicionar chaves de criptografia para proteger seus dados. Para obter mais informações, consulte Noções básicas sobre chaves de criptografia.
Eventos	Diferentemente da guia Eventos, a opção de menu Eventos da guia Configuração permite gerenciar e modificar as notificações que você e seus colegas recebem sobre diversos tópicos, como replicação, arquivo e truncamento de log. Nessa guia, você pode adicionar e editar grupos, gerenciar definições de e-mail e filtrar a quantidade de alertas de e-mail enviados ativando a redução de repetição. Para obter mais informações sobre a opção Eventos, consulte Noções básicas sobre notificações por e-mail, Configurar grupos de notificação e Configurar retenção de eventos.
Política de retenção	A guia Política de retenção permite determinar por quanto tempo um ponto de recuperação deve ser mantido antes de ser arquivado. Essa opção usa o recurso de rollup para combinar pontos de recuperação após um período predefinido, deduplicar os dados e reduzir o tamanho dos dados no repositório para economizar espaço. Para obter mais informações, consulte Gerenciar políticas de retenção.
Capacidade de anexação	Na guia Capacidade de anexação, você pode modificar as definições de verificação de capacidade de anexação das máquinas SQL Server protegidas. Uma verificação de capacidade de anexação determina se é seguro recuperar um banco de dados SQL. Para obter mais informações, consulte Configurar as definições de capacidade de anexação do SQL.

Tabela 10. Opções da guia Configuração

Elemento de UI	Descrição
Definições	As opções disponíveis na página Definições da guia Configuração se aplicam ao Core e a todas as suas máquinas protegidas. Isso inclui a capacidade de modificar definições nas seguintes categorias: • **Geral.** As definições gerais incluem o nome de exibição do Core, a porta do servidor da Web e a porta de serviço. Para obter mais informações, consulte Noções básicas sobre informações do sistema. • **Atualizações.** A seção Atualizações permite determinar quando verificar se há atualizações do AppAssure e quando instalá-las. Ela também exibe o status das atualizações disponíveis e a última vez em que o AppAssure verificou a existência de atualizações. Consulte Configuração das definições de atualização. • **Trabalhos noturnos.** Trabalhos noturnos são tarefas regulares de manutenção programadas para horários fora do expediente para não causar interrupções nos horários de trabalho mais intenso. Incluem tarefas como download de logs de máquinas protegidas, o trabalho de verificação de capacidade de anexação, rollup e truncamento de log. Para obter mais informações, consulte Noções básicas sobre trabalhos noturnos. • **Fila de transferência.** As definições de Fila de transferência determinam quantas transferências de dados devem ocorrer ao mesmo tempo e quantas vezes o AppAssure deve tentar realizar uma transferência em caso de problemas de rede. Para obter mais informações, consulte Modificar definições de fila de transferência.
Aplicação de licença	Na página Aplicação de licença, você pode alterar o tipo de licença que usa e visualizar informações sobre restrições de aplicação de licença, conjuntos de licenças e servidor de licenças. A seção Servidor de licenças indica o status da comunicação entre o Core e o Portal de licenças. Para obter mais informações, consulte Gerenciar licenças.
Cópia de segurança/ restauração	A opção Cópia de segurança/restauração permite criar uma cópia de segurança e restaurar as definições do Core. Para obter mais informações, consulte Criar cópia de segurança e restaurar definições do Core.
Definições de trabalho	Na página Definições de trabalho, você pode adicionar trabalhos e modificar as definições de trabalhos com execução programada no Core. Os trabalhos incluem ChecksumCheckJob, MountabilityCheckJob e ReplicationJob, entre outros. Para obter mais informações, consulte Configurar as definições de trabalhos do Core.

Usar a caixa de diálogo Erro

Quando um erro ocorre na interface de usuário do AppAssure Core Console, como a tentativa de inserir um parâmetro inválido, uma caixa de diálogo Erro aparece.

A caixa de diálogo geralmente indica a causa do erro, fornece alguns links para informações adicionais sobre o erro e inclui um botão Fechar. Você precisa fechar a caixa de diálogo Erro para continuar, mas talvez queira visualizar mais informações sobre o erro.

Na caixa de diálogo Erro, escolha entre as opções a seguir:

Tabela 11. Opções da caixa de diálogo Erro

Elemento de UI	Descrição
Exibir detalhes	Quando você clica nesse link, a caixa de diálogo se expande para incluir detalhes adicionais sobre o erro. Essa opção aparece apenas quando os detalhes não estão sendo exibidos.
Ocultar detalhes	Quando você clica nesse link, a caixa de diálogo se contrai e oculta os detalhes do erro. Essa opção aparece apenas quando os detalhes do erro já estão sendo exibidos.
Exibir acompanhamento de pilha	Quando você clica neste link, é exibido o nível mais alto de detalhes sobre o erro, incluindo a cadeia de exceções e o erro de acompanhamento de pilha completo
Ocultar acompanhamento de pilha	Quando você clica neste link, a caixa de diálogo se contrai, ocultando o erro de acompanhamento de pilha e os detalhes. Essa opção aparece apenas quando os detalhes de acompanhamento de pilha já estão sendo exibidos.
Pesquisar base de conhecimento	Quando você clica nesse link, uma janela de navegador se abre mostrando o site da base de conhecimento (KB) de suporte do Dell AppAssure. Detalhes sobre o erro são automaticamente aprovados como parâmetros para pesquisar a base de conhecimento por palavra-chave. Se existir quaisquer artigos da KB sobre o erro, esses artigos aparecem na página.
Fechar	Quando você clica neste botão, a caixa de diálogo Erro se fecha, permitindo que você corrija as informações incorretas inseridas no AppAssure Core Console quando o erro apareceu.

Os erros da interface de usuário que causam o aparecimento da caixa de diálogo Erro não são rastreados na guia Eventos do AppAssure, pois são apenas erros de validação ou inserção de dados. No entanto, quando você clica na opção Pesquisar base de conhecimento referente a algum erro, a URL do link fornecido é registrada no arquivo CoreAppRecovery.log. Você pode pesquisar a cadeia de caracteres de texto "KB article url generated" no log para ver a URL de cada erro que foi visualizado em um navegador. Para obter mais informações sobre download ou visualização de logs de erros do Core, consulte os tópicos Baixar os logs do Core ou Visualizar os logs do Core, respectivamente.

Noções básicas sobre o Guia de início rápido

O Guia de início rápido é um novo recurso disponível no AppAssure versão 5.4 e posterior. Esse recurso fornece um fluxo guiado de tarefas sugeridas para configurar e usar o AppAssure.

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o AppAssure Core e navega até o Core Console. Clique na página Bem-Vindo do **Guia de início** para ver as várias tarefas de configuração sugeridas. Navegue pelo guia usando as opções **Ignorar etapa** e **Voltar**. Quando tiver visto a última tarefa sugerida, clique em **Concluir** para fechar o guia.

É possível iniciar o Guia de início rápido novamente a qualquer momento. Também é possível ocultar a página Bem-Vindo do Guia de início rápido. Para obter mais informações sobre essas opções, consulte Início do Guia de início rápido.

A menos que você o oculte, o Guia de início rápido reaparecerá toda vez que você efetuar login no AppAssure Core Console e acessar a guia Início. Para obter mais informações, consulte Ocultação do Guia de início rápido.

Você não é obrigado a realizar as etapas sugeridas pelo guia. É possível simplesmente visualizar as tarefas sugeridas e navegar por elas usando as opções **Ignorar etapa** e **Voltar**. Opcionalmente, para ocultar o guia para qualquer ponto, clique em **Sair do Guia**.

Se você optar por executar alguma tarefa de configuração sugerida pelo Guia de início rápido, siga os prompts indicados em qualquer etapa do guia e aparecerá o assistente apropriado ou a área relevante da interface do usuário. Os procedimentos para executar cada tarefa sugerida pelo guia estão descritos neste documento, como indicado na tabela abaixo.

NOTA: Nem todas as tarefas de configuração sugeridas pelo Guia de início rápido são obrigatórias para todos os usuários. É preciso entender que tarefas deseja realizar para suas necessidades específicas.

O Guia de início rápido aborda as seguintes tarefas de configuração:

Tabela 12. Tarefas de configuração do Guia de início rápido

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Proteção	Proteção de uma máquina agente, um cluster de servers ou várias máquinas usando a proteção em massa	Clique em Proteger ou selecione **Proteger máquina** no menu suspenso para abrir o Assistente de proteção de máquina. Para obter informações sobre como executar o Assistente de proteção de máquina, consulte Proteger uma máquina. Selecione **Proteger cluster** no menu suspenso para abrir a caixa de diálogo Conectar-se ao cluster. Para obter mais informações sobre como proteger um cluster, consulte Proteger um cluster. Selecione **Proteção em massa** para abrir o Assistente de proteção de diversas máquinas. Para obter informações sobre como executar o Assistente de proteção de diversas máquinas, consulte Proteger várias máquinas.
Replicação	Configuração da replicação de um core principal (origem) para um secundário (de destino)	Clique em **Replicação** para abrir a guia Replicação. É solicitado que um core de destino seja adicionado usando o Assistente de replicação. Para obter informações sobre o uso do Assistente de replicação para configurar a replicação em um core autogerenciado, consulte Replicar para um Core de destino autogerenciado. Para obter informações gerais sobre replicação, consulte Configurar a replicação.
Exportação virtual	Realização de uma exportação única ou estabelecimento de exportação contínua de uma máquina agente protegida para uma máquina virtual	Clique em **Exportar** para realizar uma exportação de dados de sua máquina protegida para uma máquina virtual. É possível realizar uma exportação única ou configurar o standby virtual para exportação contínua para uma VM. Para obter informações sobre exportações virtuais, consulte Exportar dados para uma máquina virtual baseada em Windows.
Configuração	Permite definir configurações adicionais do AppAssure Core	Clique em **Configuração** para ver configurações de segurança (configuração de chaves de criptografia), notificações (configuração das notificações de eventos) e políticas de retenção (definição de critérios para rollup de pontos de recuperação do envelhecimento).
Configuração: Criptografia	Configuração de chave de criptografia que pode ser usada por um ou mais agentes	Clique em **Segurança** para abrir a página Segurança na guia Configuração. Solicita que você adicione uma chave de criptografia ou importe uma. Depois de fazer isso, você pode aplicá-la a um ou mais agentes. A criptografia é descrita no tópico Noções básicas sobre chaves de criptografia.
Configuração: Notificações	Configuração de notificações de eventos, avisos e alertas	Clique em **Eventos** para especificar os grupos de notificação de eventos, avisos e alertas. Para enviar estas informações por e-mail, você também deve estabelecer as definições do server de SMTP. Para obter informações sobre o gerenciamento de eventos, consulte o tópico Gerenciar eventos, incluindo os tópicos Configurar grupos de notificação e Configurar um servidor de e-mail.

Tabela 12. Tarefas de configuração do Guia de início rápido

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Configuração: Retenção	Visualização ou alteração da política de retenção padrão do Core	Clique em **Política de retenção** para abrir a página Política de retenção na guia Configuração. Daqui, é possível definir quanto tempo manter um ponto de recuperação antes de realizar rollup nele. Para obter informações conceituais sobre políticas de retenção, consulte o tópico Retenção e arquivamento. Para obter informações de procedimento, consulte Gerenciar políticas de retenção.
Restaurar	Restauração de dados de um ponto de recuperação do Core	Clique em **Restaurar** para abrir o Assistente de restauração de máquinas. Para obter mais informações sobre como restaurar dados, consulte o tópico Restaurar volumes a partir de um ponto de recuperação.

Início do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o AppAssure Core. A menos que você o oculte, o guia reaparece toda vez que você acessa a guia Início do Core Console.

Use o procedimento abaixo para abrir o Guia de início rápido a qualquer momento no Core Console.

Para iniciar o Guia de início rápido

1. Navegue até o AppAssure Core Console.
2. No menu Ajuda, selecione **Guia de início rápido**.

   O Guia de início rápido é exibido.

Ocultação do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o AppAssure Core.

Também aparece quando o Guia de início rápido é selecionado no menu suspenso de Ajuda e toda vez que for acessada a guia Início do Core Console.

Use o procedimento abaixo para ocultar o Guia de início rápido.

Para ocultar o Guia de início rápido a partir da página Bem-Vindo

- No AppAssure Core Console, se a página Bem-Vindo do Guia de início rápido estiver aberta, faça o seguinte:
  - Se quiser ocultar a página Bem-Vindo do Guia de início rápido, selecione **Não exibir novamente**.

    NOTA: Essa opção ocultará a página Bem-Vindo na próxima vez que o Guia de início rápido for aberto e em todas as ocasiões subsequentes até que o AppAssure Core seja atualizado.

    Se você optar por ocultar essa página e quiser acessar as opções avançadas no futuro, selecione **Voltar** no assistente para ver essa página oculta.
  - Se desejar ocultar o Guia de início rápido nesta sessão, clique em **Fechar**.

    O Guia de início rápido é fechado. Da próxima vez que for acessada a guia Início no Core Console, o Guia de início rápido reaparecerá.

    Também é possível abrir o Guia de início rápido no menu Ajuda, como descrito em Início do Guia de início rápido.

Para ocultar o Guia de início rápido em qualquer etapa

- Em qualquer página do Guia de início rápido, clique em **Sair do guia.**

  O Guia de início rápido é fechado. Se essa opção for selecionada, ainda será possível abrir o Guia de início rápido no menu Ajuda, como descrito em Início do Guia de início rápido.

Visualizar o menu de máquinas protegidas

Na interface de usuário do AppAssure, um menu Máquinas protegidas aparece na área de navegação esquerda. Por padrão, esse menu está totalmente expandido e mostra uma lista de máquinas protegidas por esse Core. Se houver clusters do servidor protegidos, eles são incluídos nessa lista.

Para expandir ou retrair a exibição de máquinas protegidas e clusters do servidor no Core, clique na seta no lado esquerdo desse menu.

O menu Máquinas protegidas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas em todas as máquinas protegidas. Clique na seta à direita de Máquina protegida para ver o menu e executar um dos seguintes:

- Forçar um snapshot incremental de todas as máquinas
- Forçar uma imagem de base de todas as máquinas
- Pausar a proteção de todas as máquinas (se estiver ativa)
- Retomar a proteção de todas as máquinas (se estiver em pausa)
- Atualizar os metadados para todas as máquinas protegidas

Cada máquina relacionada no menu Máquinas protegidas também tem um menu suspenso que controla as funções apenas daquela máquina. No menu suspenso de qualquer máquina, é possível fazer o seguinte:

- Forçar um snapshot da máquina selecionada (é possível escolher volumes na máquina e escolher um snapshot incremental ou uma imagem de base)
- Pausar a proteção da máquina selecionada (se estiver ativa)
- Retomar proteção (se estiver em pausa)
- Atualizar metadados
- Navegar até a guia Resumo da máquina selecionada
- Navegar até a guia Pontos de recuperação da máquina selecionada
- Navegar até a guia Eventos da máquina selecionada
- Navegar até a guia Ferramentas da máquina selecionada (ou selecionar qualquer função)
- Navegar até a guia Configuração da máquina selecionada
- Criar um rótulo personalizado exibido na lista de Máquinas protegidas

Se você estiver gerenciando clusters do servidor no AppAssure Core, o cluster também aparecerá no menu de navegação esquerdo. No menu suspenso de qualquer cluster, também é possível:

- Navegar até a guia Nós protegidos do cluster selecionado

Usando submenus suspensos expansíveis, é possível navegar rapidamente até determinadas funções de uma máquina.

- É possível acessar todas as funções na guia Ferramentas de uma máquina a partir do submenu suspenso expansível Ferramentas.
- É possível acessar todas as funções na guia Configuração de uma máquina a partir do submenu suspenso expansível Configuração.

Se você clicar na seta à esquerda do menu Máquinas protegidas, será exibida a lista de contratos de máquinas protegidas e clusters do servidor, e não a de máquinas. Clicar novamente nessa seta faz com que a lista de máquinas seja expandida novamente.

Clique em qualquer máquina do menu Máquinas protegidas para abrir a guia Resumo dessa máquina. Para obter mais informações sobre o que você pode realizar na guia Resumo, consulte Visualizar a guia Resumo.

Finalmente, clique diretamente no menu Máquinas protegidas para mostrar a guia Máquinas ou Máquinas protegidas na área de navegação principal, substituindo as guias Início, Replicação, Standby virtual, Eventos, Ferramentas e Configuração.

NOTA: Da guia Máquinas, é possível voltar à visualização de várias guias clicando no ícone Início na barra de ícones da área de navegação à esquerda.

Na guia Máquinas, no menu Ações, é possível proteger uma, duas ou mais máquinas ao mesmo tempo (proteção em massa), ou proteger um cluster. É possível implementar o software do Agent a uma ou múltiplas máquinas (implementação em massa) ou iniciar o assistente de Restauração de máquinas.

Ao selecionar qualquer máquina protegida, é possível, a partir do menu de configurações específico dela, forçar um snapshot, forçar o truncamento de arquivos de log de SQL, exportar para uma máquina virtual, montar um ponto de recuperação, visualizar pontos de recuperação para essa máquina, restaurar a máquina selecionada ou remover a proteção da máquina selecionada.

Visualizar a guia Máquinas de uma máquina protegida

A guia Máquinas aparece como a única guia no AppAssure Core Console quando você clica diretamente no menu Máquinas protegidas. Ela contém um painel Máquinas protegidas.

Se o seu Core replica alguma máquina de outro AppAssure Core, a guia Máquinas contém um painel Máquinas replicadas.

Visualizar o painel Máquinas protegidas

O painel Máquinas protegidas contém informações sobre todas as máquinas protegidas neste AppAssure Core. Para cada máquina protegida (se houver alguma), são fornecidas na grade as informações descritas na tabela a seguir.

Tabela 13. Informações sobre cada máquina protegida

Elemento de UI	Descrição
Indicador de status	Círculos coloridos na coluna Status mostram se uma máquina está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (online e protegida), amarelo (proteção em pausa), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome de exibição	O nome de exibição da máquina protegida.
Status da criptografia	O ícone de cadeado indica o status de criptografia da máquina de agente selecionada. Um cadeado aberto indica que não há criptografia; um cadeado fechado indica que chaves de criptografia foram estabelecidas. Clique no cadeado para configurar a criptografia. Para obter mais informações sobre criptografia, consulte Noções básicas sobre chaves de criptografia.
Versão	A versão do software AppAssure Agent carregada na máquina.
Snapshot	O próximo snapshot programado para essa máquina protegida. Se a proteção estiver em pausa, esse status será indicado.

Se alguma das máquinas protegidas nesse Core estiver configurada para standby virtual, outras informações aparecerão, conforme descrito na tabela a seguir.

Tabela 14. Informações sobre máquinas protegidas configuradas para standby virtual

Elemento de UI	Descrição
Última exportação	Data e hora da última exportação virtual.
Destino	O destino para salvar a máquina protegida como uma máquina virtual. Por exemplo, ESXi, VMware Workstation, Hyper-V ou VirtualBox.
Status	Status da máquina configurado para standby virtual. As condições de status incluem "Sincronizado", “Em pausa" e "Não ativado".

No menu suspenso Ações do painel Máquinas protegidas, é possível realizar as ações descritas na tabela a seguir.

Tabela 15. Ações disponíveis no painel Máquinas protegidas

Elemento de UI	Descrição
Proteger máquina	Inicia o assistente de proteção de máquina. Esse assistente permite proteger uma única máquina no AppAssure Core. Ao usar opções avançadas, você também pode definir um repositório no AppAssure Core e estabelecer criptografia para os dados de agente protegidos. Para obter mais informações, consulte Proteger uma máquina.
Proteger cluster	Abre a caixa de diálogo Conectar ao cluster, que permite conectar a um cluster do servidor para especificar que seja protegido no AppAssure Core. Para obter mais informações, consulte Proteger um cluster.
Proteção em massa	Inicia o assistente de proteção de diversas máquinas. Esse assistente permite estabelecer a proteção de duas ou mais máquinas no AppAssure Core simultaneamente por meio da conexão a um servidor Active Directory ou (no caso de máquinas virtuais) a um host vCenter ou ESXi. Para obter mais informações, consulte Proteger várias máquinas.
Implantar Agent	Abre a caixa de diálogo Implantar Agent, que permite implantar o software AppAssure Agent em uma única máquina específica e configurar as definições de proteção dessa máquina de agente. Para obter mais informações, consulte Implantação do Agent (instalação por push).
Implantação em massa	Permite implantar o software Agent mais recente disponível no Core em várias máquinas simultaneamente. Abre o painel Implantar Agent nas máquinas (acessível selecionando Implantação em massa no menu Ferramentas). Há várias opções de implantação em massa: • Conectar a um server Active Directory • Conectar a um host virtual vCenter ou ESXi. • Especificando o Core local, você pode implementar o software Agent mais recente nas máquinas atualmente protegidas por esse Core. • Inserir uma lista de máquinas manualmente (incluindo o nome de host ou endereço IP, credenciais de login e porta). • Definir uma nova máquina individual para conexão e proteção. Para obter mais informações, consulte Implantar em várias máquinas.
Restaurar	Inicia o assistente Restaurar máquina. Esse processo permite restaurar dados de um ponto de recuperação no Core para uma máquina protegida. Para obter mais informações, consulte Restaurar volumes a partir de um ponto de recuperação.

Você pode realizar ações em duas ou mais das máquinas relacionadas na grade de máquinas protegidas. Para realizar ações em várias máquinas, marque a caixa de seleção de cada máquina protegida e, no menu suspenso Ações expandido, execute qualquer das ações descritas na tabela a seguir.

Tabela 16. Ações adicionais disponíveis no painel Máquinas protegidas quando há máquinas selecionadas

Elemento de UI	Descrição
Proteção > Pausar ou Retomar	Permite pausar a proteção das máquinas selecionadas (se a proteção estiver ativa) ou retomar a proteção das máquinas selecionadas (se a proteção estiver em pausa). Para obter mais informações, consulte Pausar e retomar a proteção.
Forçar snapshot	Permite forçar um snapshot incremental ou uma imagem de base de todos os volumes protegidos nas máquinas de agente selecionadas. Para obter mais informações, consulte Forçar um snapshot.
Replicação	Permite ativar, forçar, copiar, pausar ou retomar uma replicação. Para obter mais informações, consulte Gerenciar definições de replicação.
Remover máquinas	Remove a máquina selecionada da proteção no AppAssure Core, permitindo que você opte por excluir ou reter os pontos de recuperação que já estão no AppAssure Core. Para obter mais informações, consulte Remover uma máquina.
Cancelar	Permite cancelar todas as operações ativas referentes às máquinas selecionadas ou apenas os snapshots que estão sendo realizados nas máquinas selecionadas. Isso não afeta as operações programadas para o futuro.

No menu suspenso Configuração de cada máquina protegida, é possível realizar as ações relacionadas na tabela a seguir. Algumas opções aparecem apenas para servidor Exchange ou SQL Server, conforme indicado.

Tabela 17. Ações disponíveis no painel Máquinas protegidas

Elemento de UI	Descrição
Forçar snapshot	Permite forçar um snapshot incremental ou uma imagem de base de um ou mais volumes na máquina selecionada. Para obter mais informações, consulte Forçar um snapshot.
Forçar truncamento de log para Exchange	No caso de uma máquina de agente do Exchange Server, força o truncamento dos logs do Exchange, liberando espaço no servidor. Para obter mais informações, consulte Forçar truncamento de log para uma máquina SQL.
Forçar truncamento de log para SQL	No caso de uma máquina agente do SQL Server, força o truncamento dos logs do SQL Server, o que identifica espaço livre no servidor. Para obter mais informações, consulte Forçar truncamento de log para uma máquina SQL.
Exportar	Inicia o assistente Exportar. Esse assistente permite exportar dados do ponto de recuperação de uma máquina protegida para uma máquina virtual em qualquer formato de VM suportado. É possível realizar uma exportação única ou configurar um standby virtual para exportações contínuas. Para obter mais informações, consulte Exportar dados protegidos de máquinas Windows para máquinas virtuais.
Montagem	Abre a caixa de diálogo Montar ponto de recuperação, que permite procurar dados de snapshot salvos no AppAssure Core para montar um ponto de recuperação específico. Para obter mais informações, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Pontos de recuperação	Abre a guia Pontos de recuperação da máquina de agente selecionada. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.
Restaurar	Inicia o assistente Restaurar máquina. Esse processo permite restaurar dados de um ponto de recuperação no Core para uma máquina protegida. Para obter mais informações, consulte Restaurar volumes a partir de um ponto de recuperação.
Remover máquina	Remove a máquina selecionada da proteção no AppAssure Core, permitindo que você opte por excluir ou reter os pontos de recuperação que já estão no AppAssure Core. Para obter mais informações, consulte Remover uma máquina.

Visualizar o painel Máquinas replicadas

Se alguma das máquinas protegidas nesse Core estiver sendo replicada, o painel Máquinas replicadas aparecerá. Essa seção contém informações sobre todas as máquinas replicadas nesse AppAssure Core, conforme descrito na tabela a seguir.

Tabela 18. Informações sobre máquinas protegidas replicadas

Elemento de UI	Descrição
Indicador de status	Status da replicação. Círculos coloridos na coluna Status mostram se uma máquina replicada está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (replicação estabelecida e online), amarelo (replicação pausada), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome da máquina	O nome de exibição da máquina replicada.
Último snapshot replicado	A data e hora do último snapshot dessa máquina replicada.
Standby virtual	Indica se o Standby virtual foi ativado, o que significa que foram definidos parâmetros de exportação contínua da máquina replicada para uma máquina virtual.
Replicado de	Indica o Core de origem do qual essa máquina protegida está sendo replicada.

No menu suspenso Ações do painel Máquinas replicadas, é possível realizar as ações descritas na tabela a seguir.

Tabela 19. Ações disponíveis no painel Máquinas replicadas

Elemento de UI	Descrição
Exportar	Permite exportar dados da máquina replicada para uma máquina virtual. Para obter mais informações, consulte Gerenciar exportações.
Montagem	Permite montar um ponto de recuperação. Para obter mais informações, consulte Montar um ponto de recuperação.
Pontos de recuperação	Abre uma visualização de todos os pontos de recuperação nessa máquina replicada. Para obter mais informações, consulte Visualizar pontos de recuperação.
Restaurar	Permite restaurar dados de um ponto de recuperação. Para obter mais informações, consulte Restaurar dados de pontos de recuperação.
Excluir	Remove a máquina replicada desse Core.

Você pode realizar ações em duas ou mais das máquinas relacionadas na grade de máquinas replicadas. Para realizar ações em várias máquinas, marque a caixa de seleção de cada máquina protegida e, no menu suspenso Ações expandido, selecione a ação que deseja realizar.

Visualizar a guia Resumo

A guia Resumo é a primeira guia exibida no AppAssure Core Console quando você seleciona uma máquina de agente protegida. Ela contém, no mínimo, um painel de Resumo e um painel de Volumes.

Visualizar o painel Resumo

O painel de Resumo contém informações resumidas sobre a máquina protegida, incluindo o nome do host, a data e a hora do último snapshot, a data e a hora do próximo snapshot agendado, as informações sobre a chave de criptografia, e a versão do software do Agent carregada nessa máquina. Há um menu de Ações descrito abaixo.

Se você tiver um ou mais servers Exchange protegidos, você também verá um painel de Informações do Server Exchange que contém informações sobre seu server Exchange protegido. Se você tiver um ou mais servers SQL protegidos, você também verá um painel de Informações do SQL Server que contém informações sobre seu server SQL protegido.

Para todas as máquinas protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Exportar uma máquina protegida para uma máquina virtual**, usando exportação única ou atualizações contínuas para uma máquina virtual exportada. Para obter mais informações, consulte Exportar dados protegidos de máquinas Windows para máquinas virtuais.
- Pausar proteção para essa máquina. Para obter mais informações, consulte Pausar e retomar a proteção.
- **Atualizar os metadados para essa máquina**. Para atualizar os metadados para uma máquina, no menu suspenso Ações, clique em **Atualizar metadados**.
- **Remover essa máquina da proteção**, escolhendo excluir ou manter os pontos de recuperação. Para obter mais informações, consulte Remover uma máquina.

As opções exibidas no menu suspenso Ações do painel de Resumo podem ser diferentes dependendo do tipo de máquina selecionada. Por exemplo, os SQL Servers incluem uma opção SQL com funções relacionadas no menu Ações. Os Servers Exchange incluem uma opção Exchange no menu de ações.

Para as máquinas do SQL Server protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Forçar truncamento de log.** Para uma máquina do SQL Server, é possível forçar o truncamento dos registros do SQL Server, que identifica espaço livre no server do SQL. Para obter mais informações, consulte Forçar o truncamento de log para uma máquina Exchange.
- **Definir as credenciais do SQL Server.** Para uma máquina do SQL Server, é possível definir credenciais padrão para todas as instâncias, ou definir credenciais da instância para uma instância única. Para obter mais informações, consulte Definir credenciais para uma máquina SQL Server.

Para as máquinas do Exchange Server protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Forçar truncamento de log.** Para uma máquina do Exchange Server, é possível forçar o truncamento dos logs do Exchange, que libera espaço no server do Exchange. Para obter mais informações, consulte Forçar o truncamento de log para uma máquina Exchange.
- **Definir credenciais do Exchange Server.** Para uma máquina do Exchange Server, é possível definir ou modificar as configurações do Exchange Server, incluindo forçar o truncamento dos logs do Exchange Server, ou configurar credenciais para uma instância do server Exchange. Para obter mais informações, consulte Definir credenciais para uma máquina Exchange Server.

Visualizar o painel Volumes

Para qualquer máquina agente, na guia Resumo, no painel Volumes, é possível realizar as seguintes ações para qualquer um dos volumes listados:

- **Definir ou modificar uma programação de proteção para um volume selecionado**. Os cronogramas de proteção são normalmente estabelecidos quando você protege uma máquina primeiro. Para obter mais informações sobre a modificação de uma programação de proteção, consulte Modificar programações de proteção.
- **Forçar uma imagem de base ou snapshot.** Os snapshots ocorrem normalmente dependendo da programação de proteção. Contudo, a qualquer momento, é possível forçar uma imagem de base ou um snapshot incremental para os volumes selecionados. Para obter mais informações, consulte Forçar um snapshot.

Visualizar a guia Pontos de recuperação

A guia Pontos de recuperação mostra uma lista dos pontos de recuperação coletados para essa máquina protegida, além de dados pertinentes sobre a máquina e o repositório. Nessa página, você pode montar, exportar e restaurar pontos de recuperação específicos ou excluir pontos de recuperação.

A guia é dividida em dois painéis: Resumo e Pontos de recuperação. O painel Resumo não contém links de ações. Ele exibe os dados relacionados a seguir sobre a máquina.

Tabela 20. Dados do painel Resumo na guia Ponto de recuperação

Elemento de UI	Descrição
Total de pontos de recuperação	O número de pontos de recuperação coletados para essa máquina protegida específica.
Total de dados protegidos	A quantidade de dados da máquina protegida armazenados no repositório.
Repositório	O nome do repositório no qual o AppAssure armazena os pontos de recuperação dessa máquina protegida.
Status do repositório	A barra de progresso exibe a porcentagem do espaço total usada no repositório. A quantidade de dados usada e o tamanho total do repositório aparecem abaixo da barra de progresso.

O painel Pontos de recuperação fornece uma lista de todos os pontos de recuperação no repositório para essa máquina protegida.

Tabela 21. Opções do painel Pontos de recuperação na guia Ponto de recuperação

Elemento de UI	Descrição
>	Expande o ponto de recuperação para mostrar opções adicionais.
Montagem	Após expandir um ponto de recuperação, essa opção permite montar o ponto de recuperação para poder explorá-lo e recuperar itens individuais. Para obter mais informações, consulte Montar um ponto de recuperação.
Exportar	Após expandir um ponto de recuperação, você pode usar essa opção para exportá-lo para um host virtual compatível e criar uma máquina virtual. Para obter mais informações, consulte Exportar dados protegidos de máquinas Windows para máquinas virtuais.
Restaurar	Após expandir um ponto de recuperação, a opção Restaurar permite restaurar um ou mais volumes no ponto de recuperação para o local desejado. Para obter mais informações, consulte Restaurar dados ou Realizar uma bare metal restore em máquinas Windows, ou, para restaurar dados em uma máquina Linux, consulte Realizar uma bare metal restore em máquinas Linux.
Status	Exibe um círculo colorido que indica o estado das verificações realizadas no ponto de recuperação. Para obter mais informações, consulte
Conteúdo	Relaciona os volumes e partições incluídos no ponto de recuperação.
Tipo	Indica se o ponto de recuperação é um snapshot de base ou incremental.
Data de criação	A data e hora em que o AppAssure criou o ponto de recuperação.
Tamanho	O tamanho do ponto de recuperação em bytes.
Ações	O menu suspenso Ações oferece as seguintes opções para remover pontos de recuperação da máquina: • **Excluir intervalo.** Exclui o intervalo selecionado de pontos de recuperação. • **Excluir tudo.** Exclui todos os pontos de recuperação coletados para essa máquina protegida. Quando você exclui todos os pontos de recuperação, não há mais pontos disponíveis para realizar uma restauração. Para obter mais informações, consulte Remover pontos de recuperação.

Visualizar a guia Eventos de uma máquina protegida

Na guia Eventos, você pode visualizar os trabalhos que ocorreram ou que estão em progresso na máquina protegida selecionada. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que o AppAssure precisa realizar para operar com êxito.
- **Alertas.** Uma notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Eventos.** Uma combinação de todas as tarefas e alertas de máquinas protegidas.

A tabela a seguir contém descrições de cada elemento da guia Eventos.

Tabela 22. Elementos da guia Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa.
Ícones de status	Cada ícone representa um status diferente do trabalho. Quando você clica em um dos ícones, a lista é filtrada por esse status, gerando um relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.** Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.** Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Noções básicas sobre replicação.) • **Concluído.** Um trabalho que foi concluído com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status. Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Ela inclui os seguintes formatos: • PDF • XLS • XLSX • RTF • CSV
Ícone Exportar	Converte o relatório de eventos para o formato selecionado.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e setas na parte inferior da guia Eventos permitem navegar pelas páginas adicionais do relatório.

A guia Eventos exibe todos os eventos em uma tabela. A tabela inclui as seguintes informações sobre cada item.

Tabela 23. Informações da tabela da guia Eventos

Elemento de UI	Descrição
>	O colchete expande o trabalho para revelar os seguintes detalhes: • **Hora inicial.** Quando o trabalho começou. • **Hora de término.** Quando o trabalho terminou. • **Tempo decorrido.** O período de tempo durante o qual o trabalho esteve ativo. • **Taxa.** A taxa em que o Core transfere os dados. • **Progresso.** Quando um trabalho está em progresso, mostra em tempo real a proporção concluída pelo Core. Quando o trabalho está concluído, mostra o quanto do trabalho o Core concluiu. • **Fase.** Quando um trabalho está em progresso, esse detalhe mostra qual é o estágio atual de progresso (por exemplo, Transferindo). • **Cancelar.** Quando um trabalho está em progresso, um link aqui permite cancelá-lo. • **Trabalho total.** Quando um trabalho está concluído, mostra o quanto do trabalho o Core concluiu. • **Tarefa subordinada.** Mostra as subtarefas associadas a esse trabalho.
Trabalho	O tipo de trabalho que o Core realizou, como transferência de volumes, manutenção de repositório ou rollup em execução.
Status	O status do trabalho, como Bem-sucedido no caso de um trabalho concluído com êxito ou Erro no caso de um trabalho que falhou devido a erros.
Hora inicial	O dia e hora em que o trabalho foi iniciado.
Hora final	O dia e hora em que o trabalho terminou.
Detalhes	Abre a janela Monitorar tarefa ativa. Inclui os detalhes exibidos quando você expande o trabalho, além dos seguintes detalhes sobre trabalhos subordinados: • Hora inicial • Hora final • Tempo decorrido • Taxa • Progresso • Trabalho total

Visualizar a guia Ferramentas de uma máquina protegida

Por padrão, a guia Ferramentas mostra informações da máquina e permite acessar ferramentas que ajudam a gerenciar essa máquina específica. Para acessar essas ferramentas, selecione uma opção no menu Ferramentas à esquerda ou no menu suspenso da guia Ferramentas. Essas ferramentas são descritas na tabela a seguir.

Tabela 24. Informações sobre as ferramentas acessíveis a uma máquina protegida

Elemento de UI	Descrição
Informações do sistema	Mostra informações sobre a máquina protegida, informações do sistema, volumes, processadores, adaptadores de rede e endereços IP referentes a essa máquina. Para obter mais informações, consulte Visualizar informações do sistema de uma máquina.

Tabela 24. Informações sobre as ferramentas acessíveis a uma máquina protegida

Elemento de UI	Descrição
Montagens	No painel Montagens locais, você pode visualizar ou desmontar volumes montados localmente. No painel Montagens remotas, você pode visualizar ou desmontar volumes montados usando o Local Mount Utility. Para obter informações sobre a desmontagem de volumes, consulte Desmontar pontos de recuperação. Para obter mais informações sobre a montagem local de um ponto de recuperação, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Diagnóstico	A página Diagnóstico é para sua conveniência, caso você encontre um problema para o qual queira solicitar assistência do Suporte do AppAssure. Aqui você pode usar a opção de menu Visualizar log para baixar o log dessa máquina protegida. Para obter mais informações, consulte Acessar o diagnóstico de máquinas protegidas.
Relatórios	A página Relatórios permite gerar relatórios de atividades para essa máquina protegida e exportá-los em diversos formatos. As opções de relatórios são: • **Conformidade.** Fornece o status de trabalhos realizados para essa máquina. • **Falha.** Um subconjunto do relatório Conformidade que mostra apenas os trabalhos com falha associados a essa máquina. Para obter mais informações, consulte Gerar e visualizar relatórios.

Visualizar a guia Configuração de uma máquina protegida

A guia Configuração de uma máquina protegida (agente) mostra definições e opções de configuração que permitem ajustar e personalizar a proteção da máquina selecionada. Para acessar essas definições, selecione uma opção no menu da página Configuração ou no menu suspenso da guia Configuração. Essas opções são descritas na tabela a seguir.

Tabela 25. Opções da guia Configuração

Elemento de UI	Descrição
Definições	As opções disponíveis na página Definições da guia Configuração se aplicam ao Core e a todas as suas máquinas protegidas. Isso inclui a capacidade de modificar definições nas seguintes categorias: • **Definições.** As definições incluem nome de exibição, nome de host, porta, chave de criptografia (se for o caso) e repositório atribuído à máquina protegida. Para obter mais informações, consulte Visualizar e modificar as definições de configuração. • **Trabalhos noturnos.** Trabalhos noturnos são tarefas regulares de manutenção programadas para horários fora do expediente para não causar interrupções nos horários de trabalho mais intenso. Incluem tarefas como download de logs de máquinas protegidas, o trabalho de verificação de capacidade de anexação, rollup e truncamento de log. Para obter mais informações, consulte Personalizar trabalhos noturnos para uma máquina protegida.
Eventos	Na página Eventos da guia Configuração da máquina, você pode criar grupos de notificação personalizados para esse agente. Para obter mais informações, consulte Configurar grupos de notificação para eventos do sistema.
Política de retenção	Na guia Política de retenção, você pode optar entre usar a política de retenção padrão determinada pelo Core ou criar e usar uma política de retenção personalizada para esse agente. Para obter mais informações sobre políticas de retenção personalizadas, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Tabela 25. Opções da guia Configuração

Elemento de UI	Descrição
Aplicação de licença	Na página Aplicação de licença, você pode visualizar a data de expiração, status e tipo da licença e o tipo do agente (virtual ou físico). Para obter mais informações, consulte Gerenciar licenças.
Definições de transferência	A página Definições de transferência permite gerenciar os dados transferidos entre o Core e o agente. Você pode definir a prioridade, o número máximo de gravações simultâneas, o tempo limite de transferência, o tempo limite de snapshot e outros parâmetros para determinar a ordem de transferência dos tipos de dados, a quantidade de dados transferidos simultaneamente e por quanto tempo o Core deve tentar fazer uma transferência antes de parar e passar para o próximo trabalho de transferência na fila. Para obter mais informações, consulte Modificar definições de transferência.

Visualizar o painel Máquinas replicadas

Na interface de usuário do AppAssure, um menu Máquinas replicadas aparece na área de navegação esquerda. Por padrão, esse menu está totalmente expandido e mostra uma lista de máquinas replicadas por esse Core.

Para expandir ou retrair a exibição de máquinas replicadas, clique na seta no lado esquerdo desse menu.

O menu Máquinas replicadas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas replicadas. Clique na seta à direita de Máquinas replicadas para ver o menu e executar qualquer das seguintes ações:

- Forçar replicação. Para obter mais informações, consulte Forçar a replicação.
- Retomar replicação (se a replicação estiver em pausa). Para obter mais informações, consulte Pausar e retomar a replicação.
- Pausar replicação (se a replicação estiver ativa). Para obter mais informações, consulte Pausar e retomar a replicação.

Visualizar o menu Apenas pontos de recuperação

O menu Apenas pontos de recuperação aparecerá na área de navegação esquerda se o AppAssure Core retiver alguns pontos de recuperação de uma máquina que foi protegida anteriormente.

Para expandir ou retrair a exibição de máquinas apenas com pontos de recuperação, clique na seta à esquerda desse menu.

O menu inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas apenas com ponto de recuperação. Nesse caso, a única função que você pode realizar é remover os pontos de recuperação do Core.

△ **CUIDADO: Essa ação remove todas as máquinas apenas com pontos de recuperação no AppAssure Core, excluindo-as permanentemente e impedindo a restauração das informações desses pontos de recuperação a partir desse Core.**

Visualizar o menu Grupos personalizados

O menu Grupos personalizados aparecerá na área de navegação esquerda apenas se você tiver definido um ou mais grupos personalizados.

Para expandir ou retrair a exibição dos itens desse menu, clique na seta à sua esquerda.

O menu Grupos personalizados inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todos os itens semelhantes desse grupo.

Para obter mais informações, consulte Noções básicas sobre grupos personalizados.

3

Configurar o AppAssure Core

Este capítulo descreve como configurar o Core no ambiente do AppAssure como preparação para o uso inicial, incluindo o gerenciamento de licenças e repositórios. Este capítulo também descreve como visualizar informações no Core com base na configuração específica (por exemplo, com grupos personalizados) e como fazer cópia de segurança e restaurar as definições de configuração do Core. Ele inclui as seguintes seções:

- Gerenciar licenças
- Noções básicas sobre repositórios
- Gerenciar um repositório
- Sobre o trabalho de verificação de integridade do repositório
- Noções básicas sobre grupos personalizados

Para usar o AppAssure, é necessário configurar o AppAssure Core. A configuração inicial do AppAssure Core requer a compreensão de alguns conceitos e a realização de algumas operações iniciais. No mínimo, isso inclui:

- **Gerenciar sua licença.** O Core exige uma chave ou arquivo de licença que se comunica com o Portal de licenças do Dell AppAssure. Para mais informações sobre como gerenciar sua licença no AppAssure Core, consulte Gerenciar licenças. Para obter mais informações, consulte o *Guia do portal de licenças do Dell AppAssure*.
- **Criar e gerenciar seu repositório.** O AppAssure Core usa um repositório para armazenar dados, o que inclui a definição de locais de armazenamento, que são os volumes em que os dados de cópia de segurança serão armazenados.
    - Para obter mais informações sobre repositórios, consulte Noções básicas sobre repositórios.
    - Para instruções sobre gerenciamento de repositórios, consulte Gerenciar um repositório.
    - Se você usar replicação, quiser ter políticas de retenção diferentes nos Cores de origem e de destino e tiver atualizado o Core de destino a partir de uma versão anterior à 5.3.6, será necessário executar um trabalho de verificação de integridade. Para obter mais informações, consulte Sobre o trabalho de verificação de integridade do repositório.

Opcionalmente, você também pode configurar um grupo de objetos personalizado disponível no Core. Esse grupo, que aparece no menu Máquinas protegidas, pode ser heterogêneo e incluir uma ou mais máquinas protegidas, máquinas replicadas ou clusters do servidor, em qualquer combinação. Se usar um grupo personalizado, você poderá executar ações de grupo que se aplicam a todos os membros desse grupo, conforme descrito em Realizar ações de grupo. Para obter mais informações sobre grupos personalizados, consulte Noções básicas sobre grupos personalizados.

Outras tarefas de configuração podem ser necessárias, dependendo dos seus requisitos de negócios. Por exemplo:

- **Configurar chaves de criptografia**. O AppAssure Core pode criptografar dados de snapshot de agente dentro do repositório usando chaves de criptografia. Para obter mais informações sobre a proteção dos dados por meio da configuração de chaves de criptografia, consulte Noções básicas sobre chaves de criptografia.
- **Configurar notificação de eventos**. O AppAssure Core pode enviar notificações sobre conjuntos de eventos específicos predefinidos usando vários métodos configuráveis. Para obter mais informações sobre a configuração de notificação de eventos, consulte Gerenciar eventos. Para incluir e-mail como um dos métodos de notificação, é preciso configurar um servidor de e-mail no AppAssure Core. Para obter mais informações, consulte Configurar um servidor de e-mail.

Você pode configurar seu repositório, definir a notificação de eventos e definir chaves de criptografia individualmente ou usar o Guia de Início Rápido para ser conduzido através dos processos de configuração do Core. O Guia de início rápido permite iniciar assistentes e etapas de configuração, ou apenas ver o fluxo recomendado de realização das tarefas de configuração.

Se o Guia de início rápido for usado na configuração, proteja primeiro a máquina usando o Assistente de proteção de máquina. Durante essa etapa, é solicitada a definição dos locais de armazenamento, incluindo a criação e o dimensionamento de um repositório. Esse guia também permitirá configurar a notificação de eventos, configurar chaves de criptografia, configurar a replicação, exportar para uma máquina virtual e visualizar ou alterar sua política de retenção. Se você tiver pontos de recuperação no Core, este guia permitirá a restauração de dados. Para obter mais informações sobre o Guia de Início Rápido, incluindo como iniciar ou ocultar esse recurso, consulte Noções básicas sobre o Guia de início rápido.

Ao realizar tarefas de configuração individualmente, será preciso executar certas tarefas de configuração iniciais, como criar e configurar o repositório para armazenar snapshots de cópia de segurança; opcionalmente, definir chaves de criptografia para manter os dados protegidos; e, opcionalmente, configurar notificações para tarefas, alertas e eventos. Depois de concluir a configuração inicial do AppAssure Core, você pode proteger uma ou mais máquinas de agente e realizar atividades de recuperação. O AppAssure inclui uma política de retenção padrão, que você talvez queira configurar de acordo com seus requisitos personalizados. Ao proteger bancos de dados SQL, é possível configurar a capacidade de anexação do SQL. Você também pode criar grupos personalizados.

A configuração adicional do AppAssure Core inclui as seguintes operações:

- **Proteger uma única máquina agente.** Para obter mais informações sobre como proteger uma máquina agente usando o Assistente de proteção de máquina, consulte Proteger uma máquina.
- **Proteger várias máquinas agente.** Para obter mais informações sobre como proteger várias máquinas agente em uma etapa usando o Assistente de proteção de máquina, consulte Proteger várias máquinas.
- **Restaurar dados de pontos de recuperação.** Para obter mais informações sobre a restauração de dados de pontos de recuperação usando o Assistente de restauração, consulte Restaurar dados de pontos de recuperação.
- **Configurar a política de retenção**. Para obter mais informações sobre a configuração de políticas de retenção, consulte Gerenciar políticas de retenção.
- **Configurar a capacidade de anexação do SQL**. Para obter mais informações sobre a configuração da capacidade de anexação do SQL, consulte Configurar as definições de capacidade de anexação do SQL.

Noções básicas sobre repositórios

Um repositório é usado para armazenar os snapshots capturados a partir de suas estações de trabalho e servers protegidos. O repositório pode residir em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

Ao criar um repositório, o AppAssure Core pré-aloca o espaço de armazenamento necessário para os dados e metadados no local especificado. É possível criar até 255 repositórios independentes em um único core, que abrangem diferentes tecnologias de armazenamento. Além disso, é possível aumentar o tamanho de um repositório adicionando novas extensões ou especificações de arquivo. Um repositório estendido pode conter até 4096 extensões que abrangem diversas tecnologias de armazenamento.

Os principais conceitos e considerações sobre repositórios incluem:

- O repositório se baseia no Sistema de arquivos de objeto escalável do AppAssure.
- Todos os dados armazenados dentro de um repositório são globalmente deduplicados.
- O Sistema de arquivos de objeto escalável proporciona um desempenho de I/O escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção.

NOTA: Os repositórios do AppAssure devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

Gerenciar um repositório

Antes de poder usar o AppAssure, é preciso configurar um ou mais repositórios no server do AppAssure Core. Um repositório armazena seus dados protegidos. Mais especificamente, armazena os snapshots capturados de seus servers protegidos no seu ambiente.

Quando você configura um repositório, pode executar uma variedade de tarefas, como especificar onde localizar o armazenamento de dados no server do Core, quantas localizações devem ser adicionadas a cada repositório, o nome do repositório, quantas operações atuais os repositórios suportam, e assim por diante.

Ao criar um repositório, o Core pré-aloca o espaço necessário para armazenar os dados e metadados no local especificado. É possível criar até 255 repositórios independentes em um único core. Para aumentar ainda mais o tamanho de um único repositório, é possível adicionar novos locais de armazenamento ou volumes.

Gerenciar um repositório envolve a criação, configuração e visualização de um repositório, e inclui as seguintes operações:

- **Acessar o Core Console.** Para obter mais informações sobre como acessar o AppAssure Core Console, consulte Noções básicas sobre o AppAssure Core Console.
- **Criar um repositório.** Para obter mais informações sobre a criação de um repositório, consulte Criar um repositório.
- **Visualizar detalhes de repositório.** Para obter mais informações sobre a visualização de detalhes de repositórios, consulte Visualizar detalhes de um repositório.
- **Modificar definições de repositório.** Para obter mais informações sobre a modificação de definições de repositório, consulte Modificar definições de repositório.
- **Adicionar um novo local de armazenamento.** Para obter mais informações sobre adicionar um novo local de armazenamento, consulte Adicionar um local de armazenamento a um repositório existente.
- **Verificar um repositório.** Para obter mais informações sobre a verificação de repositórios, consulte Verificar um repositório.
- **Excluir um repositório.** Para obter mais informações sobre a exclusão de repositórios, consulte Excluir um repositório.

Criar um repositório

Execute as seguintes etapas para criar um repositório.

Para criar um repositório

1 No AppAssure Core Console, realize um dos seguintes:

- Na página Inicial, no painel de Repositórios clique em **Adicionar novo repositório**.
- Clique na guia Configuração e, na página Repositórios, clique em **Adicionar novo**.

A caixa de diálogo Adicionar novo repositório é exibida.

2 Insira as informações conforme descrito na tabela a seguir.

Tabela 26. Definições de Adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra *Repositório* e um número de índice, que corresponde ao número do novo repositório. Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres.
Operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte. Por padrão, o valor é *64*.
Comentários	Como opção, insira uma nota descritiva sobre esse repositório. É possível digitar até 254 caracteres.

3 Clique em **Adicionar local de armazenamento** para definir o local de armazenamento ou o volume específico do repositório.

AVISO: Se o repositório do AppAssure que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você não definir uma pasta dedicada para armazenar os arquivos do repositório, os arquivos serão armazenados na raiz; excluir o repositório também excluirá todo o conteúdo da raiz, resultando em perda de dados catastrófica.

NOTA: Os repositórios do AppAssure devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

A caixa de diálogo Adicionar local de armazenamento é exibida.

4 Na área Local de armazenamento, especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.

- Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 27. Definições de disco local

Caixa de texto	Descrição
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite: `X:\Repository\Data`. As mesmas limitações do caminho se aplicam; use somente caracteres alfanuméricos, hífen ou ponto, sem espaços ou caracteres especiais.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite: `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 28. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

5 Na área Configuração de armazenamento, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 29. Detalhes do local de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O padrão é 250 MB. Você pode selecionar dentre os seguintes: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB. **NOTA:** Para que o AppAssure valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Tabela 29. Detalhes do local de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.

6 Clique em **Salvar**.

A tela Repositórios é exibida para incluir o local de armazenamento recém-adicionado.

7 Como opção, repita da Etapa 3 à Etapa 6 para adicionar outros locais de armazenamento ao repositório.

8 Clique em **Criar** para criar o repositório.

O repositório é exibido na guia Configuração.

Visualizar detalhes de um repositório

Execute as seguintes etapas para visualizar os detalhes de um repositório.

Para visualizar detalhes de um repositório

1 No AppAssure Core Console, clique na guia Configuração.

A página Repositórios é exibida.

2 Clique no símbolo de maior que (>) ao lado da coluna Status do repositório cujos detalhes você deseja visualizar.

3 No ícone Definições ao lado da coluna Taxa de compressão, é possível realizar as seguintes ações em um repositório:

- Modificar definições
- Adicionar um local de armazenamento
- Verificar o repositório
- Excluir o repositório

4 Os detalhes exibidos do repositório também incluem os locais de armazenamento e as estatísticas. Os detalhes do local de armazenamento incluem:

- Caminho de metadados
- Caminho de dados
- Tamanho

As informações estatísticas disponíveis para visualização incluem:

- Deduplicação
- I/O de registro
- Mecanismo de armazenamento

O nível de detalhes disponíveis para deduplicação é relatado como o número de ocorrências de deduplicação de bloco, erros de deduplicação de bloco e taxa de compressão de bloco.

Os detalhes renderizados para o I/O de registro consistem na taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

Os detalhes do mecanismo de armazenamento incluem a taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

Modificar definições de repositório

Depois de adicionar um repositório, você pode modificar as definições dele, como a descrição ou o máximo de operações simultâneas. Também é possível adicionar um novo local de armazenamento para o repositório. Para obter mais informações sobre adicionar um novo local de armazenamento, consulte Adicionar um local de armazenamento a um repositório existente.

Para modificar as definições de repositório

1 No AppAssure Core Console, clique na guia Configuração.

A página Repositórios é exibida.

2 Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Definições**.

A caixa de diálogo Definições do repositório é exibida.

3 Edite as informações de repositório conforme descrito na tabela a seguir.

Tabela 30. Informações do repositório

Caixa de texto	Descrição
Nome do repositório	Representa o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número de índice, que corresponde ao número do repositório. NOTA: Não é possível editar o nome do repositório.
Descrição	Como opção, insira uma nota descritiva sobre o repositório.
Máximo de operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte.
Ativar deduplicação	Desmarque essa caixa de seleção para desativar a deduplicação ou marque-a para ativar a deduplicação. NOTA: Alterar essa definição se aplica apenas a cópias de segurança feitas após a definição ser feita. Os dados existentes ou replicados de outro core ou importados de um arquivo manterão no lugar os valores de deduplicação no momento em que os dados forem capturados de um agente.
Ativar compressão	Desmarque essa caixa de seleção para desativar a compressão ou marque-a para ativar a compressão. NOTA: Essa definição se aplica apenas a cópias de segurança feitas após a definição ser alterada. Os dados existentes ou replicados de outro core ou importados de um arquivo manterão no lugar os valores de compressão no momento em que os dados forem capturados de um agente.

4 Clique em **Salvar**.

Abrir um repositório existente

Execute o procedimento a seguir para abrir um repositório existente.

Para abrir um repositório existente

1 No AppAssure Core Console, clique na guia Configuração.

2 Na página Repositórios da guia Configuração, clique em **Abrir existente**.

3 Na caixa de diálogo, insira as seguintes informações sobre o repositório que deseja abrir:

- Caminho. O caminho do repositório (por exemplo, D:\work\machine no caso de um caminho local, ou \\servername\sharename no caso de um caminho de rede).

- Nome de usuário. Se o repositório tiver um caminho de rede, insira o nome de usuário para efetuar login no compartilhamento de rede.
- Senha. Se o repositório tiver um caminho de rede, insira a senha para efetuar login no compartilhamento de rede.

4 Clique em **Abrir**.

Adicionar um local de armazenamento a um repositório existente

Adicionar um local de armazenamento permite definir onde você deseja que o repositório ou o volume seja armazenado. Execute as etapas do procedimento a seguir para especificar o local de armazenamento do repositório ou do volume.

Para adicionar um local de armazenamento a um repositório existente

1 Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Adicionar local de armazenamento**.

A caixa de diálogo Adicionar local de armazenamento é exibida.

2 Especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.

- Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 31. Definições de disco local

Caixa de texto	Descrição
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite: `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite: `X:\Repository\Data`. As mesmas limitações do caminho se aplicam; use somente caracteres alfanuméricos, hífen ou ponto, sem espaços ou caracteres especiais.

- Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 32. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

3 No painel Configuração de armazenamento, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 33. Detalhes do local de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho padrão é de 250 MB. Você pode selecionar dentre os seguintes: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB. **NOTA:** Para que o AppAssure valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.

4 Clique em **Salvar**.

A tela Repositórios é exibida para incluir o local de armazenamento recém-adicionado.

5 Como opção, repita da Etapa 3 à Etapa 6 para adicionar outros locais de armazenamento ao repositório.

6 Clique em **OK**.

Verificar um repositório

O AppAssure fornece a capacidade de realizar uma verificação de diagnóstico de um volume de repositório quando ocorrem erros. Os erros no Core podem resultar de desligamento incorreto, falha de hardware ou outros fatores ambientais de pilha de IP inferior, que podem ser expostos na funcionalidade do AppAssure.

NOTA: Este procedimento deve ser realizado apenas para fins de diagnóstico, por exemplo, em caso de falha de hardware, desligamento incorreto do Core, falha ao importar o repositório, e assim por diante.

Para verificar um repositório

1. Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Verificar**.

   A caixa de diálogo Verificar repositório é exibida.

2. Na caixa de diálogo Verificar repositório, clique em **Verificar**.

   NOTA: Ao executar uma verificação, todas as tarefas ativas associadas a esse repositório serão canceladas. Antes de a verificação começar, será exibida uma mensagem pedindo que você confirme que deseja prosseguir com a verificação. Aconselhamos e incentivamos a reconstruir o cache dos pontos de recuperação nesse ponto para atualizá-lo, visto que a falha de uma verificação resultará em você ter de restaurar o repositório a partir de um arquivo.

Excluir um repositório

Execute as etapas deste procedimento para excluir um repositório.

Para excluir um repositório

1. Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Excluir**.
2. Na caixa de diálogo Excluir repositório, clique em **Excluir**.

   Aparece uma mensagem de aviso pedindo para confirmar a exclusão.
3. Clique em **Sim** para confirmar a exclusão do repositório.

CUIDADO: Quando um repositório é excluído, os dados contidos nele são descartados e não podem ser recuperados.

Sobre o trabalho de verificação de integridade do repositório

Nas versões anteriores, a replicação incluía o processo de copiar pontos de recuperação do core de destino para o core de origem regularmente. O rollup dos pontos de recuperação do envelhecimento ocorreram somente no core de origem. Os pontos de recuperação mais antigos combinados foram sincronizados diariamente durante a execução do trabalho noturno.

A partir da versão 5.4.1, o AppAssure inclui a capacidade de definir políticas de retenção discrepantes entre os Cores de destino e de origem, contanto que os Cores de destino e de origem tenham a mesma versão (5.4.1 ou posterior). Isso permite que os administradores do AppAssure configurem o rollup em um Core de destino a uma taxa diferente (presumivelmente mais rápida) que no Core de origem. Da mesma forma, é possível definir uma política de retenção personalizada para qualquer agente replicado, fazer o rollup dos pontos de recuperação a uma taxa mais rápida e com menos granularidade no core de destino do que no core de origem, poupando espaço. Para obter mais informações, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Alguns clientes observaram inconsistências em pontos de recuperação que foram replicados para um Core de destino anterior ao AppAssure versão 5.3.6. Para solucionar deste problema, o AppAssure versão 5.4.1 e posterior inclui um novo trabalho de verificação de integridade que deve ser executado em cada repositório para que seja possível configurar políticas de retenção diferentes entre o Core de origem e um Core de destino ou configurar uma política de retenção personalizada em um agente replicado.

Quando o trabalho de confirmação de integridade é executado, o sistema confirma a integridade de todos os dados armazenados no repositório especificados, garantindo que seja possível recuperar os dados de cada Snapshot ou imagem de base. Se a verificação de integridade detectar algum problema com os dados em seu repositório, o trabalho para imediatamente. Os detalhes do evento para aquele trabalho no core solicitam que você entre em contato com o suporte do Dell AppAssure, de forma que é possível marcar o horário para trabalhar com um representante da Dell a fim realizar procedimentos adicionais de identificação e correção de inconsistências de dados.

CUIDADO: É previsto que a execução deste trabalho leve um período de tempo prolongado com base nos dados de seu repositório e no sistema de armazenamento subjacente. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.

É possível executar outras operações em outros repositórios enquanto o trabalho de verificação de integridade está em execução.

NOTA: Este trabalho verifica a integridade de *todo o conteúdo* dentro do repositório. Para obter informações sobre o trabalho de verificação do repositório, que pode ser usado para verificar a fim de garantir que um repositório está em condições de ser montado e usado, consulte Verificar um repositório.

Este é um trabalho ad hoc disponível para ser executado em cada repositório. A Dell recomenda a realização do trabalho de verificação da integridade uma única vez em cada repositório em um core de destino replicado no caso da atualização da versão 5.3.x.

Você *não* precisa executar este trabalho:

- Em um novo repositório em um core de destino criado na versão 5.4.1 ou posterior.
- Em um core de origem.
- Se você já tiver executado o trabalho de verificação de integridade neste repositório.
- Se você não tiver usado a replicação.

Para obter instruções sobre como executar esta verificação, consulte o procedimento Executar o trabalho de verificação de integridade em um repositório.

Executar o trabalho de verificação de integridade em um repositório

Execute este procedimento para verificar a integridade de todo o repositório. Ele é recomendado para Cores de destino replicados ao atualizar do AppAssure 5.3.x para a versão 5.4. Durante a execução da verificação de integridade, que pode ser prolongada, nenhuma outra ação pode ser executada no repositório.

Se você tiver vários repositórios para um core de destino, execute este processo uma vez para cada repositório.

NOTA: Se você tiver outro repositório no core de destino para o qual o trabalho de verificação de integridade já foi concluído ou se você criou um novo repositório adicional para este core de destino, poderá executar operações em um repositório secundário enquanto o trabalho de integridade está sendo executado em seu repositório principal.

Para executar o trabalho de verificação da integridade do repositório

1. Navegue até o AppAssure Core Console, clique na guia **Configuração** e depois em **Repositórios**.

   A página Repositórios é exibida, mostrando a lista de repositórios associada a este Core.

2. Clique no menu suspenso do repositório que deseja verificar, selecione **Verificar Integridade**.

É exibida uma mensagem de confirmação.

△ **CUIDADO: Antes de confirmar que deseja realizar o trabalho, você deve pensar bem sobre o tempo de duração necessário. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.**

3 Na caixa de diálogo Repositório de verificação de integridade, para realizar a verificação de integridade, clique em **Sim**.

A caixa de diálogo Verificar repositório é fechada, todos os trabalhos enfileirados em andamento são cancelados e começa o trabalho de verificação da integridade.

4 Para monitorar o andamento do trabalho de verificação de integridade de um repositório, incluindo a determinação das etapas adicionais necessárias depois da verificação, clique na guia **Eventos**.

5 Na guia Eventos, clique em **Exibir detalhes** do trabalho para visualizar mais informações sobre o status do trabalho.

- Se você vir um erro em alguma tarefas subordinada, observe o erro e forneça as informações para o representante do suporte técnico da Dell.
- Se o trabalho de verificação de integridade concluir todas as tarefas subordinadas, você pode estabelecer uma política de retenção personalizada para este repositório.

Noções básicas sobre grupos personalizados

O AppAssure Core mostra um menu Máquinas protegidas na área de navegação à esquerda. Ele inclui todas as máquinas adicionadas para proteção no seu AppAssure Core. Se houver clusters protegidos, eles também aparecerão no menu Máquinas protegidas. Abaixo deles, se houver máquinas replicadas, elas aparecerão em um menu de máquinas replicadas sob o nome do Core replicado. É possível realizar ações de grupo para todas as máquinas dispostas sob um desses menus selecionando a seta à direita do nome do menu para acessar o menu suspenso.

Da mesma forma, é possível criar um grupo personalizado para ser exibido na área de navegação à esquerda, conforme descrito em Gerenciar licenças.

O ato de criar um grupo sempre acrescenta um membro (uma máquina protegida, um cluster do servidor ou um agente replicado, dependendo da maneira como foi iniciada a criação do grupo) ao novo grupo personalizado. O ideal é, então, adicionar mais membros ao grupo. Depois disso, é possível executar ações de grupo que se aplicam a todos os membros desse grupo personalizado, conforme descrito em Realizar ações de grupo.

Os grupos personalizados podem incluir agentes protegidos, agentes replicados e clusters de servers. Os clusters de servers se comportam igual aos agentes protegidos, exceto que um cluster de servers e seus nós se comportam como uma única entidade. Se você tentar adicionar um nó de um cluster de servers a um grupo, todo o cluster será adicionado.

Um grupo personalizado pode conter membros semelhantes ou diferentes. Para grupos de membros semelhantes, todas as ações do grupo se aplicam a todos os membros do grupo. Por exemplo, se você forçar um snapshot de um grupo personalizado de agentes protegidos, será feita cópia de segurança de cada agente. Para grupos com membros diferentes (por exemplo, agentes replicados e protegidos), se você aplicar uma ação de grupo, como forçar a replicação, isto se aplicará apenas aos agentes replicados.

É possível criar um ou mais grupos. Um único agente ou máquina replicada pode ser incluído em um ou mais grupos. Dessa forma, é possível agrupar máquinas em seu core da forma que você escolher e executar ações nesse grupo específico.

Cada grupo personalizado aparece na área de navegação à esquerda, com um rótulo que você atribuir. Os grupos com agentes protegidos padrão aparecem primeiro no grupo personalizado e os agentes replicados aparecem abaixo, conforme aplicável.

Incluir uma máquina em um grupo não a remove de seu local original. Por exemplo, se você tiver três máquinas protegidas chamadas Agente1, Agente2 e Agente3 e adicionar o Agente1 ao GrupoPersonalizado1, o Agente1 aparecerá em ambos os locais.

Para obter mais informações, consulte os seguintes tópicos:

- Gerenciar licenças
- Modificar nomes de grupos personalizados
- Remover grupos personalizados
- Realizar ações de grupo
- Visualizar todas as máquinas de um grupo personalizado em uma página

Criar grupos personalizados

Ao rolar o cursor sobre o nome de qualquer máquina no menu Máquinas protegidas ou Máquinas replicadas, verá uma seta que abre um menu suspenso. Nesse menu, é possível criar um rótulo personalizado.

Use o procedimento abaixo para criar um grupo personalizado.

Para criar um grupo personalizado

1 Navegue até o AppAssure Core Console.

2 No menu Máquinas protegidas ou Máquinas replicadas, faça o seguinte:

   a Clique em uma máquina do menu.

   b Clique no menu suspenso dessa máquina.

   c Role e selecione **Rotulado como** e clique em **Novo rótulo**.

   Aparecerá um novo menu, com uma caixa de texto em branco ao lado de um ícone de rótulo. A máquina selecionada é relacionada sob o grupo personalizado.

3 Insira um rótulo adequado para seu grupo personalizado.

   Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas agente por departamento, digite Departamento de contabilidade. Posteriormente, é possível renomear o grupo.

   NOTA: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

4 Quando estiver satisfeito com o nome do rótulo, clique na marca de verificação verde para salvar o nome.

   A página é atualizada, mostrando seu grupo personalizado na área de navegação.

5 Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

   Agora você pode realizar ações de grupo nesse grupo. Para obter mais informações, consulte Realizar ações de grupo.

Modificar nomes de grupos personalizados

Ao modificar o nome de um grupo personalizado, apenas o rótulo é alterado. Os nomes das máquinas continuam os mesmos.

Use o procedimento abaixo para modificar o nome de um grupo personalizado.

Para modificar o nome de um grupo personalizado

1 Navegue até o AppAssure Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja modificar.

3 Clique no menu suspenso desse grupo e clique em **Editar**.

O nome do grupo personalizado se torna editável.

4 Digite um novo rótulo para o grupo personalizado. Quando estiver satisfeito com o nome do rótulo, clique na marca de verificação verde para salvar o nome. É possível editar esse nome mais tarde.

Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas agente por departamento, digite Departamento de contabilidade.

> **NOTA:** Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

5 Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

Remover grupos personalizados

Quando um grupo personalizado é removido, ele é excluído do menu Máquinas protegidas. As máquinas que estavam no grupo não são removidas e ainda podem ser encontradas no menu padrão apropriado.

Use o procedimento abaixo para remover um grupo personalizado.

Para remover um grupo personalizado

1 Navegue até o AppAssure Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja remover.

3 Clique no menu suspenso desse grupo e clique em **Remover rótulo**.

Aparece uma mensagem pedindo confirmação para a remoção do grupo. Confirme a ação.

A página é atualizada e o grupo personalizado é removido da área de navegação.

Realizar ações de grupo

É possível realizar ações de grupo em qualquer grupo que apareça na área de navegação à esquerda do AppAssure Core Console. Se o grupo contiver membros diferentes (por exemplo, máquinas agente padrão e agentes replicados), as ações solicitadas serão realizadas apenas nos membros do grupo relevantes.

Use o procedimento abaixo para realizar ações de grupo em um grupo personalizado.

Para realizar ações de grupo

1 Navegue até o AppAssure Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado no qual deseja realizar uma ação de grupo.

3 Clique no menu suspenso desse grupo e selecione uma ação, como a seguir:

- Para forçar um snapshot incremental ou imagem de base de um agente protegido, clique em Forçar snapshot ou Forçar imagem de base, conforme o caso. Para obter mais informações, consulte Forçar um snapshot.
- Para pausar a proteção de um agente protegido, clique em **Pausar proteção** e especifique os parâmetros de retomada. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para retomar a proteção de um agente cuja proteção tenha sido pausada, clique em Retomar proteção e confirme que deseja retomar. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para atualizar as informações exibidas, clique em **Atualizar metadados**.

- Para pausar a replicação de um agente replicado do core de destino, em Replicação clique em **Pausar**. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para retomar a replicação de um agente replicado para o qual a replicação foi pausada no core de destino, em Replicação clique em **Retomar**. Para obter mais informações, consulte Pausar e retomar a replicação
- Para forçar a replicação de uma máquina agente replicada, clique em **Forçar**. Para obter mais informações, consulte Forçar a replicação.
- Apenas para grupos personalizados, para modificar o rótulo deles, selecione **Editar**. Para obter mais informações, consulte Modificar nomes de grupos personalizados.
- Apenas para grupos personalizados, para remover o grupo, selecione **Remover rótulo**. Para obter mais informações, consulte Remover grupos personalizados.

Visualizar todas as máquinas de um grupo personalizado em uma página

Clique no nome de um grupo personalizado para ver a guia Máquinas que relaciona todas as máquinas nesse grupo personalizado. É possível então realizar algumas funções em todas as máquinas a partir do menu Ações ou realizar funções individualmente selecionando os comandos de cada máquina individual.

Realizar cópia de segurança e restauração da configuração do Core

Ao configurar um AppAssure Core, você pode criar uma cópia de segurança de todas as definições do Core armazenadas no registro do Windows. Se você criar a cópia de segurança, essas definições estarão disponíveis no futuro para restauração do arquivo de configuração para um AppAssure Core. Isso é útil quando você restaura ou substitui uma máquina Core devido a uma atualização ou após uma perda de dados.

Opcionalmente, ao restaurar a configuração armazenada em um arquivo de cópia de segurança, você também pode restaurar informações de configuração dos repositórios. Por fim, você pode restaurar o caminho associado ao armazenamento de dados ou metadados. Isso é útil em caso de alteração acidental dessas definições.

NOTA: Esse processo restaura apenas as definições de configuração, não os dados.

Informações de segurança (como credenciais de autenticação) não são armazenadas no arquivo de configuração. Salvar um arquivo de configuração de Core não acarreta riscos de segurança.

Esta seção inclui os seguintes tópicos:

- Realizar cópia de segurança da configuração do Core
- Restaurar uma cópia de segurança da configuração do Core

Realizar cópia de segurança da configuração do Core

Você pode criar uma cópia de segurança das definições de configuração do Core para restauração posterior. Execute as etapas do procedimento a seguir para criar uma cópia de segurança das informações de configuração do Core em um arquivo XML.

CUIDADO: Se as definições de configuração do Core mudarem, você deverá criar uma cópia de segurança após as alterações para manter as informações de configuração atualizadas.

A Dell recomenda mover o arquivo de cópia de segurança para um local conhecido em outra máquina, unidade de rede ou mídia de armazenamento guardada em um local externo.

Para criar a cópia de segurança da configuração do Core

1 Navegue até o AppAssure Core, clique na guia Configuração e depois em **Cópia de segurança/restauração**.

O painel Configuração de cópia de segurança do Core aparece.

2 No painel Configuração de cópia de segurança do Core, no campo de texto Caminho local, digite o caminho de um diretório local no servidor que contém o AppAssure Core e clique em **Cópia de segurança**.

Por exemplo, digite C:\Users\administrator\Documents\Config e clique em Cópia de segurança.

O arquivo é salvo como AppRecoveryCoreConfigurationBackup.xml no diretório especificado.

△ **CUIDADO: A Dell recomenda mover o arquivo de cópia de segurança para um local conhecido em outra máquina, unidade de rede ou mídia de armazenamento guardada em um local externo.**

Restaurar uma cópia de segurança da configuração do Core

Se você tiver uma cópia de segurança do arquivo de configuração de Core, poderá restaurar esse arquivo XML para um AppAssure Core. Isso é útil quando você restaura ou substitui uma máquina Core devido a uma atualização ou após uma perda de dados. Após restaurar o arquivo de cópia de segurança, as definições de configuração do arquivo são restauradas para o AppAssure Core. Isso inclui nomes das máquinas protegidas, relacionamentos de replicação, informações sobre standby virtual e chaves de criptografia, conforme aplicável.

Execute as etapas descritas no procedimento a seguir para restaurar um arquivo de configuração do Core.

ⓘ **NOTA:** Para restaurar, o arquivo de configuração deve ser armazenado localmente na máquina Core.

Para restaurar uma cópia de segurança da configuração do Core

1 Se o arquivo de cópia de segurança a ser restaurado estiver em uma unidade de rede ou outro local, copie o arquivo AppRecoveryCoreConfigurationBackup.xml para uma unidade local na máquina Core e anote sua localização.

2 Navegue até o AppAssure Core, clique na guia Configuração, passe o mouse sobre **Cópia de segurança/restauração** e clique em **Restaurar**.

O painel Restaurar configuração do Core aparece.

3 No painel Restaurar configuração do Core, no campo de texto Caminho local, digite o caminho local do arquivo de cópia de segurança.

4 Opcionalmente, se você quiser restaurar as informações de configuração de repositórios armazenadas na cópia de segurança do arquivo de configuração, selecione **Restaurar repositórios**.

5 Observe os cuidados indicados. Se o processo de restauração não for concluído conforme esperado, verifique cada um destes fatores.

6 Em seguida, clique em **Restaurar**.

Sua configuração é restaurada para o AppAssure Core.

4

Gerenciar as definições do AppAssure Core

Este capítulo descreve como gerenciar e alterar as definições do AppAssure Core a partir da guia Configuração ou do respectivo ícone. Ele inclui as seguintes seções:

- Noções básicas sobre informações do sistema
- Configuração das definições de atualização
- Noções básicas sobre trabalhos noturnos
- Modificar definições de fila de transferência
- Modificar definições de fila de transferência
- Ajustar definições de tempo limite do cliente
- Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento
- Configurar as definições do mecanismo Replay
- Configurar as definições do implantação
- Acessar os diagnósticos do Core
- Configurar definições de conexão de banco de dados
- Alterar uma licença
- Criar cópia de segurança e restaurar definições do Core
- Configurar as definições de trabalhos do Core

Por padrão, as definições do AppAssure Core são configuradas para proporcionar um desempenho ideal para a maioria dos usuários. Essas definições afetam o desempenho do AppAssure Core, ou, em alguns casos, a exibição de informações no AppAssure Core Console. Na guia Configuração, clique em Definições para acessar a maioria das definições do Core. Na mesma guia, você também pode acessar Aplicação de licença, Cópia de segurança/ restauração ou Definições de trabalho, conforme apropriado. A tabela a seguir relaciona o conjunto abrangente de definições do AppAssure Core que você pode configurar.

Tabela 34. Definições configuráveis do AppAssure Core

Definição de configuração	Descrição
Informações do sistema	As informações do sistema incluem dados sobre o AppAssure Core Server. Você pode ver o nome de host, OS, arquitetura e memória do Core. Você pode ver ou alterar o nome exibido no Core Console. Também pode visualizar o nome de domínio totalmente qualificado do Core na rede e o caminho para os metadados de cache e para o cache de deduplicação. As informações do sistema estão disponíveis no menu Ferramentas. Para obter mais informações sobre como alterar o nome de exibição, consulte Noções básicas sobre informações do sistema. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento. Para obter mais informações sobre ajuste de definições, consulte Configurar definições de cache de deduplicação.
Geral	As definições gerais incluem opções de configuração que se aplicam geralmente ao AppAssure Core, incluindo opções de exibição e portas do servidor da Web e do serviço AppAssure. Para acessar as definições gerais, selecione Definições gerais. Elas incluem: • Nome de exibição • Porta do servidor da Web • Porta de serviço • Idioma Para obter mais informações sobre as definições gerais do AppAssure Core, incluindo como configurá-las, consulte Noções básicas sobre informações do sistema.
Atualizações	As definições de atualização controlam os aspectos relacionados ao recurso de atualização automática, que verifica se há versões atualizadas do software AppAssure. As definições de atualização são: • Verificar se há novas atualizações • Instalar atualizações • Status • Última verificação Para obter mais informações sobre as definições de atualização do AppAssure Core, incluindo como configurá-las, consulte Configuração das definições de atualização.
Trabalhos noturnos	As definições de trabalhos noturnos referem-se às tarefas automatizadas que o Core realiza diariamente. Você pode configurar o horário de início e quais trabalhos são executados. A Dell recomenda programar os trabalhos fora do horário de expediente normal para reduzir a carga no sistema quando a demanda está alta. Para obter mais informações sobre trabalhos noturnos, consulte Noções básicas sobre trabalhos noturnos. Para obter mais informações sobre como configurar essas definições do Core, consulte Configurar trabalhos noturnos para o Core. Para obter mais informações sobre a configuração de trabalhos noturnos para máquinas protegidas específicas, consulte Personalizar trabalhos noturnos para uma máquina protegida.
Fila de transferência	As definições de fila de transferência se aplicam ao número de tentativas de transferência quando os trabalhos falham devido à indisponibilidade de recursos. Você pode estabelecer o número máximo de transferências simultâneas e o número máximo de tentativas de transferência de dados. Para obter mais informações sobre as definições da fila de transferência, consulte Modificar definições de fila de transferência.
Tempo limite do cliente	As definições de tempo limite do cliente determinam por quanto tempo serão realizadas tentativas de solicitações de conexão específicas ou de operações de leitura e gravação. Para obter mais informações sobre as definições de tempo limite do cliente, consulte Ajustar definições de tempo limite do cliente.

Tabela 34. Definições configuráveis do AppAssure Core

Definição de configuração	Descrição
Cache de deduplicação	O AppAssure deduplica seus dados globalmente em um repositório. A deduplicação garante que cada bloco de informações seja armazenado apenas uma vez no repositório, criando referências para blocos de dados repetidos. As referências são armazenadas em um cache de deduplicação. Quando chaves de criptografia são usadas, a deduplicação ocorre dentro de cada domínio de criptografia. As definições do cache de deduplicação permitem configurar o tamanho e especificar os locais dos caches primário e secundário, bem como do cache de metadados. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento. Para obter mais informações sobre ajuste de definições, consulte Configurar definições de cache de deduplicação.
Mecanismo Replay	As definições do mecanismo Replay controlam informações relacionadas ao canal de comunicação do mecanismo Replay. As definições incluem endereços IP, números de porta, atribuição automática de porta, tamanhos de buffer para envio e recebimento de informações e definições de tempo limite para ajustar o desempenho às necessidades da rede. Para obter mais informações sobre as definições do mecanismo de AppAssure, consulte Configurar as definições do mecanismo Replay.
Implantação	As definições de implantação permitem definir opções para implantar o software AppAssure Agent do seu Core nas máquinas que você deseja proteger. O AppAssure permite especificar o nome do arquivo de instalação, o endereço do Core e definições de tempo limite, bem como limitar o número de instalações simultâneas (para evitar sobrecarga da rede). Você também pode especificar se as máquinas protegidas são reinicializadas e se são protegidas automaticamente após a implantação do software AppAssure Agent. Para obter mais informações sobre a configuração de definições de implantação, consulte Configurar as definições do implantação.
Conexão de banco de dados	O AppAssure exibe informações sobre tarefas, eventos e alertas do Core na guia Eventos. O AppAssure armazena essas informações transacionais em um banco de dados de serviço MongoDB que, por padrão, é instalado localmente na máquina Core. Você pode configurar essas definições para alterar o tempo de retenção de informações no banco de dados ou o tamanho do pool de conexões para permitir mais ou menos conexões simultâneas. Se estiver usando um segundo AppAssure Core, você pode configurar as definições de conexão de banco de dados no primeiro Core para apontar para a segunda máquina Core. Dessa maneira, os dados de eventos dos dois Cores serão armazenados no MongoDB do segundo Core. Você também pode configurar as definições de conexão de banco de dados do Core para apontar para outra máquina que possua um MongoDB instalado separadamente e esteja acessível ao AppAssure Core através da rede. Nesse caso, os dados de transação de evento do seu Core são salvos nesse banco de dados de serviço e não localmente. Para obter mais informações sobre a configuração ou modificação de definições de conexão do banco de dados de serviço, consulte Configurar definições de conexão de banco de dados.

Tabela 34. Definições configuráveis do AppAssure Core

Definição de configuração	Descrição
Server de SMTP	O AppAssure Core monitora tarefas, eventos e alertas. Essas informações são visíveis na guia Eventos. Se você configurar definições de server de SMTP (simple mail transfer protocol) no Core, também poderá enviar essas informações por e-mail. Essas definições são o nome do server de SMTP, endereço de e-mail de origem (endereço "De"), credenciais de login, porta, tempo limite e definições de segurança para esse servidor de e-mail. Para obter mais informações sobre como configurar um server de SMTP para e-mail, consulte Configurar um servidor de e-mail. **NOTA:** Para enviar informações sobre eventos por e-mail, você também deve configurar as definições de grupo de notificação. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.
Logs de acompanhamento	As definições de logs de acompanhamento podem ser configuradas para registrar um número significativamente maior de eventos e estados no AppAssure Core do que os logs padrão. Essa funcionalidade destina-se especificamente à solução de problemas. **NOTA:** A Dell não recomenda alterar essas definições, a menos que seja solicitado pelo Suporte Dell. Manter um alto nível de registro em log por um longo período pode afetar significativamente o espaço de armazenamento e o desempenho.
Configuração da nuvem	As definições de configuração da nuvem permitem especificar definições de configuração para várias contas de armazenamento em nuvem, incluindo Microsoft Azure, Amazon S3 e provedores de nuvem gerenciada usando a tecnologia de fonte aberta OpenStack. Essas definições não criam contas de nuvem. Em vez disso, elas associam suas contas de nuvem existentes ao AppAssure Core para facilitar ações como o arquivamento de informações do AppAssure. Para obter mais informações sobre o gerenciamento de informações de conta de armazenamento em nuvem no AppAssure Core, consulte Gerenciar contas de nuvem.
Aplicação de licença	No Core Console, o AppAssure permite alterar a licença associada ao Core, visualizar informações sobre o conjunto de licenças e contatar o servidor de licenças. Para obter mais informações sobre o gerenciamento de licenças no Core, consulte Gerenciar licenças. Para obter mais informações sobre o gerenciamento de licenças, consulte o Guia do Portal de licenças do Dell AppAssure. **NOTA:** O Portal de licenças do Dell AppAssure possui um ciclo de versões diferente do software AppAssure. Para obter a documentação mais recente do produto, consulte o Site de documentação técnica da Dell.
Cópia de segurança e restauração de definições do Core	O AppAssure permite criar uma cópia de segurança das definições de configuração do Core em um arquivo XML. Você pode usar um arquivo de cópia de segurança para restaurar ou migrar as definições do Core. Para obter mais informações sobre a criação de cópia de segurança e a restauração das definições do Core, consulte Criar cópia de segurança e restaurar definições do Core.

Tabela 34. Definições configuráveis do AppAssure Core

Definição de configuração	Descrição
Trabalhos	Os trabalhos do Core são criados automaticamente quando você inicia operações, como replicação. A seção Definições de trabalho na guia Configuração permite determinar as definições para cada trabalho. Você pode configurar o número de trabalhos executados simultaneamente. Caso um erro de rede ou outro erro de comunicação impeça que o trabalho seja bem-sucedido de início, você pode definir o número de novas tentativas a serem feitas. Para obter mais informações sobre trabalhos do Core, quais trabalhos estão disponíveis e como configurá-los, consulte Configurar as definições de trabalhos do Core.
Diagnóstico (logs do Core)	Para diagnosticar possíveis problemas, você pode baixar e visualizar os logs do AppAssure Core, ou pode carregar logs do Core para qualquer máquina protegida. Esses recursos estão disponíveis no menu Ferramentas. Para mais informações sobre como baixar ou carregar logs, consulte Acessar os diagnósticos do Core.
Banco de dados local	O AppAssure exibe informações sobre tarefas, eventos e alertas do Core na guia Eventos. O AppAssure armazena essas informações transacionais em um banco de dados de serviço MongoDB, que é instalado localmente na mesma máquina do AppAssure Core. Você pode configurar informações de credencial (nome de usuário e senha) para o banco de dados de serviço Mongo local usando as definições de Banco de dados local.
Configuração de SNMP	O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo para gerenciar dispositivos em uma rede IP. O SNMP é usado principalmente para monitorar dispositivos em uma rede a fim de detectar condições que exigem atenção. O protocolo usa componentes de software (agentes) para enviar informações para computadores administrativos (gerentes). Um agente SNMP processa as solicitações do gerente para obter ou definir certos parâmetros. O agente SNMP também pode enviar traps (notificações sobre eventos específicos) ao gerente. Os objetos de dados gerenciados por agentes SNMP são organizados em uma Base de Informações de Gerenciamento (MIB) que contém Identificadores de Objeto (OIDs). Cada OID identifica uma variável que pode ser lida ou definida usando SNMP. Você pode configurar o AppAssure Core como um agente SNMP. Assim o Core pode enviar informações como alertas, status do repositório e máquinas protegidas. Um host SNMP pode ler essas informações usando um aplicativo independente, conhecido como navegador de SNMP. Você pode instalar o navegador de SNMP em qualquer máquina que o AppAssure Core possa acessar pela rede. Use as definições de SNMP para controlar a comunicação entre o Core e o navegador de SNMP. Também é possível baixar um arquivo MIB do AppAssure Core. Na guia Ferramentas, selecione Downloads e baixe o MIB no painel Outros arquivos. Um navegador de SNMP pode ler esse arquivo de forma mais acessível ao usuário que os dados recebidos diretamente do Core.

Noções básicas sobre informações do sistema

O AppAssure permite visualizar informações sobre o AppAssure Core, incluindo informações do sistema, volumes locais e montados e conexões do mecanismo Replay.

No painel Informações do sistema, você pode ver as informações descritas na tabela a seguir.

Tabela 35. Informações do sistema

Elemento de UI	Descrição
Nome do host	O nome da máquina do AppAssure Core.
Versão de OS	A versão do sistema operacional instalado no AppAssure Core.
Arquitetura de OS	Relaciona a estrutura subjacente e o design da máquina que hospeda o AppAssure Core. Pode incluir o chipset e listar um sistema de 64 bits.
Memória (física)	Mostra a quantidade de memória de acesso aleatório (RAM) instalada na máquina Core.
Nome de exibição	Mostra o nome de exibição do Core, que pode é configurável (consulte Noções básicas sobre informações do sistema).
Nome de domínio totalmente qualificado	Mostra o nome de domínio totalmente qualificado da máquina Core.
Local do cache de metadados	Mostra o caminho do local do cache de metadados. Para obter mais informações, consulte Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento.
Local do cache principal	Mostra o caminho do local do cache de deduplicação principal. Para obter mais informações, consulte Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento.
Local do cache secundário	Mostra o caminho do local do cache de deduplicação secundário. Para obter mais informações, consulte Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento.

O painel Volumes inclui as seguintes informações sobre volumes de armazenamento na máquina Core: Nome, ID de dispositivo, sistema de arquivos, capacidade bruta, capacidade formatada, capacidade utilizada e pontos de montagem.

O painel Conexões do mecanismo Replay exibe informações detalhadas sobre os pontos de recuperação montados atualmente. Essas informações incluem ID, terminal local, terminal remoto, ID do agente da imagem montada, ID da imagem montada e nome de exibição da imagem montada. Você pode ver se a montagem é gravável e visualizar o usuário autenticado, os bytes lidos e os bytes gravados.

Você pode desmontar pontos de recuperação montados localmente em um Core usando a opção Montar na guia Ferramentas. Para obter mais informações sobre desmontagem de pontos de recuperação, consulte Desmontar pontos de recuperação.

Visualizar informações do sistema

Execute as etapas deste procedimento para visualizar as informações do sistema.

Para visualizar informações do sistema

1. Navegue até o AppAssure Core e selecione a guia Ferramentas.
2. Na opção Ferramentas, clique em **Informações do sistema**.

Configurar as definições gerais do Core

Conclua as etapas deste procedimento para atualizar as definições gerais do AppAssure Core, que incluem o nome de exibição do Core, a porta do servidor da Web, a porta de serviço e o idioma de exibição do AppAssure Core.

Para configurar as definições gerais do Core

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

A caixa de diálogo Definições gerais é exibida.

2 No painel Geral, clique em **Alterar**.

A caixa de diálogo Definições gerais é exibida.

3 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 36. Informações sobre as definições gerais

Caixa de texto	Descrição
Nome de exibição	Insira um novo nome de exibição para o Core. Esse é o nome que será exibido no AppAssure Core Console. Você pode inserir até 64 caracteres.
Porta do servidor da Web	Insira um número de porta para o servidor da Web. A porta padrão é *8006*.
Porta de serviço	Insira um número de porta para o serviço AppAssure Core. A porta padrão é *8006*.
Idioma	Na lista suspensa Idioma, selecione o idioma que você deseja usar. As versões internacionais do AppAssure estão disponíveis em inglês, francês, alemão, japonês, coreano, português, chinês simplificado e espanhol.

4 Clique em **OK**.

5 Se você alterar o idioma, confirme a mensagem indicando que o serviço AppAssure Core deve ser reiniciado para que o idioma atualizado possa ser exibido no Core Console.

Configuração das definições de atualização

O AppAssure inclui o recurso de Atualização automática. Ao instalar o AppAssure Core, é possível optar por atualizar automaticamente o software AppAssure Core quando houver novas atualizações disponíveis e a frequência com que o sistema deve verificar se há atualizações.

NOTA: Para obter mais informações sobre a instalação do software AppAssure Core, consulte o *Guia de instalação e atualização do Dell AppAssure*.

É possível visualizar e alterar as definições que o sistema utiliza para verificar se há atualizações a qualquer momento.

CUIDADO: Ao usar replicação, a configuração do sistema para instalar atualizações automaticamente pode fazer com que o Core de origem seja atualizado antes do Core de destino, o que pode acarretar falha de replicação ou impedir o estabelecimento de uma nova replicação entre os Cores. Para usuários de replicação, a Dell recomenda que os administradores apliquem atualizações automáticas apenas ao Core de destino, depois atualizem manualmente o Core de origem e, por fim, atualizem as máquinas protegidas.

Execute as etapas deste procedimento para configurar as definições de atualização.

Para configurar as definições de atualização

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Atualizações, clique em **Alterar**.

A caixa de diálogo Definições de atualização é exibida.

3 Na caixa de texto Verificar novas atualizações, selecione a frequência com que oAppAssure buscará e instalará atualizações após a conclusão dos trabalhos noturnos. Você pode selecionar dentre as seguintes opções:

- Nunca
- Diariamente
- Semanalmente
- Mensalmente

4 Especifique como as atualizações disponíveis serão tratadas escolhendo uma das seguintes opções:

- **Instalá-las automaticamente (recomendado)** ou
- **Notificar-me, mas não instalá-las**

5 Clique em **OK**.

Noções básicas sobre trabalhos noturnos

Trabalhos noturnos são tarefas diárias automatizadas que ocorrem em horários predeterminados, fora do horário de expediente normal. Como demandam muita memória e incluem várias verificações de integridade e tarefas de consolidação de dados, esses trabalhos devem ser executados preferivelmente quando o AppAssure Core está menos ativo.

Os trabalhos noturnos podem ser gerenciados no nível do Core ou para cada máquina protegida. Todos os trabalhos noturnos e o escopo a que se aplicam são descritos na tabela a seguir.

Tabela 37. Trabalhos noturnos

Nome do trabalho	Escopo	Descrição
Verificação de capacidade de anexação	Máquina protegida	Verifica a integridade de pontos de recuperação que contêm bancos de dados SQL. Processo: • Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados. • Conectar ao banco de dados a partir do SQL Server. • Abrir o banco de dados. • Fechar o banco de dados. • Desmontar o ponto de recuperação. Para ativar essa verificação noturna, especifique uma instância do SQL Server a ser usada para realizar verificações de capacidade de anexação de bancos de dados SQL Server em máquinas protegidas. **NOTA:** Esta opção aparece apenas quando há um SQL Server sendo protegido no Core.

Tabela 37. Trabalhos noturnos

Nome do trabalho	Escopo	Descrição
Verificar a integridade dos pontos de recuperação	Core ou máquina protegida	Verifica a integridade dos pontos de recuperação de cada máquina protegida. Por padrão, a opção Verificar integridade dos pontos de recuperação não está ativada. Processo: • Montar o último ponto de recuperação de cada grupo de proteção. • Enumerar os arquivos e pastas de cada volume. • Examinar os pontos de recuperação para garantir sua validade. • Desmontar o ponto de recuperação.
Verificação de soma de verificação	Máquina protegida	Verifica a integridade dos pontos de recuperação que contêm bancos de dados de mensagens do Exchange (MDBs). **NOTA:** Esta opção aparece apenas quando há um Exchange Server sendo protegido no Core.
Exclusão de eventos e trabalhos antigos	Core	Mantém a escala do banco de dados de eventos removendo os eventos antigos. O número de dias pode ser alterado, sendo 30 o padrão.
Download dos logs das máquinas protegidas	Core	Baixa logs de máquinas protegidas para o Core para poder enviá-los ao servidor de logs.
Estatísticas do repositório de log	Core	Envia estatísticas de repositório para o servidor de logs.
Rollup	Core	Mantém a política de retenção combinando imagens de cópia de segurança. A política de retenção é definida para cada Core, mas pode ser substituída em uma máquina protegida específica. O trabalho de rollup é executado para o Core inteiro.
Truncamento de log	Máquina protegida	Mantém o tamanho dos logs do SQL Server truncando o log de transações de banco de dados para corresponder ao último ponto de recuperação. **NOTA:** Esta opção aparece apenas quando há um SQL Server sendo protegido no Core.
Registros truncados do Exchange	Máquina protegida	Mantém o tamanho dos logs do Exchange truncando o log de transações de banco de dados do Exchange para corresponder ao último ponto de recuperação. **NOTA:** Esta opção aparece apenas quando há um Exchange Server sendo protegido no Core.

Os procedimentos a seguir se aplicam apenas a trabalhos noturnos no nível do Core. Para obter mais informações sobre trabalhos noturnos específicos de máquinas protegidas, consulte Personalizar trabalhos noturnos para uma máquina protegida.

Configurar trabalhos noturnos para o Core

Quando qualquer opção de trabalho noturno é ativada no AppAssure Core, o trabalho selecionado é executado uma vez por dia, no horário especificado, com todas as máquinas protegidas pelo Core.

Da mesma forma, se você desabilita algum trabalho noturno no nível do Core, o trabalho especificado deixa de ser executado em todas as máquinas protegidas pelo Core.

NOTA: Se o escopo de um trabalho noturno inclui máquinas protegidas, você pode aplicar esse trabalho apenas a máquinas protegidas individualmente. O escopo de cada trabalho noturno é descrito no tópico Noções básicas sobre trabalhos noturnos. Para obter mais informações sobre como aplicar definições de trabalhos noturnos específicas a uma máquina protegida, consulte Personalizar trabalhos noturnos para uma máquina protegida.

Como os trabalhos noturnos usam muita memória, a Dell recomenda configurar o Core para executá-los durante um período de baixa atividade. Por padrão, os trabalhos noturnos são programados para serem executados à meia-noite. Se outro horário for mais adequado, altere essa definição no campo Horário dos trabalhos noturnos usando este procedimento.

Para configurar trabalhos noturnos para o Core

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
3. Para alterar o horário em que os trabalhos noturnos são executados, insira um novo horário na caixa de texto Horário dos trabalhos noturnos.
4. Selecione a opção de trabalhos noturnos que deseja definir para o Core. Você pode optar por selecionar todos ou selecionar individualmente apenas aqueles que se aplicam.
5. Clique em **OK**.

Modificar definições de fila de transferência

As definições da fila de transferência são em nível de core e estabelecem o número máximo de transferências simultâneas e de novas tentativas de transferência de dados.

Execute as etapas deste procedimento para modificar as definições da fila de transferência.

Para modificar as definições da fila de transferência

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Fila de transferência, clique em **Alterar**.

   Aparece a caixa de diálogo Fila de transferência.
3. Na caixa de texto Máximo de transferências simultâneas, insira um valor para atualizar o número de transferências simultâneas.

   Defina um número de 1 a 60. Quanto menor o número, menor a carga sobre a rede e outros recursos do sistema. À medida que o número de agentes processados aumenta, o mesmo acontece com a carga sobre o sistema.
4. Na caixa de texto Máximo de novas tentativas, insira um valor para atualizar o número máximo de novas tentativas.
5. Clique em **OK**.

Ajustar definições de tempo limite do cliente

As definições de tempo limite do cliente controlam por quanto tempo diferentes operações serão tentadas antes que o tempo se esgote.

NOTA: A Dell recomenda manter as definições padrão de tempo limite, a menos que você tenha problemas específicos em seu ambiente e um representante do Suporte Dell recomende a modificação das definições.

Essas definições permitem configurar os parâmetros descritos na tabela a seguir.

Tabela 38. Definições de tempo limite

Definição	Descrição
Tempo limite de conexão	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao enviar dados usando o protocolo de transferência de hipertexto (HTTP).
Tempo limite de leitura/gravação	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao ler ou gravar dados de fluxo através por HTTP. Um exemplo é o recebimento pelo Core de blocos de dados alterados de uma máquina protegida para criar um snapshot incremental.
Tempo limite da UI	Controla o tempo limite da conexão entre a interface gráfica de usuário e o serviço Core por HTTP.
Tempo limite da UI de leitura/gravação	Controla o tempo limite da conexão para leitura e gravação de fluxos de dados entre a interface gráfica de usuário e o serviço Core por HTTP.

Execute as etapas deste procedimento para ajustar as definições de tempo limite do cliente.

Para ajustar as definições de tempo limite de cliente

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.
2. Na área de configuração das Definições de tempo limite do cliente, clique em **Alterar**.

   Aparece a caixa de diálogo Definições de tempo limite do cliente.
3. Na caixa de texto Tempo limite de conexão, insira o número de minutos e segundos antes de ocorrer o tempo limite de uma conexão.
4. Na caixa de texto Tempo limite da UI de conexão, digite o número de minutos e segundos antes de ocorrer o tempo limite da UI de uma conexão.
5. Na caixa de texto Tempo limite de leitura/gravação, insira o número de minutos e segundos que você deseja que passem antes de ocorrer o tempo limite durante um evento de leitura/gravação.
6. Na caixa de texto Tempo limite de UI de leitura/gravação, digite o número de minutos e segundos que passarão antes de ocorrer o tempo limite da UI de leitura/gravação.
7. Clique em **OK**.

Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento

A deduplicação global reduz a quantidade de espaço de armazenamento em disco necessário para seus dados salvos em cópias de segurança. O gerenciador de volume de deduplicação (DVM) do AppAssure combina um conjunto de locais de armazenamento em um único repositório. Cada repositório é deduplicado, armazenando cada bloco único uma vez fisicamente em disco, e utilizando referências virtuais ou indicadores a esses blocos em cópias de segurança subsequentes. Para identificar blocos duplicados, o AppAssure inclui um cache de deduplicação que contém referências a blocos únicos.

Por padrão, esse cache de deduplicação tem 1.5 GB em tamanho. Esse é um tamanho suficiente para muitos repositórios. Até esse cache ser excedido, seus dados são deduplicados em todo o repositório. Se a quantidade de informações redundantes for tão grande que o cache de deduplicação fique cheio, seu repositório não

poderá mais tirar total vantagem de deduplicação adicional em todo seu repositório para dados recém-adicionados. A quantidade de dados salvos em seu repositório antes que o cache de deduplicação encha varia por tipo de dados salvos em cópias de segurança e é diferente para cada usuário.

É possível aumentar o tamanho do cache de deduplicação alterando a configuração do cache de deduplicação no AppAssure Core. Para obter mais informações sobre como realizar isso, consulte o tópico Configurar definições de cache de deduplicação.

Quando você aumentar o tamanho do cache de deduplicação, há dois fatores a considerar: espaço em disco e uso de RAM.

Espaço em disco. Duas cópias do cache são armazenadas em disco: um cache primário, e um cache secundário, que é uma cópia paralela. Então, com um tamanho de cache padrão de 1.5 GB, 3 GB de armazenamento em disco são utilizados em seu sistema. À medida que você aumenta o tamanho do cache, a quantidade de espaço em disco utilizado continua proporcionalmente o dobro do tamanho do cache. Para garantir o desempenho adequado e resistente a erros, o Core altera de forma dinâmica a prioridade desses caches. Ambos são necessários, a única diferença é que o cache designado como principal é salvo primeiro.

Uso de RAM. Quando o AppAssure Core inicia, ele carrega o cache de deduplicação para a memória RAM. O uso da memória para seu sistema é, portanto, afetado pelo tamanho do cache. A quantidade total de RAM utilizada pelo Core depende de muitos fatores, incluindo quais operações são executadas, o número de usuários, o número de agentes, bem como o tamanho do cache de deduplicação. Toda operação realizada pelo Core (transferência, replicação, rollup e assim por diante) consome mais RAM. Depois que uma operação é concluída, o consumo de memória diminui cada vez mais. Contudo, os administradores devem considerar o requisito mais alto do carregamento de RAM para obterem operações eficientes.

As definições padrão do AppAssure Core colocam os caches principal, secundário e de metadados no diretório do AppRecovery utilizado pelo AppAssure.

NOTA: Dependendo de suas definições, o diretório do AppRecovery pode não estar visível no AppAssure Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas.

Supondo que o AppAssure Core esteja instalado na unidade C, esses locais geralmente são os seguintes:

Tabela 39. Os locais de armazenamento padrão para configurações do cache de deduplicação

Definição	Local de armazenamento padrão
Local do cache principal	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Local do cache secundário	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Local do cache de metadados	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

É possível alterar o local de armazenamento desses caches. Por exemplo, para aumentar a tolerância a falhas, é possível alterar o local do cache secundário para uma unidade física diferente da principal, presumindo-se que o AppAssure Core tenha acesso ao local.

Para obter mais informações sobre como alterar os locais de armazenamento para qualquer dessas definições, consulte o tópico Configurar definições de cache de deduplicação.

Configurar definições de cache de deduplicação

Execute as etapas deste procedimento para configurar as definições de cache de deduplicação.

Para configurar as definições de cache de deduplicação

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Configuração do cache de deduplicação, clique em **Alterar**.

   A caixa de diálogo Configuração do cache de deduplicação é exibida, permitindo especificar os locais de armazenamento de cache e o tamanho dele.

Uma vez que o cache principal e o secundário têm o mesmo tamanho, o armazenamento coletivo para esses dois caches exige duas vezes a quantidade de espaço da quantidade alocada para o tamanho do cache de deduplicação. Por exemplo, se você especificar a quantidade padrão de 1.5 GB para o tamanho do cache de deduplicação, precisará assegurar que cada um dos dois locais de armazenamento tenha, pelo menos, 1.5 GB. Em especial, se ambos os locais pertencerem à mesma unidade (por exemplo, a unidade C), deve haver pelo menos 3 GB de espaço livre em disco.

3 Se você desejar alterar o local do cache primário, na caixa de texto Local de cache primário, insira o caminho para um local de armazenamento acessível ao Core.

4 Se você desejar alterar o local do cache secundário, na caixa de texto Local de cache secundário, insira o caminho para um local de armazenamento acessível ao Core.

5 Se você desejar alterar o local do cache de metadados, na caixa de texto Local de cache de metadados, insira o caminho para um local de armazenamento acessível ao Core.

6 Se você desejar alterar o tamanho do cache de deduplicação, realize os seguintes:

   a Na caixa de texto Tamanho do cache dedupe, insira um valor correspondente à quantidade de espaço que você desejar alocar para o cache de deduplicação.

   Por exemplo, se desejar aumentar o tamanho do cache de deduplicação para 3 GB, insira 3 nesse campo.

   b No campo suspenso do tamanho da unidade, selecione GB (gigabytes) ou TB (terabytes), conforme adequado, para especificar a unidade de medida para o valor na caixa de texto Tamanho do cache dedupe.

NOTA: A definição mínima de tamanho do cache é de 1,5 GB. Além disso, o tamanho do cache não pode exceder 50% da RAM instalada.

7 Clique em **OK**.

NOTA: É preciso reiniciar o serviço AppAssure Core para que as alterações entrem em vigor.

Configurar as definições do mecanismo Replay

Você pode configurar as informações relacionadas ao mecanismo Replay, que é o canal de comunicação do AppAssure. Esses parâmetros determinam as definições do Core para proporcionar uma comunicação eficaz.

Em geral, a Dell recomenda usar as definições padrão. Em alguns casos, o Suporte Dell pode solicitar que você modifique essas definições para ajustar o desempenho às suas necessidades de rede.

Conclua as etapas deste procedimento para configurar as definições do mecanismo Replay.

Para configurar as definições do mecanismo Replay

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Configuração do mecanismo de reprodução, clique em **Alterar**.

É exibida a caixa de diálogo Configuração do mecanismo de reprodução.

3 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 40. Definições do mecanismo Replay

Caixa de texto	Descrição
Endereço IP	Especifique o endereço IP escolhendo uma das seguintes opções: • Clique em **Automaticamente determinado** para usar o endereço IP preferencial do seu TCP/IP. • Ou clique em **Usar um endereço específico** para inserir manualmente um endereço IP.
Porta de preferência	Insira um número de porta ou aceite a definição padrão. A porta padrão é *8007*. A porta é usada para especificar o canal de comunicação do mecanismo Replay.
Porta em uso	Representa a porta em uso para a configuração do mecanismo Replay.
Permitir atribuição automática de porta	Clique para permitir a atribuição automática de porta TCP.
Grupo de administradores	Insira um novo nome para o grupo de administração. O nome padrão é *BUILTIN\Administrators*.
Comprimento de I/O assíncrono mínimo	Insira um valor ou escolha a definição padrão. Descreve o comprimento mínimo assíncrono de entrada/saída. A definição padrão é *65536*.
Tamanho da memória intermediária de recebimento	Insira um tamanho de memória intermediária de entrada ou aceite a definição padrão. A definição padrão é *8192*.
Tamanho da memória intermediária de envio	Insira um tamanho de memória intermediária de saída ou aceite a definição padrão. A definição padrão é *8192*.
Tempo limite de leitura	Insira um valor de tempo limite de leitura ou escolha a definição padrão. A definição padrão é *00:05:00*.
Tempo limite de gravação	Insira um valor de tempo limite de gravação ou escolha a definição padrão. A definição padrão é *00:05:00*.
Sem atraso	Recomendamos deixar essa caixa de seleção desmarcada visto que, se isso não for feito, a eficiência da rede poderá ser afetada. Se for determinado que é preciso modificar essa configuração, entre em contato com o Suporte da Dell para obter orientações de como fazer isso.

4 Clique em **OK**.

A caixa de diálogo Configuração do mecanismo Replay é fechada e suas novas definições de trabalho são aplicadas.

Configurar as definições do implantação

O AppAssure permite baixar instaladores do AppAssure Core para as máquinas que você deseja proteger.

Você pode configurar definições relacionadas à implantação do software AppAssure Agent do seu Core para as máquinas que deseja proteger.

Conclua as etapas deste procedimento para configurar as definições de implantação.

Para configurar as definições de implantação

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Definições de implementação, clique em **Alterar**.

A caixa de diálogo Definições de implantação aparece.

3 Insira as definições de implantação conforme descrito na tabela a seguir.

Tabela 41. Definições de implantação

Caixa de texto	Descrição
Nome do Agent installer	Especifique o nome do arquivo executável do Core Web Installer. Esse arquivo gera um fluxo de download da versão mais recente do AppAssure Core Installer, que é executada diretamente da Web e permite pausar e retomar o processo conforme necessário. O nome padrão do arquivo é Agent-Web.exe.
Endereço do Core	Insira o endereço do seu servidor Core. Geralmente isso consiste no protocolo, nome e porta do servidor Core e diretório em que os arquivos do Core residem. Por exemplo, se o servidor fosse Sample, a definição seria https://sample:8006/apprecovery/admin/Core
Tempo limite de falha de recebimento	Por quanto tempo a implantação do software Agent deve ser tentada antes de atingir o tempo limite. A definição padrão é 20 minutos.
Máximo de instalações paralelas	Essa definição controla o número máximo de implantações do software Agent que o Core deve tentar ao mesmo tempo. A definição padrão é 100.
Reinício automático após a instalação	Essa caixa de seleção controla se as máquinas que recebem o software AppAssure Agent são reiniciadas automaticamente após a instalação. A reinicialização após a instalação é necessária para proteger a máquina que está usando o software recém-instalado. Por padrão, essa opção é definida como ativada.
Proteger após implantação	Esta caixa de seleção controla se as máquinas devem começar a transmitir informações de cópia de segurança para o AppAssure Core imediatamente após a implantação e reinicialização. Se for desabilitada, as máquinas não estarão protegidas até que o usuário force uma cópia de segurança, ou até o próximo horário de cópia de segurança programado.

4 Clique em **Salvar**.

A caixa de diálogo Definições de implantação é fechada e as novas definições de implementação são aplicadas.

Configurar definições de conexão de banco de dados

Você pode ver eventos do sistema relacionados ao AppAssure Core na guia Eventos. O AppAssure Core armazena essas informações transacionais em um banco de dados de serviço MongoDB. Por padrão, esse banco de dados é instalado localmente na máquina Core.

NOTA: Para obter mais informações sobre como visualizar informações de eventos no AppAssure Core, consulte Visualizar tarefas, alertas e eventos.

Os clientes podem optar por especificar a instalação do banco de dados de serviço MongoDB em outra máquina que seja acessível ao AppAssure Core na rede. Se o banco de dados de serviço do AppAssure Core estiver instalado em uma máquina diferente daquela que hospeda o AppAssure Core, você deverá fornecer credenciais de banco de dados (nome de usuário e senha) nessas definições.

Conclua as etapas deste procedimento para modificar as definições de conexão do banco de dados de serviço usado pelo AppAssure Core.

Para modificar as definições de conexão do banco de dados

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Definições de conexão do banco de dados, realize um dos seguintes:

- Clique em **Restaurar padrão**.
- Ou clique em **Alterar**.

A caixa de diálogo Definições de conexão do banco de dados é exibida.

3 Insira as definições para modificar a conexão do banco de dados conforme descrito na tabela a seguir.

Tabela 42. Definições de conexão de banco de dados

Caixa de texto	Descrição
Nome do host	Insira um nome de host para a conexão de banco de dados. **NOTA:** Quando localhost é o parâmetro especificado como host, o MongoDB é instalado localmente na máquina que hospeda o Core.
Porta	Insira o número da porta para a conexão do banco de dados. **NOTA:** A definição padrão é 27017.
Nome de usuário	Insira o nome de um usuário com privilégios administrativos para o banco de dados de serviço MongoDB. **NOTA:** Se o parâmetro do nome do host é localhost, esse campo não é necessário.
Senha	Insira a senha associada ao nome de usuário que você especificou. **NOTA:** Se o parâmetro do nome do host é localhost, esse campo não é necessário.
Reter histórico de eventos e trabalhos por ___ dias	Insira o número de dias de retenção do histórico de eventos e trabalhos no banco de dados de serviço.
Tamanho máximo do pool de conexão	Define o número máximo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTA:** A definição padrão é 100.
Tamanho mínimo do pool de conexão	Define o número mínimo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTA:** A definição padrão é 0.

4 Clique em **Testar conexão** para confirmar as definições.

5 Clique em **Salvar**.

Gerenciar licenças

O AppAssure permite gerenciar licenças diretamente a partir do AppAssure Core Console. Você pode alterar o arquivo ou chave de licença associado ao Core e entrar em contato com o servidor de licenças. Também é possível acessar o Portal de licenças do Dell AppAssure diretamente a partir da página Aplicação de licença no console.

Essa página de Aplicação de licença inclui as seguintes informações:

Detalhes da licença:

- **Tipo de licença.** Os tipos de licenças incluem Teste, Assinatura e Empresa. Para obter mais informações, consulte o tópico Sobre os tipos de licença do software AppAssure no *Guia do usuário do Portal de licenças do Dell AppAssure*.
- **Status da licença.** Indica o status da licença. Um status ativo garante que os snapshots podem continuar conforme programado. Se a licença estiver bloqueada ou expirada ou se o Core não conseguir se comunicar com o Portal de licenças do Dell AppAssure após o período de avaliação, os snapshots serão pausados até que o status da licença seja corrigido.

Conjunto de licenças.

- **Tamanho do conjunto de licenças.** O conjunto de licenças é o número de licenças que não são de teste disponíveis para alocação entre grupos e subgrupos no Portal de licenças do Dell AppAssure. O tamanho do conjunto indica quantas licenças podem ser alocadas. Para obter mais informações, consulte o tópico Sobre conjuntos de licenças no *Guia do usuário do Portal de licenças do Dell AppAssure*.
- **Protegido por este Core.** Indica o número de máquinas deste conjunto de licenças que são protegidas por este Core.
- **Total de protegidos no grupo.** Indica o número total de máquinas protegidas no mesmo grupo de licenças deste Core.

Servidor de licenças. Essas definições se aplicam a licenças padrão (phone home). Essas definições não se aplicam a appliances e a outras licenças que não sejam do tipo phone home:

- **Endereço do servidor de licenças.** Exibe uma URL ativa do servidor de licenças associado a este Core.
- **Última resposta do servidor de aplicação de licença.** Indica se a última tentativa de comunicação com o portal do servidor de licenças teve êxito.
- **Último contato com o servidor de aplicação de licença.** Exibe a data e hora do último contato bem-sucedido com o servidor de aplicação de licença.
- **Próxima tentativa de contato com o servidor de aplicação de licença**. Indica a próxima data e hora programada para a tentativa de comunicação com o servidor de aplicação de licença.

Para obter mais informações, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.

Você também pode visualizar as informações de aplicação de licença relativas a uma única máquina protegida. Para obter mais informações, consulte Visualizar informações de licença em uma máquina.

Alterar uma licença

Muitos usuários começam com uma licença de teste, que tem recursos limitados. Uma licença de teste é válida por 14 dias e pode ser estendida uma única vez pelo administrador do grupo para 28 dias. Quando o período de teste expira, o AppAssure Core para de criar snapshots até você obter uma licença válida.

Assim que você tiver atualizado ou adquirido sua licença do AppAssure, você receberá um arquivo de licença ou uma chave de licença.

Conclua as etapas deste procedimento para atualizar sua licença de teste ou alterar sua licença a partir do AppAssure Core Console.

NOTA: Para obter informações sobre como obter uma chave de licença, consulte o *Guia do usuário do portal de licenças do Dell AppAssure*.

Para alterar uma chave ou arquivo de licença

1. Navegue até o AppAssure Core Console e selecione a guia Configuração.
2. Clique em **Aplicação de licença**.

   A página Aplicação de licença é exibida.
3. No painel Detalhes da licença, clique em **Alterar licença.**

   A caixa de diálogo Alterar licença aparece.
4. Na caixa de diálogo Alterar licença, para inserir uma chave de licença, siga para Etapa 6.
5. Para carregar um arquivo de licença, faça o seguinte:
   a. Selecione **Atualizar arquivo de licenças** e clique em **Procurar**.

      A caixa de diálogo Carregamento de arquivo aparece.
   b. Navegue até o local em que seu arquivo de licença está armazenado e clique para selecioná-lo.
   c. Na caixa de diálogo Carregamento de arquivo, clique em **Abrir**.

O arquivo de licença é autenticado. Vá para Etapa 7.

6 Na caixa de diálogo Alterar licença, selecione **Inserir chave de licença** e, no campo de texto Chave de licença, insira a chave de licença.

7 Clique em **Continuar**.

A caixa de diálogo Alterar licença é fechada.

8 No painel Servidor de licenças, clique em **Contatar agora**.

Assim que a licença é aplicada ao servidor de licenças, todas as máquinas protegidas associadas são atualizadas automaticamente com a nova licença.

Contatar o servidor do Portal de licenças do Dell AppAssure

O AppAssure Core Console frequentemente entra em contato com o server do portal para permanecer atualizado com as mudanças feitas no Portal de licenças do Dell AppAssure.

No caso de licenças que não são de teste, o AppAssure Core entra em contato com o portal de licenças a cada três dias. Se não consegue se conectar ao portal de licenças após o período de avaliação, o Core para de criar snapshots.

Normalmente, a comunicação com o server do portal ocorre automaticamente em intervalos designados. No entanto, é possível iniciar a comunicação sob demanda.

Execute as etapas deste procedimento para entrar em contato com o server do portal.

Para entrar em contato com o server do portal

1 Navegue até o AppAssure Core Console e clique na guia Configuração.

2 Clique em **Aplicação de licença**.

A página Aplicação de licença é exibida.

3 Na opção Server de licenças, clique em **Entrar em contato agora**.

Criar cópia de segurança e restaurar definições do Core

Você pode criar uma cópia de segurança em arquivo das informações de definição e, posteriormente, restaurar essas definições caso haja problemas com a máquina Core você queira migrar essas definições para uma máquina diferente. As informações incluídas na cópia de segurança incluem os metadados do repositório (como o nome do repositório, o caminho de dados e o caminho de metadados); as máquinas protegidas no Core; os relacionamentos de replicação (destinos e origens); quais máquinas estão configuradas para standby virtual; e informações sobre chaves de criptografia.

CUIDADO: Você deve primeiramente criar uma cópia de segurança das informações de definição do Core para poder usar esse processo para restaurar as definições.

Use este procedimento para criar uma cópia de segurança das definições do Core e restaurá-las.

Para criar uma cópia de segurança e restaurar as definições do Core

1 Navegue até o AppAssure Core Console.

2 Clique na guia Configuração e depois em Cópia de segurança/restauração.

A página Configuração de cópia de segurança do Core aparece.

3 Caso queira criar uma cópia de segurança das definições do Core, vá para **Etapa 4**. Caso queira restaurar definições, vá para **Etapa 5**.

4 Para criar uma cópia de segurança das definições atuais em um arquivo XML, na caixa de texto Caminho local, digite o caminho de um diretório acessível localmente à máquina Core no qual você deseja armazenar as definições do Core em um arquivo XML e clique em Cópia de segurança.

Por exemplo, digite C:\Users\Your_User_Name\Documents\AA5CoreSettings e clique em Cópia de segurança.

Um arquivo chamado AppRecoveryCoreConfigurationBackup.xml é salvo no destino local que você especificou.

5 Para restaurar as definições do Core a partir de um arquivo XML de cópia de segurança salvo anteriormente usando esse método, execute as etapas a seguir.

CUIDADO: Quando você restaura as definições de configuração do Core, o serviço AppAssure Core é reiniciado.

a Na guia Configuração, selecione Cópia de segurança/restauração e clique em Restaurar.

A página Restaurar configuração do Core aparece.

b Na caixa de texto Caminho local, digite o caminho local onde você armazenou as definições de configuração do Core.

Por exemplo, digite C:\Users\Your_User_Name\Documents\AA5CoreSettings.

c Caso não queira restaurar as informações de repositório, vá para **Etapa f**.

d Opcionalmente, caso queira restaurar as informações de repositório para a configuração do arquivo de cópia de segurança, selecione Restaurar repositórios e clique em **Restaurar**.

A página é atualizada.

Se você optar por restaurar as informações de repositório a partir da cópia de segurança dos dados de configuração, os repositórios configurados quando as definições do Core foram salvas serão exibidos para confirmação. Por padrão, todos os repositórios estão selecionados.

e Confirme as informações de repositório que você deseja restaurar. Se vários repositórios aparecerem na lista para confirmação e você quiser restaurar as informações de apenas alguns deles, desmarque a seleção dos repositórios que não deseja restaurar.

f Clique em **Restaurar**.

O processo de restauração começa. Um alerta aparece, indicando que a configuração do serviço de repositório foi alterada.

g Caso não tenha sido possível restaurar alguma definição de configuração, uma mensagem de erro será exibida. Confira os detalhes do erro para ver se há alguma ação necessária da sua parte. Para obter mais informações, consulte **Visualizar tarefas, alertas e eventos**. Para continuar, clique em **Fechar** para limpar a caixa de diálogo de erro.

h Depois de restaurar a configuração, siga a orientação na interface de usuário. Por exemplo:

- Desbloqueie todas as chaves de criptografia
- Confirme as credenciais de standby virtual. Se tiver estabelecido a exportação contínua para uma máquina virtual, você terá que especificar suas credenciais para que a sincronização tenha êxito.
- Se a replicação estiver configurada e você quiser restaurar para um Core de destino, confirme as definições do Core de destino no Core de origem.

Configurar as definições de trabalhos do Core

Os trabalhos do Core são criados automaticamente quando você inicia operações, como replicação. A seção Definições de trabalho da guia Configuração permite determinar as definições para cada trabalho, incluindo o número de trabalhos que devem ocorrer de uma vez e quantas vezes um trabalho deve ser tentado, caso um erro de rede ou outro erro de comunicação impeça que o trabalho seja bem-sucedido de início.

- O AppAssure pode executar os seguintes trabalhos do Core:
- AdHocDeleteRecoveryPointsJob
- AutoUpdateJob
- BackupJob
- BootCdBulderJob
- CheckAgentRecoveryPointsJob
- CheckRepositoryIntegrityJob
- DeleteAllRecoveryPointsJob
- DeleteOrphanVolumeImagesChainJob
- DeleteRecoveryPointsChainJob
- DownloadExchangeDllsJob
- ExportJob
- ImportJob
- LocalMountRecoveryPointJob
- MaintainRepositoryJob
- NightlyAttachabilityJob
- PushInstallJob
- RecoveryPointAttachabilityJob
- RollbackJob
- RollupJob
- UploadCoreLogsJob

Editar as definições de trabalhos do Core

Execute as etapas do procedimento a seguir para editar as definições de um trabalho.

Para editar as definições de trabalhos do Core

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Clique na guia Configuração e em **Definições de trabalho**.
- No menu suspenso, clique na guia Configuração e em **Definições de trabalho**.
- Na barra de ícones, clique no menu suspenso ao lado do ícone Configuração e depois em Definições de trabalhos.

2 Na página Definições de trabalho, selecione o trabalho que deseja alterar. No menu suspenso de configuração do trabalho, selecione **Editar**.

3 A caixa de diálogo Definições de trabalho: [JobName] é aberta.

4 Para alterar o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto Máximo de trabalhos simultâneos, insira um novo valor entre 1 e 50.

5 Para alterar a definição relativa ao número de tentativas que o Core deve fazer antes de abandonar o trabalho, na caixa de texto Contagem de tentativas, insira um novo valor entre 1 e 10.

6 Clique em **Salvar**.

A caixa de diálogo Definições de trabalho é fechada e as novas definições de trabalho são aplicadas.

Adicionar trabalhos ao Core

Execute as etapas do procedimento a seguir para adicionar um trabalho ao Core.

Para adicionar trabalhos ao Core

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Clique na guia Configuração e em **Definições de trabalho**.
- No menu suspenso, clique na guia Configuração e em **Definições de trabalho**.
- Na barra de ícones, clique no menu suspenso ao lado do ícone Configuração e depois em Definições de trabalhos.

2 Na página Definições de trabalho, clique em **Adicionar**.

A caixa de diálogo Definições de trabalho é exibida.

3 Na caixa de diálogo Definições de trabalho, no campo Trabalhos, selecione o nome de um trabalho que você deseja adicionar.

Esses trabalhos são descritos no tópico Configurar as definições de trabalhos do Core.

4 Para definir o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto Máximo de trabalhos simultâneos, insira um novo valor entre 1 e 50.

5 Para definir o número de tentativas que o Core deve fazer antes de abandonar o trabalho, na caixa de texto Contagem de tentativas, insira um novo valor entre 1 e 10.

6 Clique em **Salvar**.

A caixa de diálogo Definições de trabalho é fechada e as novas definições de trabalho são aplicadas.

Acessar os diagnósticos do Core

No AppAssure, as informações de diagnóstico estão disponíveis para que você baixe e carregue dados de log do Core. Você também pode baixar e visualizar informações de diagnóstico de máquinas protegidas individuais. Para obter mais informações sobre logs de máquina, consulte Acessar o diagnóstico de máquinas protegidas. A capacidade de acessar logs pode ser útil para solucionar um problema ou trabalhar com o Suporte do AppAssure. Para acessar os logs do Core, consulte os procedimentos a seguir:

- Baixar os logs do Core
- Visualizar os logs do Core
- Carregar logs

Baixar os logs do Core

Se você encontrar erros ou problemas com o Core, poderá baixar os logs do Core para visualizá-los ou carregá-los no Suporte do AppAssure.

Para baixar os logs do Core

1. Navegue até o AppAssure Core Console.
2. Clique no menu suspenso ou aba Ferramentas, clique em **Diagnóstico** e, em seguida, clique em **Visualizar log**.
3. Na página Baixar log do Core da guia Ferramentas, clique em **Clique aqui para iniciar o download**.
4. Na caixa de diálogo Abrindo CoreAppRecovery.log, selecione **Salvar arquivo**.
5. Clique em **OK**.

   O arquivo CoreAppRecovery.log é salvo na sua pasta Downloads.

Visualizar os logs do Core

Se você encontrar erros ou problemas com o Core, talvez seja útil examinar os logs.

Para visualizar os logs do Core

1. Navegue até o AppAssure Core Console.
2. Clique no menu suspenso ou aba Ferramentas, clique em **Diagnóstico** e, em seguida, clique em **Visualizar log**.
3. Na página Baixar log do Core da guia Ferramentas, clique no link **Clique aqui para iniciar o download**.
4. Na caixa de diálogo Abrindo CoreAppRecovery.log, selecione **Abrir com** e use a lista suspensa para selecionar um programa com o qual deseja abrir o arquivo (por exemplo, Bloco de Notas).
5. Clique em **OK**.

   O arquivo é aberto no programa que você selecionou.

Carregar logs

O procedimento a seguir permite carregar logs que você baixou do Core ou de máquinas protegidas. Execute as etapas do procedimento a seguir para carregar os logs de máquina.

Para carregar logs

1. Navegue até o AppAssure Core Console.
2. Clique na guia Ferramentas e em **Diagnóstico**.
3. Clique em **Carregar log**.
4. Na página Carregar log do Core da guia Ferramentas, clique em **Clique aqui para iniciar o upload**.

   A guia Eventos mostra o progresso do carregamento das informações de log do Core e de todas as máquinas protegidas.

5

Noções básicas sobre chaves de criptografia

Este capítulo descreve o processo de proteger dados no seu ambiente usando chaves de criptografia. Ele inclui as seguintes seções:

- Aplicar ou remover criptografia de uma máquina protegida
- Gerenciar chaves de criptografia

O AppAssure Core pode criptografar dados de snapshot de todos os volumes em qualquer repositório usando chaves de criptografia que você define e gerencia.

Em vez de criptografar todo o repositório, o AppAssure permite especificar uma chave de criptografia para uma ou mais máquinas protegidas em um único AppAssure Core. Cada chave de criptografia ativa cria um domínio de criptografia. Não há limite para o número de chaves de criptografia que podem ser criadas no Core. Em um ambiente multilocatário (quando um único Core hospeda vários domínios de criptografia), os dados são particionados e deduplicados dentro de cada domínio de criptografia. Por isso, a Dell recomenda usar uma única chave de criptografia para várias máquinas protegidas se você deseja maximizar os benefícios da deduplicação entre um conjunto de máquinas protegidas.

Como você gerencia as chaves de criptografia, a perda do volume não pode vazar as chaves.

Você também pode compartilhar chaves de criptografia entre Cores usando um de três métodos. Um dos métodos é exportar a chave de criptografia de um AppAssure Core como um arquivo e importá-la para outro Core. Um segundo método é arquivar dados protegidos com uma chave de criptografia e então importar esses dados arquivados para outro AppAssure Core. O terceiro método é replicar os pontos de recuperação de uma máquina protegida usando uma chave de criptografia. Depois que você replica máquinas protegidas, as chaves de criptografia usadas no Core de origem aparecem como chaves de criptografia replicadas no Core de destino.

Em todos os casos, depois de importada, qualquer chave de criptografia aparece no Core com o estado Bloqueado. Para acessar dados de uma chave de criptografia bloqueada, é necessário desbloqueá-la. Para obter informações sobre importação, exportação, bloqueio ou desbloqueio de chaves de criptografia, consulte o tópico Gerenciar chaves de criptografia.

Os principais conceitos e considerações sobre segurança incluem:

- A criptografia é feita usando o padrão AES (Advanced Encryption Standard) de 256 bits no modo CBC (Cipher Block Chaining), que é compatível com SHA-3.
- A deduplicação opera dentro de um domínio de criptografia para garantir a privacidade.
- A criptografia é realizada sem impacto no desempenho.
- Você pode aplicar uma única chave de criptografia a qualquer número de máquinas protegidas, mas uma máquina protegida só pode ter apenas uma chave de criptografia aplicada a qualquer momento.
- É possível adicionar, remover, importar, exportar, modificar e excluir as chaves de criptografia configuradas no AppAssure Core.

△ **CUIDADO: O AppAssure cria uma nova imagem de base quando você aplica uma chave de criptografia a uma máquina protegida ou quando edita o nome, a descrição ou a frase de acesso de uma chave de criptografia aplicada a uma ou mais máquinas protegidas. Uma nova imagem de base também é acionada quando você desassocia uma chave de criptografia de uma máquina protegida. A imagem de base resultante é capturada no próximo snapshot programado (ou imediatamente se você forçar um snapshot).**

As chaves de criptografia geradas a partir do AppAssure Core são arquivos de texto que contêm quatro parâmetros, descritos na tabela a seguir:

Tabela 43. Componentes de uma chave de criptografia

Componente	Descrição
Nome	Este valor é equivalente ao nome atribuído ao adicionar uma chave no AppAssure Core Console.
Chave	Este parâmetro consiste em 107 caracteres do alfabeto inglês, numéricos e matemáticos gerados aleatoriamente.
ID	O ID da chave consiste em 26 caracteres do alfabeto inglês, maiúsculos e minúsculos, gerados aleatoriamente.
Comentários	O comentário contém o texto da descrição da chave inserido quando a chave foi criada.

Aplicar ou remover criptografia de uma máquina protegida

Você pode proteger os dados protegidos no seu Core a qualquer momento definindo uma chave de criptografia e aplicando-a a uma ou mais máquinas protegidas no seu repositório. Você pode aplicar uma única chave de criptografia a qualquer número de máquinas protegidas, mas uma máquina protegida só pode usar uma única chave de criptografia a qualquer momento.

O escopo da deduplicação no AppAssure é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia. Por isso, para maximizar o valor da deduplicação, a Dell recomenda aplicar uma única chave de criptografia a tantas máquinas protegidas quanto seja viável. No entanto, não há limite para o número de chaves de criptografia que podem ser criadas no Core. Portanto, se a conformidade legal, as regras de segurança, as políticas de privacidade ou outras circunstâncias o exigirem, você pode adicionar e gerenciar qualquer número de chaves de criptografia. Nesse caso, você pode aplicar cada chave a apenas uma máquina protegida ou a qualquer conjunto de máquinas no seu repositório.

Quando você aplica uma chave de criptografia a uma máquina protegida ou modifica as propriedades de uma chave de criptografia que está em uso em uma ou mais máquinas protegidas (incluindo a remoção da criptografia), o AppAssure cria uma nova imagem de base para a máquina no próximo snapshot programado ou forçado. Os dados armazenados nessa imagem de base (e em todos os snapshots incrementais subsequentes criados enquanto a chave de criptografia está aplicada) são protegidos por um padrão de criptografia avançado de 256 bits. Não existem métodos conhecidos para violar esse método de criptografia.

Depois que uma chave de criptografia é criada e aplicada a uma máquina protegida, há dois conceitos envolvidos na remoção dessa criptografia. O primeiro é desassociar a chave da máquina protegida. Opcionalmente, depois que a chave de criptografia é desassociada de todas as máquinas protegidas, é possível excluí-la do AppAssure Core.

Esta seção inclui os seguintes tópicos:

- Associar uma chave de criptografia a uma máquina protegida
- Aplicar uma chave de criptografia na guia Máquinas
- Desassociar uma chave de criptografia de uma máquina protegida

Associar uma chave de criptografia a uma máquina protegida

Você pode aplicar uma chave de criptografia a uma máquina protegida usando um de dois métodos:

- **Como parte da proteção de uma máquina.** Usando esse método, você pode aplicar criptografia a uma ou a várias máquinas simultaneamente. Esse método permite adicionar uma nova chave de criptografia ou aplicar uma chave existente à máquina ou máquinas selecionadas.

Para usar criptografia ao definir inicialmente a proteção de uma máquina, você deve selecionar as opções avançadas no assistente de proteção de máquinas relevante. Essa seleção adiciona uma página Criptografia ao fluxo de trabalho do assistente. Nessa página, selecione **Ativar criptografia** e depois selecione uma chave de criptografia existente ou especifique parâmetros para uma nova chave. Para obter mais informações, consulte Proteger uma máquina ou Proteger várias máquinas, respectivamente.

- **Modificando as definições de configuração de uma máquina.** Esse método aplica uma chave de criptografia a uma máquina protegida por vez. Há duas abordagens para modificar as definições de configuração de uma máquina na UI do AppAssure:
    - Modificar as definições do Core na guia Configuração para uma máquina protegida específica. A chave de criptografia que você deseja usar nesta abordagem já deve existir no AppAssure Core. Para obter mais informações, consulte Visualizar e modificar as definições de configuração.
    - Clique no ícone de criptografia na guia Máquinas. Usando esta abordagem, você pode criar e aplicar uma nova chave de criptografia ou atribuir uma chave existente à máquina protegida especificada. Para obter mais informações, consulte Aplicar uma chave de criptografia na guia Máquinas.

Aplicar uma chave de criptografia na guia Máquinas

Depois de ser adicionada a um AppAssure Core, uma chave de criptografia pode ser usada para qualquer número de máquinas protegidas.

Se você selecionar uma chave de criptografia durante a proteção inicial de uma ou mais máquinas, a chave será automaticamente aplicada às máquinas que você proteger usando esse assistente. Nesses casos, este procedimento não é necessário.

Execute este procedimento se você tiver adicionado uma chave de criptografia usando o processo descrito no tópico Adicionar uma chave de criptografia.

△ **CUIDADO: Depois que você aplica uma chave de criptografia a uma máquina protegida, o AppAssure cria uma nova imagem de base da máquina no próximo snapshot programado ou forçado.**

Para aplicar uma chave de criptografia

1. Navegue até o AppAssure Core e clique em **Máquinas protegidas**.

   A guia Máquinas aparece, relacionando todas as máquinas protegidas por este Core. Um cadeado aberto aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado indica que a máquina protegida está com a criptografia aplicada.

2. No painel Máquinas protegidas, clique no ícone de cadeado da máquina protegida que deseja configurar.

   A caixa de diálogo Configuração de criptografia é exibida.

3. Realize um dos procedimentos a seguir:
    - Se você deseja aplicar uma chave de criptografia existente a essa máquina, no menu suspenso Selecionar chave de criptografia, selecione a chave apropriada.
    - Se deseja criar uma nova chave de criptografia e aplicá-la a essa máquina protegida, clique em **Adicionar nova chave de criptografia**. Em seguida, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 44. Detalhes de nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 130 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário para a chave de criptografia. Estas informações aparecem no campo Descrição ao visualizar as chaves de criptografia na guia Configuração do AppAssure Core Console. As descrições podem conter até 454 caracteres. É uma boa prática evitar o uso de caracteres proibidos e frases proibidas.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. É uma boa prática evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. Dell O suporte não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

4 Clique em **OK**.

A caixa de diálogo é fechada. A chave de criptografia que você especificou será aplicada às cópias de segurança futuras dessa máquina protegida e o cadeado agora aparece fechado.

Opcionalmente, se quiser que a chave de criptografia seja aplicada imediatamente, force um snapshot. Para obter mais informações, consulte Forçar um snapshot.

△ **CUIDADO: O AppAssure usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Desassociar uma chave de criptografia de uma máquina protegida

Depois que uma chave de criptografia é aplicada a uma máquina protegida, todos os dados de snapshot subsequentes armazenados no AppAssure Core são criptografados.

Você pode desassociar uma chave de criptografia de uma máquina protegida. Essa ação não descriptografa as cópias de segurança existentes, mas gera uma nova imagem de base da máquina no momento do próximo snapshot programado ou forçado.

ⓘ **NOTA:** Se você quiser remover uma chave de criptografia do Core, conforme descrito no tópico Remover uma chave de criptografia, deverá primeiramente desassociar essa chave de criptografia de todas as máquinas protegidas.

Realize este procedimento para desassociar uma chave de criptografia de uma máquina protegida específica.

Para desassociar uma chave de criptografia de uma máquina protegida

1 Navegue até o AppAssure Core e clique em **Máquinas protegidas**.

A guia Máquinas aparece, relacionando todas as máquinas protegidas por este Core. Um cadeado aberto aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado indica que a máquina protegida está com a criptografia aplicada.

2 No painel Máquinas protegidas, clique no ícone de cadeado fechado da máquina protegida que você deseja configurar.

   A caixa de diálogo Configuração de criptografia é exibida.

3 No menu suspenso Selecionar chave de criptografia, selecione **(Nenhuma)** e clique em **OK**.

4 Se quiser remover a chave de criptografia do AppAssure Core, repita este procedimento em todas as máquinas protegidas que usam essa chave. Em seguida, execute o procedimento descrito no tópico Remover uma chave de criptografia.

Gerenciar chaves de criptografia

Para gerenciar chaves de criptografia do AppAssure Core, na guia Configuração, clique em **Segurança**. O painel Chaves de criptografia aparece. Para cada chave de criptografia adicionada ao seu AppAssure Core (se houver alguma), você verá as informações descritas na tabela a seguir.

Tabela 45. Informações sobre cada chave de criptografia

Elemento de UI	Descrição
Nome	O nome associado à chave de criptografia.
Impressão digital	Esse parâmetro é uma cadeia de caracteres gerada aleatoriamente com as 26 letras maiúsculas e minúsculas do alfabeto inglês, que ajuda a identificar exclusivamente cada chave de criptografia.
Status	Status descreve o ponto de origem de uma chave de criptografia e sua capacidade de ser aplicada. Uma chave de criptografia pode ter uma de duas condições de status possíveis: **Universal**. O status Universal é a condição padrão quando você cria uma chave de criptografia. Uma chave com o status Universal, combinada ao estado Bloqueado, indica que a chave pode ser aplicada a uma máquina protegida. Você não pode bloquear manualmente uma chave com o status Universal; em vez disso, você deve primeiro alterar seu status como descrito no procedimento Alterar o status da chave de criptografia. **Replicação.** Quando uma máquina protegida em um Core de origem possui criptografia ativada e os pontos de recuperação da máquina são replicados em um Core de destino, qualquer chave de criptografia usada na origem aparece automaticamente no Core de destino com o status de Replicação. O estado padrão após receber uma chave replicada é *bloqueado*. Para desbloquear uma chave de criptografia com o status de Replicação, forneça a frase de acesso. Quando a chave tem o status Desbloqueado, você pode bloqueá-la manualmente. Para obter mais informações, consulte o tópico Bloquear ou desbloquear uma chave de criptografia.

Tabela 45. Informações sobre cada chave de criptografia

Elemento de UI	Descrição
Estado	O estado indica se uma chave de criptografia pode ser usada. Os dois estados possíveis são: **Desbloqueado.** Um estado Desbloqueado indica que a chave pode ser usada imediatamente. Por exemplo, você pode criptografar snapshots de uma máquina protegida ou recuperar dados de um ponto de recuperação replicado no Core de destino. **Bloqueado.** Um estado Bloqueado indica que a chave não pode ser usada até ser desbloqueada por meio de uma frase de acesso. Bloqueado é o estado padrão de uma chave de criptografia recém-importada ou replicada. Quando o estado de uma chave de criptografia é Bloqueado, ela deve ser desbloqueada para ser usada. Se você tiver desbloqueado anteriormente uma chave de criptografia bloqueada e a duração de desbloqueio expirar, seu estado mudará de Desbloqueado para Bloqueado. Depois que a chave é bloqueada automaticamente, você deve desbloqueá-la novamente para usá-la. Para obter mais informações, consulte o tópico Bloquear ou desbloquear uma chave de criptografia.
Descrição	A descrição é um campo opcional, no qual recomendamos incluir informações úteis sobre a chave de criptografia, como o uso pretendido ou uma dica sobre a frase de acesso.

No nível superior do painel Chaves de criptografia, você pode adicionar uma chave de criptografia ou importar uma chave usando um arquivo exportado de outro AppAssure Core.

Uma vez que exista uma chave de criptografia em um Core, você pode gerenciar as chaves existentes, editando as propriedades de nome e descrição, alterando a frase de acesso, desbloqueando uma chave de criptografia bloqueada ou removendo a chave do AppAssure Core. Você também pode exportar uma chave para um arquivo, que pode ser importado para outro AppAssure Core.

Quando você adiciona uma chave de criptografia na guia Configuração, ela aparece na lista de chaves de criptografia, mas não é aplicada a uma máquina protegida específica. Para obter informações sobre como aplicar uma chave de criptografia que você criou no painel Chaves de criptografia ou excluir totalmente uma chave do AppAssure Core, consulte Aplicar ou remover criptografia de uma máquina protegida.

No painel Chaves de criptografia, para gerenciar a segurança dos dados de cópia de segurança de qualquer máquina protegida salvos no repositório do Core, faça o seguinte:

- Adicionar uma chave de criptografia
- Importar uma chave de criptografia
- Bloquear ou desbloquear uma chave de criptografia
- Editar uma chave de criptografia
- Alterar a frase de acesso de uma chave de criptografia
- Exportar uma chave de criptografia
- Remover uma chave de criptografia
- Alterar o status da chave de criptografia

Adicionar uma chave de criptografia

Depois de definir uma chave de criptografia, você pode usá-la para proteger seus dados. As chaves de criptografia podem ser usadas em qualquer número de máquinas protegidas.

Esta etapa descreve como adicionar uma chave de criptografia no AppAssure Core Console. Esse processo não aplica a chave a nenhuma máquina que esteja sendo protegida atualmente no Core. Você também pode adicionar uma chave de criptografia durante o processo de proteção de uma máquina. Para obter mais

informações sobre como adicionar criptografia como parte da proteção de uma máquina, consulte Proteger uma máquina. Para obter mais informações sobre como adicionar criptografia a duas ou mais máquinas ao protegê-las inicialmente, consulte Proteger várias máquinas.

Execute as etapas deste procedimento para adicionar uma chave de criptografia.

Para adicionar uma chave de criptografia

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida.

2 No menu suspenso Ações, selecione **Adicionar chave de criptografia**.

Aparece a caixa de diálogo Criar chave de criptografia.

3 Na caixa de diálogo Criar chave de criptografia, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 46. Criar detalhes da chave de criptografia.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 130 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console. Você pode inserir até 254 caracteres. É uma boa prática evitar o uso de caracteres proibidos e frases proibidas.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. É uma boa prática evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. Dell O suporte não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

4 Clique em **OK**.

A caixa de diálogo é fechada e a chave de criptografia criada fica visível na página Chaves de criptografia.

5 Para aplicar uma chave de criptografia a uma máquina protegida, consulte Aplicar uma chave de criptografia na guia Máquinas.

△ **CUIDADO: O AppAssure usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Importar uma chave de criptografia

Você pode importar uma chave de criptografia de outro AppAssure Core e usá-la para criptografar dados de uma máquina protegida no Core. Para importar a chave, é necessário que ela possa ser acessada pela máquina Core, localmente ou através da rede.

Execute as etapas deste procedimento para importar uma chave de criptografia.

NOTA: Este procedimento não aplica a chave a nenhuma máquina protegida. Para obter mais informações sobre a aplicação da chave, consulte Aplicar uma chave de criptografia na guia Máquinas.

Para importar uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

   A página Chaves de criptografia é exibida.

2. No menu suspenso Ações, selecione **Importar**.

   Aparece a caixa de diálogo Importar chave.

3. Na caixa de diálogo Importar chave, clique em **Procurar** para localizar a chave de criptografia que você deseja importar.

   O nome de arquivo da chave começa com "EncryptionKey-", seguido do ID da chave e terminando com a extensão .key. Um exemplo de nome de chave de criptografia é **EncryptionKey-RandomAlphabeticCharacters.key**.

4. Selecione a chave que você deseja importar e clique em **Abrir**.

5. Na caixa de diálogo Importar chave, clique em **OK**.

   A caixa de diálogo é fechada e a chave de criptografia importada fica visível na página Chaves de criptografia. Se a chave de criptografia foi usada para proteger um volume antes de ser exportada, o estado da chave é Bloqueado.

Bloquear ou desbloquear uma chave de criptografia

Chaves de criptografia podem estar em estado bloqueado ou desbloqueado. Uma chave de criptografia desbloqueada pode ser aplicada a uma máquina protegida para proteger os dados de cópia de segurança dessa máquina salvos no repositório. Em um AppAssure Core usando uma chave de criptografia desbloqueada, você também pode recuperar dados de um ponto de recuperação.

Quando você importa uma chave de criptografia para um AppAssure Core, o estado padrão é Bloqueado. Isso é verdadeiro quer você tenha importado a chave de criptografia explicitamente ou ela tenha sido adicionada ao AppAssure Core pela replicação de máquinas protegidas criptografadas ou pela importação de um arquivo de pontos de recuperação criptografados.

No caso de chaves de criptografia adicionadas ao AppAssure Core apenas por replicação, ao desbloquear uma chave, você pode especificar um período de tempo (em horas, dias ou meses) durante o qual ela continuará desbloqueada. Cada dia é baseado em um período de 24 horas começando no momento em que a solicitação de desbloqueio é salva no AppAssure Core. Por exemplo, se a chave for desbloqueada às 11h24 na terça-feira e a duração selecionada for de dois dias, a chave será bloqueada outra vez, automaticamente, às 11h24 de quinta-feira.

CUIDADO: Não é possível usar uma chave de criptografia bloqueada para recuperar dados nem aplicá-la a uma máquina protegida. Você deve primeiro fornecer a frase de acesso, desbloqueando assim a chave.

Você também pode bloquear uma chave de criptografia desbloqueada, garantindo que ela não possa ser aplicada a uma máquina protegida até ser desbloqueada. Para bloquear uma chave de criptografia com o estado Universal, é necessário primeiramente alterar o status para Replicado.

Se uma chave de criptografia desbloqueada está sendo usada atualmente para proteger uma máquina no Core, é preciso primeiro desassociá-la da máquina protegida para poder bloqueá-la.

Conclua as etapas deste procedimento para desbloquear uma chave de criptografia bloqueada.

Para desbloquear uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida. A coluna Estado indica quais chaves de criptografia estão bloqueadas.

2 No menu suspenso Configuração da chave de criptografia que você deseja desbloquear, selecione **Desbloquear**.

A caixa de diálogo Desbloquear chave aparece.

3 Na caixa de diálogo Desbloquear chave, no campo Frase de acesso, insira a frase de acesso para desbloquear esta chave.

4 Para especificar o período em que a chave permanecerá desbloqueada, na opção Duração, execute um destes procedimentos:

- Para especificar que a chave continuará desbloqueada até você bloqueá-la explicitamente, AppAssure selecione **Até ser esquecida explicitamente**.

  Essa opção está disponível para desbloquear qualquer chave de criptografia.

- Para especificar que a chave continuará bloqueada por um período de tempo configurado por você:

  - Selecione o campo numérico e, digitando ou usando as setas para cima e para baixo, especifique um número inteiro.
  - No campo de duração, selecione horas, dias ou meses, respectivamente.
  - Depois, clique em **OK**.

  Essa opção está disponível para chaves de criptografia adicionadas por replicação.

A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.

Conclua as etapas deste procedimento para bloquear uma chave de criptografia.

Para bloquear uma chave de criptografia desbloqueada

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida. A coluna Estado indica quais chaves de criptografia estão desbloqueadas e mostra o status de cada chave.

2 Se o status da chave de criptografia que você deseja desbloquear é Universal, no menu suspenso Configuração, selecione **Alterar o status de criptografia para Replicado**.

A caixa de diálogo Alterar status da chave de criptografia aparece.

3 Na caixa de diálogo Alterar status da chave de criptografia, confirme que deseja alterar o status da chave para Replicado.

4 Se você alterar com êxito o status da chave de criptografia para Replicado, no menu suspenso Configuração da chave de criptografia que você deseja bloquear, selecione **Bloquear**.

A caixa de diálogo Bloquear chave aparece.

5 Na caixa de diálogo Bloquear chave, confirme que deseja bloquear a chave.

A caixa de diálogo é fechada e o estado da chave de criptografia selecionada agora é bloqueado.

NOTA: Essa opção está disponível para chaves de criptografia adicionadas por replicação.

Editar uma chave de criptografia

Depois que uma chave de criptografia é definida, você pode editar o nome ou a descrição da chave. Essas propriedades aparecem quando você visualiza a lista de chaves de criptografia no painel Chaves de criptografia.

Execute as etapas deste procedimento para editar o nome ou a descrição de uma chave de criptografia existente.

△ **CUIDADO: Quando você edita o nome ou a descrição de uma chave de criptografia que é usada para proteger uma ou mais máquinas, o AppAssure cria uma nova imagem de base. O snapshot da imagem de base dessa máquina ocorre no próximo snapshot programado ou forçado.**

Para editar uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

   A página Chaves de criptografia é exibida.

2. No menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Editar**.

   Aparece a caixa de diálogo Editar chave de criptografia.

3. Na caixa de diálogo Editar chave de criptografia, edite o nome ou a descrição da chave de criptografia e clique em **OK**.

   A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.

Alterar a frase de acesso de uma chave de criptografia

Para manter máxima segurança, você pode alterar a frase de acesso de qualquer chave de criptografia existente. Execute as etapas deste procedimento para alterar a frase de acesso de uma chave de criptografia.

△ **CUIDADO: Quando você edita a frase de acesso de uma chave de criptografia que é usada para proteger uma ou mais máquinas, uma nova imagem de base da máquina é criada no próximo snapshot programado ou forçado.**

Para alterar a frase de acesso de uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

   A página Chaves de criptografia é exibida.

2. No menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Alterar frase de acesso**.

   Aparece a caixa de diálogo Alterar frase de acesso.

3. Na caixa de diálogo Alterar frase de acesso, insira a nova frase de acesso para a criptografia e depois insira novamente a frase de acesso para confirmar o que inseriu.

4. Clique em **OK**.

   A caixa de diálogo é fechada e a frase de acesso é atualizada.

△ **CUIDADO: O AppAssure usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Recomendamos que você proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Exportar uma chave de criptografia

Você pode exportar uma chave de criptografia de qualquer AppAssure Core com a finalidade específica de usá-la em outro Core. Quando você realiza esse procedimento, a chave é salva na pasta Downloads da conta de usuário do Windows ativa.

Execute as etapas deste procedimento para exportar uma chave de criptografia.

Para exportar uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.
2. No menu suspenso Configuração da chave de criptografia que você deseja exportar, selecione **Exportar**.

   Aparece a caixa de diálogo Exportar chave.
3. Na caixa de diálogo Exportar chave, clique em **Salvar arquivo** para salvar e armazenar as chaves de criptografia em um local seguro e clique em **OK**.

Remover uma chave de criptografia

Quando você remove uma chave de criptografia na guia Configuração, a chave é excluída do AppAssure Core.

Você não pode remover uma chave de criptografia que já esteja associada a uma máquina protegida. Você deve primeiramente visualizar as definições de criptografia de cada máquina protegida que use a chave e desassociar a chave de criptografia que deseja remover. Para obter mais informações, consulte o tópico Desassociar uma chave de criptografia de uma máquina protegida.

Execute as etapas deste procedimento para remover uma chave de criptografia.

Para remover uma chave de criptografia

1. Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.
2. No menu suspenso Configuração da chave de criptografia que você deseja remover, selecione **Remover**.

   Você verá uma mensagem confirmando a ação de remover a chave de criptografia.
3. Na caixa de diálogo Remover chave, confirme que deseja remover a chave de criptografia.

   NOTA: Remover uma chave de criptografia não remove a criptografia dos dados.

   A caixa de diálogo é fechada e a chave de criptografia removida não aparece mais na página Chaves de criptografia.

Alterar o status da chave de criptografia

Chaves de criptografia podem ter uma de duas condições de status no painel Chaves de criptografia: Universal ou Replicação. O status indica a origem provável da chave de criptografia e determina se você pode alterar seus detalhes ou sua frase de acesso. Esse atributos só podem ser modificados quando o status é Universal. Se for necessário modificar esses atributos em uma chave com status Replicado, será necessário alterar o status para Universal usando este procedimento. Quando você altera o status de uma chave de criptografia para Universal, ela é desbloqueada manualmente e pode ser usada para criptografar outras máquinas protegidas.

CUIDADO: É necessário saber a frase de acesso para alterar o status de Replicado para Universal.

As chaves de criptografia também têm dois estados possíveis: Bloqueado ou Desbloqueado. O estado determina se é possível aplicar uma chave de criptografia a uma máquina protegida ou restaurar dados de um ponto de recuperação criptografado. Você pode alterar o status de uma chave de criptografia manualmente apenas se o estado for Desbloqueado.

Quando você cria uma chave de criptografia, o status é Universal e o estado é Desbloqueado. Você pode usar essa chave imediatamente (por exemplo, para criptografar cópias de segurança de uma máquina protegida). No entanto, uma chave com status Universal não pode ser bloqueada manualmente. Se quiser bloquear manualmente uma chave de criptografia com o status Universal, você terá que alterar seu status para Replicado usando este procedimento.

Siga este procedimento para alterar o status de uma chave de criptografia.

Para alterar o status de uma chave de criptografia

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois selecione **Segurança**.

Todas as chaves de criptografia acessíveis ao Core aparecem no painel Chaves de criptografia. Cada uma tem um status Universal ou Replicado.

2 Para alterar o status de Universal, no menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Alterar o status para replicado**.

Você verá uma mensagem confirmando a ação de alterar o status da chave de criptografia.

3 Para alterar o status de Replicado, no menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Alterar o status para universal**.

Você verá uma mensagem confirmando a ação de alterar o status da chave de criptografia.

4 Insira a frase de acesso da chave de criptografia e clique em OK.

A caixa de diálogo é fechada e o status da chave de criptografia é atualizado na página Chaves de criptografia.

6

Proteger máquinas usando o AppAssure Core

Este capítulo descreve como proteger, configurar e gerenciar as máquinas protegidas em seu ambiente do AppAssure. Ele inclui as seguintes seções:

- Limitações de suporte para volumes dinâmicos e básicos
- Sobre o Agent Installer
- Implantação do Agent (instalação por push)
- Noções básicas sobre implantação em massa
- Noções básicas sobre programações de proteção
- Proteger uma máquina
- Proteger várias máquinas

Para proteger seus dados usando o AppAssure, é preciso adicionar as estações de trabalho e servidores para proteção no AppAssure Core Console; por exemplo, seu Exchange Server, SQL Server, servidor Linux e assim por diante.

No AppAssure Core Console, é possível identificar a máquina em que o software AppAssure Agent está instalado e especificar quais volumes proteger – por exemplo, um espaço de armazenamento do Microsoft Windows. É possível definir as programações de proteção, adicionar medidas adicionais de segurança, como criptografia, e muito mais. Para obter mais informações sobre como acessar o AppAssure Core Console para proteger estações de trabalho e servers, consulte Proteger uma máquina.

△ **CUIDADO: O AppAssure não oferece suporte a bare metal restores (BMRs) de máquinas Linux com partições de inicialização EXT2. Uma BMR realizada em uma máquina com esse tipo de partição resulta em uma máquina não inicializável. Se quiser realizar uma BMR dessa máquina no futuro, você terá que converter as partições EXT2 para EXT3 ou EXT4 antes de começar a proteger e criar cópias de segurança da máquina.**

Limitações de suporte para volumes dinâmicos e básicos

O AppAssure suporta a obtenção de snapshots de todos os volumes dinâmicos e básicos. O AppAssure também suporta a exportação de volumes dinâmicos simples que estão em um único disco físico. Como o próprio nome indica, os volumes dinâmicos simples não são volumes distribuídos, espelhados ou estendidos.

Discos dinâmicos (com exceção de discos dinâmicos simples, conforme descrito anteriormente) não estão disponíveis para seleção no Assistente de exportação. Volumes dinâmicos não simples têm geometrias de disco arbitrárias, que não podem ser totalmente interpretadas. Logo, o AppAssure não suporta a exportação de volumes dinâmicos complexos ou não simples.

Uma notificação aparece na interface do usuário para avisar que as exportações são limitadas e estão restritas a volumes dinâmicos simples. Se você tentar exportar algo que não seja um volume único simples, a tarefa de exportação falhará.

Sobre o Agent Installer

O AppAssure permite baixar instaladores a partir do AppAssure Core. Na guia Ferramentas, você pode optar por baixar o Agent Installer ou o Local Mount Utility (LMU). Para obter mais informações sobre o LMU, consulte Noções básicas do Local Mount Utility.

NOTA: Para acessar o Agent Installer, consulte Download do Agent Installer. Para obter mais informações sobre a implantação do Agent Installer, consulte o *Guia de instalação e atualização do Dell AppAssure*.

O Agent Installer é usado para instalar o aplicativo AppAssure Agent em máquinas que devem ser protegidas pelo AppAssure Core. Se você determinar que possui uma máquina que exige o Agent Installer, poderá baixar o instalador da Web a partir da guia Ferramentas do AppAssure Core.

NOTA: O download do Core é realizado a partir do Portal de licenças do Dell AppAssure. Para obter mais informações ou baixar o AppAssure Core installer, acesse https://licenseportal.com.

Download do Agent Installer

É possível baixar o AppAssure Agent Installer e implementá-lo em qualquer máquina que será protegida pelo AppAssure Core. Execute as etapas deste procedimento para baixar o instalador da Web.

Para baixar o AppAssure Agent Installer

1. Baixe o arquivo do AppAssure Agent installer no Portal de licenças do Dell AppAssure ou no AppAssure Core. Por exemplo:

   `Agent-X64-5.2.1.xxxxx.exe`

2. Clique em **Salvar arquivo**.

   Para obter mais informações sobre a instalação de agentes, consulte o *Guia de instalação e atualização do Dell AppAssure*.

Implantação do Agent (instalação por push)

O AppAssure permite implementar o AppAssure Agent Installer em máquinas Windows individuais para proteção. Execute as etapas do procedimento a seguir para enviar por push o instalador para um agente.

Para implementar agentes em várias máquinas ao mesmo tempo, consulte Implantar em várias máquinas.

NOTA: Os agentes devem ser configurados com uma política de segurança que possibilite a instalação remota.

Para implantar o agente

1. No AppAssure Core Console, na área de navegação à esquerda, clique em Máquinas protegidas para abrir a página Máquinas.
2. No menu suspenso **Ações**, clique em **Implementar Agent**.

   A caixa de diálogo Implementar Agent é exibida.
3. Na caixa de diálogo Implementar Agent, insira as definições de login, como descrito na tabela a seguir.

Tabela 47. Definições de login da máquina

Caixa de texto	Descrição
Máquina	Insira o nome de host ou o endereço IP da máquina agente que deseja implementar.
Nome de usuário	Insira o nome de usuário para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	Insira a senha para se conectar a essa máquina
Reinício automático após a instalação	Selecione para especificar se o Core deve iniciar após a conclusão da implementação e instalação do AppAssure Agent Installer.

4 Clique em **Confirmar** para validar as credenciais inseridas.

A caixa de diálogo Implementar Agent exibe uma mensagem para indicar que a validação está sendo realizada. Clique em **Abortar** se quiser cancelar o processo de confirmação. Após a conclusão do processo de confirmação, será exibida uma mensagem indicando que a confirmação foi concluída.

5 Clique em **Implementar**.

É exibida uma mensagem indicando que a implementação foi iniciada. É possível visualizar o progresso na guia Eventos. Clique em **Exibir detalhes** para visualizar mais informações sobre o status da implementação do agente.

6 Clique em **OK**.

Modificar definições de implantação

Execute as etapas deste procedimento para modificar as definições de implementação.

Para modificar as definições de implementação

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Definições de implementação, clique em **Alterar**.

A caixa de diálogo Definições de implementação é exibida.

3 Na caixa de texto Nome do Agent Installer, digite o nome do arquivo executável do agente. O padrão é Agent-web.exe.

4 Na caixa de texto Endereço do core, digite o endereço do core.

5 Na caixa de texto Falha no tempo limite de recebimento, insira o número de minutos a aguardar sem atividade antes do tempo limite.

6 Na caixa de texto Máximo de instalações paralelas, insira o número máximo de instalações que podem ser instaladas em paralelo.

7 Selecione uma ou ambas as seguintes definições opcionais:

- **Reinício automático após a instalação**
- **Proteger após implantação**

8 Clique em **OK**.

Noções básicas sobre implantação em massa

Este tópico descreve as tarefas que os administradores realizam para implantar o software AppAssure Agent simultaneamente em várias máquinas Windows. Esse recurso de processamento em lote é conhecido como recurso de implantação em massa.

Para implementar e proteger vários agentes, realize as seguintes tarefas:

1 Implante o AppAssure Agent em várias máquinas. Consulte Implantar em várias máquinas.

2 Monitorar a atividade de implementação em lote. Consulte Confirmar a implantação em várias máquinas.

3 Proteger várias máquinas. Consulte Proteger várias máquinas.

> **NOTA:** Essa etapa pode ser ignorada se você tiver selecionado a opção **Proteger máquina após instalação** durante a implementação.

4 Monitorar a atividade de proteção em lote. Consulte Monitorar a proteção de várias máquinas.

Implantar em várias máquinas

É possível simplificar a tarefa de implementar o software AppAssure Agent em várias máquinas com Windows usando o recurso de implementação em massa do Dell AppAssure. Do Core Console, é possível especificamente implementar em massa em:

- Máquinas em um domínio Active Directory
- Máquinas em um host virtual VMware vCenter/ESX(i)
- Máquinas em qualquer outro host

O recurso de implementação em massa detecta automaticamente as máquinas em um host e permite selecionar aqueles nas quais deseja implementar. Como alternativa, é possível inserir manualmente as informações de host e máquina.

> **NOTA:** É possível usar o recurso de implementação em massa para implementar o software do Agent em até 50 máquinas agente. As máquinas em que você está implantando devem ter acesso à Internet para baixar e instalar trechos do programa, visto que o AppAssure Core usa a versão para Web do AppAssure Agent Installer para implantar os componentes de instalação. Se o acesso à Internet não estiver disponível, você terá que baixar manualmente o AppAssure Agent Installer do Portal de licenças do Dell AppAssure e implantá-lo nas máquinas individuais que deseja proteger.
>
> Para obter mais informações, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.

Implantar em máquinas de um domínio Active Directory

Antes de iniciar este procedimento, é preciso ter as informações de domínio e credenciais de login para o server Active Directory.

Para implantar em máquinas de um domínio Active Directory

1 No AppAssure Core Console, clique na guia Ferramentas e depois em **Implementação em massa**.

2 No painel Implantar Agent nas máquinas, clique em **Active Directory**.

3 Na caixa de diálogo Conectar-se ao Active Directory, insira as informações de domínio e credenciais de login, conforme descrito na tabela a seguir.

Tabela 48. Informações e credenciais do domínio

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory.
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

4 Clique em **Conectar.**

5 Na caixa de diálogo Adicionar máquinas do Active Directory, selecione as máquinas em que deseja implantar o software AppAssure Agent e clique em **Adicionar**.

As máquinas adicionadas são exibidas no painel Implantar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

6 Como opção, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.

7 Verifique o ícone e a mensagem de status de cada máquina na página Implementar Agents em máquinas. Eles refletem a preparação de cada máquina para implementação, como segue:

- Ícone verde - o AppAssure pode se conectar à máquina e está pronto para ser implementado.
- Ícone amarelo - o AppAssure pode se conectar à máquina; contudo, o AppAssure Agent na máquina já está pareado com um AppAssure Core.
- Ícone vermelho - o AppAssure não pode se conectar à máquina. Isso talvez ocorra porque as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego, ou outro problema.

  NOTA: O software Agent não será implementado em nenhuma máquina com um ícone de status vermelho.

- Se a mensagem de status de cada máquina indicar que ela está pronta para implementação, vá para a Etapa 9.
- Como opção, se a mensagem de status mostrar um link Detalhes, clique em **Detalhes** para determinar se consegue corrigir o problema.

8 Para corrigir problemas relacionados a qualquer máquina que mostre um status vermelho, ou para habilitar a proteção automática, alterar as informações de porta ou autenticação, alterar o nome de exibição, especificar um repositório ou estabelecer uma chave de criptografia, clique em **Definições** na barra de ferramentas ou no link **Editar** ao lado da máquina e depois faça o seguinte:

a Na caixa de diálogo Editar definições, especifique as definições, como descrito na tabela a seguir.

Tabela 49. Definições do Active Directory

Caixa de texto	Descrição
Nome do host	Fornecido automaticamente da Etapa 3.
Nome de usuário	*Fornecido automaticamente da* Etapa 3.
Senha	*Insira a senha da máquina.*
Reinício automático após a instalação	Obrigatória. Reinicia a máquina após a implementação, o que é necessário antes de proteger qualquer máquina agente.
Proteger máquina após instalação	Selecionado por padrão. Se estiver selecionado, o sistema protegerá a máquina automaticamente após a implementação. (Isso permite ignorar Proteger várias máquinas.)
Nome de exibição	Atribuído automaticamente com base no nome de host fornecido na Etapa 3. Esse é o nome que aparece no Core Console da máquina selecionada.
Porta	O número da porta pela qual o AppAssure Core se comunica com o agente na máquina. A porta padrão é 8006.

Tabela 49. Definições do Active Directory

Caixa de texto	Descrição
Repositório	Use a lista suspensa para selecionar o repositório no AppAssure Core no qual os dados das máquinas especificadas devem ser armazenados. Essa opção está disponível apenas quando você seleciona **Proteger máquina após instalação**.
Chave de criptografia	(Opcional) Use a lista suspensa para especificar se a criptografia deve ser aplicada aos dados na máquina especificada. A chave de criptografia é atribuída a todas as máquinas que estão sendo protegidas. **NOTA:** Essa opção está disponível apenas quando você seleciona **Proteger máquina após instalação**.

b Clique em **Salvar**.

9 Após as máquinas serem confirmadas com êxito, selecione cada máquina para a qual deseja implementar o AppAssure Agent e clique em **Implementar**.

Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Implantar em máquinas de um host virtual VMware vCenter/ESX(i)

Antes de iniciar este procedimento, é preciso ter as informações de localização do host e credenciais de login do host virtual VMware vCenter/ESX(i).

NOTA: Todas as máquinas virtuais devem ter Ferramentas de VM instaladas; caso contrário, o AppAssure não consegue detectar o nome do host da máquina virtual na qual implementar. Em vez do nome do host, o AppAssure usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

Para implantar em máquinas de um host virtual vCenter/ESX(i)

1 Navegue até o AppAssure Core Console, clique na guia Ferramentas e depois em **Implementação em massa**.

2 Na janela Implementar Agent nas máquinas, clique em **vCenter/ESX(i)**.

3 Na caixa de diálogo Conectar-se ao vCenter Server/ESX(i), insira as informações de host e credenciais de login, conforme descrito a seguir, e clique em **Conectar**.

Tabela 50. Definições de conexão do vCenter/ESX(i)

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESX(i).
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao host virtual.

4 Na caixa de diálogo Adicionar máquinas do VMware vCenter Server/ESX(i), faça o seguinte:

a Em Opções, insira o nome de usuário e senha das máquinas virtuais selecionadas.

b Explore as máquinas, expandindo ou recolhendo os clusters, conjuntos de recursos, vApps e máquinas virtuais, por meio de cliques nas setas ao lado de cada nó.

c Selecione as máquinas às quais deseja implementar e clique em **Adicionar**.

As máquinas adicionadas são exibidas na janela Implementar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

5 Como opção, você pode confirmar qualquer máquina, o status da máquina ou editar as definições de conexão dela, como descrito na Etapa 6 à Etapa 8 do procedimento Implantar em máquinas de um domínio Active Directory.

6 Após as máquinas serem confirmadas com êxito, marque a caixa ao lado de cada máquina para a qual deseja implementar o AppAssure Agent e clique em **Implementar**.

Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Implantar nas máquinas de qualquer outro host

Conclua o procedimento a seguir para implantar o AppAssure Agent em várias máquinas de qualquer outro tipo de host.

Para implantar em máquinas de qualquer outro host

1 Navegue até o AppAssure Core Console, clique na guia Ferramentas e depois em **Implementação em massa**.

2 Na janela Implementar Agent nas máquinas, realize um dos procedimentos a seguir:

- Clique em **Novo** para inserir um novo host de máquina, credenciais de login, nome de exibição opcional, repositório, chave de criptografia e outras informações. Para obter detalhes de cada definição, consulte Implantar em máquinas de um domínio Active Directory.

  Após inserir essas informações, clique em **OK** para adicioná-las à lista Implementar Agent nas máquinas ou clique em **OK e Novo** para adicionar outra máquina.

  > **NOTA:** Se você quiser proteger automaticamente a máquina após a implementação, marque a caixa **Proteger máquina após instalação**. Se você marcar a caixa, a máquina será reiniciada automaticamente antes de ativar a proteção.

- Para especificar várias máquinas em uma lista, clique em **Manualmente**, insira os detalhes da máquina na caixa de diálogo Adicionar máquinas manualmente e clique em **Adicionar**. Para cada máquina, será preciso inserir o endereço IP ou nome da máquina, o nome de usuário, a senha separada por um delimitador de dois-pontos duplo e a porta, como mostrado no seguinte formato:

  ```
  hostname::username::password::port
  ```

  Por exemplo:

  ```
  10.255.255.255::administrator::&11@yYz90z::8006
  ```

  ```
  abc-host-00-1::administrator::99!zU$o83r::168
  ```

As máquinas adicionadas são exibidas na janela Implementar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

3 Como opção, você pode confirmar qualquer máquina, o status da máquina ou editar as definições de conexão dela, como descrito na Etapa 6 à Etapa 8 do procedimento Implantar em máquinas de um domínio Active Directory.

4 Após as máquinas serem confirmadas com êxito, marque a caixa ao lado de cada máquina para a qual deseja implementar o AppAssure Agent e clique em **Implementar**.

Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Confirmar a implantação em várias máquinas

Depois de fazer a implementação em massa do software AppAssure Agent em duas ou mais máquinas, poderá confirmar o êxito visualizando cada máquina agente relacionada no menu Máquinas protegidas.

Também é possível visualizar informações sobre o processo de implementação em massa na guia Eventos. Execute as etapas deste procedimento para confirmar a implementação.

Para confirmar a implementação em várias máquinas

1. Navegue até o AppAssure Core Console, clique na guia Eventos e em **Alertas**.
2. Navegue até a guia Início do AppAssure Core e clique na guia **Eventos**.

   Aparecem eventos de alerta na lista, mostrando a hora que o evento iniciou e uma mensagem. Para cada implementação bem-sucedida do software Agent, você verá um alerta indicando que a máquina protegida foi adicionada.
3. Como opção, clique em qualquer link de uma máquina protegida.

   A guia Resumo da máquina selecionada é exibida, mostrando informações pertinentes, incluindo:

   - O nome de host da máquina protegida
   - O último snapshot, se aplicável
   - O horário programado do próximo snapshot, com base na programação de proteção selecionada
   - A chave de criptografia, se houver, utilizada para esse agente protegido.
   - A versão do software Agent.

Noções básicas sobre programações de proteção

Uma programação de proteção define quando as cópias de segurança são transferidas de máquinas agente protegidas para o AppAssure Core.

As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas. É possível então modificar a programação existente a qualquer momento na guia Resumo de uma máquina agente específica.

NOTA: Para obter informações sobre a proteção de uma única máquina, consulte Proteger uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteger várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criar programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificar programações de proteção.

O AppAssure oferece uma programação de proteção padrão, que inclui um único período abrangendo todos os dias da semana, com um único período de tempo definido (das 0h00 às 23h59). O intervalo padrão (o período entre os snapshots) é de 60 minutos.

Quando a proteção é ativada pela primeira vez, a programação é ativada. Assim, ao usar as definições padrão, independentemente da hora do dia atual, a primeira cópia de segurança ocorrerá a cada hora cheia (0h, 1h, 2h, e assim por diante).

A primeira transferência de cópia de segurança salva no Core é chamada de snapshot de imagem de base. Todos os dados em todos os volumes especificados (incluindo o sistema operacional, aplicativos e definições) são salvos no Core. Subsequentemente, snapshots incrementais (cópias de segurança menores, contendo apenas os dados alterados na máquina protegida desde a última cópia de segurança) são salvos regularmente no Core com base no intervalo definido (por exemplo, a cada 60 minutos).

É possível criar uma programação personalizada para alterar a frequência de cópias de segurança. Por exemplo, uma alteração simples que pode ser feita é alterar o intervalo do período de dia da semana para 20 minutos, resultando em três snapshots a cada hora. Alternativamente, você pode aumentar o intervalo de 60 para 180 minutos nos fins de semana, quando há pouco tráfego, resultando em um snapshot a cada três horas.

Você também pode definir horários de pico e fora do pico. Por exemplo, se suas máquinas protegidas são mais usadas durante a semana, você pode definir o Período nº 1 para incluir apenas os dias de semana, desmarcando Sábado e Domingo no menu suspenso Período nº 1. Em seguida, selecione o Período nº 2, que automaticamente cobre o período de tempo não incluído no Período nº 1 (no caso, Sábado e Domingo). Você pode então aumentar o intervalo do segundo período para, por exemplo, 360 minutos, resultando em um snapshot a cada seis horas nos fins de semana e um snapshot por hora nos dias de semana.

Alternativamente, você pode alterar a programação padrão para definir horários diários de pico e fora do pico. Para fazer isso usando o assistente Programação de proteção, altere os horários padrão de início e término para um intervalo de tempo menor (por exemplo, das 0h00 às 16h59) e defina um intervalo adequado (por exemplo, 20 minutos). Isso representa cópias de segurança frequentes nos períodos de pico.

Em seguida, selecione **Período nº 2**, altere o intervalo de tempo para o período restante (17h00 às 23h59) e defina um intervalo apropriado (presumivelmente maior, como 180 minutos). Essas definições configuram um período fora do pico que vai das 17h00 à meia-noite todos os dias. Isso resulta em snapshots a cada três horas das 17h00 às 23h59 e snapshots a cada 20 minutos da meia-noite às 16h59.

Outras opções na página do Assistente de programação de proteção incluem a definição da hora de proteção diária. Isso resulta em uma única cópia de segurança diária no período definido (a definição padrão é 12h).

A opção de pausar inicialmente a proteção impede a ocorrência de uma imagem de base (e, de fato, impede todas as cópias de segurança) até que a proteção seja retomada explicitamente. Quando você estiver pronto para começar a proteger as suas máquinas com base na programação de proteção estabelecida, você deve retomar explicitamente a proteção. Para obter mais informações sobre a retomada da proteção, consulte Pausar e retomar a proteção. Como opção, caso queira proteger uma máquina imediatamente, você pode forçar um snapshot. Para obter mais informações, consulte Forçar um snapshot.

Proteger uma máquina

Este tópico descreve como começar a proteger os dados em uma única máquina especificada usando o Assistente de proteção de máquina.

NOTA: A máquina deve ter o software AppAssure Agent instalado para ser protegida. Você pode optar por instalar o software Agent antes deste procedimento ou implantá-lo na máquina de destino como parte da conclusão do Assistente de proteção de máquina. Para obter mais informações sobre a instalação do software Agent, consulte "Instalar o software AppAssure Agent" no *Guia de instalação e atualização doDell AppAssure*.

Se o software Agent não estiver instalado antes de proteger uma máquina, não será possível selecionar volumes específicos para proteção como parte desse assistente. Nesse caso, por padrão, todos os volumes na máquina agente serão incluídos para proteção.

O AppAssure suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas com Windows 8 e 8.1, e Windows 2012 e 2012 R2, que usam o Windows Recovery Environment (Windows RE).

Para proteger várias máquinas simultaneamente usando um único processo, consulte Proteger várias máquinas.

Ao adicionar proteção, é preciso definir as informações de conexão, como o endereço IP e a porta, e fornecer credenciais para a máquina que deseja proteger. Como opção, você pode fornecer um nome de exibição para aparecer no Core Console em vez do endereço IP. Se isso for alterado, o endereço IP da máquina protegida não

aparecerá quando você visualizar detalhes no Core Console. Defina também a programação de proteção da máquina.

Esse processo inclui etapas opcionais que podem ser acessadas se você selecionar uma configuração avançada. As opções avançadas incluem funções de repositório e criptografia. Por exemplo, você pode especificar um repositório existente do AppAssure para salvar snapshots ou criar um novo. Também é possível especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para ser aplicada aos dados dessa máquina salvos no Core.

O fluxo de trabalho do assistente pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, se o software AppAssure Agent estiver instalado na máquina que você deseja proteger, o assistente não solicitará que ele seja instalado. De forma semelhante, se um repositório já existir no Core, você não será solicitado a criar outro.

△ **CUIDADO: O AppAssure não oferece suporte a bare metal restores (BMRs) de máquinas Linux com partições de inicialização EXT2. Uma BMR realizada em uma máquina com esse tipo de partição resulta em uma máquina não inicializável. Se quiser realizar uma BMR dessa máquina no futuro, você terá que converter as partições EXT2 para EXT3 ou EXT4 antes de começar a proteger e criar cópias de segurança da máquina.**

Para proteger uma máquina

1 Se o software AppAssure Agent já estiver instalado na máquina que você deseja proteger, mas ela ainda não foi reiniciada, faça isso agora.

2 Na máquina do core, navegue até o AppAssure Core Console e, na barra de botões, clique em **Proteger**.

Aparece o Assistente de proteção de máquina.

3 Na página Bem-Vindo, selecione as opções de instalação apropriadas:

- Se não for preciso definir um repositório ou estabelecer a criptografia, selecione **Típico**.
- Se você precisar criar um repositório ou definir um repositório diferente para cópias de segurança da máquina selecionada, ou ainda se desejar estabelecer a criptografia usando o assistente, selecione **Avançado (exibir etapas opcionais)**.
- Como opção, se você não quiser ver a página Bem-Vindo do Assistente de proteção de máquina no futuro, selecione a opção **Ignorar a página Bem-Vindo na próxima vez que o assistente for aberto**.

4 Quando estiver satisfeito com suas seleções na página Bem-Vindo, clique em **Avançar**.

A página Conexão é exibida.

5 Na página Conexão, insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 51. Definições de conexão da máquina

Caixa de texto	Descrição
Host	O nome de host ou endereço IP da máquina que deseja proteger.
Porta	O número da porta pela qual o AppAssure Core se comunica com o Agent na máquina. O número de porta padrão é 8006.
Nome de usuário	O nome de usuário utilizado para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar à máquina.

6 Se a página Atualizar Agent aparecer em seguida no Assistente de proteção de máquina, isso significa que uma versão mais antiga do software AppAssure Agent está instalada na máquina a ser protegida. Realize um dos procedimentos a seguir e, em seguida, clique em **Avançar**:

- Para implantar a nova versão do software Agent (correspondendo à versão do AppAssure Core), selecione **Atualizar o Agent para a versão mais recente do software**.

- Para continuar protegendo a máquina sem atualizar a versão do software Agent, desmarque a opção **Atualizar o Agent para a versão mais recente do software**.

7 Se a página Proteção for exibida em seguida no Assistente de proteção de máquina, vá para a Etapa 8.

Se a página Instalar Agent aparecer em seguida no Assistente de proteção de máquina, isso indicará que o software Agent ainda não está instalado na máquina designada. Clique em **Avançar** para instalar o software Agent.

> **NOTA:** O software Agent deve ser instalado na máquina que você deseja proteger, e a máquina deve ser reiniciada antes que possa fazer a cópia de segurança no Core. Para fazer o instalador reiniciar a máquina protegida, selecione a opção **Após a instalação, reiniciar a máquina automaticamente (recomendado)** antes de clicar em **Avançar**.

A página Proteção é exibida.

8 Opcionalmente, se você quiser um nome que não seja o endereço IP para ser exibido no AppAssure Core Console para essa máquina protegida, no campo Nome de exibição, digite um nome na caixa de diálogo.

Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico caracteres proibidos. Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico frases proibidas.

9 Selecione a programação de proteção apropriada, conforme descrito a seguir. Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão**.

Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a guia Resumo da máquina protegida específica.

- Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

10 Prossiga com a configuração da seguinte maneira:

- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.

  Da primeira vez que a proteção for adicionada a uma máquina, a imagem de base (isto é, um snapshot de todos os dados dos volumes protegidos) será transferida para o repositório no AppAssure Core de acordo com a programação definida, a não ser que tenha sido especificado pausar inicialmente a proteção.

- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** para definir uma programação de proteção personalizada. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.

- Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina, além da proteção padrão, clique em **Avançar** e vá para a Etapa 14 para ver as opções de repositório e criptografia.

- Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e vá para a Etapa 11 para escolher os volumes a proteger.

11 Na página Volumes de proteção, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

> **NOTA:** Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

12 Na página Programação de proteção, defina uma programação de proteção personalizada e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.

13 Se as informações de repositório já estiverem configuradas, a página Criptografia aparecerá. Siga para a Etapa 19

14 Na página Repositório, realize um dos procedimentos a seguir:

- Se você deseja armazenar os dados dessa máquina para proteção em um repositório existente, selecione **Utilizar um repositório existente**, selecione o repositório apropriado na lista e clique em **Avançar**.

  A página Criptografia é exibida. Como opção, vá para a Etapa 19 para definir a criptografia.

- Se você deseja criar um novo local de armazenamento no Core, faça o seguinte:

  a Selecione **Criar um repositório**.

  b Na página Repositório, no campo **Nome**, especifique o nome do repositório que deseja criar.

  Em geral é a palavra Repositório e um número de índice, que corresponde ao número do novo repositório (por exemplo, **Repository1**). Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres. Esse nome precisa ser exclusivo desse core.

  NOTA: Ao especificar o nome do repositório, use somente caracteres alfanuméricos ou o hífen. Nenhum outro símbolo ou caractere de pontuação é permitido. Não use combinações de letras que especificam comandos ou palavras reservadas (como con, prn, aux ou null) ou que representam portas (como com ou lpt).

  c No campo **Local**, insira um caminho de diretório para o repositório. Por exemplo, em um computador local, digite **C:\Repository**. Esse local precisa ser exclusivo desse core. Se você estiver armazenando o repositório em uma unidade compartilhada, insira no formato \\servidor\compartilhamento.

CUIDADO: Se você excluir o repositório no futuro, o programa Instalador removerá todo o conteúdo do caminho do repositório. Por esse motivo, não crie o local de armazenamento na raiz (por exemplo, c:\), o que pode resultar na perda de todos os dados armazenados no volume.

  d Se o repositório for armazenado em um volume compartilhado, no campo **Nome de usuário**, insira o nome de usuário com privilégios para acessar a unidade compartilhada e, no campo **Senha**, insira a senha desse usuário.

  e No campo **Caminho de metadados**, insira o caminho onde deseja que os metadados sejam armazenados. Esse deve ser um subdiretório do local de armazenamento. Por exemplo, se o local de armazenamento for C:\Repository, digite **C:\Repository\Metadata**. Esse precisa ser um caminho exclusivo desse core.

15 Depois de inserir todos os dados necessários na página Repositório, clique em **Avançar**.

A página Configuração do repositório é exibida.

16 Especifique o tamanho do repositório.

NOTA: Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB.

Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB.

Para que o AppAssure valide o local do armazenamento, o Windows Management Instrumentation (WMI) deve estar instalado e acessível no sistema operacional que hospeda o AppAssure Core.

17 Para especificar bytes por setor, bytes por registro ou controlar a política de cache de gravação, selecione **Exibir opções avançadas** e, em seguida, insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 52. Opções avançadas para armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

18 Quando estiver satisfeito com as informações de configuração do repositório inseridas, clique em **Avançar**.

A página Criptografia é exibida.

19 Como opção, para habilitar a criptografia, na página Criptografia, selecione **Habilitar criptografia**.

O campo Chave de criptografia é exibido na página Criptografia.

NOTA: Se você habilitar a criptografia, ela será aplicada a dados de todos os volumes protegidos para essa máquina agente.

É possível alterar as definições mais tarde na guia Configuração no AppAssure Core Console.

Para obter mais informações sobre criptografia, consulte o tópico Noções básicas sobre chaves de criptografia.

CUIDADO: O AppAssure usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

20 Caso queira criptografar essa máquina protegida usando uma chave de criptografia já definida nesse AppAssure Core, selecione **Criptografar dados usando uma chave de criptografia existente** e selecione a chave apropriada no menu suspenso.

Vá para a Etapa 22.

21 Caso queira adicionar uma nova chave de criptografia ao Core e aplicá-la a essa máquina protegida, insira as informações conforme descrito na tabela a seguir.

Tabela 53. Definições de chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 130 caracteres alfanuméricos. Não é possível incluir caracteres especiais, como barra, barra invertida, barra vertical, ponto e vírgula, asterisco, aspas, ponto de interrogação, colchetes, e comercial ou cerquilha.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. É uma boa prática evitar o uso dos caracteres especiais relacionados acima. Armazene a frase de acesso em um local seguro. Dell O suporte não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso que você acabou de inserir.

22 Clique em **Concluir** para salvar e aplicar suas definições.

Da primeira vez que a proteção for adicionada a uma máquina, a imagem de base (isto é, um snapshot de todos os dados dos volumes protegidos) será transferida para o repositório no AppAssure Core de acordo com a programação definida, a não ser que tenha sido especificado pausar inicialmente a proteção.

Criar programações de proteção personalizadas

Ao definir a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de várias máquinas, é preciso definir uma programação de proteção.

A programação de proteção padrão inclui um único período abrangendo todos os dias da semana. O intervalo de tempo padrão é das 0h00 às 23h59, abrangendo um período total de 24 horas. O intervalo padrão é de 60 minutos.

Usando o assistente, é possível personalizar as programações de proteção, podendo escolher entre períodos ou um período de proteção diário.

A seleção de períodos permite visualizar a programação de proteção padrão e fazer os ajustes necessários. A seleção de um período de proteção diário faz o AppAssure efetuar a cópia de segurança das máquinas protegidas designadas uma vez por dia em um horário especificado.

Ao usar períodos, você pode fazer alterações simples na programação de proteção padrão. Por exemplo, talvez você queira simplesmente alterar o intervalo na programação padrão de dias da semana para 20 minutos, resultando em cópias de segurança três vezes por hora em vez de uma vez por hora, ou para 180 minutos, resultando em uma cópia de segurança a cada três horas.

É possível criar também programações de proteção mais complexas. Por exemplo, é possível criar períodos de pico para os dias úteis e períodos fora do pico nos fins de semana, como descrito em Noções básicas sobre programações de proteção.

Finalmente, ao proteger uma ou várias máquinas usando o assistente, é possível inicialmente pausar a proteção, o que define a programação de proteção sem iniciá-la. Quando você estiver pronto para começar a proteger as suas máquinas com base na programação de proteção estabelecida, você deve retomar explicitamente a proteção. Para obter mais informações sobre a retomada da proteção, consulte Pausar e retomar a proteção. Como opção, caso queira proteger uma máquina imediatamente, você pode forçar um snapshot. Para obter mais informações, consulte Forçar um snapshot.

NOTA: Para obter informações conceituais sobre programações de proteção, consulte Noções básicas sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteger uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteger várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criar programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificar programações de proteção.

Execute as etapas deste procedimento para criar programações personalizadas para a proteção de dados em máquinas agente ao definir a proteção usando um assistente.

Para criar programações personalizadas

1 Na página Programação de proteção do Assistente de proteção de máquina ou do Assistente de proteção de diversas máquinas, para alterar a programação de intervalo para qualquer período, faça o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados. Os campos editáveis incluem hora inicial, hora final e intervalo (em minutos) de cada período.

   b Clique no campo de intervalo e digite um intervalo adequado em minutos.

   Por exemplo, destaque o intervalo existente e substitua-o pelo valor **20** para realizar snapshots a cada 20 minutos durante esse período.

2 Para criar um período de pico e fora do pico nos dias da semana, altere o intervalo de tempo do período em dias da semana para que ele não inclua um período de 24 horas, defina um intervalo ideal para o pico, selecione **Tirar snapshots no período restante** e defina um intervalo fora do pico, fazendo o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados.

   b Clique na caixa **De** para alterar a hora inicial desse período.

   A caixa de diálogo Selecionar hora é exibida.

   c Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

   Por exemplo, arraste o controle Horas para exibir o horário de 8h00.

   d Clique na caixa **A** para alterar a hora final desse período.

   A caixa de diálogo Selecionar hora é exibida.

   e Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

   Por exemplo, arraste o controle Horas para exibir o horário 04:59 AM

3 Para definir uma única hora do dia para uma única cópia de segurança diária, selecione **Tempo de proteção diária** e insira a hora no formato HH:MM. Por exemplo, para fazer uma cópia de segurança diária às 21h, insira 21:00.

4 Para definir a programação sem iniciar as cópias de segurança, selecione **Pausar proteção inicialmente**.

   Depois que a proteção é pausada no assistente, ela permanece em pausa até que você a retome explicitamente. Depois de retomar a proteção, as cópias de segurança ocorrerão com base na programação estabelecida. Para obter mais informações sobre a retomada da proteção, consulte Pausar e retomar a proteção.

5 Quando estiver satisfeito com as alterações feitas na sua programação de proteção, clique em **Concluir** ou **Avançar**, conforme o caso. Retorne ao procedimento do assistente apropriado para concluir os requisitos restantes.

Modificar programações de proteção

Uma programação de proteção define quando as cópias de segurança são transferidas de máquinas agente protegidas para o AppAssure Core. As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.

É possível modificar a programação de proteção existente a qualquer momento na guia Resumo de uma máquina agente específica.

NOTA: Para obter informações conceituais sobre programações de proteção, consulte Noções básicas sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteger uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteger várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criar programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificar programações de proteção.

Execute as etapas deste procedimento para modificar uma programação de proteção existente para volumes de uma máquina protegida.

Para modificar programações de proteção

1 Navegue até o AppAssure Core Console.

2 Na lista de máquinas protegidas, selecione a máquina com uma programação de proteção definida que você deseja alterar.

A guia Resumo é exibida para a máquina.

3 Selecione os volumes da máquina protegida que você deseja alterar e clique em **Definir uma programação**. Para selecionar todos os volumes de uma só vez, clique na caixa de seleção na linha de cabeçalho.

Inicialmente, todos os volumes compartilham a mesma programação de proteção. Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

A caixa de diálogo Programação de proteção é exibida.

4 Na caixa de diálogo Programação de proteção, se você já tiver criado um modelo de programação de proteção e quiser aplicá-lo a esse agente, selecione o modelo na lista suspensa e depois vá para a Etapa 10.

5 Se você quiser salvar essa nova programação de proteção como um modelo, insira um nome para o modelo na caixa de texto.

6 Se você quiser remover um período existente da programação, desmarque as caixas de seleção ao lado de cada opção de período. Entre as opções estão:

- **Seg.-Sex.** Esse intervalo de tempo indica uma semana típica de cinco dias de trabalho.
- **Sáb.-Dom.** Esse intervalo de tempo indica um fim de semana típico.

7 Se a hora inicial e final do dia da semana forem 0h a 23h59, existe um único período. Para alterar a hora inicial e final de um período definido, faça o seguinte:

a Selecione o período adequado.

b Clique na caixa **Hora inicial** para alterar a hora inicial desse período.

A caixa de diálogo Selecionar hora é exibida.

c Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

Por exemplo, arraste o controle Horas para exibir o horário de 8h00.

d Clique na caixa **Hora final** para alterar a hora final desse período.

A caixa de diálogo Selecionar hora é exibida.

e Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

Por exemplo, arraste o controle Horas para exibir o horário 04:59 AM

f Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período de pico, altere o intervalo de 60 para 20 minutos para tirar snapshots três vezes por hora.

8 Se um período diferente de 0h a 23h59 tiver sido definido no Etapa 7, então se desejar que as cópias de segurança ocorram nos intervalos de tempo restantes, será preciso adicionar períodos adicionais para definir a proteção, fazendo o seguinte:

a Clique em **+ Adicionar período.**

Sob a categoria apropriada (dias de semana ou fins de semana), um novo período aparece. Se o primeiro período começou depois de 0h, o AppAssure inicia automaticamente esse período à 0h. De acordo com o exemplo acima, esse segundo período inicia à 0h. Pode ser necessário ajustar horas ou minutos das horas inicial e final.

b Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial ou final, conforme o caso.

Por exemplo, defina a hora inicial em 0h e a hora final em 7h59.

c Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período fora do pico, altere o intervalo de 60 para 120 minutos para tirar snapshots a cada duas horas.

9 Se necessário, continue a criar períodos adicionais, definindo horas iniciais e finais e intervalos conforme apropriado.

NOTA: Se você quiser remover um período que adicionou, clique no **X** na extrema direita desse período. Caso tenha sido um erro remover o período, clique em **Cancelar**.

10 Quando sua programação de proteção atender às suas necessidades, clique em **Aplicar**.

A caixa de diálogo Programação de proteção é fechada.

Pausar e retomar a proteção

Ao pausar a proteção, você interrompe temporariamente todas as transferências de dados da máquina selecionada para o AppAssure Core. Ao retomar a proteção, o AppAssure Core segue os requisitos da programação de proteção, fazendo a cópia de segurança de seus dados regularmente com base nessa programação.

É possível pausar a proteção de qualquer máquina agente do AppAssure:

- Ao estabelecer a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.
- No menu Máquinas protegidas na área de navegação à esquerda do AppAssure Core (pausando a proteção de todos os agentes).
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Em uma máquina protegida específica no menu Máquinas protegidas.
- Na guia Resumo de qualquer máquina agente protegida.

Se você pausar a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas, ela será pausada até ser retomada explicitamente.

Se você pausar a proteção fora de um assistente, poderá escolher se quer fazer isso até ela ser retomada ou por um período designado (especificado em qualquer combinação de dias, horas e minutos). Se você pausar por um período, quando esse tempo acabar, o sistema retomará automaticamente a proteção com base na programação de proteção.

É possível retomar a proteção de qualquer agente do AppAssure em pausa:

- No menu Máquinas protegidas na área de navegação à esquerda do AppAssure Core (retomando a proteção de todos os agentes).
- Em uma máquina protegida específica no menu Máquinas protegidas.
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Na guia Resumo de qualquer máquina agente protegida.

Use o procedimento a seguir para pausar ou retomar a proteção, conforme o caso.

Para pausar e retomar a proteção

1 No AppAssure Core Console, para pausar ou retomar a proteção de todas as máquinas, clique no menu suspenso **Máquinas protegidas** na área de navegação à esquerda.

- Caso queira pausar a proteção, faça o seguinte:

  a Selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

  - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
  - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

- Caso queira retomar a proteção, faça o seguinte:

  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para todas as máquinas.

2 Para pausar ou retomar a proteção de uma única em qualquer guia, na área de navegação à esquerda, na lista de máquinas protegidas, clique na seta à direita da máquina que deseja operar.

- Caso queira pausar a proteção, faça o seguinte:

  a Selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

  - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
  - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

- Caso queira retomar a proteção, faça o seguinte:

  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.

3 Para pausar ou retomar a proteção de uma única máquina na guia Resumo, navegue até a máquina que deseja operar.

A guia Resumo é exibida para a máquina selecionada.

- Caso queira pausar a proteção, faça o seguinte:
  a No menu suspenso **Ações** dessa máquina, selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

  - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
  - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.
- Caso queira retomar a proteção, faça o seguinte:
  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.

Proteger várias máquinas

É possível adicionar simultaneamente duas ou mais máquinas do Windows para proteção no AppAssure Core usando o Assistente de proteção de diversas máquinas. Esse recurso é chamado de proteção em massa.

Como na proteção de máquinas individuais, a proteção em massa exige que o software AppAssure Agent seja instalado em cada máquina que você deseja proteger e que a máquina seja reiniciada após a instalação do software Agent. Há mais de um método de implementar o software Agent em várias máquinas simultaneamente. Por exemplo:

- É possível instalar o software AppAssure Agent em diversas máquinas usando o recurso de implantação em massa, acessado na guia Ferramentas. (Se você tiver selecionado **Proteger máquina após instalação** quando implementou o Agent, poderá ignorar este procedimento.) Para obter mais informações sobre o uso de implementação em massa, consulte Implantar em várias máquinas.
- É possível implantar o software AppAssure Agent como parte desse assistente.

NOTA: As máquinas protegidas devem ser configuradas com uma política de segurança que possibilite a instalação remota.

Esse processo inclui etapas opcionais que podem ser acessadas se você selecionar uma configuração avançada. As opções avançadas incluem funções de repositório e criptografia. Por exemplo, você pode especificar um repositório existente do AppAssure para salvar snapshots ou criar um novo. Também é possível especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para ser aplicada aos dados dessa máquina salvos no Core.

O fluxo de trabalho do Assistente de proteção de diversas máquinas pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, se o software AppAssure Agent estiver instalado nas máquinas que você deseja proteger, o assistente não solicitará a sua instalação. De forma semelhante, se um repositório já existir no Core, você não será solicitado a criar outro.

Para proteger várias máquinas

1 Se o software AppAssure Agent já estiver instalado nas máquinas que deseja proteger, mas elas ainda não foram reiniciadas, faça isso agora.

2 Na máquina do Core, navegue até o AppAssure Core Console, clique no menu suspenso ao lado do ícone Proteger e selecione **Proteção em massa**.

Aparece o Assistente de proteção de diversas máquinas.

3 Na página Bem-Vindo, selecione as opções de instalação apropriadas:

- Se não for preciso definir um repositório ou estabelecer a criptografia, selecione **Típico**.
- Se você precisar criar um repositório ou definir um repositório diferente para cópias de segurança das máquinas selecionadas, ou ainda se desejar estabelecer a criptografia usando o assistente, selecione **Avançado (exibir etapas opcionais)**.
- Como opção, se você não quiser ver a página Bem-Vindo do Assistente de proteção de máquina no futuro, selecione a opção **Ignorar a página Bem-Vindo na próxima vez que o assistente for aberto**.

4 Quando estiver satisfeito com suas seleções na página Bem-Vindo, clique em **Avançar**.

A página Conexão é exibida.

5 Selecione o método adequado para identificar as máquinas que você deseja adicionar para a proteção.

As máquinas devem estar operando e acessíveis para conexão a elas. Para obter uma conexão bem-sucedida utilizando o Active Directory, a proteção em massa e a implementação em massa devem ser mais bem-sucedidas se conectadas nas máquinas como o administrador do domínio.

- Para identificar as máquinas que deseja proteger em um domínio Active Directory, selecione **Conectar-se ao Active Directory**, insira as credenciais, como descrito na tabela a seguir, e clique em **Avançar**. Vá para Etapa 7.
- Para identificar as máquinas que deseja proteger em um host virtual VMware vCenter/ESX(i), selecione **Conectar-se ao vCenter/ESX(i)**, insira as credenciais, como descrito na tabela a seguir, e clique em **Avançar**. Vá para Etapa 7.

Tabela 54. Credenciais do vCenter/ESX(i)

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory ou do host virtual VMware vCenter Server/ESX(i).
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

> **NOTA:** Todas as máquinas virtuais devem ter Ferramentas de VM instaladas. Caso contrário, o AppAssure não consegue detectar o nome do host da máquina virtual na qual implementar o software do Agent, e não poderá protegê-la. Em vez do nome do host, o AppAssure usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

- Para adicionar as máquinas manualmente, selecione **Adicionar as máquinas manualmente** e clique em **Avançar**.

Aparece a página Máquinas.

6 Na página Máquinas, para especificar as máquinas manualmente, digite os detalhes da conexão de cada máquina em uma linha separada e depois clique em **Avançar**. Utilize o seguinte formato:

```
host::login::senha::porta
```

> **NOTA:** O parâmetro da porta é opcional. Se omitido, será utilizada a porta 8006 por padrão. Se você desejar especificar uma porta diferente da 8006, então é necessário incluir esse parâmetro.

7 Na página Máquinas, para especificar as máquinas identificadas de um domínio Active Directory ou de um host virtual VMware vCenter/ESX(i), selecione na lista cada máquina apropriada que deseja proteger. Certifique-se de que desmarcou a opção da caixa de seleção para qualquer máquina que você não deseja proteger nesse momento. Quando estiver satisfeito, clique em **Avançar**.

   O sistema confirma todas as máquinas que você adicionou automaticamente.

8 Se a página Proteção for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 12.

   Se o software Agent ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página Avisos de máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

9 Como opção, na página Avisos de máquinas, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.

10 Como opção, na página Avisos de máquinas, selecione **Após a instalação do Agent, reiniciar as máquinas automaticamente**.

   NOTA: A Dell recomenda essa opção. Reinicie as máquinas agente antes de protegê-las.

11 Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

   A página Proteção é exibida.

12 Na página Proteção, selecione a programação de proteção adequada, como descrito a seguir.

   - Se desejar usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (snapshots horários de todos os volumes)**.
   - Se desejar definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada** e clique em **Avançar**.

13 Prossiga com a configuração da seguinte maneira:

   - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de diversas máquinas, além da proteção padrão, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
   - Se a configuração Típico para o Assistente de proteção de diversas máquinas e a proteção personalizada específica tiverem sido selecionadas, na página Proteção, clique em **Avançar**, e na página Programação de proteção, defina uma programação personalizada conforme descrito no tópico Criar programações de proteção personalizadas, e clique em **Concluir** para confirmar suas escolhas, feche o assistente e proteja as máquinas especificadas.
   - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina, clique em **Avançar** e vá para a Etapa 14 a fim de ver as opções de repositório e criptografia.

14 Na página Repositório, se você deseja armazenar os dados de todas as máquinas especificadas para proteção em um repositório existente, selecione **Utilize um repositório existente**, selecione o repositório apropriado na lista e clique em **Avançar** e prossiga para Etapa 19.

   Se você deseja criar um novo local de armazenamento no Core, faça o seguinte:

   a Selecione **Criar um repositório**.

   b Na página Repositório, no campo **Nome**, especifique o nome do repositório que deseja criar.

      Em geral é a palavra Repositório e um número de índice, que corresponde ao número do novo repositório (por exemplo, **Repository1**). Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres. Esse nome precisa ser exclusivo desse core.

      NOTA: Ao especificar o nome do repositório, use somente caracteres alfanuméricos ou o hífen. Nenhum outro símbolo ou caractere de pontuação é permitido. Não use combinações de letras que especificam comandos ou palavras reservadas (como con, prn, aux ou nul) ou que representam portas (como com ou lpt).

c No campo **Local**, insira um caminho de diretório para o repositório. Por exemplo, em um computador local, digite **C:\Repository**. Esse local precisa ser exclusivo desse core. Se você estiver armazenando o repositório em uma unidade compartilhada, insira no formato \\servidor\compartilhamento.

△ **CUIDADO: Se você excluir o repositório no futuro, o programa Instalador removerá todo o conteúdo do caminho do repositório. Por esse motivo, não crie o local de armazenamento na raiz (por exemplo, c:\), o que pode resultar na perda de todos os dados armazenados no volume.**

d Se o repositório for armazenado em um volume compartilhado, no campo **Nome de usuário**, insira o nome de usuário com privilégios para acessar a unidade compartilhada e, no campo **Senha**, insira a senha desse usuário.

e No campo **Caminho de metadados**, insira o caminho onde deseja que os metadados sejam armazenados. Esse deve ser um subdiretório do local de armazenamento. Por exemplo, se o local de armazenamento for C:\Repository, digite **C:\Repository\Metadata**. Esse precisa ser um caminho exclusivo desse core.

15 Depois de inserir todos os dados necessários na página Repositório, clique em **Avançar**.

A página Configuração do repositório é exibida.

16 Especifique o tamanho do repositório.

ⓘ **NOTA:** Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB.

Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB.

Para que o AppAssure valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.

17 Para especificar bytes por setor, bytes por registro ou controlar a política de cache de gravação, selecione **Exibir opções avançadas** e, em seguida, insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 55. Opções avançadas para armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

18 Quando estiver satisfeito com as informações de configuração do repositório inseridas, clique em **Avançar**.

A página Criptografia é exibida.

19 Como opção, para habilitar a criptografia, na página Criptografia, selecione **Habilitar criptografia**.

O campo Chave de criptografia é exibido na página Criptografia.

NOTA: Se você habilitar a criptografia, ela será aplicada a dados de todos os volumes protegidos das máquinas especificadas para proteção. É possível alterar as definições mais tarde na guia Configuração no AppAssure Core Console. Para obter mais informações sobre criptografia, consulte Noções básicas sobre chaves de criptografia.

CUIDADO: O AppAssure usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

20 Caso queira criptografar essas máquinas protegidas usando uma chave de criptografia já definida nesse AppAssure Core, selecione **Criptografar dados usando uma chave de criptografia existente** e selecione a chave apropriada no menu suspenso.

Vá para a Etapa 22.

21 Caso queira adicionar uma nova chave de criptografia ao Core e aplicá-la a essas máquinas protegidas, insira as informações conforme descrito na tabela a seguir.

Tabela 56. Definições de chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 130 caracteres alfanuméricos. Não é possível incluir caracteres especiais, como barra, barra invertida, barra vertical, ponto e vírgula, asterisco, aspas, ponto de interrogação, colchetes, e comercial ou cerquilha.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. É uma boa prática evitar o uso dos caracteres especiais relacionados acima. Armazene a frase de acesso em um local seguro. Dell O suporte não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso que você acabou de inserir.

22 Clique em **Concluir** para salvar e aplicar suas definições.

O assistente é fechado. O software AppAssure Agent é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Monitorar a proteção de várias máquinas

É possível monitorar o progresso à medida que o AppAssure aplica as programações e políticas de proteção às máquinas.

Para monitorar a proteção de várias máquinas

- No AppAssure Core Console, navegue até a guia AppAssure **Início** e clique na guia **Eventos**.

  A guia Eventos é exibida, dividida em Tarefas, Alertas e Eventos. À medida que os volumes são transferidos, o status e as horas inicial e final são exibidos no painel Tarefas.

  Também é possível filtrar as tarefas por status (ativa, em espera, concluída e com falha). Para obter mais informações, consulte Visualizar tarefas.

  > **NOTA:** Para ver apenas as tarefas que estão esperando para serem realizadas, certifique-se de selecionar o ícone Tarefas em espera.

  À medida que cada máquina protegida é adicionada, um alerta é registrado no log, relacionando se a operação foi bem-sucedida ou se foram registrados erros no log. Para obter mais informações, consulte Visualizar alertas.

  Para obter informações sobre visualização de todos os eventos, consulte Visualizar todos os eventos.

7

Gerenciar servidores Microsoft Exchange e SQL

Este capítulo descreve como configurar e gerenciar a proteção de servidores Microsoft Exchange e SQL no seu ambiente de AppAssure. Ele inclui as seguintes seções:

- Configurar definições de Exchange e SQL Server
- Gerenciar a capacidade de anexação do SQL e o truncamento de log
- Gerenciar verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log

As opções específicas para o Exchange Server e o SQL Server são exibidas no AppAssure Core Console quando uma instância do software e bancos de dados associados são detectados em servers protegidos. Esta seção inclui os seguintes tópicos específicos para o gerenciamento de máquinas protegidas que utilizam o Exchange Server ou o SQL Server:

Esta seção inclui os seguintes tópicos:

- Modificar as definições do Exchange Server
- Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange
- Forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server
- Modificar as definições do SQL Server
- Forçar uma verificação de capacidade de anexação do SQL Server
- Forçar truncamento de log para uma máquina SQL

Quando você protege os SQL Servers e Exchange Servers, há funções específicas para esses tipos de server que você pode realizar. Elas incluem:

- **Forçamento do truncamento de log do server.** Os SQL Servers e Exchange Servers incluem os logs de server. O processo para truncar os logs do SQL identifica o espaço disponível no server. Quando você truncar logs do server do Exchange, além de identificar o espaço disponível, o processo libera mais espaço no server. Para obter informações sobre o truncamento de log forçado, consulte Forçar truncamento de log para uma máquina SQL.
- **Definição de credenciais para o respectivo server.** Os servers do Exchange permitem que você defina credenciais para a máquina protegida na guia Resumo para o server protegido. Os SQL Servers permitem que você defina credenciais para uma máquina com SQL Server protegida, ou defina credenciais padrão para todos os SQL Servers.
    - Para obter informações sobre a definição de credenciais para os servers Exchange, consulte Definir credenciais para uma máquina Exchange Server.
    - Para obter informações sobre a definição de credenciais para os servers SQL, consulte Definir credenciais para uma máquina SQL Server.
    - Para obter informações sobre a realização de outras ações acessíveis a todos os agentes protegidos na guia Resumo do agente, consulte Visualizar a guia Resumo.

Configurar definições de Exchange e SQL Server

Se você protege dados de servidores Exchange ou SQL no seu AppAssure Core, pode estabelecer credenciais para que o Core se autentique nessas máquinas. Navegue até o server protegido no AppAssure Core Console para configurar essas definições de servidor, como é descrito nos tópicos a seguir.

Definir credenciais para uma máquina Exchange Server

Depois que você proteger dados em um server do Microsoft Exchange, é possível definir credenciais de login no AppAssure Core Console.

Para definir credenciais para uma máquina Exchange Server

1. Depois de incluir a máquina do Exchange Server na proteção, navegue até o AppAssure Core Console e selecione a máquina no painel Navegação.

   A guia Resumo é exibida para a máquina.

2. Na guia Resumo, no menu suspenso **Ações**, clique em **Exchange** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

3. Para definir credenciais para um server do Exchange único, clique em **Definir credenciais** e, na caixa de diálogo Editar credenciais do Exchange, faça o seguinte:

   a. No campo de texto Nome de usuário, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

   b. No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.

   c. Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Definir credenciais para uma máquina SQL Server

Depois que você proteger dados em um server SQL Exchange, é possível definir credenciais de login no AppAssure Core Console.

Para definir credenciais para uma máquina SQL Server

1. Depois de incluir a máquina do SQL Server na proteção, no AppAssure Core Console, selecione a máquina no painel Navegação.

   A guia Resumo é exibida para a máquina.

2. Na guia Resumo, clique no menu suspenso **Ações** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

   - Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias** e, na caixa de diálogo Editar credenciais padrão, faça o seguinte:

     a. No campo de texto Nome de usuário, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

     b. No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.

c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

- Se desejar definir credenciais para uma instância do SQL Server database, clique em **Definir credenciais da instância** e, na caixa de diálogo Editar credenciais da instância, faça o seguinte:

  a Selecione o tipo de credencial (Padrão, Windows ou SQL)

  b No campo de texto Nome de usuário, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

  c No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.

  d Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Noções básicas sobre indicadores de status de ponto de recuperação

Depois que um ponto de recuperação é criado em um SQL ou Exchange server protegido, o aplicativo exibe um indicador de status colorido correspondente na tabela Pontos de recuperação. A cor exibida se baseia nas definições de verificação da máquina protegida e no êxito ou fracasso dessas verificações, conforme descrito nas tabelas Cores de status de ponto de recuperação para bancos de dados SQL e Cores de status de ponto de recuperação para bancos de dados do Exchange, a seguir.

NOTA: Para obter mais informações sobre como visualizar pontos de recuperação, consulte Visualizar pontos de recuperação.

Cores de status de ponto de recuperação para bancos de dados SQL

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados SQL.

Tabela 57. Indicadores de status de banco de dados SQL

Cor de status	Descrição
Branco	Indica a existência de uma das seguintes condições: • Não existe banco de dados do SQL, • As verificações da capacidade de anexação não foram ativadas; ou • As verificações da capacidade de anexação ainda não foram executadas.
Amarelo	Indica que o banco de dados do SQL estava offline e não foi possível executar a verificação.
Vermelho	Indica falha na verificação de capacidade de anexação.
Verde	Indica que a verificação de capacidade de anexação foi aprovada.

Cores de status de ponto de recuperação para bancos de dados Exchange

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados Exchange.

Tabela 58. Indicadores de status de banco de dados Exchange

Cor de status	Descrição
Branco	Indica a existência de uma das seguintes condições: • Não existe banco de dados do Exchange; ou • As verificações da montabilidade não foram ativadas. **NOTA:** Isso pode se aplicar a determinados volumes dentro de um ponto de recuperação.
Amarelo	Indica que as verificações da montabilidade do banco de dados do Exchange estão ativadas, mas ainda não foram executadas.
Vermelho	Indica que as verificações de montabilidade ou de soma de verificação falharam em pelo menos um banco de dados.
Verde	Indica que a verificação de montabilidade ou a verificação de soma de verificação foi aprovada.

NOTA: Os pontos de recuperação que não têm banco de dados do Exchange ou do SQL associado a eles aparecerão com indicador de status branco. Em situações em que existe banco de dados do Exchange e do SQL para o ponto de recuperação, o indicador de status mais grave é exibido no ponto de recuperação.

Modificar as definições do Exchange Server

Se você estiver protegendo dados de um Microsoft Exchange server, precisará configurar as definições adicionais no AppAssure Core Console.

Para modificar as definições do Exchange Server

1 Depois de incluir a máquina do Exchange Server na proteção, navegue até o AppAssure Core Console e selecione a máquina no painel Navegação.

A guia Resumo é exibida para a máquina.

2 Na guia Resumo, no menu suspenso **Ações**, clique em **Exchange** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

- Se desejar truncar os registros do server do Exchange, clique em **Forçar truncamento de log**.
- Se desejar definir credenciais para um server do Exchange único, clique em **Definir credenciais**, e na caixa de diálogo Editar credenciais do Exchange, faça o seguinte:

a No campo de texto Nome de usuário, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

b No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.

c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Modificar as definições do SQL Server

Se você estiver protegendo dados de um Microsoft SQL Server, precisará configurar as definições adicionais no AppAssure Core Console.

Para modificar as definições do SQL Server

1 Depois de incluir a máquina do SQL Server na proteção, no AppAssure Core Console, selecione a máquina no painel Navegação.

A guia Resumo é exibida para a máquina.

2 Na guia Resumo, clique no menu suspenso **Ações** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

- Se desejar truncar os registros do server do SQL ou do Exchange, clique em **Forçar truncamento de log**.
- Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias** e, na caixa de diálogo Editar credenciais padrão, faça o seguinte:
  - a No campo de texto Nome de usuário, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  - b No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao server.ke do SQL conforme descrito na tabela a seguir.
  - c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.
- Se desejar definir credenciais para uma instância do SQL Server database, clique em **Definir credenciais da instância** e, na caixa de diálogo Editar credenciais da instância, faça o seguinte:
  - a Selecione o tipo de credencial (Padrão, Windows ou SQL)
  - b No campo de texto Nome de usuário, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  - c No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
  - d Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Gerenciar a capacidade de anexação do SQL e o truncamento de log

A configuração da capacidade de anexação do SQL permite que o AppAssure Core anexe arquivos de banco de dados e log do SQL Server em um snapshot de um server SQL usando uma instância local do Microsoft SQL Server. O teste da capacidade de anexação permite que o Core verifique a consistência dos bancos de dados SQL e garanta que todos os arquivos de dados (arquivos MDF e LDF) estejam disponíveis no snapshot de cópia de segurança. As verificações da capacidade de anexação podem ser executadas sob demanda para pontos de recuperação específicos ou como parte de um trabalho noturno.

A capacidade de anexação exige uma instância local do Microsoft SQL Server na máquina do AppAssure Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou através de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

A capacidade de anexação suporta SQL Server 2005, 2008, 2008 R2, 2012 e 2014. À conta usada para realizar o teste deve ser concedida a função sysadmin na instância do SQL Server.

O formato de armazenamento em disco do SQL Server é o mesmo em ambientes de 64 e 32 bits, e a capacidade de anexação funciona em ambas as versões. Um banco de dados separado da instância do server que está sendo executado em um ambiente pode ser anexado em uma instância de server que é executado em outro ambiente.

O truncamento de log identifica o espaço livre disponível nos registros do banco de dados do SQL, mas não os minimiza. É possível programar o truncamento de log para acontecer com trabalhos noturnos ou você pode forçá-lo sob demanda. Para forçar o truncamento de log, consulte Forçar truncamento de log para uma máquina SQL.

NOTA: A versão do SQL Server no Core deve ser igual ou mais recente que aquela em todas as máquinas agente com o SQL Server instalado.

Esta seção inclui os seguintes tópicos:

- Configurar as definições de capacidade de anexação do SQL
- Configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log em todas as máquinas protegidas

Para obter mais informações sobre o gerenciamento de máquinas protegidas que utilizam o SQL Server, consulte Modificar as definições do SQL Server ou Personalizar trabalhos noturnos para uma máquina protegida.

Configurar as definições de capacidade de anexação do SQL

Antes de executar verificações da capacidade de anexação de bancos de dados SQL protegidos, primeiro é preciso selecionar uma instância local do SQL Server na máquina do Core que será usada para executar as verificações em relação à máquina agente.

NOTA: A capacidade de anexação exige uma instância local do Microsoft SQL Server na máquina do AppAssure Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou através de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

Execute as etapas deste procedimento para configurar as definições de capacidade de anexação do SQL.

Para configurar as definições da capacidade de anexação do SQL

1. Navegue até o AppAssure Core e clique na guia Configuração.
2. Clique em **Definições**.
3. No painel Trabalhos noturnos, clique em **alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
4. Selecione **Trabalho de verificação de capacidade de anexação** e clique em **Definições**.

   A caixa de diálogo Configuração é exibida, permitindo que você escolha a instância local do SQL Server a fim de utilizar para a realização das verificações da capacidade de anexação dos SQL Server databases protegidos.
5. Use os menus suspensos para selecionar a instância do SQL Server instalado no Core a partir das seguintes opções:
   - SQL Server 2005
   - SQL Server 2008
   - SQL Server 2008 R2
   - SQL Server 2012
   - SQL Server 2014

   NOTA: As opções que aparecem na lista suspensa são preenchidas com base nas instâncias locais do SQL Server em seu ambiente.
6. Selecione o tipo de credencial. Você pode selecionar dentre:
   - Windows ou
   - SQL
7. Especifique as credenciais com privilégios administrativos para instâncias do Windows ou do SQL Server, conforme descrito na tabela a seguir.

Tabela 59. Credenciais de administrador do SQL Server

Caixa de texto	Descrição
Nome de usuário	Insira um nome de usuário para obter permissões de login no SQL Server.
Senha	Insira uma senha para a capacidade de anexação do SQL. Usada para controlar a atividade de login.

8 Clique em **Testar conexão**.

NOTA: Se as credenciais forem inseridas de forma incorreta, será exibida uma mensagem para alertá-lo de que o teste das credenciais falhou. Corrija as informações de credenciais e execute novamente o teste de conexão.

9 Clique em **Salvar**.

As verificações da capacidade de anexação agora estão disponíveis para serem executadas em bancos de dados protegidos do SQL Server.

10 Na janela Trabalhos noturnos, clique em **OK**.

As verificações da capacidade de anexação agora são programadas para acontecer com os trabalhos noturnos.

Configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log em todas as máquinas protegidas

É possível visualizar, ativar ou desativar as definições do server do banco de dados do SQL, incluindo verificação da capacidade de anexação e truncamento de log noturno na caixa de diálogo Trabalhos noturnos acessada a partir do Core. As alterações feitas aqui se aplicam a todas as máquinas SQL protegidas pelo Core.

Execute as etapas deste procedimento para que o sistema realize verificações noturnas de capacidade de anexação dos pontos de recuperação do SQL Server.

Para configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log

1 Navegue até o AppAssure Core e clique na guia Configuração.

2 Clique em **Definições**.

3 Na seção Trabalhos noturnos, clique em **Alterar**.

4 Selecione ou desmarque as definições do SQL Server com base nas necessidades da sua organização:

- Trabalho de verificação de capacidade de anexação
- Trabalho de truncamento de log (apenas modelo de recuperação simples)

5 Clique em **OK**.

As definições de capacidade de anexação e de truncamento de log entrarão em vigor no SQL Server protegido.

Forçar uma verificação de capacidade de anexação do SQL Server

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de capacidade de anexação de um ponto específico de recuperação do SQL Server.

NOTA: Para ter a capacidade de forçar uma verificação de capacidade de anexação, um banco de dados do SQL deve estar presente em um volume protegido. Se o AppAssure não detecta a presença de um banco de dados, a função de verificação da capacidade de anexação não é exibida no Core Console.

Para forçar uma verificação de capacidade de anexação do SQL Server

1. Na área de navegação esquerda do AppAssure Core, selecione a máquina para a qual deseja forçar a verificação de capacidade de anexação e clique na guia **Pontos de recuperação**.
2. Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.
3. Clique em **Verificar**, e depois em **Forçar a verificação da capacidade de anexação**.

   Aparecerá a janela Forçar verificação de capacidade de anexação onde você pode indicar se deseja forçar a verificação de capacidade de anexação.
4. Clique em **Sim.**

   O sistema realiza a verificação de capacidade de anexação.

   NOTA: Para obter informações sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualizar tarefas, alertas e eventos.

Forçar truncamento de log para uma máquina SQL

O truncamento de log está disponível para máquinas que utilizam o SQL Server. Execute as etapas deste procedimento para forçar o truncamento de log.

NOTA: Quando realizado em uma máquina com SQL, o truncamento identifica o espaço livre em um disco, mas não reduz o tamanho dos logs.

Para forçar truncamento de log para uma máquina SQL

1. No AppAssure Core Console, navegue até a máquina protegida na qual deseja forçar o truncamento de log.
   - Na guia Resumo da máquina protegida, clique no menu suspenso **Ações**, selecione **SQL** e clique em **Forçar truncamento de log**.
2. Clique em **Sim** para confirmar que deseja forçar o truncamento de log.

Gerenciar verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log

Ao usar o AppAssure para fazer cópias de segurança de Microsoft Exchange Servers, poderão ser feitas verificações de montabilidade em todos os bancos de dados Exchange após cada snapshot. Esse recurso de detecção de corrupção alerta os administradores sobre possíveis falhas e garante que todos os dados nos Exchange servers sejam recuperados com êxito em caso de falha.

O truncamento de log minimiza o tamanho dos registros a partir de um banco de dados do Exchange diariamente quando agendado para acontecer com trabalhos noturnos. Para obter informações sobre o forçamento do truncamento de log, consulte Forçar o truncamento de log para uma máquina Exchange.

NOTA: As verificações de montabilidade somente se aplicam ao Microsoft Exchange 2007, 2010 e 2013. Além disso, a conta de serviço do AppAssure Agent deve ter a função de Administrador organizacional atribuída a ela no Exchange.

Configurar verificações noturnas de soma de verificação do banco de dados do Exchange e truncamento de log

É possível visualizar, ativar ou desativar as definições do server do banco de dados do Exchange, incluindo verificação automática de capacidade de montagem, verificação de soma de verificação noturna ou truncamento de log noturno, na guia de Configuração do nível do Core. As alterações feitas nas configurações nessa guia se aplicam a todas as máquinas Exchange protegidas pelo Core.

Execute as etapas deste procedimento para configurar as definições de montabilidade e truncamento de log do banco de dados do Exchange.

Para configurar a montabilidade de banco de dados do Exchange e o truncamento de log

1. Navegue até o AppAssure Core e clique na guia Configuração.
2. Clique em **Definições**.
3. Na seção Trabalhos noturnos, clique em **Alterar**.
4. Selecione ou desmarque as definições do Exchange Server com base nas necessidades da sua organização:
   - Trabalho de verificação de soma de verificação
   - Registros truncados do Exchange
5. Clique em **OK**.

   As definições de soma de verificação e de truncamento de log entrarão em vigor no Exchange Server protegido.

   NOTA: Para obter informações sobre o truncamento de log forçado, consulte Forçar o truncamento de log para uma máquina Exchange.

Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de montabilidade de um ponto específico de recuperação do Exchange Server.

NOTA: Para ter a capacidade de forçar uma verificação de capacidade de montagem, um banco de dados do Exchange deve estar presente em um volume protegido. Se o AppAssure não detecta a presença de um banco de dados, a função de verificação de capacidade de montagem não é exibida no Core Console.

Para forçar uma verificação de montabilidade

1. Na área de navegação esquerda do AppAssure Core Console, selecione a máquina para a qual deseja forçar a verificação de montabilidade e clique na guia **Pontos de recuperação**.
2. Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.
3. Clique em **Verificar**, e depois em **Forçar verificação de capacidade de montagem**.

   Uma janela pop-up é exibida perguntando se você deseja forçar uma verificação de montabilidade.
4. Clique em **Sim.**

   O sistema realiza a verificação de montabilidade.

   NOTA: Para obter instruções sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualizar tarefas, alertas e eventos.

Forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de soma de verificação de um ponto específico de recuperação do Exchange Server.

NOTA: Para ter a capacidade de forçar uma verificação de soma de verificação, um banco de dados do Exchange deve estar presente em um volume protegido. Se o AppAssure não detecta a presença de um banco de dados, a função de verificação de soma de verificação não é exibida no Core Console.

Para forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server

1. Na área de navegação esquerda do AppAssure Core Console, selecione a máquina para a qual deseja forçar a verificação de soma de verificação e clique na guia **Pontos de recuperação**.
2. Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.
3. Clique em **Verificar**, e depois em **Forçar a verificação de soma de verificação**.

   Aparecerá a janela Forçar verificação de capacidade de anexação onde você pode indicar se deseja forçar a verificação de soma de verificação.
4. Clique em **Sim.**

   O sistema realiza a verificação de soma de verificação.

   NOTA: Para obter informações sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualizar tarefas, alertas e eventos.

Forçar o truncamento de log para uma máquina Exchange

O truncamento de log está disponível para máquinas que utilizam o Exchange Server. Quando o truncamento de log é realizado para uma máquina com Exchange, o tamanho dos logs é reduzido. Execute as etapas deste procedimento para forçar o truncamento de log.

Para forçar o truncamento de log para uma máquina Exchange

1. No AppAssure Core Console, navegue até a máquina protegida na qual deseja forçar o truncamento de log.
   - Na guia Resumo da máquina protegida, clique no menu suspenso **Ações**, selecione **Exchange** e clique em **Forçar truncamento de log**.
2. Clique em **Sim** para confirmar que deseja forçar o truncamento de log.

8

Proteger clusters do servidor

Este capítulo descreve como proteger informações nos clusters do Microsoft SQL Server ou Exchange Server usando o AppAssure. Os seguintes tópicos estão incluídos:

- Aplicativos e tipos de cluster suportados
- Proteger um cluster
- Proteger nós em um cluster
- Modificar definições de nó de cluster
- Configurar definições de cluster
- Converter um nó de cluster protegido em uma máquina protegida
- Visualizar informações de cluster do servidor
- Trabalhar com pontos de recuperação de cluster
- Gerenciar os snapshots de um cluster
- Realizar uma restauração de clusters e nós de cluster
- Replicar dados de cluster
- Remover um cluster da proteção
- Remover nós de cluster da proteção
- Visualizar um relatório de cluster ou nó

No AppAssure, a proteção de cluster do servidor está associada às máquinas protegidas do AppAssure instaladas em nós de cluster individuais (ou seja, máquinas individuais no cluster) e ao AppAssure Core, que protege essas máquinas como se fossem uma única máquina composta.

É fácil configurar um AppAssure Core para proteger e gerenciar um cluster. No Core Console, um cluster é organizado como entidade separada, que atua como contêiner que inclui os nós relacionados. Por exemplo, na área de navegação à esquerda, no menu Máquinas protegidas, os clusters protegidos são relacionados. Diretamente abaixo de cada cluster, os nós individuais associados ou máquinas agente aparecem. Cada um desses é uma máquina protegida na qual o software AppAssure Agent é instalado. Se você clicar no cluster, a guia aparece no Core Console

Nos níveis de Core e cluster, é possível visualizar informações sobre o cluster, como a lista de nós relacionados e volumes compartilhados. Um cluster aparece no Core Console na guia Nós protegidos e é possível alternar a visualização (usando Exibir/ocultar) para visualizar os nós incluídos no cluster. No nível de cluster, também é possível visualizar os metadados de clusters correspondentes do Exchange e SQL para os nós do cluster. É possível especificar definições para todo o cluster e os volumes compartilhados nesse cluster ou então navegar até um nó (máquina) individual do cluster para configurar as definições apenas para esse nó e os volumes locais associados.

Aplicativos e tipos de cluster suportados

Para proteger seu cluster corretamente, é preciso ter o software AppAssure Agent instalado em cada uma das máquinas ou nós do cluster. O AppAssure suporta as versões de aplicativos e as configurações de cluster relacionadas na tabela a seguir.

Tabela 60. Versões de aplicativos e configurações de cluster suportadas

Aplicativo	Versão do aplicativo e configuração do cluster relacionado	Cluster de ativação pós-falha do Windows
Microsoft Exchange Server	2007 Single Copy Cluster (SCC) 2007 Cluster Continuous Replication (CCR)	2003, 2008, 2008 R2
	2010 Grupo de disponibilidade de banco de dados (DAG)	2008, 2008 R2
	2013 Grupo de disponibilidade de banco de dados (DAG)	2008 R2 SP1, 2012, 2012 R2
Microsoft SQL Server	2005	2003, 2008, 2008 R2
	2008, 2008 R2 Single Copy Cluster (SCC)	2003, 2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Single Copy Cluster (SCC)	2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Grupos de Disponibilidade	Server 2012, 2012 R2

Os tipos de disco suportados incluem:

- Discos de tabela de partição GUID (GPT) maiores que 2 TB
- Discos básicos

Os tipos de montagem suportados incluem:

- Unidades compartilhadas conectadas como letras de unidade (por exemplo, D:)
- Volumes dinâmicos simples em um único disco físico (volumes não distribuídos, espelhados ou estendidos)
- Unidades compartilhadas conectadas como pontos de montagem

Suporte limitado para volumes compartilhados de cluster

O suporte do AppAssure a volumes compartilhados de cluster (CSV) aplica-se apenas a cópias de segurança nativas de CSVs em agentes Windows 2008 R2.

No caso de outros sistemas operacionais, o serviço de agente pode ser executado em todos os nós de um cluster e o cluster pode ser protegido como um cluster dentro do AppAssure Core, mas os CSVs não são exibidos no Core Console e não estão disponíveis para proteção. Todos os discos locais (como o volume do sistema operacional) estão disponíveis para proteção.

A tabela a seguir descreve o suporte atual no AppAssure Core para volumes compartilhados de cluster.

Tabela 61. Compatibilidade com volumes compartilhados de cluster no AppAssure

AppAssure Suporte a volumes compartilhados de cluster	Proteger, replicar, rollup, montar arquivo		Restaurar volumes CSV		Exportação virtual para Hyper-V CSV	
Versão do AppAssure	5,3	5,4	5,3	5,4	5,3	5,4
Windows 2008 R2	Sim	Sim	Não	Sim	Sim	Sim
Windows 2012	Não	Não	Não	Não	Não	Não
Windows 2012 R2	Não	Não	Não	Não	Não	Não

Proteger um cluster

Este tópico descreve como adicionar um cluster para proteção no AppAssure. Ao adicionar um cluster para proteção, você precisa especificar o nome do host ou endereço IP do cluster, o aplicativo de cluster, ou um dos nós ou máquinas do cluster que inclua o software AppAssure Agent.

NOTA: Um repositório é usado para armazenar os snapshots de dados capturados a partir de seus nós protegidos. Antes de começar a proteger os dados em seu cluster, você deve ter definido pelo menos um repositório associado ao AppAssure Core.

Para obter informações sobre definição de repositórios, consulte Noções básicas sobre repositórios.

Para proteger um cluster

1 No Core Console, navegue até a guia Inicial, clique no botão **Proteger** no menu suspenso e, em seguida, clique em **Proteger cluster**.

2 Na caixa de diálogo Conectar-se ao cluster, insira as seguintes informações e depois clique em **Conectar**.

Tabela 62. Definições de Conectar-se ao cluster

Caixa de texto	Descrição
Host	O nome do host ou endereço IP do cluster, o aplicativo de cluster ou um dos nós do cluster.
Porta	O número da porta na máquina em que o AppAssure Core se comunica com o Agent. A porta padrão é 8006.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a essa máquina; por exemplo, domain_name\administrator ou administrator@domain_name.com **NOTA:** O nome de domínio é obrigatório. Não é possível conectar-se ao cluster usando o nome de usuário do administrador local.
Senha	A senha usada para se conectar à máquina.

3 Na caixa de diálogo Proteger cluster, selecione um repositório para esse cluster.

4 Para proteger os pontos de recuperação desse cluster, selecione uma chave de criptografia.

5 Se não quiser que a proteção comece imediatamente após a conclusão desse procedimento, selecione **Pausar proteção inicialmente**.

6 Para proteger o cluster com base em definições padrão, selecione os nós para a proteção padrão e siga para Etapa 8.

NOTA: As definições padrão garantem que todos os volumes sejam protegidos com uma programação a cada 60 minutos.

7 Para inserir definições personalizadas para o cluster (por exemplo, para personalizar a programação de proteção dos volumes compartilhados), clique em **definições** ao lado do nó cuja proteção você deseja personalizar e consulte Criar programações de proteção personalizadas.

Para obter mais informações sobre a personalização de nós, consulte Proteger nós em um cluster.

8 Na caixa de diálogo Proteger cluster, clique em **Proteger**.

Proteger nós em um cluster

Este tópico descreve como proteger os dados em um nó de cluster ou máquina com um AppAssure Agent instalado. Ao adicionar proteção, é preciso selecionar um nó na lista de nós disponíveis, além de especificar o nome do host e o nome de usuário, e a senha do administrador do domínio.

Para proteger nós em um cluster

1 No AppAssure Core Console, depois de adicionar o cluster, navegue até o cluster que deseja proteger.

A guia Resumo do cluster selecionado é exibida.

2 Clique na guia Nós protegidos e, no menu **Ações**, selecione **Proteger nó de cluster**.

3 Na caixa de diálogo Proteger nó de cluster, selecione ou insira, conforme o caso, as seguintes informações e clique em **Conectar** para adicionar a máquina ou o nó.

Tabela 63. Definições de Proteger nó de cluster

Caixa de texto	Descrição
Host	Uma lista suspensa de nós disponíveis para proteção no cluster.
Porta	O número da porta em que o AppAssure Core se comunica com o Agent no nó.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a esse nó; por exemplo, example_domain\administrator ou administrator@example_domain.com.
Senha	A senha usada para se conectar à máquina.

4 Clique em **Proteger** para começar a proteger essa máquina com as definições de proteção padrão.

NOTA: As definições padrão garantem que todos os volumes da máquina sejam protegidos com uma programação a cada 60 minutos.

5 Para inserir as definições personalizadas dessa máquina (por exemplo, alterar o nome de exibição, adicionar criptografia ou personalizar a programação de proteção), clique em **Exibir opções avançadas**.

6 Se necessário, edite as seguintes definições, conforme descrito na tabela a seguir.

Tabela 64. Definições de Opções avançadas

Caixa de texto	Descrição
Nome de exibição	Digite um novo nome para a máquina a ser exibido no Core Console.
Repositório	Selecione o repositório no AppAssure Core em que os dados dessa máquina devem ser armazenados.
Criptografia	Especifique se a criptografia deve ser aplicada aos dados de todos os volumes dessa máquina a serem armazenados no repositório. **NOTA:** As definições de criptografia de um repositório são configuradas na guia Configuração do AppAssure Core Console.
Programação	Selecione uma das seguintes opções. • Proteger todos os volumes com uma programação padrão • Proteger volumes específicos com uma programação personalizada. Depois, em Volumes, selecione um volume e clique em **Editar**. Para obter mais informações sobre a definição de intervalos personalizados, consulte a Etapa 7 em Proteger um cluster.

Modificar definições de nó de cluster

Depois de ter adicionado a proteção para nós do cluster, é fácil modificar as definições básicas dessas máquinas ou nós (por exemplo, nome de exibição, nome de host, e assim por diante), definições de proteção (por exemplo, alteração da programação de proteção para volumes locais da máquina, adição ou remoção de volumes ou pausa na proteção), e muito mais.

Para modificar as definições do nó de cluster, é preciso executar as seguintes tarefas:

1. No AppAssure Core Console, navegue até o cluster que contém o nó a ser modificado e selecione a máquina ou nó que deseja modificar.
2. Para modificar e visualizar as definições de configuração, consulte Configurar grupos de notificação para eventos do sistema.
3. Para configurar grupos de notificação para eventos de sistema, consulte Visualizar e modificar as definições de configuração.
4. Para personalizar as definições de política de retenção, consulte Personalizar as definições de política de retenção de uma máquina protegida.
5. Para modificar a programação de proteção, consulte Modificar programações de proteção.
6. Para modificar as definições da transferência, consulte Modificar definições de transferência.

Configurar definições de cluster

Para configurar as definições de cluster, as seguintes tarefas devem ser executadas:

- **Modificar definições de cluster.** Para obter mais informações sobre a modificação de definições de cluster, consulte Modificar definições de cluster.
- **Configurar as notificações de eventos de cluster.** Para obter mais informações sobre a configuração de notificação de evento de cluster, consulte Configurar as notificações de eventos de cluster.
- **Modificar a política de retenção de cluster.** Para obter mais informações sobre a modificação da política de retenção de cluster, consulte Modificar a política de retenção do cluster.
- **Modificar as programações de proteção de cluster.** Para obter mais informações sobre a modificação de programações de proteção de cluster, consulte Modificar programações de proteção de cluster.
- **Modificar as definições de transferência de cluster.** Para obter mais informações sobre a modificação de definições de transferência de cluster, consulte Modificar definições de transferência de cluster.

Modificar definições de cluster

Depois de ter adicionado um cluster, é fácil modificar as definições básicas (por exemplo, nome de exibição), definições de proteção (por exemplo, programações de proteção, adição ou remoção de volumes ou pausa na proteção), e muito mais.

Para modificar definições de cluster

1. No AppAssure Core Console, navegue até o cluster que deseja modificar.
2. Clique na guia Configuração.

   A página Definições é exibida.
3. Clique em **Editar** para modificar as definições nessa página do cluster, como descrito na tabela a seguir.

Tabela 65. Definições de cluster

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para o cluster. O nome desse cluster é exibido no AppAssure Core Console. Por padrão, esse é o nome de host do cluster. Se necessário, é possível mudá-lo para algo mais descritivo.
Repositório	Insira o repositório de Core associado ao cluster. NOTA: Se já tiverem sido feitos snapshots desse cluster, essa definição estará relacionada aqui apenas para fins informativos e não poderá ser modificada.
Chave de criptografia	Edite e selecione uma chave de criptografia se necessário. Especifica se a criptografia deve ser aplicada aos dados de todos os volumes desse cluster a ser armazenado no repositório.

Configurar as notificações de eventos de cluster

É possível configurar como os eventos do sistema são relatados para seu cluster criando grupos de notificação. Esses eventos podem ser alertas do sistema ou erros. Execute as etapas deste procedimento para configurar os grupos de notificação para eventos.

Para configurar as notificações de eventos de cluster

1 No AppAssure Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração e em **Eventos**.

3 Selecione uma das opções descritas na tabela a seguir.

Tabela 66. Opções de notificação de eventos

Opção	Descrição
Usar definições de alerta do Core	Adota as definições usadas pelo core associado: • Clique em **Aplicar** e execute a Etapa 5.
Usar definições de alerta personalizadas	Permite configurar definições personalizadas: • Vá para a Etapa 4.

4 Se tiver selecionado definições de alerta personalizadas, faça o seguinte:

a Clique em **Adicionar grupo** para adicionar um novo grupo de notificação para o envio de uma lista de eventos do sistema.

A caixa de diálogo Adicionar grupo de notificação é aberta.

b Adicione as opções de notificação conforme descrito na tabela a seguir.

Tabela 67. Definições de notificação de eventos

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.

Tabela 67. Definições de notificação de eventos

Caixa de texto	Descrição
Habilitar eventos	Selecione os eventos para notificação, por exemplo, Clusters. Também é possível optar por selecionar por tipo: • Erro • Aviso • Informações **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher Aviso, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão são ativados.
Opções de notificação	Selecione o método para especificar como lidar com as notificações. Você pode selecionar dentre as seguintes opções: • **Notificar por e-mail**. Especifique a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e Cco. • **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação. • **Notificar por syslogd.** Especifique o nome de host e a porta aos quais enviar os eventos. • **Notificar através de alertas do sistema.** Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

c Clique em **OK** para salvar suas alterações e clique em **Aplicar**.

5 Para editar um grupo de notificação existente, ao lado de um grupo de notificação na lista, clique em **Editar**.

A caixa de diálogo Editar grupo de notificação é exibida para que as definições possam ser editadas.

Modificar a política de retenção do cluster

A política de retenção de um cluster especifica por quanto tempo os pontos de recuperação de volumes compartilhados do cluster são armazenados no repositório. As políticas de retenção são usadas para reter snapshots de cópia de segurança por períodos mais longos e para ajudar com o gerenciamento desses snapshots de cópia de segurança. A política de retenção é imposta pelo processo de rollup que ajuda no processo de envelhecimento e exclusão das cópias de segurança antigas.

Para modificar a política de retenção de cluster

1 No AppAssure Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração e em **Política de retenção**.

3 Selecione uma das opções na tabela a seguir.

Tabela 68. Opções de política de retenção

Opção	Descrição
Usar política de retenção padrão do Core	Adota as definições usadas pelo core associado. • Clique em **Aplicar**.
Usar a política de retenção personalizada	Permite configurar definições personalizadas.

NOTA: Se você tiver selecionado definições de alerta personalizadas, siga as instruções para definir uma política de retenção personalizada, conforme descrito em Personalizar trabalhos noturnos para uma máquina protegida.

Modificar programações de proteção de cluster

No AppAssure, é possível modificar as programações de proteção somente se o cluster tiver volumes compartilhados.

Para modificar as programações de proteção de cluster

1. No AppAssure Core Console, navegue até o cluster que deseja modificar e selecione-o.
2. Siga as instruções para modificar as definições de proteção, conforme descrito em Modificar programações de proteção.

Modificar definições de transferência de cluster

No AppAssure, é possível modificar as definições para gerenciar os processos de transferência de dados de um cluster protegido.

NOTA: É possível modificar as definições da transferência de cluster somente se seu cluster tiver volumes compartilhados.

Há três tipos de transferência no AppAssure:

- **Snapshots.** Faz a cópia de segurança de dados no seu cluster protegido.
- **Exportação da VM.** Cria uma máquina virtual com todas as informações de cópia de segurança e parâmetros especificados pela programação definida para proteger o cluster.
- **Restaurar**. Restaura as informações de cópia de segurança de um cluster protegido.

Para modificar as definições de transferência de cluster

1. No AppAssure Core Console, navegue até o cluster que deseja modificar.
2. Clique na guia Configuração e em **Definições de transferência**.
3. Modifique as definições de proteção, conforme descrito em Modificar programações de proteção.

Converter um nó de cluster protegido em uma máquina protegida

No AppAssure, é possível converter um nó de cluster protegido em uma máquina protegida, de modo que ela ainda seja gerenciada pelo Core, mas não faça mais parte do cluster. Isso é útil, por exemplo, se você precisar remover do cluster o nó de cluster, mas ainda mantê-lo protegido.

Para converter um nó de cluster protegido em uma máquina protegida

1. No AppAssure Core Console, navegue até o cluster que contém a máquina a ser convertida e clique em **Nós protegidos**.
2. Na página Nós protegidos do nó específico que você deseja converter, clique no menu suspenso **Ações** e selecione **Converter em Agent**.
3. Para adicionar a máquina de volta ao cluster, selecione-a e depois, na guia **Resumo** do menu Ações, selecione **Converter para nó de cluster** e clique em **Sim** para confirmar a ação.

Visualizar informações de cluster do servidor

Execute as etapas dos procedimentos a seguir para visualizar informações de resumo, evento, alerta e assim por diante referentes aos clusters de servers.

Visualizar informações de sistema de cluster

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de um cluster.

Para visualizar as informações do sistema do cluster

1. No AppAssure Core Console, navegue até o cluster que deseja visualizar.
2. Clique na guia Ferramentas.

   Aparece a página de informações do sistema e mostra detalhes do sistema sobre o cluster, como nome, nós incluídos com estado associado e versões do Windows, informações de interface de rede e de capacidade de volume.

Visualizar tarefas, eventos e alertas de cluster

Execute as etapas deste procedimento para visualizar eventos e alertas de um cluster.

Para obter informações sobre visualização de eventos e alertas de uma máquina ou nó individual em um cluster, consulte Visualizar tarefas, alertas e eventos.

Para visualizar tarefas, eventos e alertas de cluster

1. No AppAssure Core Console, navegue até o cluster que deseja visualizar.
2. Clique na guia Eventos, que se abre para mostrar todas as tarefas desse cluster.
3. É possível filtrar as tarefas exibidas desse cluster. Para obter mais informações, consulte Visualizar tarefas.
4. Para visualizar apenas os alertas, no canto superior esquerdo da página, clique em **Alertas**.

   A lista de eventos é filtrada para exibir apenas os alertas do cluster ou nó selecionado.
5. Como opção, se você quiser remover todos os alertas da página, clique em **Descartar tudo**.
6. Para visualizar todos os eventos, no canto superior esquerdo da página, clique em **Eventos**.

   Todos os eventos são exibidos para o cluster ou nó selecionado.

Visualizar informações de resumo

Execute as etapas deste procedimento para visualizar as informações de resumo de um cluster, incluindo informações sobre o quórum associado ao cluster.

Para visualizar as informações de resumo

1. No AppAssure Core Console, navegue até o cluster que deseja visualizar.
2. Na guia Resumo, é possível visualizar informações como nome do cluster, tipo de cluster, tipo de quórum (se aplicável) e caminho do quórum (se aplicável). Essa guia também mostra informações de relance sobre os volumes nesse cluster, incluindo o tamanho e programação de proteção. Se aplicável, também é possível visualizar informações do SQL Server ou Exchange Server para um cluster diferente.

3 Para que essas informações fiquem mais atualizadas, clique no menu suspenso **Ações** e em **Atualizar metadados**.

Para obter informações sobre visualização de informações de resumo e status de uma máquina ou nó individual no cluster, consulte Visualizar o status da máquina e outros detalhes.

Trabalhar com pontos de recuperação de cluster

Um ponto de recuperação, também chamado de snapshot, é uma cópia pontual das pastas e arquivos dos volumes compartilhados em um cluster, que estão armazenados no repositório. Os pontos de recuperação são utilizados para recuperar as máquinas protegidas ou para montar um sistema de arquivos local. No AppAssure, é possível visualizar as listas de pontos de recuperação no repositório. Execute as etapas do procedimento a seguir para revisar os pontos de recuperação.

NOTA: Se você estiver protegendo dados a partir de um cluster de servers DAG ou CCR, os pontos de recuperação associados não aparecerão no nível de cluster. Estarão visíveis apenas no nível de nó ou máquina.

Para obter informações sobre visualização de pontos de recuperação de máquinas individuais em um cluster, consulte Visualizar pontos de recuperação.

Para trabalhar com pontos de recuperação de cluster

1 No AppAssure Core Console, navegue até o cluster cujos pontos de recuperação você deseja visualizar.

2 Clique na guia Pontos de recuperação.

3 Para visualizar informações detalhadas de um ponto de recuperação específico, clique no símbolo de maior que (>) ao lado de um ponto de recuperação na lista para expandir a visualização.

4 Para obter informações sobre as operações que podem ser executadas nos pontos de recuperação, consulte Visualizar um ponto de recuperação específico.

5 Selecione um ponto de recuperação para montar.

Para obter informações sobre como montar um ponto de recuperação, consulte Montar um ponto de recuperação.

6 Para excluir pontos de recuperação, consulte Remover pontos de recuperação.

Gerenciar os snapshots de um cluster

No AppAssure, é possível gerenciar snapshots, forçando um snapshot ou pausando os snapshots atuais. Forçar um snapshot permite forçar uma transferência de dados para o cluster atualmente protegido. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior são transferidos. Se não existir um ponto de recuperação anterior, todos os dados (a imagem de base) nos volumes protegidos são transferidos. Ao pausar o snapshot, você interrompe temporariamente todas as transferências de dados da máquina atual.

Para obter informações sobre como forçar snapshots de máquinas individuais em um cluster, consulte Forçar um snapshot. Para obter informações sobre como pausar e retomar snapshots de máquinas individuais em um cluster, consulte Pausar e retomar a proteção.

Forçar um snapshot de um cluster

Execute as etapas deste procedimento para forçar um snapshot de cluster.

Para forçar um snapshot em um cluster

1. No AppAssure Core Console, navegue até o cluster cujos pontos de recuperação você deseja visualizar.
2. Na guia Resumo, clique no menu suspenso **Ações** e depois em **Forçar snapshot**.

Pausar e retomar snapshots de cluster

Execute as etapas deste procedimento para pausar e retomar um snapshot de cluster.

Para pausar e retomar os snapshots de cluster

1. No AppAssure Core Console, navegue até o cluster cujos pontos de recuperação você deseja visualizar.
2. Na guia Resumo, clique no menu suspenso **Ações** e depois em **Pausar snapshots**.
3. Na caixa de diálogo Pausar proteção, selecione uma das opções descritas na tabela a seguir.

Tabela 69. Opções de Pausar proteção

Opção	Descrição
Pausar até que retomado	Pausa o snapshot até você retomar manualmente a proteção. • Para retomar a proteção, clique no menu **Ações** e depois em **Retomar**.
Pausar por	Permite especificar uma quantidade de tempo em dias, horas e minutos para pausar os snapshots.

Realizar uma restauração de clusters e nós de cluster

A restauração é o processo de restaurar os volumes em uma máquina a partir de pontos de recuperação. Para um cluster de servers, realize a restauração no nível de nó ou da máquina. Esta seção fornece orientações sobre como realizar uma restauração em volumes de cluster.

Realizar uma restauração de clusters CCR e DAG (Exchange)

Execute as etapas deste procedimento para realizar uma restauração de clusters CCR e DAG (Exchange).

Para realizar uma restauração de clusters CCR e DAG (Exchange)

1. Desative todos os nós, com exceção de um.
2. Execute uma restauração usando o procedimento padrão do AppAssure para a máquina, como descrito em Restaurar volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.
3. Quando a restauração for concluída, monte todos os bancos de dados para os volumes de cluster.
4. Ative todos os outros nós.

5 Para o Exchange, navegue até o Console de gerenciamento do Exchange e, para cada banco de dados, execute a operação **Atualizar cópia de banco de dados**.

Realizar uma restauração de clusters SCC (Exchange, SQL)

Execute as etapas deste procedimento para realizar uma restauração em clusters de SCC (Exchange, SQL).

Para realizar uma restauração em clusters de SCC (Exchange, SQL)

1 Desative todos os nós, com exceção de um.

2 Execute uma restauração usando o procedimento padrão do AppAssure para a máquina, como descrito em Restaurar volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.

3 Depois que a restauração for concluída, monte todos os bancos de dados a partir dos volumes de cluster.

4 Ative todos os outros nós, um por um.

> **NOTA:** Não é preciso executar nenhuma reversão no disco de quórum. Ele pode ser regenerado automaticamente ou usando a funcionalidade do serviço de cluster.

Replicar dados de cluster

Ao replicar dados de um cluster, você deve replicar todo o cluster. Por exemplo, se você selecionar um nó para replicar, o cluster será selecionado automaticamente. Da mesma forma, se você selecionar o cluster, todos os nós desse cluster também serão selecionados.

Para obter mais informações e instruções sobre a replicação de dados, consulte Configurar a replicação.

Remover um cluster da proteção

Execute as etapas do procedimento a seguir para remover um cluster da proteção.

Para remover um cluster da proteção

1 No AppAssure Core Console, navegue até o cluster que deseja remover.

2 Clique no menu suspenso **Ações** e depois em **Remover cluster**.

3 Selecione uma das seguintes opções.

Tabela 70. Opções de Remover cluster

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster.

Remover nós de cluster da proteção

Execute as etapas dos procedimentos a seguir para remover nós de cluster da proteção.

Se quiser apenas remover um nó do cluster, consulte Converter um nó de cluster protegido em uma máquina protegida.

Para remover um nó de cluster da proteção

1 No AppAssure Core Console, navegue até a guia Nós protegidos do cluster.

2 Clique no menu suspenso Ações e depois em **Remover nó**.

3 Selecione uma das opções descritas na tabela a seguir.

Tabela 71. Opções de Remover nó

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados desta máquina ou nó.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados desta máquina ou nó.

Remover todos os nós de um cluster da proteção

Execute as etapas deste procedimento para remover todos os nós em um cluster da proteção.

△ | **CUIDADO: Se você remover todos os nós do cluster, o cluster também será removido.**

Para remover todos os nós em um cluster da proteção

1 No AppAssure Core Console, navegue até a guia Nós protegidos do cluster.

2 Na guia Nós Protegidos, selecione todos os nós.

3 Clique no menu suspenso Ações na parte superior da guia Nós protegidos, clique em **Remover nós** e depois selecione uma das opções descritas na tabela a seguir.

Tabela 72. Opções de Remover nós

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster.

Visualizar um relatório de cluster ou nó

É possível criar e visualizar relatórios de conformidade e de erros sobre as atividades do AppAssure em um cluster e em nós individuais. Os relatórios incluem informações sobre as atividades do AppAssure no cluster, no nó e nos volumes compartilhados.

Para obter mais informações sobre relatórios no AppAssure, consulte Gerar e visualizar relatórios. Para obter mais informações sobre as opções de exportação e impressão localizadas na barra de ferramentas de relatórios, consulte Usar a barra de ferramentas de relatórios.

Para visualizar um relatório de cluster ou nó

1 No AppAssure Core Console, navegue até o cluster para o qual deseja criar um relatório.

2 Se quiser criar um relatório de um nó sob um cluster, selecione o nó.

3 Clique na guia Ferramentas e, no menu Relatórios, selecione uma das seguintes opções:

- Relatório de conformidade
- Relatório de falhas

4 No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

> **NOTA:** Não há dados disponíveis anteriores ao horário em que o AppAssure Core ou Agent foi implantado.

5 No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.

6 Clique em **Gerar relatório**. Os resultados do relatório aparecem na página.

Se o relatório ocupar diversas páginas, você clicar nos números de página ou nos botões de seta no alto dos resultados do relatório para mudar de página.

7 Para exportar os resultados do relatório em um dos formatos disponíveis — PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV ou imagem — selecione o formato para exportação na lista suspensa e, em seguida, faça um dos seguintes:

- Clique no primeiro ícone Salvar para exportar um relatório e salvá-lo no disco.
- Clique no segundo ícone Salvar para exportar um relatório e exibi-lo em uma nova janela de navegador da Web.

8 Para imprimir os resultados do relatório, use uma das seguintes opções:

- Clique no primeiro ícone de Impressora para imprimir todo o relatório.
- Clique no segundo ícone de Impressora para imprimir a página atual do relatório.

9

Exportar dados protegidos de máquinas Windows para máquinas virtuais

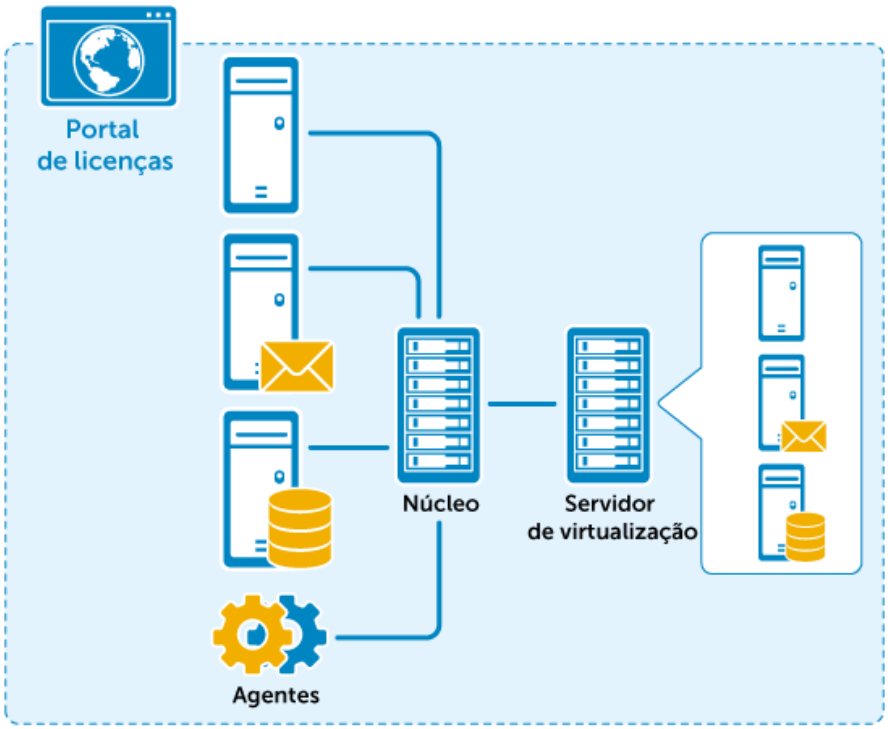
Este capítulo explica como exportar um ponto de recuperação para criar uma máquina virtual. Os seguintes tópicos estão incluídos:

- Gerenciar exportações
- Exportar dados para uma máquina virtual baseada em Windows
- Exportar dados para uma máquina virtual ESXi
- Exportar dados para uma máquina virtual VMWare Workstation
- Exportar dados para uma máquina virtual Hyper-V
- Exportar dados para uma máquina virtual VirtualBox

O AppAssure oferece suporte à exportação única ou contínua (suporte a standby virtual) das informações de uma cópia de segurança do Windows para uma máquina virtual. Exportar seus dados para uma máquina Virtual Standby fornece-lhe uma cópia de alta disponibilidade dos dados. Se uma máquina protegida ficar inativa, você poderá inicializar a máquina virtual e realizar a recuperação.

O diagrama a seguir mostra uma implementação típica de exportação de dados para uma máquina virtual.

Figura 4. Implementação de standby virtual



Ao exportar para uma máquina virtual, todos os dados de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos para a programação de proteção da sua máquina são exportados. Também é possível criar um "standby virtual" fazendo os dados protegidos serem exportados continuamente da máquina protegida para uma máquina virtual.

Você pode realizar uma exportação virtual dos pontos de recuperação de máquinas protegidas Windows ou Linux para VMware, ESXi, Hyper-V e VirtualBox.

NOTA: Para ESXi, VMware Workstation ou Hyper-V, a versão da máquina virtual deve ser uma versão licenciada dessas máquinas virtuais e não as versões gratuitas ou de teste.

Se a replicação estiver definida entre dois cores (origem e destino), será possível exportar dados do core de destino apenas após a replicação inicial estar concluída.

Gerenciar exportações

Standby virtual é um processo físico para virtual (P2V) que cria uma máquina virtual ou clone de uma máquina protegida. Um standby virtual pode ser criado usando um processo de exportação único ou de atualização contínua. Um standby virtual criado usando atualização contínua é atualizado de forma incremental após cada snapshot capturado na máquina de origem.

NOTA: O AppAssure suporta a exportação do Hyper-V para Window 8, Window 8.1, Windows Server 2012 e 2012 R2.

Na guia Standby virtual do Core Console, é possível visualizar o status das exportações atualmente definidas, incluindo exportações únicas e exportações contínuas para standby virtual. Nessa guia, é possível realizar uma variedade de ações para gerenciar as exportações, incluindo pausar, parar ou remover as exportações. Também é possível visualizar uma fila de futuras exportações.

Para gerenciar exportações

1 No Core Console, navegue até a guia Standby virtual.

Na guia Standby virtual, é possível visualizar uma tabela de definições de exportação salvas, incluindo as informações descritas na tabela a seguir.

Tabela 73. Definições de exportação para Standby virtual

Coluna	Descrição
Status	O status da configuração de standby virtual, exibido como ícone. Podem aparecer os seguintes ícones de status: • Ícone verde - Standby virtual configurado com sucesso, ativo e não pausado. A próxima exportação de Standby virtual será realizada logo após o próximo snapshot. • Ícone amarelo - Standby virtual em pausa e ainda salvo pelo Core. No entanto, após uma nova transferência, o trabalho de exportação não será iniciado automaticamente e não haverá novas exportações de Standby virtual para essa máquina protegida.
Nome da máquina	O nome da máquina de origem.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Última exportação	Data e hora da última exportação. Se uma exportação acaba de ser adicionada, mas não foi concluída, será exibida uma mensagem informando que a exportação ainda não foi realizada. Se uma exportação tiver falhado ou tiver sido cancelada, também será exibida uma mensagem correspondente.

2 Para gerenciar as definições de exportação salvas, selecione uma exportação e clique em um dos seguintes:

- **Pausar** - para pausar a exportação.
- **Retomar** - para reiniciar uma exportação em pausa.
- **Forçar** - para forçar uma nova exportação. Essa opção pode ser útil quando o standby virtual está em pausa e é retomado, o que significa que o trabalho de exportação será reiniciado somente após uma nova transferência. Se não quiser esperar a nova transferência, poderá forçar uma exportação.

3 Para remover uma exportação do sistema, clique em **Remover**. Ao remover uma exportação, ela é permanentemente removida do sistema e você não poderá reiniciá-la.

4 Para visualizar detalhes sobre as exportações ativas atualmente na fila a serem concluídas, clique em **Exibir fila de exportação**.

É exibida a tabela Fila de exportação na tabela Standby virtual e inclui as informações descritas na tabela a seguir.

Tabela 74. Informações sobre a tabela Fila de exportação

Coluna	Descrição
Nome da máquina	O nome da máquina de origem.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Tipo de programação	O tipo de exportação (Única ou Contínua).
Status	O progresso da exportação, exibido como porcentagem em uma barra de progresso.

5 Para gerenciar o número de exportações que podem ser executadas ao mesmo tempo, faça o seguinte:

- Na tabela Fila de exportação, clique em **Máximo de exportações simultâneas**.
- Na caixa de diálogo Máximo de exportações simultâneas, insira um número e clique em **Salvar**. O padrão é 5.

6 Para cancelar uma exportação na Fila de exportação, selecione uma exportação na tabela Fila de exportação e clique em **Cancelar**.

7 Para adicionar uma nova exportação de standby virtual, é possível clicar em **Adicionar** para iniciar o Assistente de exportação. Para obter mais informações sobre a definição de standby virtual para uma máquina virtual específica, consulte um dos seguintes tópicos:

- Exportar dados para uma máquina virtual ESXi
- Exportar dados para uma máquina virtual VMWare Workstation
- Exportar dados para uma máquina virtual Hyper-V
- Exportar dados para uma máquina virtual VirtualBox
- Exportar dados para uma máquina virtual VirtualBox baseada em Linux

Exportar dados para uma máquina virtual baseada em Windows

No AppAssure é possível exportar os dados de suas máquinas com Windows para uma máquina virtual (VMware, ESXi, Hyper-V e VirtualBox) exportando todas as informações de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos da programação de proteção da sua máquina.

Para exportar informações de cópia de segurança do Windows para uma máquina virtual

- No AppAssure Core Console, navegue até a máquina que deseja exportar. Na guia Resumo, no menu suspenso **Ações**, clique em **Exportar** e selecione o tipo de exportação que deseja realizar (Única ou Standby virtual). O Assistente de exportação é exibido.

  Vá aos seguintes tópicos para obter mais informações sobre exportação de dados do Windows para um tipo específico de máquina virtual.

  - Exportar dados para uma máquina virtual ESXi
  - Exportar dados para uma máquina virtual VMWare Workstation
  - Exportar dados para uma máquina virtual Hyper-V
  - Exportar dados para uma máquina virtual VirtualBox

Exportar dados para uma máquina virtual ESXi

No AppAssure, é possível optar por exportar dados para ESXi realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para ESXi

Execute as etapas deste procedimento para realizar uma exportação única para o ESXi.

Para realizar uma exportação ESXi única

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:

  a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.

  b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.

- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação a ser exportado no AppAssure Core e clique em **Avançar**.

Definir as informações da máquina virtual para realizar uma exportação para ESXi

Execute as etapas deste procedimento para definir as informações da máquina virtual.

Para definir as informações da máquina virtual para realizar uma exportação ESXi

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESX(i)**.

2 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 75. Parâmetros da máquina virtual

Opções	Descrição
Nome do host	Insira um nome para a máquina de host.
Porta	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

3 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 76. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco como Thin ou Thick.
Mapeamento de disco	Especifique o tipo de mapeamento de disco como Automático ou Manual.
Versão	Selecione a versão da máquina virtual.

4 Clique em **Avançar**.

5 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

6 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para ESXi

Conclua as etapas deste procedimento para realizar uma exportação contínua para ESXi.

Para realizar uma exportação contínua (Standby virtual) para ESXi

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESXi**.

3 Insira as informações para acessar a máquina virtual, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 77. Credenciais de ESXi

Opção	Descrição
Nome do host	Insira um nome para a máquina de host.
Porta	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

4 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 78. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco como Thin ou Thick.
Mapeamento de disco	Especifique o tipo de mapeamento de disco conforme adequado (Automático, Manual ou com VM).
Versão	Selecione a versão da máquina virtual.
Realizar exportação única inicial	Selecione para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado (opcional)

5 Clique em **Avançar**.

6 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

7 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportar dados para uma máquina virtual VMWare Workstation

No AppAssure, é possível optar por exportar dados para VMware Workstation realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para VMware Workstation

Execute as etapas deste procedimento para realizar uma exportação única para VMware Workstation.

Para realizar uma exportação VMware Workstation única

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
  - a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
  - b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação a ser exportado no AppAssure Core e clique em **Avançar**.

Configurar definições únicas para realizar uma exportação para VMware Workstation

Execute as etapas deste procedimento para determinar as definições de realização de uma exportação única VMware Workstation.

Para determinar as definições únicas para realizar uma exportação VMware Workstation

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

2 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 79. Parâmetros da máquina virtual

Opção	Descrição
Local	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.

Tabela 79. Parâmetros da máquina virtual

Opção	Descrição
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. NOTA: O nome padrão é o nome da máquina de origem.
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

3 Clique em **Avançar**.

4 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

5 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para VMware Workstation

Siga este procedimento para realizar uma exportação contínua para VMWare Workstation.

Para realizar uma exportação contínua (Standby virtual) para VMware Workstation

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar**> **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

3 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 80. Parâmetros da máquina virtual

Opção	Descrição
Caminho de destino	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA:** O nome padrão é o nome da máquina de origem.
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

4 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

5 Clique em **Avançar**.

6 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

7 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportar dados para uma máquina virtual Hyper-V

No AppAssure, é possível optar por exportar dados utilizando a Exportação para Hyper-V realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual).

O AppAssure oferece suporte à exportação de primeira geração do Hyper-V para os seguintes hosts:

- Windows 8
- Windows 8,1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

O AppAssure oferece suporte à exportação de segunda geração do Hyper-V para os seguintes hosts:

- Windows 8,1
- Windows Server 2012 R2

NOTA: Nem todas as máquinas protegidas podem ser exportadas a hosts de segunda geração do Hyper-V.

Somente máquinas protegidas com os seguintes sistemas operacionais da Interface Unificada de Firmware Extensível (UEFI) suportam exportação virtual para hosts de segunda geração do Hyper-V:

- Windows 8 (UEFI)
- Windows 8,1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

NOTA: A exportação do Hyper-V para VM de segunda geração poderá falhar caso o host do Hyper-V não tenha RAM suficiente alocada para realizar a exportação.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única de Hyper-V

Execute as etapas deste procedimento para realizar uma exportação única para o Hyper-V.

Para realizar uma exportação do Hyper-V única

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
  - a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
  - b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação a ser exportado no AppAssure Core e clique em **Avançar**.

Configurar definições únicas para realizar uma exportação de Hyper-V

Execute as etapas deste procedimento para determinar as definições de realização de uma exportação única do Hyper-V.

Para determinar as definições únicas para realizar uma exportação do Hyper-V

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **Hyper-V**.

2 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.

3 Para indicar que o server Hyper-V está localizado em uma máquina remota, clique na opção **Host remoto** e insira as informações do host remoto, conforme descrito na tabela a seguir.

Tabela 81. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Porta	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

4 Clique em **Avançar**.

5 Na página Opções de máquina virtual na caixa de texto Local da máquina de VM, insira o caminho para a máquina virtual, por exemplo, D:\export. Isso é usado para identificar o local da máquina virtual.

> **NOTA:** Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas, por exemplo, \\Dados\Compartilhamento, não é permitida.

6 Insira o nome da máquina virtual na caixa de texto **Nome da máquina virtual**.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

7 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem** - para identificar que o uso de RAM é idêntico entre as máquinas virtual e de origem.
- **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB**

  A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- **VHDX**
- **VHD**

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

9 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

10 Especifique o adaptador de rede adequado para a VM exportada.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

12 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para Hyper-V

Siga este procedimento para realizar uma exportação contínua para Hyper-V

Para realizar uma exportação contínua (Standby virtual) para Hyper-V

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.

3 Para indicar que o server Hyper-V está localizado em uma máquina remota, clique na opção **Host remoto** e insira os parâmetros do host remoto, conforme descrito na tabela a seguir.

Tabela 82. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Porta	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.

Tabela 82. Informações do host remoto

Caixa de texto	Descrição
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

4 Clique em **Avançar**.

5 Na página Opções de máquina virtual na caixa de texto Local da máquina de VM, insira o caminho para a máquina virtual, por exemplo, D:\export. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas, por exemplo, \\Dados\Compartilhamento, não é permitida.

6 Insira o nome da máquina virtual na caixa de texto **Nome da máquina virtual**.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

7 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem** - para identificar que o uso de RAM é idêntico entre as máquinas virtual e de origem.
- **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB**

  A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- **VHDX**
- **VHD**

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

9 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

10 Especifique o adaptador de rede adequado para a VM exportada.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

12 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

13 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportar dados para uma máquina virtual VirtualBox

No AppAssure, é possível optar por exportar dados utilizando a Exportação para VirtualBox realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual).

Também é possível exportar para uma VM do VirtualBox instalada em uma máquina Linux. Para obter mais informações, consulte Exportar dados para uma máquina virtual VirtualBox baseada em Linux.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

NOTA: Para realizar esse tipo de exportação, é preciso ter o VirtualBox instalado na máquina do Core. O Virtual Box Versão 4.2.18 ou superior é suportado para hosts Windows.

Realizar uma exportação única de VirtualBox

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

Para realizar uma exportação única para o VirtualBox

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
  - a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
  - b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação a ser exportado no AppAssure Core e clique em **Avançar**.

3 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.

4 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

5 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 83. Parâmetros da máquina virtual

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. NOTA: O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. NOTA: O caminho de destino não deve ser um diretório raiz. Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

6 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- **Nome de usuário** - insira o nome de usuário com o qual a máquina virtual é registrada.
- **Senha** - insira a senha dessa conta de usuário.

7 Clique em **Avançar**.

8 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua de VirtualBox (Standby virtual)

Conclua as etapas deste procedimento para criar um Standby virtual e realizar uma exportação contínua para VirtualBox.

Para realizar uma exportação contínua de VirtualBox (Standby virtual)

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.

3 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

4 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 84. Parâmetros da máquina virtual

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. **NOTA:** O caminho de destino não deve ser um diretório raiz. Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

5 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- **Nome de usuário** - insira o nome de usuário com o qual a máquina virtual é registrada.
- **Senha** - insira a senha dessa conta de usuário.

6 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

7 Clique em **Avançar**.

8 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

10

Gerenciar máquinas protegidas

Este capítulo descreve como visualizar, configurar e gerenciar as máquinas protegidas no seu ambiente AppAssure. Ele inclui as seguintes seções:

- Configurar as definições da máquina
- Acessar o diagnóstico de máquinas protegidas
- Gerenciar máquinas
- Gerenciar snapshots e pontos de recuperação

Na guia Início do AppAssure Core Console, você pode visualizar informações resumidas sobre qualquer máquina protegida pelo Core.

NOTA: Um agente de software atua em nome do usuário para realizar ações específicas. As máquinas protegidas também são chamadas de *agentes*, porque executam o software AppAssure Agent para facilitar a criação de cópias de segurança e a replicação de dados no AppAssure Core.

Você pode visualizar o status, o nome de exibição de cada máquina, o repositório que ela usa, a data e hora do último snapshot, o número de pontos de recuperação que existem no repositório da máquina e a quantidade total de espaço de armazenamento que os snapshots usam no repositório.

Para começar a gerenciar aspectos de qualquer máquina protegida, navegue até a máquina que deseja visualizar, configurar ou gerenciar. Na guia Início, há três maneiras de navegar até uma máquina protegida:

- Você pode clicar no nome de exibição de qualquer máquina protegida. Isso abre a guia Resumo da máquina protegida. Para ver uma descrição detalhada dessa página, consulte Visualizar a guia Máquinas de uma máquina protegida.
- Na área de navegação esquerda, você pode clicar em **Máquinas protegidas**. A guia Máquinas aparece. No painel Máquinas protegidas, você pode ver informações resumidas sobre cada máquina. Para ver uma descrição detalhada dessa página, consulte Visualizar a guia Resumo.
- Na área de navegação esquerda, em Máquinas protegidas, você pode clicar no nome de exibição de qualquer máquina. Isso abre a guia Resumo da máquina protegida. Para ver uma descrição detalhada dessa página, consulte Visualizar a guia Resumo

As tarefas que você pode realizar para gerenciar máquinas protegidas são divididas em algumas categorias.

- Você pode configurar as definições da máquina, acessar informações do sistema ou configurar notificações de eventos referentes a uma determinada máquina. Para obter mais informações, consulte Configurar as definições da máquina.
- Você pode acessar o diagnóstico de uma máquina protegida. Para obter mais informações, consulte Acessar o diagnóstico de máquinas protegidas.
- Você pode remover uma máquina da proteção, cancelar as operações atuais ou visualizar informações de licença de uma máquina protegida. Para obter mais informações, consulte Gerenciar máquinas.
- Você pode visualizar e gerenciar os dados salvos no Core. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.

Configurar as definições da máquina

Depois de adicionar proteção para máquinas no AppAssure, é fácil modificar as definições básicas da configuração da máquina (nome de exibição, nome de host, porta, chave de criptografia e repositório), as definições de proteção (alterar a programação de proteção de volumes na máquina, adicionar ou remover volumes ou pausar a proteção) e outras. Esta seção descreve as várias maneiras de visualizar e modificar as definições da máquina no AppAssure.

Visualizar e modificar as definições de configuração

Siga este procedimento para visualizar e modificar as definições de configuração.

Essa tarefa também é uma das etapas do Modificar definições de nó de cluster.

Para visualizar e modificar as definições de configuração

1 No AppAssure Core Console, navegue até a máquina da qual deseja visualizar e modificar as definições de configuração.

2 Clique na guia Configuração.

A página Definições é exibida.

3 Clique em **Alterar** para modificar as definições da máquina, como descrito na tabela a seguir.

Tabela 85. Definições da máquina

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para a máquina. Esse é o nome da máquina protegida que será exibido no AppAssure Core Console. Você pode inserir até 64 caracteres. Por padrão, esse é o nome de host da máquina. Se necessário, é possível mudá-lo para algo mais amigável. Não use caracteres proibidos ou frases proibidas.
Nome do host	Insira um nome de host para a máquina.
Porta	Insira um número de porta para a máquina. A porta é usada pelo serviço AppAssure Core para se comunicar com essa máquina. A porta padrão é *8006*.
Chave de criptografia	Se quiser que a criptografia definida para esse AppAssure Core seja aplicada aos dados de todos os volumes nessa máquina protegida, você pode especificar a chave de criptografia aqui. Se não existe uma chave de criptografia, você pode adicionar uma. Para obter mais informações sobre o gerenciamento de chaves de criptografia, consulte Se os volumes dessa máquina protegida estiverem criptografados, você pode alterar para uma chave de criptografia diferente. Alternativamente, você pode desassociar uma chave de criptografia selecionando (nenhuma) no menu suspenso Chave de criptografia. **NOTA:** Após aplicar uma chave de criptografia, alterar uma chave ou desassociar uma chave de uma máquina protegida, o AppAssure gera uma nova imagem de base no próximo snapshot programado ou forçado.
Repositório	Selecione um repositório para os pontos de recuperação. Exibe o repositório no AppAssure Core no qual devem ser armazenados os dados dessa máquina. **NOTA:** Essa definição pode ser alterada apenas se não houver pontos de recuperação ou se o repositório anterior estiver ausente.

Visualizar informações do sistema de uma máquina

O AppAssure Core Console fornece acesso fácil a todas as máquinas que estão sendo protegidas.

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de uma máquina protegida.

Para visualizar informações do sistema de uma máquina

1. Na área de navegação à esquerda do Core Console, em Máquinas protegidas, selecione a máquina da qual deseja exibir informações detalhadas do sistema.
2. Clique na guia Ferramentas dessa máquina, que abre exibindo a página Informações do sistema.

   A página Informações do sistema exibe informações detalhadas sobre a máquina, incluindo:

   - Nome do host
   - Versão de OS
   - Arquitetura de OS
   - Memória (Física)
   - Nome de exibição
   - Nome de domínio totalmente qualificado
   - Tipo de máquina virtual (se aplicável)

   Informações detalhadas sobre os volumes contidos nessa máquina também são exibidas e incluem:

   - Nome
   - ID do dispositivo
   - Sistemas de arquivos
   - Capacidade (incluindo Bruta, Formatada e Usada)

   Outras informações da máquina que são exibidas incluem:

   - Processadores
   - Adaptadores de rede
   - Endereços IP associados a essa máquina

Configurar grupos de notificação para eventos do sistema

No AppAssure, é possível configurar como os eventos do sistema são relatados por uma máquina individual criando grupos de notificação. Esses eventos podem ser alertas do sistema, erros, e assim por diante.

Para configurar grupos de notificação para eventos de sistema

1. No AppAssure Core Console, navegue até a máquina que deseja modificar.

   A guia Resumo é exibida.
2. Clique na guia Configuração e em **Eventos**.

   Aparece a página Grupos de notificação.
3. Clique em **Usar definições de alerta personalizadas**.

   A tela Grupos de notificação personalizados é exibida.
4. Clique em **Adicionar grupo** para adicionar novos grupos de notificação para o envio de uma lista de eventos do sistema.

A caixa de diálogo Adicionar grupo de notificação é exibida.

NOTA: Para usar as definições de alerta padrão, selecione a opção **Usar definições de alerta do Core**.

5 Adicione as opções de notificação conforme descrito na tabela a seguir.

Tabela 86. Opções de notificação

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.
Habilitar alertas	Selecione os eventos a compartilhar com esse grupo de notificação. É possível selecionar **Todos** ou um subconjunto de eventos que inclui: • Exchange • Atualização automática • Cache de deduplicação • Verificação de ponto de recuperação • Montagem remota • CD de inicialização • Segurança • Retenção do banco de dados • Montagem local • Metadados • Clusters • Notificação • Scripts do Power Shell • Instalação de envio por push • Capacidade de anexação • Trabalhos • Aplicação de licença • Truncamento de log • Arquivo • Serviço do Core • Exportar • Proteção • Replicação • Repositório • Reversão (Restauração) • Rollup **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher *Aviso*, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão (Restauração) são ativados.

Tabela 86. Opções de notificação

Caixa de texto	Descrição

Opções de notificação	Selecione o método para especificar como lidar com as notificações.
	Você pode selecionar dentre as seguintes opções:
	• **Notificar por e-mail**. É preciso especificar a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e, opcionalmente, Cco.
	NOTA: Para receber e-mail, o SMTP deve ser configurado antes.
	• **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação.
	• **Notificar por syslogd**. É preciso especificar a qual nome de host e porta enviar os eventos.
	  • **Host.** Insira o nome de host para o server.
	  • **Porta.** Insira o número da porta para a comunicação com o server.
	• **Notificar através de alertas do sistema.** Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

6 Clique em **OK** para salvar suas alterações.

7 Para editar um grupo de notificação existente, clique em **Editar** ao lado do grupo de notificação que **deseja editar**.

A caixa de diálogo Editar grupo de notificação é exibida para que as definições possam ser editadas.

Editar grupos de notificação para eventos do sistema

Execute as etapas do procedimento a seguir para editar grupos de notificação para eventos de sistema.

Para editar grupos de notificação para eventos de sistema

1 No AppAssure Core Console, navegue até a máquina que deseja modificar.

A guia Resumo é exibida.

2 Clique na guia Configuração e em **Eventos**.

3 Clique em **Usar definições de alerta personalizadas**.

A tela Grupos de notificação personalizados é exibida.

4 Clique no ícone Editar na coluna Ação.

A caixa de diálogo Editar grupo de notificação é exibida.

5 Edite as opções de notificação conforme descrito na tabela a seguir.

Tabela 87. Opções de notificação

Caixa de texto	Descrição
Nome	Representa o nome do grupo de notificação. NOTA: Não é possível editar o nome do grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.

Tabela 87. Opções de notificação

Caixa de texto	Descrição
Habilitar alertas	Selecione os eventos a compartilhar com o grupo de notificação. É possível selecionar **Todos** ou um subconjunto de eventos que inclui: • Exchange • Atualização automática • Cache de deduplicação • Verificação de ponto de recuperação • Montagem remota • CD de inicialização • Segurança • Retenção do banco de dados • Montagem local • Metadados • Clusters • Notificação • Scripts do Power Shell • Instalação de envio por push • Capacidade de anexação • Trabalhos • Aplicação de licença • Truncamento de log • Arquivo • Serviço do Core • Exportar • Proteção • Replicação • Repositório • Reversão (Restauração) • Rollup Também é possível optar por selecionar por tipo, incluindo: Informações, Aviso e Erro. **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher *Aviso*, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão (Restauração) são ativados.

Tabela 87. Opções de notificação

Caixa de texto	Descrição

Opções de notificação	Selecione o método para especificar como lidar com as notificações. As opções são:
	• **Notificar por e-mail**. É preciso especificar a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e, opcionalmente, Cco.
	NOTA: Para receber e-mail, o SMTP deve ser configurado antes.
	• **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação.
	• **Notificar por syslogd**. É preciso especificar o nome de host e a porta aos quais enviar os eventos.
	  • **Host.** Insira o nome de host para o server.
	  • **Porta.** Insira o número da porta para a comunicação com o server.
	• **Notificar através de alertas do sistema.** Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

6 Clique em **OK**.

Modificar definições de transferência

No AppAssure, é possível modificar as definições para gerenciar os processos de transferência de dados para uma máquina protegida. As definições de transferência descritas nesta seção são configuradas no nível de máquina protegida. Para fazer transferências no nível de core, consulte Modificar definições de fila de transferência.

O AppAssure suporta o Windows 8 e o Windows Server 2012 para transferências normais, de base e incrementais, bem como para restauração, bare metal restore e exportação de máquina virtual.

Há três tipos de transferência no AppAssure:

- **Snapshot.** Faz a cópia de segurança de dados na sua máquina protegida. São possíveis dois tipos de snapshots: a imagem de base de todos os dados protegidos e um snapshot incremental de dados atualizados desde o último snapshot. Esse tipo de transferência cria pontos de recuperação que são armazenados no repositório associado ao Core. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.
- **Exportação de máquina virtual.** Cria uma máquina virtual (VM) a partir de um ponto de recuperação, contendo todos os dados da cópia de segurança da máquina protegida, bem como o sistema operacional e os drivers e dados associados para garantir que a VM seja inicializável. Para obter mais informações, consulte Exportar dados protegidos de máquinas Windows para máquinas virtuais.
- **Restaurar**. Restaura as informações de cópia de segurança para uma máquina protegida. Para obter mais informações, consulte Restaurar volumes a partir de um ponto de recuperação.

  NOTA: O volume inteiro é sempre regravado durante a restauração de sistemas Windows usando partições do sistema EFI.

A transferência de dados no AppAssure envolve a transmissão de um volume de dados ao longo de uma rede, das máquinas protegidas do AppAssure para o Core. No caso de replicação, a transferência também ocorre do Core de origem ou fonte para o Core de destino.

A transferência de dados pode ser otimizada para seu sistema por meio de determinadas definições de opções de desempenho. Essas definições controlam o uso de largura de banda de dados durante o processo de criação de cópia de segurança de máquinas protegidas, exportação de VM ou restauração. Estes são alguns fatores que afetam o desempenho da transferência de dados:

- Número de transferências simultâneas de dados de agentes
- Número de fluxos simultâneos de dados

- Quantidade de alterações de dados no disco
- Largura de banda de rede disponível
- Desempenho do subsistema do disco do repositório
- Quantidade de memória disponível para armazenamento em buffer dos dados

É possível ajustar as opções de desempenho para melhor atender às suas necessidades de negócios e fazer o ajuste do desempenho com base em seu ambiente.

Para modificar as definições da transferência

1 No AppAssure Core Console, navegue até a máquina que deseja modificar.

2 Clique na guia Configuração e em **Definições de transferência**.

As definições atuais de transferência são exibidas.

3 Na página Definições de transferência, clique em **Alterar**.

A caixa de diálogo Definições de transferência é exibida.

4 Insira as opções de Definições de transferência para a máquina, como descrito na tabela a seguir.

Tabela 88. Opções de Definições de transferência

Caixa de texto	Descrição
Prioridade	Define a prioridade de transferência entre máquinas protegidas. Permite atribuir prioridade por comparação com outras máquinas protegidas. Selecione um número de 1 a 10, sendo 1 a maior prioridade. A definição padrão estabelece uma prioridade de 5. **NOTA:** A prioridade é aplicada às transferências que estão na fila.
Máximo de fluxos simultâneos	Define o número máximo de links TCP enviados para o Core para serem processados em paralelo para cada máquina protegida. **NOTA:** A Dell recomenda definir esse valor em 8. Se houver perda de pacotes, tente aumentar essa definição.
Máximo de gravações simultâneas	Define o número máximo de ações simultâneas de gravação em disco por conexão de máquina protegida. **NOTA:** A Dell recomenda defini-lo com o mesmo valor selecionado para Máximo de fluxos simultâneos. Se houver perda de pacotes, defina um valor ligeiramente mais baixo; por exemplo, se Máximo de fluxos simultâneos for 8, mude este para 7.
Usar o Número máximo de novas tentativas padrão do Core	Selecione essa opção para usar o número de tentativas padrão para cada máquina protegida, se algumas das operações não forem concluídas.
Tamanho máximo do segmento	Especifica a maior quantidade de dados, em bytes, que um computador pode receber em um único segmento TCP. A definição padrão é 4194304. **CUIDADO: Não altere essa configuração padrão.**
Profundidade máxima da fila de transferência	Especifica a quantidade de comandos que podem ser enviados simultaneamente. É possível ajustá-la para um número maior se o seu sistema possuir um número elevado de operações simultâneas de entrada/saída.
Leituras pendentes por fluxo	Especifica quantas operações de leitura em fila serão armazenadas no back-end. Essa definição ajuda a controlar o enfileiramento de máquinas protegidas. **NOTA:** A Dell recomenda definir esse valor em 24.

Tabela 88. Opções de Definições de transferência

Caixa de texto	Descrição
Gravadores excluídos	Selecione um gravador que deseja excluir. Como os gravadores que aparecem na lista são específicos para a máquina que você está configurando, você não verá todos os gravadores em sua lista. Por exemplo, alguns gravadores que você pode ver incluem: • Gravador ASR • Gravador COM+ REGDB • Gravador de contadores de desempenho • Gravador de registro • Gravador Shadow Copy Optimization • SQLServerWriter • Gravador de sistema • Gravador do programador de tarefas • Gravador de armazenamento de metadados VSS • Gravador WMI
Porta do server de dados de transferência	Define a porta para transferências. A definição padrão é 8009.
Tempo limite de transferência	Especifica em minutos e segundos o tempo a permitir que um pacote permaneça estático sem transferência.
Tempo limite de snapshot	Especifica em minutos e segundos o tempo máximo a aguardar para tirar um snapshot.
Tempo limite de leitura da rede	Especifica em minutos e segundos o tempo máximo a aguardar por uma conexão de leitura. Se a leitura de rede não puder ser realizada naquele tempo, a operação será tentada novamente.
Tempo limite de gravação da rede	Especifica o tempo máximo em segundos a aguardar por uma conexão de gravação. Se a gravação de rede não puder ser realizada naquele tempo, a operação será tentada novamente.

5 Clique em **OK**.

Personalizar trabalhos noturnos para uma máquina protegida

Os trabalhos noturnos podem ser configurados no nível do Core e no nível da máquina na guia Configuração adequada. Quando as configurações de trabalho noturno são alteradas no nível do Core, as alterações são aplicadas a todas as máquinas relevantes protegidas por esse Core. As alterações feitas nos trabalhos noturnos no nível da máquina substituem as alterações feitas no nível do Core.

Para obter uma lista de todos os trabalhos noturnos, incluindo descrições e o escopo disponível para cada um, consulte o tópico Noções básicas sobre trabalhos noturnos.

Execute as etapas do procedimento a seguir para realizar alterações em trabalhos noturnos em uma única máquina.

Personalizar trabalhos noturnos para uma máquina protegida

1 Na área de navegação à esquerda do AppAssure Core, selecione a máquina para a qual deseja personalizar trabalhos noturnos.

A guia Resumo da máquina selecionada é exibida.

2 Clique na guia Configuração para a máquina, e depois em **Configurações**.

3 Ao lado de Trabalhos noturnos, clique em **Alterar**.

A caixa de diálogo Trabalhos noturnos é exibida.

4 Selecione os trabalhos que deseja incluir nos trabalhos noturnos ou desmarque as opções que deseja omitir para essa máquina.

> **NOTA:** As opções podem variar por máquina. Por exemplo, uma máquina protegida que utiliza o Exchange Server poderá incluir os logs de trabalho de verificação de soma de verificação e de truncamento do Exchange.

5 Clique em **OK**.

> **NOTA:** Os resultados desse procedimento aplicam-se apenas à máquina protegida selecionada. Para serem aplicados em outro local, repita o procedimento para cada máquina que desejar personalizar. Para alterar as configurações de trabalho noturno para todas as máquinas protegidas por um Core, consulte Configurar trabalhos noturnos para o Core, Configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log em todas as máquinas protegidas ou Configurar verificações noturnas de soma de verificação do banco de dados do Exchange e truncamento de log.

Acessar o diagnóstico de máquinas protegidas

No AppAssure, você pode baixar e visualizar informações de diagnóstico de máquinas protegidas individuais. Além disso, o AppAssure permite baixar, visualizar e carregar dados de log no Core. Para obter mais informações sobre logs do Core, consulte Acessar os diagnósticos do Core. Para acessar os logs de máquina, consulte os procedimentos a seguir:

- Baixar logs de máquina
- Visualizar logs de máquina

Baixar logs de máquina

Se você encontrar erros ou problemas com uma máquina protegida, poderá baixar os logs da máquina para visualizá-los ou carregá-los no Suporte do AppAssure.

Para baixar logs da máquina

1 Navegue até o AppAssure Core Console e selecione a máquina protegida cujos logs você deseja baixar.

2 Clique no menu suspenso ou aba Ferramentas, clique em **Diagnóstico** e, em seguida, clique em **Visualizar log**.

3 Na página Baixar log de agente da guia Ferramentas, clique em **Clique aqui para iniciar o download**.

4 Na caixa de diálogo Abrindo AgentAppRecovery.log, selecione **Salvar arquivo**.

5 Clique em **OK**.

O arquivo é salvo na sua pasta Downloads.

Visualizar logs de máquina

Se você encontrar quaisquer erros ou problemas com a máquina, poderá ser útil visualizar os logs.

Para visualizar logs de máquina

1 Navegue até o AppAssure Core Console e selecione a máquina cujos dados de log você deseja visualizar.

2 Clique no menu suspenso ou aba Ferramentas, clique em **Diagnóstico** e, em seguida, clique em **Visualizar log**.

3 Na página Baixar log de agente da guia Ferramentas, clique em **Clique aqui para iniciar o download**.

4 Na caixa de diálogo Abrindo AgentAppRecovery.log, selecione **Abrir com** e use a lista suspensa para selecionar o programa com o qual deseja abrir o arquivo (por exemplo, Bloco de notas).

5 Clique em **OK**.

6 O arquivo é aberto no programa que você selecionou.

Visualizar o status da máquina e outros detalhes

Execute a etapa deste procedimento para visualizar o status e outros detalhes de uma máquina.

Para visualizar o status da máquina e outros detalhes

- No AppAssure Core Console, navegue até a máquina protegida que deseja visualizar.

  As informações sobre a máquina são exibidas na guia Resumo. Os detalhes exibidos incluem:

  - Nome do host
  - Último snapshot tirado
  - Próximo snapshot programado
  - Status da criptografia
  - Número da versão

  Se o Exchange Server estiver instalado na máquina, informações detalhadas sobre o server também serão exibidas, incluindo:

  - Última verificação de capacidade de montagem bem-sucedida realizada
  - Última verificação de soma de verificação bem-sucedida realizada
  - Último truncamento de log realizado

  As informações dos detalhes sobre os volumes contidos nessa máquina também são exibidas e incluem:

  - Nome
  - Tipo de sistema de arquivos
  - Uso de espaço
  - Programação
  - Programação atual
  - Próximo snapshot
  - Tamanho total

  Se o SQL Server estiver instalado na máquina, informações detalhadas sobre o server também serão exibidas, incluindo:

  - Status online
  - Nome
  - Caminho de instalação
  - Versão

  Se o Exchange Server estiver instalado na máquina, informações detalhadas sobre o server e os armazenamentos de e-mail também serão exibidas, incluindo:

  - Versão

- Caminho de instalação
- Caminho de dados
- Nome do banco de dados
- Caminho dos bancos de dados do Exchange
- Caminho do arquivo de log
- Prefixo do log
- Caminho do sistema
- Tipo de MailStore

Gerenciar máquinas

Esta seção descreve as diferentes tarefas que você pode executar para gerenciar suas máquinas. Os tópicos são:

- Remover uma máquina
- Cancelar operações em uma máquina
- Visualizar informações de licença em uma máquina

Remover uma máquina

Ao remover uma máquina da proteção no AppAssure Core, você tem duas opções: manter os pontos de recuperação salvos até o momento no AppAssure Core ou removê-los. Se você mantiver os pontos de recuperação, terá o que é conhecido como máquina “apenas com pontos de recuperação". Usando esses pontos de recuperação para a máquina que foi removida da proteção atual, você pode continuar a restaurar a máquina no futuro, mas apenas até o estado capturado em um ponto de recuperação salvo.

Se você remover os pontos de recuperação, essa ação excluirá do AppAssure Core todos os dados de snapshot da máquina anteriormente protegida.

△ **CUIDADO: Se você excluir pontos de recuperação, não poderá mais restaurar os dados dessa máquina.**

Execute as etapas do procedimento a seguir para remover uma máquina da proteção no seu ambiente do AppAssure.

Para remover uma máquina

1 No AppAssure Core Console, navegue até a máquina que deseja remover.

2 No menu suspenso **Ações**, clique em **Remover máquina** e selecione uma das opções descritas na tabela a seguir.

Tabela 89. Opções de Remover máquina

Opção	Descrição
Manter pontos de recuperação	Mantém todos os pontos de recuperação atualmente armazenados desta máquina.
Remover pontos de recuperação	Remove do repositório todos os pontos de recuperação atualmente armazenados desta máquina.

Cancelar operações em uma máquina

É possível cancelar operações atualmente em execução em uma máquina. Você pode especificar o cancelamento de apenas um snapshot atual ou cancelar todas as operações atuais, incluindo exportações, replicações, e assim por diante.

Para cancelar operações em uma máquina

1. No AppAssure Core Console, navegue até a máquina da qual deseja cancelar operações.
2. Clique na guia Eventos.
3. Expanda os detalhes de evento referentes ao evento ou operação que deseja cancelar.
4. Clique em **Cancelar**.

Visualizar informações de licença em uma máquina

É possível visualizar informações atuais de status da licença do software AppAssure Agent instalado em uma máquina protegida.

Para visualizar informações da licença

1. No AppAssure Core Console, navegue até a máquina que deseja visualizar.
2. Clique na guia Configuração e em **Aplicação de licença**.

   Aparece a tela Status e apresenta os seguintes detalhes sobre a aplicação de licença do produto:

   - Data de expiração
   - Status da licença
   - Tipo de licença
   - Tipo de agente

Gerenciar snapshots e pontos de recuperação

Um ponto de recuperação é uma coleção de snapshots tirados de volumes de disco individuais e armazenados no repositório. Os snapshots capturam e armazenam o estado de um volume de disco em determinado momento, enquanto os aplicativos que geram os dados ainda estão em uso. No AppAssure, é possível forçar um snapshot, pausar temporariamente os snapshots e visualizar as listas de pontos de recuperação atuais no repositório, além de excluí-los se necessário. Os pontos de recuperação são utilizados para restaurar as máquinas protegidas ou para montar um sistema de arquivos local.

Os snapshots capturados pelo AppAssure são feitos no nível do bloco e reconhecem o aplicativo. Isso significa que todas as transações abertas e os logs de transação contínua são concluídos e os caches são descarregados em disco antes da criação do snapshot.

O AppAssure usa um driver de filtro de volume de baixo nível, que se anexa aos volumes montados e depois rastreia todas as alterações no nível de bloco para o próximo snapshot iminente. O Microsoft Volume Shadow Services (VSS) é usado para facilitar snapshots consistentes de falhas de aplicativos.

Visualizar pontos de recuperação

Execute as etapas do procedimento a seguir para visualizar os pontos de recuperação.

Para visualizar pontos de recuperação

1 No AppAssure Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

Você pode visualizar informações sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 90. Informações do ponto de recuperação

Informações	Descrição
Status	Indica o status atual do ponto de recuperação.
Criptografado	Indica se o ponto de recuperação é criptografado.
Conteúdo	Relaciona os volumes incluídos no ponto de recuperação.
Tipo	Define um ponto de recuperação como uma imagem de base ou um snapshot (diferencial) incremental.
Data de criação	Exibe a data em que o ponto de recuperação foi criado.
Tamanho	Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.

Visualizar um ponto de recuperação específico

Execute as etapas do procedimento a seguir para visualizar detalhes sobre um ponto de recuperação específico.

Para visualizar um ponto de recuperação específico

1 No AppAssure Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

3 Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.

Você pode visualizar informações mais detalhadas sobre o conteúdo do ponto de recuperação da máquina selecionada, bem como acessar uma variedade de operações que podem ser realizadas no ponto de recuperação, como descrito na tabela a seguir.

Tabela 91. Detalhes do ponto de recuperação

Informações	Descrição
Ações	O menu Ações inclui as seguintes operações que podem ser realizadas no ponto de recuperação selecionado: **Montar**. Selecione essa opção para montar o ponto de recuperação selecionado. Para obter mais informações, consulte Montar um ponto de recuperação. **Exportar**. Usando a opção Exportar, é possível exportar o ponto de recuperação selecionado para ESXi, VMWare Workstation, HyperV ou Virtual Box. Para obter mais informações, consulte Exportar dados para uma máquina virtual baseada em Windows. **Restaurar**. Selecione essa opção para restaurar do ponto de recuperação selecionado em um volume especificado. Para obter mais informações, consulte Selecionar um ponto de recuperação e iniciar a BMR. **Verificar.** Se a máquina protegida possui um Exchange Server instalado, selecione essa opção para forçar uma verificação de soma de verificação ou de capacidade de montagem. Para obter mais informações, consulte Gerenciar verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log. Se a máquina protegida possui um SQL Server instalado, selecione essa opção para forçar uma verificação de capacidade de anexação. Para obter mais informações, consulte Forçar uma verificação de capacidade de anexação do SQL Server.
Conteúdo	A área Conteúdo inclui uma linha para cada volume no ponto de recuperação expandido, relacionando as seguintes informações de cada volume: **Status**. Indica o status atual do ponto de recuperação. **Título**. Relaciona o volume específico no ponto de recuperação. **Tipo**. Indica se um ponto de recuperação específico é uma imagem de base ou um snapshot (diferencial) incremental. **Tamanho**. Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.

4 Clique no símbolo de maior que (>) ao lado de um volume no ponto de recuperação selecionado para expandir a visualização.

Você pode visualizar informações sobre o volume selecionado no ponto de recuperação expandido, conforme descrito na tabela a seguir.

Tabela 92. Informações do volume

Caixa de texto	Descrição
Título	Indica o volume específico no ponto de recuperação.
Sistemas de arquivos	Indica o tipo do sistema de arquivos para o volume selecionado.
Capacidade bruta	Indica a quantidade de espaço de armazenamento bruto em todo o volume.
Capacidade formatada	Indica a quantidade de espaço de armazenamento no volume que está disponível para dados após o volume ser formatado.
Capacidade usada	Indica a quantidade de espaço de armazenamento atualmente em uso no volume.

Montar um ponto de recuperação

No AppAssure, você pode montar um ponto de recuperação de uma máquina com Windows para acessar dados armazenados por meio de um sistema de arquivos local.

NOTA: Para montar um ponto de recuperação do Linux com o utilitário aamount, consulte Montar um volume de ponto de recuperação em máquina Linux.

NOTA: Ao montar pontos de recuperação de dados restaurados de uma máquina com deduplicação de dados ativada, será preciso ativar também a deduplicação no servidor do Core.

Para montar um ponto de recuperação

1 No AppAssure Core Console, navegue até a máquina que deseja montar em um sistema de arquivos local.

A guia Resumo da máquina selecionada é exibida.

2 Clique na guia Pontos de recuperação.

3 Na lista de pontos de recuperação, clique no símbolo de maior que (>) para expandir o ponto de recuperação que deseja montar.

4 Nos detalhes expandidos desse ponto de recuperação, clique em **Montar**.

A caixa de diálogo Montar pontos de recuperação é exibida.

5 Na caixa de diálogo Montar ponto de recuperação, edite as definições de montagem de um ponto de recuperação, conforme descrito na tabela a seguir.

Tabela 93. Definições de Montar ponto de recuperação

Opção	Descrição
Local de montagem: Pasta local	Especifique o caminho usado para acessar o ponto de recuperação montado.
Opções de montagem: Tipo de montagem	Especifique o modo de acessar os dados do ponto de recuperação montado: • Montagem de apenas leitura • Montagem de apenas leitura com gravações anteriores • Montagem gravável
Imagens de volume	Especifique as imagens de volume que deseja montar
Criar um compartilhamento do Windows para essa montagem	Como opção, marque a caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e defina os direitos de acesso a ele, incluindo o nome de compartilhamento e os grupos permitidos.

6 Clique em **Montar** para montar o ponto de recuperação.

NOTA: Se você desejar copiar diretórios ou arquivos de um ponto de recuperação montado para outra máquina com Windows, use o Windows Explorer para copiá-los com as permissões padrão ou permissões de acesso do arquivo original. Para obter mais detalhes, consulte Restaurar um diretório ou arquivo usando o Windows Explorer a Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

7 Como opção, enquanto a tarefa estiver em andamento, você poderá visualizar seu progresso no menu suspenso Tarefas em execução no Core Console ou visualizar informações detalhadas na guia Eventos. Para obter mais informações sobre o monitoramento de eventos do AppAssure, consulte Visualizar tarefas, alertas e eventos.

Desmontar pontos de recuperação

Conclua as etapas deste procedimento para desmontar os pontos de recuperação que estão montados no Core.

NOTA: Ao desmontar um ponto de recuperação montado remotamente, isso é denominado *desconectar*.

Para desmontar pontos de recuperação

1 No AppAssure Core Console, clique no menu suspenso Ferramentas e depois em **Montagens**.

A página de Montagens aparece. Há um painel para Montagens locais (pontos de recuperação montados a partir do Core) e outro para Montagens remotas (pontos de recuperação montados por meio do Local Mount Utility). Em cada painel, os respectivos pontos de recuperação montados aparecem na lista.

2 Para os pontos de recuperação que você deseja desmontar, faça o seguinte:

- No painel **Montagens locais**, para cada ponto de recuperação montado localmente na lista que você deseja desmontar, clique em **Desmontar**. Para desmontar todos os pontos de recuperação montados localmente, clique em **Desmontar todos**.
- No painel **Montagens remotas**, para cada ponto de recuperação montado remotamente na lista que você deseja desmontar, clique em **desconectar**. Para desmontar todos os pontos de recuperação montados remotamente, clique em **Desconectar todos**.

3 Na caixa de diálogo Desmontagem dos pontos de recuperação, clique em **Sim** para confirmar.

4 Confirme que os pontos de recuperação montados anteriormente não são mais exibidos na lista de Montagens remotas ou locais, conforme adequado.

Forçar um snapshot

Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior são transferidos. Se não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos são transferidos, o que é chamado de imagem de base.

NOTA: O AppAssure suporta Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 para transferências de base e incrementais.

Para forçar um snapshot

1 No AppAssure Core Console, navegue até a máquina ou cluster com o ponto de recuperação no qual deseja forçar um snapshot.

2 Na guia Resumo da seção Volumes, especifique os volumes para os quais se deve fazer snapshots e, em seguida, clique no botão **Forçar snapshot** ou **Forçar imagem de base**.

Tabela 94. Opções de Forçar snapshot

Opção	Descrição
Forçar snapshot	Faz um snapshot incremental dos dados atualizados desde a captura do último snapshot.
Forçar imagem de base	Tira um snapshot completo de todos os dados nos volumes da máquina.

Remover pontos de recuperação

É fácil remover do repositório os pontos de recuperação de determinada máquina. Ao excluir pontos de recuperação no AppAssure, especifique uma das seguintes opções.

- **Excluir todos os pontos de recuperação.** Remove do repositório todos os pontos de recuperação da máquina protegida selecionada.
- **Excluir um intervalo de pontos de recuperação**. Remove todos os pontos de recuperação em um intervalo especificado antes do atual, até e incluindo a imagem de base, ou seja, todos os dados da máquina, além de todos os pontos de recuperação após o atual até a próxima imagem de base.

NOTA: Não é possível recuperar os pontos de recuperação excluídos.

Para remover pontos de recuperação

1. No AppAssure Core Console, navegue até a máquina da qual deseja visualizar os pontos de recuperação.
2. Clique na guia Pontos de recuperação.
3. Clique no menu **Ações**.
4. Selecione uma das opções a seguir:
   - Para excluir todos os pontos de recuperação atualmente armazenados, clique em **Excluir tudo**.
   - Para excluir um conjunto de pontos de recuperação em um intervalo de dados específico, clique em **Excluir intervalo**.

     A caixa de diálogo Excluir será exibida.

     - Na caixa de diálogo Excluir intervalo, especifique o intervalo de pontos de recuperação que deseja excluir usando uma data e hora inicial e final e clique em **Excluir**.

Excluir uma cadeia de pontos de recuperação órfãos

Um ponto de recuperação órfão é um snapshot incremental que não está associado a uma imagem de base. Snapshots subsequentes continuam a se acumular sobre esse ponto de recuperação. No entanto, sem a imagem de base, os pontos de recuperação resultantes são incompletos e é improvável que contenham os dados necessários para concluir uma recuperação. Esses pontos de recuperação são considerados parte da cadeia de pontos de recuperação órfãos. Se essa situação ocorrer, a melhor solução é excluir a cadeia e criar uma nova imagem de base.

Para obter mais informações sobre como forçar uma imagem de base, consulte Forçar um snapshot.

Para excluir uma cadeia de pontos de recuperação órfãos

1. No AppAssure Core Console, navegue até a máquina protegida da qual deseja excluir a cadeia de pontos de recuperação órfãos.
2. Clique na guia Pontos de recuperação.
3. Em Pontos de recuperação, expanda o ponto de recuperação órfão.

   Esse ponto de recuperação é chamado, na coluna Tipo, de “Incremental, Órfão”.
4. A seguir, em Ações, clique em **Excluir**.

   Aparece a janela Excluir pontos de recuperação.
5. Na janela Excluir pontos de recuperação, clique em **Sim**.

CUIDADO: Excluir esse ponto de recuperação exclui toda a cadeia de pontos de recuperação, incluindo os pontos de recuperação incremental que ocorrem antes ou depois dela, até a próxima imagem de base. Essa operação não pode ser desfeita.

A cadeia de pontos de recuperação órfãos é excluída.

Migrar pontos de recuperação para um repositório diferente

Se quiser remover de um repositório os pontos de recuperação de uma máquina protegida sem excluí-los, você poderá migrá-los para outro repositório usando este procedimento. Por exemplo, se quiser remover os pontos de recuperação de uma máquina protegida porque o repositório está cheio ou porque você pretende proteger uma máquina usando outro Core e repositório, você poderá usar o procedimento a seguir para migrar os dados com segurança.

Para migrar pontos de recuperação para um repositório diferente

1. No AppAssure Core Console, pause a proteção das máquinas protegidas ou máquinas cujos pontos de recuperação você deseja migrar. Para obter mais informações, consulte Pausar e retomar a proteção.
2. Cancele todas as operações atuais das máquinas protegidas ou máquinas cujos pontos de recuperação você deseja migrar. Para obter mais informações, consulte Cancelar operações em uma máquina.
3. Arquive os pontos de recuperação das máquinas que você pausou. Para obter mais informações, consulte Criar um arquivo.
4. Crie um novo repositório para os pontos de recuperação migrados. Para obter mais informações, consulte Criar um repositório.
    - Se quiser usar um repositório existente, siga para a Etapa 5.
5. Quando terminar de criar o arquivo, exclua do repositório original todos os pontos de recuperação das máquinas pausadas usando a opção **Excluir todos**. Para obter mais informações, consulte Remover pontos de recuperação.
6. Altere o repositório de cada máquina que você pausou concluindo as etapas a seguir:
    a. No Core Console, clique na máquina protegida na árvore de navegação.
    b. Clique na guia Configuração.
    c. Ao lado de Definições, clique em **Alterar**.
    d. Na lista suspensa Repositório, selecione o nome do repositório que você criou na Etapa 4.
        - Se quiser usar um repositório existente, selecione o nome de um repositório.

    NOTA: Ao migrar pontos de recuperação para um repositório existente, certifique-se de que o repositório possui espaço livre suficiente para conter os pontos de recuperação migrados.

    e. Clique em **OK**.
7. Retome a proteção das máquinas que você pausou. Para obter mais informações, consulte Pausar e retomar a proteção.
8. Gere uma nova imagem de base de cada máquina protegido que você moveu. Para obter mais informações, consulte Forçar um snapshot e use a opção **Forçar imagem de base**.
9. Importe os dados arquivados das máquinas que você deseja migrar. Para obter mais informações, consulte Importar um arquivo.

11

Noções básicas sobre replicação

Este capítulo descreve como configurar e gerenciar a replicação de dados protegidos de um Core de origem do AppAssure para um Core de destino do AppAssure para recuperação após desastres. Ele inclui as seguintes seções:

- Noções básicas sobre unidades de propagação
- Noções básicas sobre ativação pós-falha e reativação pós-falha no AppAssure
- Considerações sobre desempenho para transferência de dados replicados
- Configurar a replicação
- Replicar para um Core de destino autogerenciado
- Replicar para um Core de destino de terceiros
- Adicionar uma máquina a uma replicação existente
- Consumir a unidade de propagação em um Core de destino
- Gerenciar definições de replicação
- Remoção da replicação
- Recuperar dados replicados
- Noções básicas sobre ativação pós-falha e reativação pós-falha

Esta seção fornece informações conceituais e de procedimentos para ajudá-lo a entender e configurar a replicação no AppAssure.

Replicação é o processo de copiar pontos de recuperação de um core AppAssure e transmiti-los a outro core AppAssure em um local separado para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais cores.

Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para um site de recuperação após desastres remoto (ou seja, um core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um core de origem pode ser configurada para replicar em um core de destino.

Os possíveis cenários de replicação incluem:

- **Replicação para uma localização local.** O core de destino situa-se em um centro de dados local ou localização no local e a replicação é sempre mantida. Nessa configuração, a perda do Core não impediria a recuperação.
- **Replicação para uma localização externa.** O core de destino está localizado em uma instalação de recuperação após desastres externa para recuperação em caso de perda.
- **Replicação mútua.** Dois datacenters em locais diferentes, cada um contendo um Core, protegendo máquinas e atuando mutuamente como cópia de segurança externa para recuperação após desastres. Nesse cenário, cada Core replica as máquinas protegidas do Core localizado no outro datacenter.

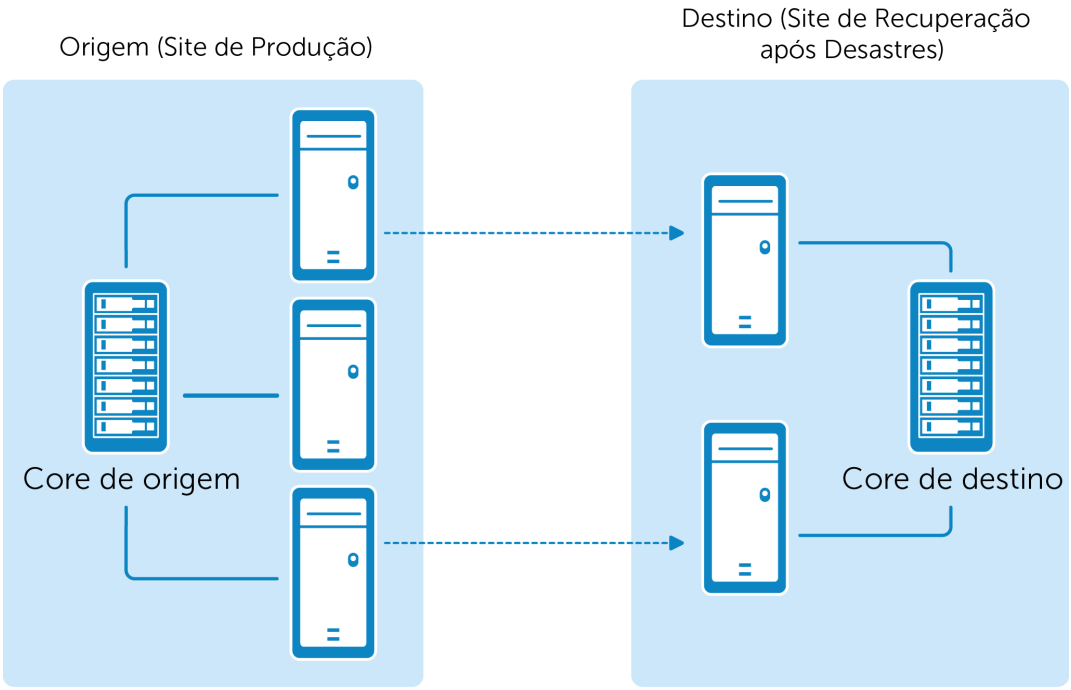
- **Replicação hospedada e na nuvem.** Os parceiros MSP do AppAssure mantêm vários cores de destino em um centro de dados ou uma nuvem pública. Em cada um desses cores, o parceiro MSP permite que um ou mais dos seus clientes replique os pontos de recuperação a partir de um core de origem no local do cliente para o core de destino do MSP por uma taxa.

  NOTA: Nesse cenário, os clientes têm acesso apenas aos próprios dados.

As possíveis configurações de replicação incluem:

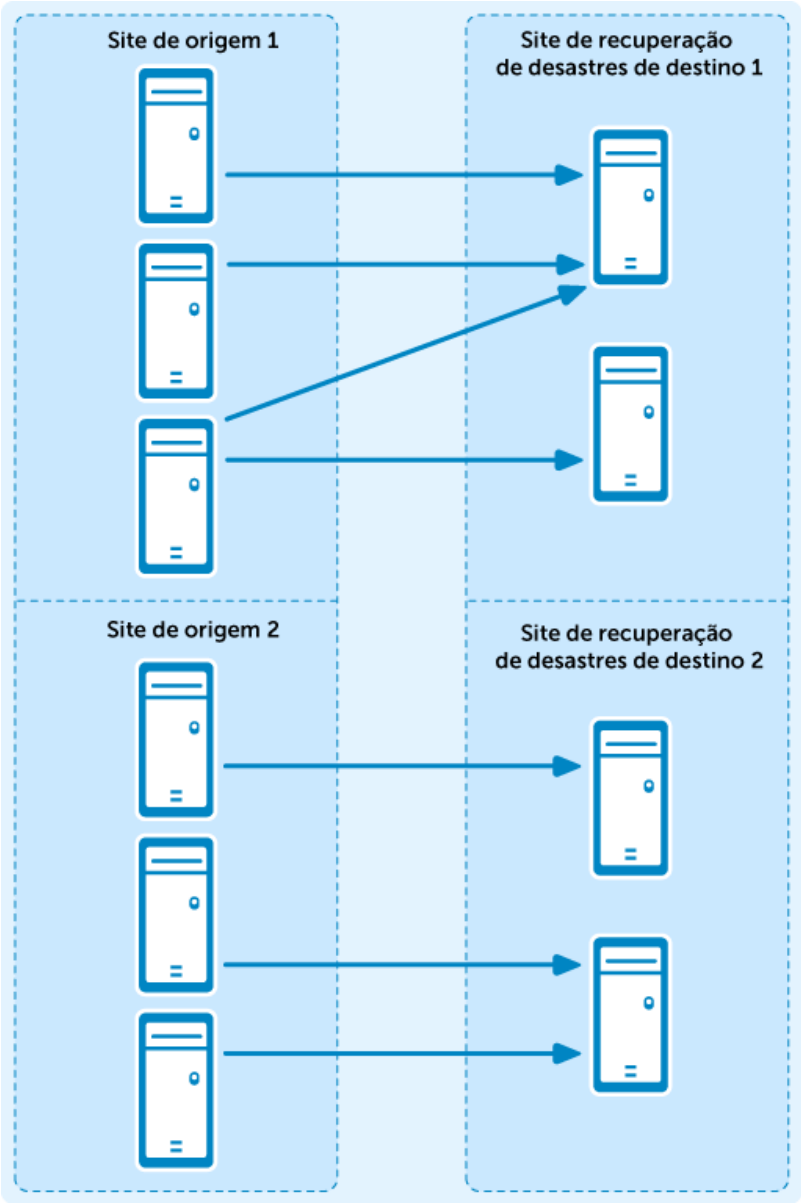
- **Ponto a ponto.** Replica uma única máquina protegida de um único Core de origem para um único Core de destino.

  Figura 5. Configuração ponto a ponto



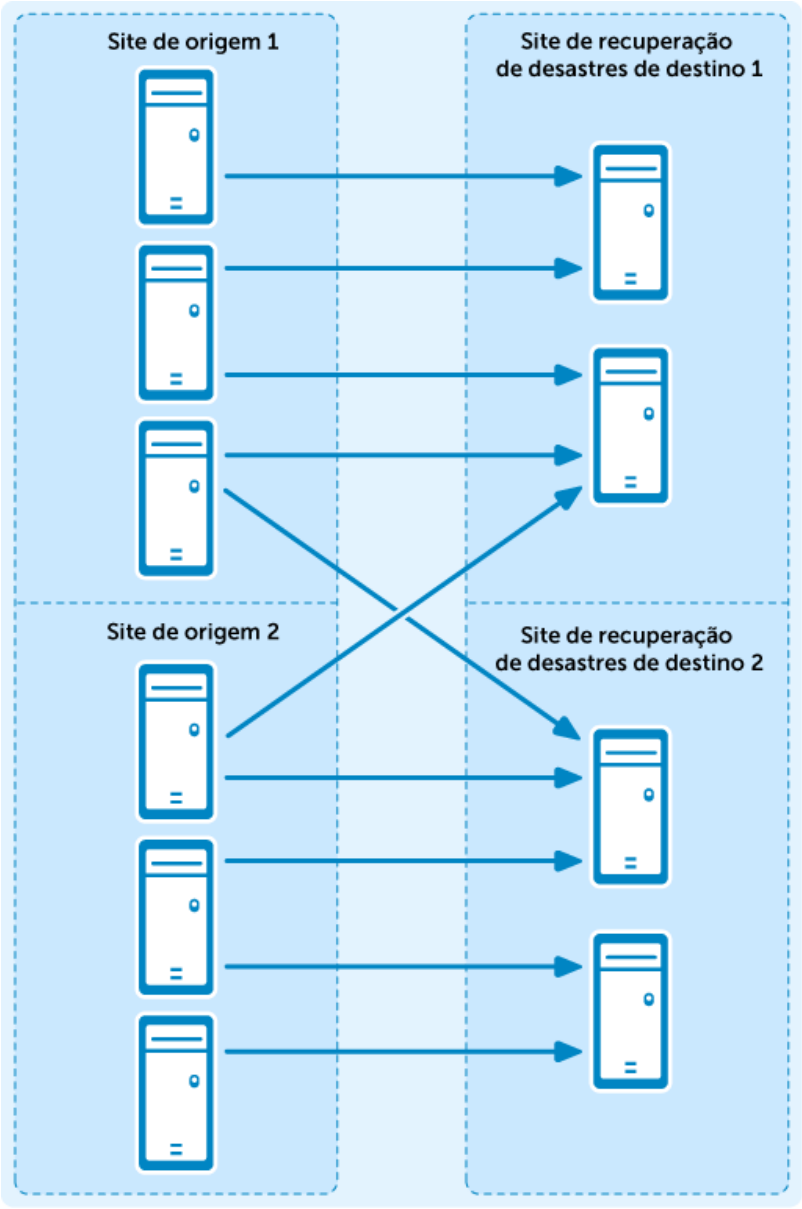
- **Multiponto a ponto.** Replica máquinas protegidas de vários Cores de origem para um único Core de destino.

Figura 6. Configuração multiponto a ponto



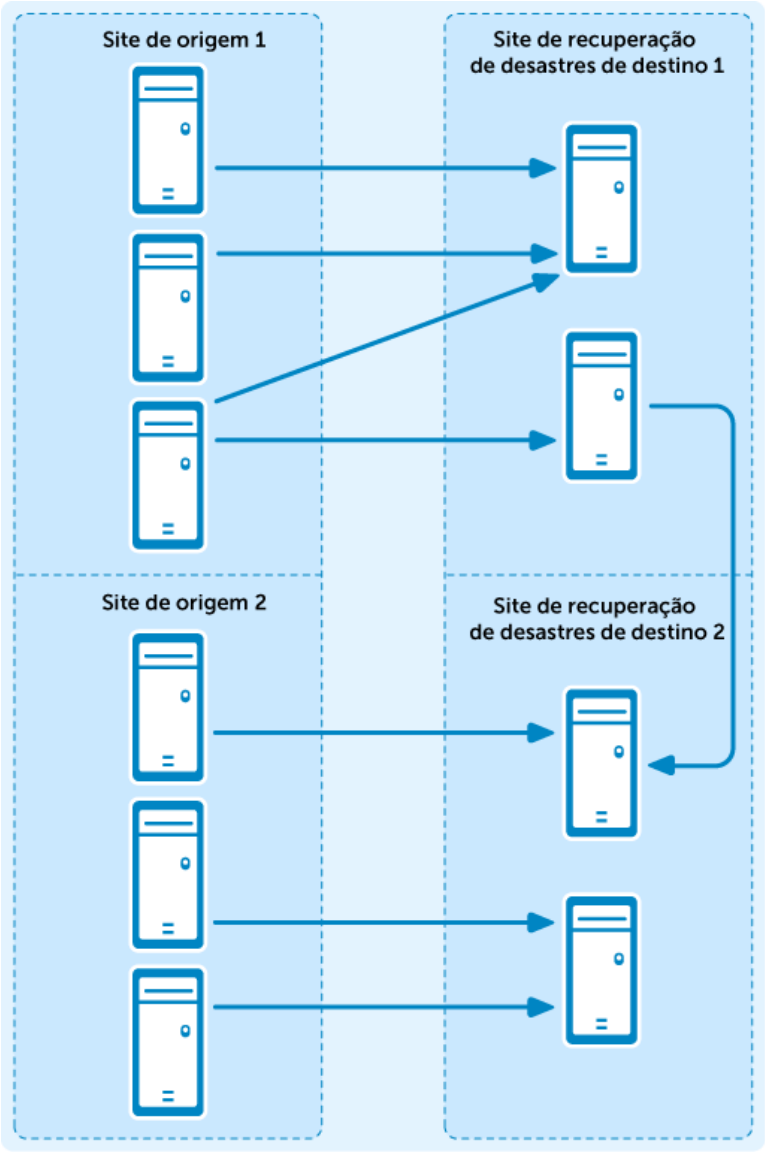
- **Ponto a multiponto.** Replica uma máquina protegida de um único Core de origem para mais de um Core de destino.

Figura 7. Configuração ponto a multiponto



- **Saltos múltiplos.** Replica uma máquina protegida replicada de um Core de destino para outro Core de destino, produzindo uma opção adicional de ativação pós-falha ou recuperação.

Figura 8. Configuração de saltos múltiplos



Noções básicas sobre unidades de propagação

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e snapshots incrementais das máquinas protegidas, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino por uma conexão de rede ou criando e salvando uma unidade de seeding em mídia externa e, depois, transferindo os dados iniciais para o core de destino. Normalmente, essa unidade de seeding é útil para grandes conjuntos de dados ou sites com links lentos.

NOTA: Embora seja possível propagar os dados da base por uma conexão de rede, isso não é recomendado. A propagação inicial envolve quantidades de dados potencialmente muito grandes, o que pode sobrecarregar uma conexão WAN típica. Por exemplo, se os dados de propagação medirem 10 GB e o link WAN transferir 24 Mbps, a transferência pode demorar cerca de uma hora para ser concluída.

Os dados do arquivo de propagação são compactados e, opcionalmente, criptografados e deduplicados. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Após a replicação ser estabelecida, todos os pontos de recuperação criados após o estabelecimento da unidade de seeding são replicados para o local de destino antes da transferência dos dados arquivados. Quando a unidade de seeding é consumida, os dados arquivados são sincronizados com os pontos de recuperação replicados presentes no repositório do core de destino.

A propagação é um processo de duas partes (também conhecido como copiar-consumir):

- A primeira parte envolve a cópia, que é a gravação dos dados replicados iniciais em uma fonte de mídia removível. Há duas opções de cópia: a duplicação de pontos de recuperação ainda não replicados a partir do core de origem para um dispositivo de armazenamento removível local, como unidade USB, ou duplicação de todos os pontos de recuperação existentes [opção Construir cadeias de RP (corrigir órfãos)]. Após a cópia estar concluída, você deve transportar a unidade do local do core de origem para o local remoto do core de destino.
- A segunda parte é consumir, o que ocorre quando um core de destino recebe a unidade transportada e copia os dados replicados no repositório. O Core de destino consome então os pontos de recuperação e os usa para formar agentes replicados (máquinas protegidas).

  NOTA: Embora a replicação de snapshots incrementais possa ocorrer entre os cores de origem e de destino antes de a propagação ser concluída, os snapshots replicados transmitidos da origem para o destino permanecem “órfãos” até que os dados iniciais sejam consumidos, e eles são combinados com as imagens de base replicadas. Para obter mais informações sobre pontos de recuperação órfãos, consulte Excluir uma cadeia de pontos de recuperação órfãos.

Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

A propagação é uma opção disponível no procedimento de replicação para um Core de destino autogerenciado e no procedimento de replicação para um Core gerenciado por terceiros (como um provedor de serviço gerenciado, ou MSP). Para obter mais informações, consulte Replicar para um Core de destino autogerenciado e Replicar para um Core de destino de terceiros, respectivamente.

Noções básicas sobre ativação pós-falha e reativação pós-falha no AppAssure

No caso de uma interrupção grave com falha do Core de origem e das máquinas protegidas, o AppAssure suporta a ativação e a reativação pós-falha em ambientes replicados. Ativação pós-falha refere-se à alternância para um AppAssure Core de destino redundante ou em standby em caso de falha do sistema ou encerramento anormal de um Core de origem e das máquinas protegidas associadas. O principal objetivo da ativação pós-falha é iniciar uma nova máquina protegida idêntica àquela que falhou e estava protegida pelo Core de origem com falha. O objetivo secundário é colocar o Core de destino em um novo modo para que ele proteja a máquina protegida de ativação pós-falha da mesma forma que o Core de origem protegia a máquina inicial antes da falha. O Core de destino pode recuperar instâncias das máquinas protegidas replicadas e iniciar imediatamente a proteção nas máquinas de ativação pós-falha.

Reativação pós-falha é o processo de restaurar uma máquina protegida e um Core aos seus estados originais (antes da falha). O principal objetivo da reativação pós-falha é restaurar a máquina protegida (na maioria dos casos, essa é uma nova máquina substituindo uma máquina com falha) a um estado idêntico ao último estado da nova máquina protegida temporária. Depois de restaurado, é protegido por um core de origem restaurado. A replicação também é restaurada, e o core de destino atua novamente como destino de replicação. Para obter mais informações, consulte Noções básicas sobre ativação pós-falha e reativação pós-falha.

Considerações sobre desempenho para transferência de dados replicados

Se a largura de banda entre o core de origem e o de destino não puder acomodar a transferência de pontos de recuperação armazenados, a replicação começa com propagação do core de destino com imagens de base e pontos de recuperação dos servers protegidos selecionados no core de origem. O processo de propagação pode ser realizado a qualquer momento, como parte da transferência inicial de dados para servir de base para a replicação regularmente programada, ou no caso de restabelecer a replicação de uma máquina anteriormente replicada cuja replicação tinha sido pausada ou excluída. Nesse caso, a opção Criar cadeia de ponto de recuperação deixaria copiar os pontos de recuperação ainda não replicados para uma unidade de propagação.

Ao se preparar para a replicação, você deve considerar os seguintes fatores:

- **Taxa de alteração.** A taxa de alteração é a taxa de acumulação da quantidade de dados protegidos. A taxa depende da quantidade de dados alterados em volumes protegidos e do intervalo de proteção dos volumes. Se um conjunto de blocos altera o volume, reduzir o intervalo de proteção reduz a taxa de alteração.
- **Largura de banda.** A largura de banda é a velocidade de transferência disponível entre o core de origem e o de destino. É vital que a largura de banda seja superior à taxa de alteração para que a replicação acompanhe os pontos de recuperação criados pelos snapshots. Devido à quantidade de dados transmitidos de um core para outro, vários fluxos paralelos podem ser necessários para se obter velocidades por fio de uma conexão Ethernet de 1GB.

  > **NOTA:** A largura de banda especificada pelo ISP é a largura de banda total disponível. A largura de banda de saída é compartilhada por todos os dispositivos na rede. Certifique-se de que haja largura de banda livre suficiente para replicação a fim de acomodar a taxa de alteração.

- **Número de máquinas protegidas.** É importante considerar o número de máquinas protegidas por Core de origem e quantas você pretende replicar no Core de destino. O AppAssure permite executar a replicação com base em server protegido, de modo que você pode decidir replicar alguns servers. Se todos os servers protegidos precisarem ser replicados, isso afetará drasticamente a taxa de alteração, em especial se a largura de banda entre os cores de origem e de destino for insuficiente para a quantidade e o tamanho dos pontos de recuperação a serem replicados.

Dependendo da configuração de rede, a replicação pode ser um processo demorado.

A Taxa de alteração máxima por Tipo de conexão de WAN é mostrada na tabela abaixo com exemplos da largura de banda necessária por gigabyte para uma taxa de alteração razoável.

Tabela 95. Exemplos de largura de banda por gigabyte

Banda larga	Largura de banda	Taxa de alteração máxima
DSL	768 Kbps ou mais	330 MB por hora
Cabo	1 Mbps ou mais	429 MB por hora
T1	1,5 Mbps ou mais	644 MB por hora
Fibra	20 Mbps ou mais	8,38 GB por hora

NOTA: Para obter resultados ideais, respeite as recomendações relacionadas na tabela acima.

Se um link falhar durante a transferência de dados, a replicação é retomada a partir do ponto de falha anterior da transferência, assim que a funcionalidade do link for restaurada.

Sobre replicação e pontos de recuperação criptografados

Embora a unidade de propagação não contenha cópias de segurança do registro e dos certificados do Core de origem, ela conterá as chaves de criptografia do Core de origem se os pontos de recuperação que estão sendo replicados da origem para o destino estiverem criptografados. Os pontos de recuperação replicados permanecem criptografados depois de transmitidos para o core de destino. Os proprietários ou administradores do core de destino precisam da frase de acesso para recuperar os dados criptografados.

Sobre políticas de retenção para replicação

As políticas de retenção nos Cores de origem e de destino não são sincronizadas. Rollup e exclusão ad hoc são executadas de forma independente em cada core na ação inicial, bem como durante os trabalhos ad hoc noturnos.

Para obter mais informações sobre as políticas de retenção, consulte Gerenciar políticas de retenção.

Configurar a replicação

Para replicar os dados usando o AppAssure, é preciso configurar os cores de origem e de destino para a replicação. Depois de configurar a replicação, você pode replicar dados de máquina protegida, monitorar e gerenciar a replicação e realizar a recuperação.

A realização da replicação no AppAssure envolve as seguintes operações:

- **Definir um repositório no core de destino.** Para obter mais informações sobre adicionar um repositório ao core de destino, consulte Criar um repositório.
- **Configurar a replicação autogerenciada.** Para obter mais informações sobre replicar em um core de destino autogerenciado, consulte Replicar para um Core de destino autogerenciado.
- **Configurar a replicação de terceiros.** Para obter mais informações sobre replicar em um core de destino de terceiros, consulte Replicar para um Core de destino de terceiros.
- **Replicar uma máquina protegida existente.** Para obter mais informações sobre replicação de uma máquina já protegida pelo Core de origem, consulte Adicionar uma máquina a uma replicação existente.
- **Consumir a unidade de seeding.** Para obter mais informações sobre consumir dados da unidade de seeding no core de destino, consulte Consumir a unidade de propagação em um Core de destino.

- **Definir a prioridade de replicação de uma máquina protegida.** Para obter mais informações sobre priorização da replicação de máquinas protegidas, consulte Definir a prioridade de replicação de uma máquina protegida.
- **Definir uma programação de replicação para uma máquina protegida.** Para obter mais informações sobre a definição de uma programação de replicação, consulte Programar a replicação.
- **Monitorar replicação conforme necessário.** Para obter mais informações sobre monitoramento de replicação, consulte Monitorar a replicação.
- **Gerenciar as definições de replicação conforme necessário.** Para obter mais informações sobre gerenciamento das definições de replicação, consulte Gerenciar definições de replicação.
- **Recuperar dados replicados em caso de desastre ou perda de dados.** Para obter mais informações sobre a recuperação de dados replicados, consulte Recuperar dados replicados.

Replicar para um Core de destino autogerenciado

Um core autogerenciado é um core ao qual você tem acesso, muitas vezes porque é gerenciado por sua empresa em um local externo. A replicação pode ser executada totalmente no core de origem, a menos que você escolha executar a propagação dos seus dados. A propagação exige que você consuma a unidade de seeding no core de destino depois de configurar a replicação no core de origem.

NOTA: Essa configuração se aplica à Replicação para localização externa e à Replicação mútua. O AppAssure Core deve ser instalado em todas as máquinas de origem e de destino. Se estiver configurando o AppAssure para replicação Multiponto a ponto, será preciso realizar essa tarefa em todos os cores de origem e no core de destino único.

Execute as etapas do procedimento a seguir para configurar seu core de origem a fim de replicar em um core de destino autogerenciado.

Para replicar um core de destino autogerenciado

1 Navegue até o AppAssure Core Console e clique na guia ou no ícone Replicação.

2 Na guia Replicação, clique em **Adicionar core de destino**.

O Assistente de replicação é exibido.

3 Na página Core de destino do Assistente de replicação, selecione **Tenho meu próprio core de destino** e insira as informações conforme descrito na tabela a seguir.

NOTA: Com o AppAssure, é possível replicar para o Dell DL-4000. Para obter mais informações sobre esse recurso, consulte as *Notas de versão do Dell AppAssure* ou a Base de conhecimento do AppAssure.

Tabela 96. Informações do Core de destino

Caixa de texto	Descrição
Nome do host	Insira o nome do host ou o endereço IP da máquina do Core na qual está replicando.
Porta	Insira o número da porta pela qual o AppAssure Core se comunicará com a máquina. O número de porta padrão é *8006*.
Nome de usuário	Insira o nome de usuário para acessar a máquina.
Senha	Insira a senha para acessar a máquina.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:

a Selecione **Usar um core de destino existente**.

b Selecione o core de destino na lista suspensa.

c Clique em **Avançar**.

d Vá para Etapa 7.

4 Clique em **Avançar**.

NOTA: Se não existir repositório no Core de destino, aparecerá um aviso informando que o Core de origem pode ser pareado ao de destino, mas você não poderá replicar agentes (máquinas protegidas) para esse local até que um repositório seja estabelecido. Para obter informações sobre como definir um repositório em um core, consulte Criar um repositório.

5 Na página Detalhes, digite um nome para essa configuração de replicação, por exemplo, SourceCore1.

- Se você estiver reiniciando ou reparando uma configuração de replicação anterior, selecione **Meu Core foi migrado e eu gostaria de reparar a replicação**.

6 Clique em **Avançar**.

7 Na página Máquinas, selecione as máquinas protegidas que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada máquina protegida.

8 Se desejar realizar o processo de propagação para a transferência dos dados de base, conclua as seguintes etapas:

NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página Máquinas, selecione *Usar uma unidade de propagação para realizar a transferência inicial*.

- Se você já tem uma ou mais máquinas protegidas replicando para um Core de destino, poderá incluí-las na unidade de propagação selecionando **Com já replicado**.

b Clique em **Avançar**.

c Na página Local da unidade de propagação, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa c.

Tabela 97. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.

Tabela 97. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 98. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione o tamanho máximo do segmento que deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding para uso futuro (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado se for necessário para copiar a unidade de seeding, mas não será reservado imediatamente após o início do processo de cópia). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.

Tabela 98. Opções da unidade de propagação

Item	Descrição
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3.x são compatíveis com o AppAssure 5.4.x e posterior.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h Na página Máquinas, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de propagação.

9 Clique em **Concluir**.

10 Se tiver criado uma unidade de seeding, envie-a para seu core de destino.

O emparelhamento do core de origem com o de destino está concluído. A replicação começa, mas produz pontos de recuperação órfãos no core de destino até que a unidade de seeding seja consumida e forneça as imagens de base necessárias.

Replicar para um Core de destino de terceiros

Um core de terceiros é um core de destino gerenciado e mantido por um MSP. Replicar em um core gerenciado por terceiros não exige que o cliente tenha acesso ao core de destino.

O processo de replicação em um core de terceiros envolve tarefas que devem ser executadas pelo cliente, bem como por terceiros. Depois de o cliente enviar uma solicitação de replicação nos cores de origem, o MSP deve executar a configuração do core de destino, revisando a solicitação.

NOTA: Essa configuração se aplica a replicação hospedada e na nuvem. O AppAssure Core deve ser instalado em todas as máquinas de core de origem. Se estiver configurando o AppAssure para replicação Multiponto a ponto, será preciso realizar essa tarefa em todos os cores de origem.

Para replicar em um core de destino gerenciado por terceiros, execute as seguintes tarefas:

1 Enviar uma solicitação de replicação para um provedor de serviços terceirizado

2 Revisar uma solicitação de replicação de um cliente ou Ignorar uma solicitação de replicação de um cliente

Enviar uma solicitação de replicação para um provedor de serviços terceirizado

Se você for um usuário final que assina um core gerenciado por terceiros, como um MSP, execute as etapas deste procedimento para enviar uma solicitação de replicação ao seu provedor de serviços de terceiros.

Para enviar uma solicitação de replicação a um provedor de serviços de terceiros

1 Navegue até o AppAssure Core e clique na guia Replicação ou no símbolo de replicação na coluna à esquerda.

2 Na guia Replicação, clique em **Adicionar core de destino**.

O Assistente de replicação é exibido.

3 Na página Core de destino do Assistente de replicação, selecione **Eu possuo uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação após desastres** e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 99. Informações sobre o Core de destino de terceiros

Caixa de texto	Descrição
Nome do host	Insira o nome de host, endereço IP ou FQDN da máquina de core de terceiros.
Porta	Insira o número da porta lhe foi fornecido pelo seu provedor de serviços de terceiros. O número de porta padrão é *8006*.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:
  a Selecione **Usar um core de destino existente**.
  b Selecione o core de destino na lista suspensa.
  c Clique em **Avançar**.
  d Vá para Etapa 7.

4 Clique em **Avançar**.

5 Na página Detalhes, insira as informações conforme descrito na tabela a seguir.

Tabela 100. Detalhes do Core de destino de terceiros

Caixa de texto	Descrição
Endereço de e-mail	Insira o endereço de e-mail associado à sua assinatura de serviço de terceiros.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

6 Clique em **Avançar**.

7 Na página Máquinas, selecione as máquinas protegidas que você deseja replicar no Core de terceiros.

8 Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas.

NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página Máquinas, selecione *Usar uma unidade de propagação para realizar a transferência inicial*.

- Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de propagação selecionando **Com já replicado**.

b Clique em **Avançar**.

c Na página Local da unidade de propagação, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou na Etapa c.

Tabela 101. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 102. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

Tabela 102. Opções da unidade de propagação

Item	Descrição
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3.x são compatíveis com o AppAssure 5.4.x e posterior.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h Na página Máquinas, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de propagação.

9 Clique em **Concluir**.

10 Se tiver criado uma unidade de seeding, envie-a conforme indicado pelo seu provedor de serviços de terceiros.

Revisar uma solicitação de replicação de um cliente

Depois que o usuário final concluir o procedimento Enviar uma solicitação de replicação para um provedor de serviços terceirizado, uma solicitação de replicação será enviada do core de origem para o core de destino de terceiros. Como terceiro, você pode revisar a solicitação e aprová-la para começar a replicação para seu cliente, ou pode negá-la para impedir que a replicação ocorra.

Escolha entre as opções a seguir:

- Aprovar uma solicitação de replicação
- Negar uma solicitação de replicação

Aprovar uma solicitação de replicação

Execute o procedimento a seguir para aprovar uma solicitação de replicação em um core de destino de terceiros.

Para aprovar uma solicitação de replicação

1. No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela Revisar solicitações de replicação é exibida.

   NOTA: As informações que aparecem na seção Identidade do core de origem dessa janela são determinadas pela solicitação executada pelo cliente.
4. Em Identidade do core de origem, realize um dos procedimentos a seguir:
   - Selecione Substituir um Core replicado existente e selecione um core na lista suspensa.
   - Selecione Criar um novo Core de origem e confirme se o Nome do Core, Endereço de e-mail do cliente e ID do cliente fornecidos estão corretos. Edite as informações conforme necessário.
5. Em Agentes, selecione as máquinas às quais se aplica a aprovação e use as listas suspensas na coluna Repositório para selecionar o repositório apropriado a cada máquina.
6. Como opção, na caixa de texto Comentário, insira uma descrição ou mensagem para ser incluída na resposta ao cliente.
7. Clique em **Enviar resposta**.

   A replicação é aceita.

Negar uma solicitação de replicação

Execute as etapas do procedimento a seguir para negar uma solicitação de replicação enviada a um core de terceiros a partir de um cliente.

Para negar uma solicitação sem revisá-la, consulte Ignorar uma solicitação de replicação de um cliente.

Para negar uma solicitação de replicação

1. No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela Revisar solicitações de replicação é exibida.
4. Clique em **Negar**.

   A replicação é negada. A notificação de negação aparece sob Alertas na guia Eventos do core de origem.

Ignorar uma solicitação de replicação de um cliente

Como prestador de serviço de terceiros de um core de destino, você tem a opção de ignorar uma solicitação de replicação enviada por um cliente. Essa opção pode ser usada se a solicitação tiver sido enviada por engano ou se você quiser negar uma solicitação sem revisá-la.

Para obter mais informações sobre solicitações de replicação, consulte Revisar uma solicitação de replicação de um cliente.

Execute o procedimento a seguir para ignorar uma solicitação de replicação de um cliente.

Para ignorar uma solicitação de replicação de um cliente

1. No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja ignorar e depois clique em **Ignorar**.
4. Na caixa de diálogo Desconsideração de solicitação, clique em **Sim** para confirmar o comando.

   Uma notificação de que a solicitação foi ignorada é enviada ao core de origem, e a solicitação é removida da guia Replicação do core de destino.

Adicionar uma máquina a uma replicação existente

Após o estabelecimento da replicação entre um Core de origem e um de destino, é possível adicionar novas máquinas protegidas para replicação no destino. Conclua as etapas do procedimento a seguir para adicionar uma nova máquina protegida a um Core de destino pareado para replicação.

Para obter mais informações sobre a replicação, consulte Noções básicas sobre replicação e Replicar para um Core de destino autogerenciado.

Para adicionar uma máquina a uma replicação existente

1. No AppAssure Core Console, clique no ícone ou guia Replicação.
2. Clique no menu suspenso ao lado do core de destino ao qual deseja replicar uma nova máquina e depois clique em **Adicionar máquinas**.

   O Assistente de replicação é aberto na página Máquinas.
3. Na página Máquinas, selecione as máquinas protegidas que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada máquina protegida.
4. Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas:

   NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

   a. Na página Máquinas, selecione *Usar uma unidade de propagação para realizar a transferência inicial*.

      - Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de propagação selecionando **Com já replicado**.

   b. Clique em **Avançar**.

c Na página Local da unidade de seeding, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa c.

Tabela 103. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 104. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

Tabela 104. Opções da unidade de propagação

Item	Descrição
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3.x são compatíveis com o AppAssure 5.4.x e posterior.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 5.

h Na página Máquinas, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de propagação.

5 Clique em **Concluir**.

Consumir a unidade de propagação em um Core de destino

Execute o procedimento a seguir para consumir os dados da unidade de seeding no core de destino.

NOTA: Esse procedimento é necessário apenas se uma unidade de seeding tiver sido criada como parte de Replicar para um Core de destino autogerenciado ou Replicar para um Core de destino de terceiros.

Para consumir a unidade de seeding em um core de destino

1 Se a unidade de seeding tiver sido salva em um dispositivo de armazenamento portátil, como uma unidade USB, conecte a unidade ao core de destino.

2 No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.

3 Na guia Replicação, em Replicação de entrada, clique no menu suspenso, no core de origem correto e, em seguida, clique em **Consumir**.

Será exibida a janela Consumir.

4 Para **Tipo de localização**, selecione uma das seguintes opções na lista suspensa:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa 4.

Tabela 105. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Verificar arquivo**.

O Core procura o arquivo.

Depois de localizar o arquivo, as seguintes caixas de texto aparecem na janela Consumir pré-preenchida com os dados obtidos em Etapa 4, Etapa 5 e o arquivo. O Período exibe as datas dos pontos de recuperação mais antigos e mais novos contidos na unidade de seeding. Qualquer comentário inserido quando a unidade de seeding foi criada é importado automaticamente.

7 Na janela Consumir, em Agentes, selecione as máquinas para as quais deseja consumir dados.

8 Clique em **Consumir**.

9 Para monitorar o progresso do consumo de dados, clique na guia Eventos.

Abandonar uma unidade de propagação

Se você criar uma unidade de seeding com a intenção de consumi-la no core de destino, mas optar por não enviá-la para o local remoto, um link para a Unidade de seeding pendente permanecerá na guia de replicação do core de origem. Nesse caso, você talvez queira abandonar a unidade de seeding pendente em favor de dados diferentes ou mais atuais.

Execute as etapas do procedimento a seguir para abandonar uma unidade de seeding pendente.

NOTA: Esse procedimento remove o link da unidade pendente do AppAssure Core Console no core de origem. Não remove a unidade do local de armazenamento no qual ela foi salva. Abandonar a unidade replica automaticamente todos os pontos de recuperação da unidade de seeding abandonada durante o próximo trabalho de replicação.

Para abandonar uma unidade de propagação

1. No core de origem, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Unidades de seeding pendentes (#)**.

   A seção Unidades de seeding pendentes aparece. Ela inclui o nome do core de destino remoto, a data e hora em que a unidade de seeding foi criada e o intervalo de dados dos pontos de recuperação incluídos na unidade de seeding.
3. Em Unidades de seeding pendentes, clique no menu suspenso da unidade que deseja abandonar e em **Abandonar**.

   A janela Unidades de seeding pendentes aparece.
4. Na janela Unidades de seeding pendentes, clique em **Sim** para confirmar.

   A unidade de seeding é removida.

   Se não houver mais unidades de seeding no core de origem, o link Unidades de seeding pendentes (#) e a seção Unidades de seeding pendentes serão removidos da guia Replicação.

Gerenciar definições de replicação

O AppAssure permite monitorar, programar e ajustar a replicação nos níveis global, de Core e de máquina protegida.

É possível editar as seguintes definições de replicação:

- Para programar trabalhos de replicação, consulte Programar a replicação.
- Para criar uma unidade de propagação de uma máquina protegida que já está pareada para replicação, consulte Usar a função Copiar para criar uma unidade de propagação
- Para monitorar o progresso de um trabalho de replicação, consulte Monitorar a replicação.
- Para pausar ou retomar um trabalho de replicação em pausa, consulte Pausar e retomar a replicação.
- Para forçar a replicação de uma máquina protegida de entrada ou saída, consulte Forçar a replicação.
- Para gerenciar as definições de todos os cores de destino e procedimentos de replicação, consulte Gerenciar definições para replicação de saída.
- Para gerenciar as definições de um core de destino individual, consulte Alterar as definições do Core de destino.
- Para gerenciar as definições de prioridade de uma máquina protegida individual que está sendo replicada para um Core de destino, consulte Definir a prioridade de replicação de uma máquina protegida.

Programar a replicação

É possível usar o programador de replicação para definir o momento, como em um dia específico ou fora do horário de pico, para a transferência de dados replicados do core de origem para o de destino.

Para programar a replicação

1. No AppAssure Core Console, clique no ícone ou guia Replicação.
2. Na guia Replicação, clique no menu suspenso ao lado do core para o qual deseja programar uma replicação e depois clique em **Programar**.

Abre-se a Programação de replicação para [NomeCore].

3 Selecione uma das três opções a seguir:

- **Sempre.** Replica após cada novo snapshot, verificação de soma de verificação e verificação de capacidade de anexação, e depois da conclusão de trabalhos noturnos.
- **Diário (Iniciar replicação somente durante o período especificado).** Começa a replicar apenas dentro do intervalo de tempo fornecido.
  a Na caixa de texto **De**, digite o primeiro horário em que a replicação deve começar.
  b Na caixa de texto **A**, digite o último horário em que a replicação deve começar.

> **NOTA:** Se a replicação estiver em andamento quando terminar o tempo programado, o trabalho de replicação é concluído depois do período de tempo alocado.

- **Personalizado.** Replica apenas dentro do intervalo de tempo fornecido no momento especificado da semana.
  a Ao lado de Dias da semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em um dia da semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em um dia da semana.
  b Ao lado de Fins de semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em fins de semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em fins de semana.

4 Clique em **Salvar**.

A programação é aplicada a todas as replicações do core de destino selecionado.

Usar a função Copiar para criar uma unidade de propagação

Caso tenha optado por não criar uma unidade de propagação ao configurar a replicação, você pode criar uma unidade de propagação usando a função Copiar no menu suspenso da máquina protegida.

Para usar a função Copiar para criar uma unidade de propagação

1 No AppAssure Core Console do Core de origem, clique na guia Replicação.

2 Em Replicação de saída, expanda o Core que protege a máquina para a qual você quer criar uma unidade de propagação e selecione a máquina.

3 No cabeçalho da tabela, clique no menu suspenso e selecione **Copiar**.

4 Na página Local da unidade de seeding, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa c.

Tabela 106. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Avançar**.

7 Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 107. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.

Tabela 107. Opções da unidade de propagação

Item	Descrição
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. NOTA: A propagação típica no AppAssure 5.4.x replica apenas o último ponto de recuperação para a unidade de propagação, o que reduz o tempo e a quantidade de espaço necessários para a criação da unidade de propagação. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure Core. NOTA: O formato atual da unidade de propagação não é compatível com as versões 5.3.x do Core. Os arquivos criados no AppAssure 5.3.x são compatíveis com o AppAssure 5.4.x e posterior.

8 Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 10.

9 Na página Máquinas, selecione as máquinas protegidas para as quais deseja criar uma unidade de propagação.

10 Clique em **Concluir**.

Monitorar a replicação

Quando a replicação está definida, é possível monitorar o status das tarefas de replicação dos cores de origem e de destino. É possível atualizar as informações de status, visualizar detalhes de replicação, e muito mais.

Para monitorar a replicação

1 No Core Console, clique no ícone ou guia Replicação.

2 Nessa guia, é possível visualizar informações sobre tarefas de replicação e monitorar o status delas, conforme descrito na tabela a seguir.

Tabela 108. Tarefas de replicação

Seção	Descrição	Ações disponíveis
Solicitações de replicação pendentes	Relaciona seu ID de cliente, endereço de e-mail e nome de host quando uma solicitação de replicação é enviada a um provedor de serviços de terceiros. Isso é relacionado aqui até que a solicitação seja aceita pelo MSP.	No menu suspenso, clique em **Ignorar** para ignorar ou rejeitar a solicitação.
Unidades de seeding pendentes	Relaciona as unidades de seeding gravadas, mas ainda não consumidas pelo core de destino. Inclui o nome de core remoto, data de criação e o período.	No menu suspenso, clique em **Abandonar** para abandonar ou cancelar o processo de propagação.

Tabela 108. Tarefas de replicação

Seção	Descrição	Ações disponíveis
Replicação de saída	Relaciona todos os cores de destino nos quais o core de origem está replicando. Inclui o nome do Core de destino, o estado de existência, o número de máquinas que estão sendo replicadas e o progresso de uma transmissão de replicação.	Em um core de origem, no menu suspenso, é possível selecionar as seguintes opções: • **Detalhes.** Relaciona o ID, URL, nome de exibição, estado, ID do cliente, endereço de e-mail e comentários do Core replicado. • **Alterar definições.** Relaciona o nome de exibição e permite editar o host e a porta do core de destino. • **Excluir.** Permite excluir o core de destino do core de origem. Fazer isso cessa toda a replicação para esse core. • **Programar.** Permite definir uma programação personalizada para replicação nesse core de destino. • **Adicionar máquinas.** Permite selecionar um host em uma lista suspensa, selecionar máquinas protegidas para replicação e criar uma unidade de propagação para a transferência inicial da nova máquina protegida.
Replicação de entrada	Relaciona todas as máquinas de origem a partir das quais o destino recebe os dados replicados. Inclui o nome de core remoto, estado, máquinas e progresso.	Em um core de destino, no menu suspenso, é possível selecionar as seguintes opções: • **Detalhes.** Relaciona o ID, nome do host, ID do cliente, endereço de e-mail e comentários para o core replicado. • **Consumir.** Consome os dados iniciais da unidade de seeding e os salva no repositório local. • **Excluir.** Permite excluir o core de origem do core de destino. Fazer isso cessa toda a replicação desse core.

Pausar e retomar a replicação

É possível pausar a replicação temporariamente para os Cores de origem (saída) ou de destino (entrada).

Para pausar e retomar uma replicação

1 No Core Console, clique na guia Replicação.

2 Use o sinal de maior que (>) para expandir o core de origem ou de destino adequado.

3 Selecione as máquinas protegidas cuja replicação deseja pausar, clique no menu suspenso ao lado de Nome do agente e clique em **Pausar** para pausar temporariamente a replicação.

O status da máquina aparece como “Estabelecido (em pausa)” na coluna Estado.

4 Para retomar a replicação, selecione o agente em pausa, clique no menu suspenso Nome do agente e em **Retomar**.

Forçar a replicação

Execute as etapas do procedimento a seguir para forçar a replicação a partir do core de origem ou de destino.

Para forçar a replicação

1 No AppAssure Core Console, clique no ícone ou guia Replicação.

2 Use o sinal de maior que (>) para expandir o core de origem ou de destino adequado.

3 Realize um dos procedimentos a seguir:

- Clique no menu suspenso ao lado da máquina protegida para a qual deseja forçar a replicação e depois clique em **Forçar**.
- Selecione as máquinas protegidas para as quais deseja forçar a replicação, clique no menu suspenso ao lado do nome da máquina e clique em **Forçar**.

4 Na caixa de diálogo, você tem a opção de selecionar **Restaurar apenas cadeias de Ponto de recuperação órfãs** para reparar cadeias órfãs de pontos de recuperação dessa máquina no core de destino.

5 Clique em **Sim.**

Gerenciar definições para replicação de saída

As alterações feitas nessas definições afetam a transferência de dados para todos os cores de destino associados a esse core de origem.

Para gerenciar definições para replicação de saída

1 No Core Console, clique no ícone ou guia Replicação.

2 Clique em **Definições**.

3 Na janela Definições de replicação, edite as definições de replicação, como descrito na tabela a seguir.

Tabela 109. Definições de replicação

Opção	Descrição
Duração do cache (segundos)	Especificar a quantidade de tempo entre cada solicitação de status de core de destino feita pelo core de origem.
Tempo limite da sessão de imagem do volume (minutos)	Especificar a quantidade de tempo que o core de origem gasta tentando transferir uma imagem de volume para o core de destino.
Máximo de fluxos paralelos	Especificar o número de conexões de rede com uso simultâneo permitido por uma única máquina protegida para replicar os dados dessa máquina.
Velocidade máxima de transferência (MB/s)	Especificar o limite de velocidade para a transferência de dados replicados.

4 Clique em **Salvar**.

Alterar as definições do Core de destino

O AppAssure permite alterar as definições de host e de porta para cores de destino individuais.

Para alterar as definições de core de destino

1 No AppAssure Core Console, clique no ícone ou guia Replicação.

2 Ao lado do core de destino apropriado, clique no menu suspenso e em **Alterar definições**.

Aparece a janela Definições.

3 Edite uma das opções descritas na tabela a seguir.

Tabela 110. Definições do Core de destino

Opção	Descrição
Host	Insira o host do core de destino.
Porta	Insira uma porta para que o core de destino use para comunicação com o core de origem. **NOTA:** A porta padrão é 8006.

4 Clique em **Salvar**.

Definir a prioridade de replicação de uma máquina protegida

Conclua as etapas a seguir para editar as definições que priorizam a replicação de uma máquina protegida.

Para definir a prioridade de replicação de uma máquina protegida

1 No AppAssure Core Console, clique no ícone ou guia Replicação.

2 Ao lado do Core de destino, clique no sinal de maior que (>) para expandir as máquinas protegidas que estão sendo replicadas.

3 Clique no menu suspenso da máquina protegida que deseja priorizar e depois clique em Definições.

4 Use a lista suspensa Prioridade para selecionar uma das seguintes opções. Você pode selecionar entre 1 (mais alto) e 10 (mais baixo). A definição padrão é 5.

5 Clique em **Salvar**.

Remoção da replicação

É possível descontinuar a replicação e remover as máquinas protegidas da replicação de várias maneiras. As opções incluem:

- Remover uma máquina protegida da replicação no Core de origem
- Remover uma máquina protegida no Core de destino
- Remover um Core de destino da replicação
- Remover um Core de origem da replicação

NOTA: A remoção de um Core de origem resulta na remoção de todas as máquinas replicadas protegidas por esse Core.

Remover uma máquina protegida da replicação no Core de origem

Conclua as etapas deste procedimento para remover uma máquina protegida da replicação no Core de origem.

Para remover uma máquina protegida da replicação no Core de origem

1. No core de origem, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Expanda a seção Replicação de saída.
3. No menu suspenso da máquina protegida que deseja remover da replicação, clique em **Excluir**.
4. Na caixa de diálogo Replicação de saída, clique em **Sim** para confirmar a exclusão.

Remover uma máquina protegida no Core de destino

Conclua as etapas deste procedimento para remover uma máquina protegida no Core de destino.

Para remover uma máquina protegida no Core de destino

1. No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Expanda a seção Replicação de entrada.
3. No menu suspenso da máquina protegida que deseja remover da replicação, clique em **Excluir**.
4. Se, além de remover a máquina protegida, você também quiser excluir todos os pontos de recuperação replicados recebidos dessa máquina, selecione **Com pontos de recuperação**.
5. Na caixa de diálogo Replicação de entrada, clique em **Sim** para confirmar a exclusão.

Remover um Core de destino da replicação

Execute as etapas deste procedimento para remover um core de destino da replicação.

Para remover um Core de destino da replicação

1. No core de origem, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Em Replicação de saída, clique no menu suspenso ao lado do core remoto que deseja excluir e em **Excluir**.
3. Na caixa de diálogo Replicação de saída, clique em **Sim** para confirmar a exclusão.

Remover um Core de origem da replicação

Execute as etapas deste procedimento para remover um core de origem da replicação.

NOTA: A remoção de um Core de origem resulta na remoção de todas as máquinas replicadas protegidas por esse Core.

Para remover um Core de origem da replicação

1. No core de destino, abra o AppAssure Core Console e clique na guia ou no ícone Replicação.
2. Em Replicação de entrada, no menu suspenso, clique em **Excluir**.
3. Se você deseja excluir todos os pontos de recuperação replicados recebidos dessa máquina, além de remover o core de origem, selecione **Com pontos de recuperação**.
4. Na caixa de diálogo Replicação de entrada, clique em **Sim** para confirmar a exclusão.

Recuperar dados replicados

A funcionalidade de replicação “Dia a dia” é mantida no core de origem, enquanto apenas o core de destino é capaz de executar as funções necessárias para a recuperação após desastres.

Para recuperação após desastres, o Core de destino pode usar os pontos de recuperação replicados para recuperar as máquinas protegidas e o Core. É possível executar as seguintes opções de recuperação no core de destino:

- Montar pontos de recuperação. Para obter mais informações, consulte Montar um ponto de recuperação.
- Rollback para pontos de recuperação. Para obter mais informações, consulte Restaurar volumes a partir de um ponto de recuperação ou Restaurar volumes em uma máquina Linux usando a linha de comando.
- Realizar uma exportação de máquina virtual (VM). Para obter mais informações, consulte Exportar dados para uma máquina virtual baseada em Windows.
- Realizar uma bare metal restore (BMR). Para obter mais informações, consulte Realizar uma bare metal restore em máquinas Windows.
- Realizar reativação pós-falha (no caso de haver um ambiente de replicação de ativação/reativação pós-falha definido). Para obter mais informações, consulte Realizar reativação pós-falha.

Noções básicas sobre ativação pós-falha e reativação pós-falha

Quando se deparar com uma situação de desastre em que seu Core de origem e a máquina protegida associada falharam, você pode habilitar a ativação pós-falha no AppAssure para alternar a proteção para um Core (de destino) de ativação pós-falha idêntico ao que falhou e iniciar uma nova máquina protegida (replicada) idêntica à máquina com falha. Depois que o Core de origem e as máquinas protegidas tiverem sido reparados, você poderá realizar uma reativação pós-falha para restaurar os dados a partir do Core e da máquina protegida de ativação pós-falha para o Core de origem e a respectiva máquina protegida. No AppAssure, a ativação e reativação pós-falha envolvem os seguintes procedimentos.

- **Definição de seu ambiente para ativação pós-falha.** Consulte a seção Definir um ambiente de ativação pós-falha.
- **Execução da ativação pós-falha do Core de destino e da máquina protegida associada.** Consulte a seção Realizar ativação pós-falha no Core de destino.
- **Restauração de um core de origem com a realização da reativação pós-falha.** Consulte a seção Realizar reativação pós-falha.

Definir um ambiente de ativação pós-falha

Para definir um ambiente de ativação pós-falha, é necessário que o AppAssure Core de origem e de destino e as respectivas máquinas protegidas estejam configurados para replicação. Execute as etapas deste procedimento para definir a replicação para ativação pós-falha.

Para definir um ambiente para ativação pós-falha

1. Instale um AppAssure Core para a origem e outro AppAssure Core para o destino. Para obter mais informações, consulte o *Guia de instalação e atualização do Dell AppAssure*.
2. Instale o software AppAssure Agent em qualquer máquina a ser protegida pelo Core de origem. Para obter mais informações, consulte o *Guia de instalação e atualização do Dell AppAssure*.
3. Crie um repositório no core de origem e um no core de destino. Para obter mais informações, consulte Criar um repositório.

4 Adicione a máquina para proteção no Core de origem. Para obter mais informações, consulte Proteger uma máquina.

5 Configure a replicação do Core de origem para o de destino e replique a máquina protegida com todos os pontos de recuperação. Siga as instruções na seção Replicar para um Core de destino autogerenciado para adicionar o core de destino no qual replicar.

Realizar ativação pós-falha no Core de destino

Ao se deparar com uma situação de desastre em que seu Core de origem e as máquinas protegidas associados falham, você pode habilitar a ativação pós-falha no AppAssure para alternar a proteção para seu Core idêntico de ativação pós-falha (de destino). O Core de destino torna-se o único Core que protege os dados em seu ambiente e então você inicia uma nova máquina protegida para substituir temporariamente a máquina com falha.

Antes de realizar este procedimento, você deve concluir as etapas descritas em Definir um ambiente de ativação pós-falha.

Para realizar a ativação pós-falha no core de destino

1 Navegue até o AppAssure Core Console no core de destino e clique na guia ou no ícone Replicação.

2 Em Replicação de entrada, expanda os detalhes do core de origem selecionado.

3 Clique no menu suspenso da máquina protegida preferida e selecione **Ativação pós-falha**.

A caixa de diálogo Ativação pós-falha aparece e relaciona as próximas etapas necessárias para executar uma ativação pós-falha.

- Para interromper qualquer tarefa de replicação que esteja em progresso nessa máquina protegida, selecione **Cancelar trabalho de replicação se estiver em execução**.

4 Clique em **Continuar**.

5 Na área de navegação esquerda, em Máquinas protegidas, selecione a máquina que tem a máquina protegida do AppAssure associada com pontos de recuperação.

6 Exporte as informações do ponto de recuperação de cópia de segurança nessa máquina protegida para uma máquina virtual. Para obter mais informações, consulte Exportar dados para uma máquina virtual baseada em Windows.

7 Inicie a máquina virtual que agora inclui as informações de cópia de segurança exportadas. É preciso aguardar o software de driver do dispositivo ser instalado.

8 Reinicie a máquina virtual e aguarde a inicialização do serviço AppAssure Agent.

9 Volte ao AppAssure Core Console do Core de destino e confirme se a nova máquina protegida aparece na área de navegação esquerda, em Máquinas protegidas, e na guia Replicação, em Replicação de entrada.

10 Force vários snapshots e confirme se eles são executados corretamente. Para obter mais informações, consulte Forçar um snapshot.

11 Agora, continue com a realização da reativação pós-falha. Consulte a próxima seção, Realizar reativação pós-falha.

Realizar reativação pós-falha

Depois de reparar ou substituir o Core de origem e as máquinas protegidas com falha, você terá que mover os dados das máquinas de ativação pós-falha para restaurar as máquinas de origem.

Para realizar a reativação pós-falha

1 Navegue até o AppAssure Core Console no core de destino e clique na guia ou no ícone Replicação.

2 Em Replicação de entrada, selecione a máquina protegida de ativação pós-falha e expanda os detalhes.

3 No menu Ações, clique em **Reativação pós-falha**.

A caixa de diálogo Reativação pós-falha é aberta e descreve as etapas que precisam ser seguidas antes de clicar no botão Continuar para executar a reativação pós-falha.

4 Clique em **Cancelar**.

5 Se a máquina com falha estiver executando o Microsoft SQL Server ou o Microsoft Exchange Server, interrompa esses serviços.

6 Force um snapshot da máquina. Para obter mais informações, consulte Forçar um snapshot.

7 Desligue a máquina com falha.

8 Crie um arquivo da máquina protegida de ativação pós-falha e salve-o no disco ou em um local de compartilhamento de rede. Para obter mais informações, consulte a seção Criar um arquivo.

9 Após a criação do arquivo, navegue até o AppAssure Core Console no core de origem recém-reparado e clique na guia Ferramentas.

10 Importe o arquivo que você acabou de criar na Etapa 8. Para obter mais informações, consulte a seção Importar um arquivo.

11 Volte ao Core Console no core de destino e clique na guia Replicação.

12 Em Replicação de entrada, selecione a máquina protegida de ativação pós-falha e expanda os detalhes.

13 No menu suspenso da máquina protegida, clique em **Reativação pós-falha**.

14 Na caixa de diálogo Reativação pós-falha, clique em **Continuar**.

15 Desligue a máquina que contém a máquina protegida exportada criada durante a ativação pós-falha.

16 Realize uma bare metal restore (BMR) do Core de origem e da máquina protegida. Para obter mais informações, consulte Realizar uma bare metal restore em máquinas Windows.

> **NOTA:** Ao iniciar a restauração conforme descrito em Selecionar um ponto de recuperação e iniciar a BMR, você precisará usar os pontos de recuperação que foram importados do Core de destino para a máquina protegida na máquina virtual.

17 Aguarde a reinicialização da BMR e o reinício do serviço AppAssure Agent e, em seguida, visualize e registre os detalhes da conexão de rede da máquina.

18 Navegue até o Core Console no core de origem, navegue até a máquina e modifique as definições de proteção da máquina para adicionar os novos detalhes de conexão de rede. Para obter mais informações, consulte Configurar as definições da máquina.

19 Navegue até o Core Console no Core de destino e exclua a máquina protegida da guia Replicação. Para obter mais informações, consulte Remoção da replicação.

20 No Core Console do core de origem, defina novamente a replicação entre origem e destino clicando na guia Replicação e depois adicione o core de destino para a replicação. Para obter mais informações, consulte a seção Replicar para um Core de destino autogerenciado.

12

Gerenciar eventos

Este capítulo descreve como gerenciar eventos no AppAssure Core que monitoram o estado do AppAssure Core e de suas máquinas protegidas. Ele inclui os seguintes tópicos:

- Visualizar tarefas, alertas e eventos
- Noções básicas sobre notificações por e-mail
- Configurar grupos de notificação
- Configurar redução de repetição
- Configurar retenção de eventos

O Core inclui conjuntos predefinidos de eventos, que podem ser usados para notificar os administradores sobre problemas críticos no Core ou nos trabalhos de cópia de segurança em máquinas protegidas.

- Você define os tipos de eventos que acionam alertas e quais abordagens usar para essas notificações configurando grupos de notificação. Para obter mais informações, consulte Configurar grupos de notificação.
- Se quiser que os administradores recebam notificações usando e-mail, consulte a seção Configurar redução de repetição. Além da configuração de um grupo de notificação, para receber alertas por e-mail é necessário Configurar um servidor de e-mail e Configurar um modelo de e-mail de notificação.
- Você pode reduzir o número de eventos do mesmo tipo e escopo que aparecem na guia Eventos usando o recurso de redução de repetição, que está ativado por padrão. Você pode desabilitar esse recurso ou controlar o intervalo de tempo para o qual os eventos são combinados em uma única ocorrência no log de eventos. Para obter mais informações, consulte Configurar redução de repetição.
- Você pode controlar o tempo de retenção das informações do histórico de eventos e trabalhos na guia Eventos do Core Console. Para obter mais informações, consulte Configurar retenção de eventos.

Visualizar tarefas, alertas e eventos

A guia Eventos no Core Console exibe um log de todos os eventos de sistema relacionados ao AppAssure Core. Ao visualizar a guia Eventos de uma máquina selecionada, você vê um log de todos os eventos do sistema relacionados a essa máquina específica.

O conteúdo da guia Eventos está dividido em três seções: Tarefas, Alertas e Eventos, onde você pode visualizar detalhes sobre cada evento, conforme apropriado.

É possível definir a forma de notificação de vários eventos configurando os grupos de notificação. Para obter mais informações, consulte Configurar grupos de notificação.

Execute as etapas dos procedimentos abaixo para visualizar as tarefas, alertas ou todos os eventos, respectivamente.

Visualizar tarefas

Uma tarefa é um trabalho que o AppAssure Core deve realizar, como transferir dados em uma cópia de segurança programada regular ou realizar uma restauração a partir de um ponto de recuperação.

Quando uma tarefa está em execução, ela é relacionada no menu suspenso Tarefas em execução no alto do Core Console.

Também é possível visualizar todas as tarefas do AppAssure Core ou todas as tarefas associadas a uma máquina específica.

Para visualizar as tarefas

1 Para visualizar todas as tarefas do AppAssure Core, navegue até a guia Inicial do AppAssure Core e clique na guia **Eventos**.

Se você quiser visualizar as tarefas de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar apenas as tarefas, no canto superior esquerdo da página, clique em **Tarefas**.

A lista de eventos é filtrada para exibir apenas as tarefas do Core ou da máquina selecionada.

3 Como opção, para filtrar a lista de tarefas por palavra-chave, data inicial, data final ou qualquer combinação, faça o seguinte:

a Para filtrar por palavra-chave, insira-a na caixa de texto Pesquisar palavra-chave.

b Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto De, digite a data e hora em formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2014 às 8h da manhã, insira 1/1/2013 8:00 AM.
- Para selecionar a data e hora atuais, clique no widget Calendário na caixa de texto De e clique em **Agora**.
- Clique no widget Calendário, selecione a data e a hora usando o calendário e os controles deslizantes e, em seguida, clique em **Concluído**.

c Para refinar ainda mais a lista de tarefas que aparece, você também pode definir uma data e hora final no mesmo formato.

A lista de tarefas é filtrada imediatamente com base nos critérios selecionados.

4 Como opção, você pode filtrar as tarefas que aparecem na lista da seguinte forma:

- Para ver apenas as tarefas ativas, clique no ícone **Tarefas ativas**.
- Para ver apenas as tarefas que estão na fila para serem executadas, clique no ícone **Enfileirado**.
- Para ver apenas as tarefas que estão esperando para serem realizadas, clique no ícone **Tarefas em espera**.
- Para ver apenas as tarefas que foram concluídas, clique no ícone **Tarefas concluídas**.
- Para ver apenas as tarefas com falha, clique no ícone **Tarefas com falha**.

5 Para exportar a lista de tarefas, selecione um formato na lista e clique em **Exportar o relatório**.

É possível exportar usando os seguintes formatos:

Tabela 111. Formatos de exportação

Formato	Descrição
PDF	Portable Document Format
XLS	Pasta de trabalho do Excel 1997 - 2003
XLSX	Pasta de trabalho do Excel

Tabela 111. Formatos de exportação

Formato	Descrição
RTF	Rich Text Format
CSV	Valores separados por vírgula

6 Clique no ícone **Detalhes do trabalho** de qualquer tarefa para iniciar uma nova janela com os detalhes da tarefa, incluindo:

- Hora inicial
- Hora final
- Status
- Tempo decorrido
- Progresso
- Taxa
- Trabalho total (tamanho ou porcentagem concluída)
- Tarefas subordinadas (se aplicável)
- Motivo da falha (se aplicável)

Visualizar alertas

Um alerta é uma notificação relacionada a uma tarefa ou evento. Os tipos de alertas incluem erros, avisos ou informações.

É possível exibir todos os alertas do AppAssure Core ou todos os alertas associados a uma máquina específica.

Para visualizar alertas

1 Para exibir todos os alertas do AppAssure Core, navegue até a guia Início do AppAssure Core e clique na guia **Eventos**.

Se você quiser visualizar os alertas de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar apenas os alertas, no canto superior esquerdo da página, clique em **Alertas**.

A lista de eventos é filtrada para exibir apenas os alertas do Core ou da máquina selecionada.

3 De forma opcional, se você quiser remover todos os alertas, clique em **Descartar tudo**.

Visualizar todos os eventos

É possível visualizar todos os eventos de um AppAssure Core ou todos os eventos associados a uma máquina específica.

Para visualizar eventos

1 Para visualizar todos os eventos do AppAssure Core, navegue até a guia **Inicial** do AppAssure Core e clique na guia **Eventos**.

Se você quiser visualizar os eventos de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar todos os eventos, no canto superior esquerdo da página, clique em **Eventos**.

Todos os eventos são exibidos para o Core ou a máquina selecionada.

Noções básicas sobre notificações por e-mail

Os eventos que geram alertas são definidos no grupo de notificação.

NOTA: É necessário estabelecer grupos de notificação mesmo que você não use e-mail como método de notificação. Para obter mais informações, consulte Configurar grupos de notificação.

Se você escolher e-mail como uma das opções de notificação, também precisará configurar um server de SMTP para e-mail. O AppAssure Core usa o server definido por você para enviar alertas com base nos parâmetros do grupo de notificação.

Também é necessário definir um modelo de e-mail de notificação. O Core usa isso para definir a linha de assunto do e-mail relativo a cada alerta e o conteúdo no corpo da mensagem. O modelo possui definições padrão, que você pode usar como estão ou testar e modificar para atender às suas necessidades.

Esta seção inclui os seguintes tópicos:

- Configurar um servidor de e-mail
- Configurar um modelo de e-mail de notificação

Configurar um servidor de e-mail

Execute as etapas deste procedimento para configurar um server de e-mail.

NOTA: Você também deve configurar as definições de grupo de notificação, incluindo a ativação da opção Notificar por e-mail, antes de as mensagens de alerta por e-mail serem enviadas. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

Para configurar um server de e-mail

1. Navegue até o AppAssure Core, clique na guia Configuração e depois em **Eventos**.
2. No painel Definições de e-mail, clique em **Server de SMTP**.

   A caixa de diálogo Definições de server de SMTP é exibida.
3. Insira os detalhes do server de e-mail conforme descrito na tabela a seguir.

Tabela 112. Definições do server de SMTP

Caixa de texto	Descrição
Server de SMTP	Digite o nome do server de e-mail a ser usado pelo modelo de notificação de e-mail. A convenção de nomenclatura inclui o nome do host, domínio e sufixo; por exemplo, smtp.gmail.com.
De	Insira o endereço de e-mail de devolução. Usado para especificar o endereço de e-mail de devolução para o modelo de notificação de e-mail; por exemplo, noreply@localhost.com.
Nome de usuário	Insira um nome de usuário do server de e-mail.
Senha	Insira a senha associada ao nome de usuário necessário para acessar o server de e-mail.
Porta	Insira um número de porta. Utilizado para identificar a porta do server de e-mail; por exemplo, porta 587 para o Gmail. O padrão é *25*.

Tabela 112. Definições do server de SMTP

Caixa de texto	Descrição
Tempo limite (segundos)	Insira um valor de número inteiro para especificar quanto tempo deve-se tentar se conectar ao server de e-mail. Utilizado para estabelecer o tempo em segundos antes de ocorrer o tempo limite. O padrão é 60 *segundos*.
TLS	Selecione essa opção se o server de e-mail usar uma conexão segura, como Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

4 Clique em **Enviar e-mail de teste** e faça o seguinte:

   a Na caixa de diálogo Enviar e-mail de teste, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.

   b Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Enviar e-mail de teste e revise suas definições de configuração do server de e-mail. Depois, repita a Etapa 4.

   c Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.

   d Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

   e Quando estiver satisfeito com os resultados de seus testes, retorne à caixa de diálogo Definições do server de SMTP e clique em **Salvar** para fechar a caixa de diálogo e salvar as definições.

Configurar um modelo de e-mail de notificação

Execute as etapas deste procedimento para configurar um modelo de notificação de e-mail. Esse modelo é usado pelo seu server de e-mail SMTP para enviar notificações sobre eventos do AppAssure por e-mail.

NOTA: Você também deve configurar um server de e-mail e as definições de grupo de notificação, incluindo a ativação da opção **Notificar por e-mail**, antes de as mensagens de alerta por e-mail serem enviadas. Para obter mais informações sobre como configurar um server de e-mail para o envio de alertas, consulte Configurar um servidor de e-mail. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

Para configurar um modelo de notificação de e-mail

1 Navegue até o AppAssure Core, clique na guia Configuração e depois em **Eventos**.

2 No painel Definições de e-mail, clique em **Alterar**.

   Aparece a caixa de diálogo Editar configuração de notificação de e-mail.

3 Selecione **Ativar notificações de e-mail**.

4 Na caixa de texto Assunto do e-mail, insira um assunto para o modelo de e-mail.

   O Assunto do e-mail é usado para definir o assunto do modelo de notificação por e-mail, por exemplo, <hostname> - <nível> <nome>.

5 Na caixa de texto E-mail, insira as informações do corpo do modelo que descrevem o evento, quando ocorreu e a gravidade.

6 Clique em **Enviar e-mail de teste** e faça o seguinte:

   a Na caixa de diálogo Enviar e-mail de teste, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.

   b Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Enviar e-mail de teste, clique em **OK** para salvar as definições do modelo de e-mail atuais e modificar as definições do server de e-mail, conforme descrito no procedimento Configurar um servidor de e-mail, sem deixar de inserir novamente a senha da conta de e-mail. Salve essas definições e volte a esse procedimento.

c Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.

d Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

Quando estiver satisfeito com os resultados de seus testes, retorne à caixa de diálogo Editar configuração de notificação de e-mail e clique em **OK** para fechar a caixa de diálogo e salvar as definições.

Configurar grupos de notificação

Os grupos de notificação permitem definir conjuntos de eventos específicos sobre os quais os usuários são alertados e a maneira como essa notificação ocorre. Você pode configurar os seguintes métodos para o envio de alertas:

- Por e-mail
- No log de eventos do Windows
- Usar syslogd
- Usar alertas do sistema
- Usar alertas
- Usar trap de SNMP

NOTA: Deve-se também configurar as definições do server SMTP se desejar enviar alertas como mensagens de e-mail, conforme descrito neste procedimento. Para obter mais informações sobre como definir as definições do server de e-mail, consulte Configurar um servidor de e-mail.

Execute as etapas deste procedimento para configurar os grupos de notificação para alertas.

Para configurar grupos de notificação

1 Navegue até o AppAssure Core, clique na guia Configuração e depois em **Eventos**.

2 Clique em **Adicionar grupo**.

A caixa de diálogo Adicionar grupo de notificação é exibida.

A caixa de diálogo Adicionar grupo de notificação contém uma área de descrição geral e duas guias:

- Habilitar alertas
- Opções de notificação

3 Insira as informações básicas para o grupo de notificação, conforme descrito na tabela a seguir.

Tabela 113. Informações do grupo de notificação

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação de eventos. Estas informações são obrigatórias.
Descrição	Insira uma descrição que explique a finalidade do grupo de notificação de eventos. Estas informações são opcionais.

4 Na guia Habilitar alertas, defina o conjunto de eventos do sistema que deseja registrar em log, criar relatórios e para o qual deseja ser alertado, como segue:

- Se desejar criar alertas para todos os eventos, selecione **Todos os alertas**.
- Se desejar criar alertas específicos para erros, avisos, mensagens informativas ou uma combinação desses, ao lado de Selecionar tipos, clique na opção apropriada:
  - Erro (ícone de triângulo vermelho)
  - Aviso (ícone de triângulo amarelo)

- Informações (círculo azul)
- Restaurar padrão (seta curvada)

- Se desejar criar alertas para eventos específicos, faça o seguinte:
  a Clique no símbolo de maior que (>) ao lado de Todos os alertas para expandir a exibição e mostrar Grupos. Em seguida, clique no símbolo de maior que (>) ao lado de Grupos para exibir os grupos de eventos relacionados para os quais é possível definir alertas. As categorias de grupo de eventos incluem:
    - Nuvens
    - Logs de servidor
    - Exchange
    - Arquivos programados
    - Atualização automática
    - Cache de deduplicação
    - Verificação de ponto de recuperação
    - Montagem remota
    - CD de inicialização
    - Segurança
    - Retenção do banco de dados
    - Montagem local
    - Metadados
    - Clusters
    - Notificação
    - PowerShell Scripting
    - Instalação de envio por push
    - Capacidade de anexação
    - Trabalhos
    - Aplicação de licença
    - Truncamento de log
    - Arquivo
    - Serviço do Core
    - Exportar
    - Proteção
    - Replicação
    - Repositório
    - Reversão (Restauração)
    - Rollup
  b Para visualizar eventos individuais em qualquer grupo, clique no símbolo de maior que (>) ao lado do grupo relevante e selecione os eventos específicos para os quais deseja registrar, emitir relatórios e definir alertas.
  c Para definir alertas para todos os eventos dentro de qualquer grupo, marque a caixa de seleção ao lado desse grupo.

5 Clique na guia Opções de notificação.

6 Na guia Opções de notificação, especifique como lidar com o processo de notificação.

A tabela a seguir descreve as opções de notificação.

Tabela 114. Opções de notificação

Caixa de texto	Descrição
Notificar por e-mail	Designe os destinatários da notificação de e-mail. É possível optar por especificar vários endereços de e-mail separados, bem como cópias carbono e ocultas. Você pode selecionar: • Para: • CC: • BCC:
Notificar pelo Log de eventos do Windows	Selecione essa opção se deseja que os alertas sejam comunicados por meio do Log de Eventos do Windows.
Notificar por sys logd	Selecione essa opção se deseja que os alertas sejam comunicados por meio de syslogd. Especifique os detalhes do syslogd nas seguintes caixas de texto: • Host: • Porta:
Notificar por alertas do sistema	Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.
Notificar por meio de alertas	
Notificar por trap SNMP	O AppAssure Core atua como um agente de SNMP, enviando traps (notificações sobre eventos específicos) para um gerenciador de SNMP. Isso permite que o Core transmita certas informações, como alertas, status do repositório e máquinas protegidas. Selecione essa opção se quiser que os eventos do Core sejam comunicados por trap de SNMP. Você também especificar um número de trap. Por exemplo, o número de trap padrão usado pelo AppAssure Core é 162.

7 Clique em **OK**.

Você verá uma mensagem indicando que o nome do grupo de notificação definido não pode ser alterado após a criação do grupo. Outras propriedades dentro do grupo de notificação podem ser alteradas a qualquer momento.

- Se você estiver satisfeito com o nome do grupo, confirme essa mensagem e salve o seu trabalho.
- Se quiser alterar o nome do grupo, clique em **Não** para voltar à janela Criar grupo de notificação, atualize o nome do grupo e outras definições de grupo de notificação e salve seu trabalho.

Configurar redução de repetição

É essencial que os administradores recebam alertas sobre certos eventos. No entanto, em certas circunstâncias, pode ser frustrante ou inconveniente receber notificações repetidas sobre um evento do qual você está ciente. Mesmo que um alerta seja gerado por uma falha ambiental da qual você deseja ficar sabendo imediatamente, é possível que a mesma condição de erro gere centenas ou milhares de eventos no log. Para reduzir a repetição no log de eventos e a inconveniência de receber repetidos e-mails sobre o mesmo evento no Core Console, o AppAssure inclui uma definição de redução de repetição, que está ativada por padrão e definida em cinco minutos. Essa definição pode ser ajustada entre 1 e 60 minutos. Também é possível desabilitá-la completamente.

Quando a redução de repetição está desabilitada, cada vez que ocorre um evento do mesmo tipo e escopo, ele é registrado no banco de dados. Independentemente do tempo decorrido desde a ocorrência anterior do evento, cada nova ocorrência é mostrada na seção Alertas da guia Eventos.

Quando a redução de repetição está configurada (por exemplo, com o tempo padrão de cinco minutos), o evento é registrado no banco de dados e mostrado no log de alertas quando ocorre pela primeira vez. Se subsequentemente um evento do mesmo tipo e escopo é novamente registrado dentro do limite de tempo estabelecido, a contagem do evento no banco de dados aumenta em 1 para cada ocorrência repetida dentro do limite. No entanto, o log exibido na seção Alertas da guia Eventos mostra o evento apenas uma vez, com a data e a hora da ocorrência mais recente. Ela não é atualizada com o mesmo evento até que o limite de tempo da primeira ocorrência expire.

NOTA: As definições de redução de repetição aplicam-se apenas ao log de eventos e não afetam as notificações por e-mail.

Execute as etapas deste procedimento para configurar a redução de repetição dos eventos.

Para configurar a redução de repetição

1. Na página inicial do AppAssure Core, clique no menu suspenso Configuração e clique em **Eventos**.
2. Na área Redução de repetição, clique em **Alterar**.

   A caixa de diálogo Redução de repetição é exibida.
3. Selecione **Ativar redução de repetição**.
4. Na caixa de texto **Armazenar eventos para**, use as setas para cima e para baixo a fim de inserir o número de minutos a armazenar os eventos para redução de repetição.
5. Clique em **OK**.

Configurar retenção de eventos

Execute as etapas deste procedimento para configurar a retenção de eventos.

Para configurar a retenção de eventos

1. Na página inicial do AppAssure Core, clique no menu suspenso Configuração e clique em **Definições**.
2. Em Definições de conexão do banco de dados, clique em **Alterar**.

   A caixa de diálogo Definições de conexão do banco de dados é exibida.
3. Na caixa de texto **Reter histórico de eventos e trabalhos por**, digite o número de dias pelos quais deseja reter as informações sobre eventos; por exemplo, *30 dias* (padrão).
4. Clique em **Salvar**.

13

Gerar e visualizar relatórios

Este capítulo fornece uma visão geral dos relatórios disponíveis no Dell AppAssure. Ele consiste nos seguintes tópicos:

- Noções básicas sobre relatórios de conformidade
- Noções básicas sobre relatórios de falha
- Noções básicas sobre o relatório resumido
- Gerar um relatório sobre um Core ou agente
- Noções básicas sobre os relatórios do Central Management Console no Core
- Gerar um relatório no Central Management Console

O AppAssure permite gerar e visualizar informações de conformidade, erro e resumo de várias máquinas core e agente.

Você pode optar por visualizar os relatórios on-line, imprimi-los ou exportá-los e salvá-los em um dos vários formatos suportados. Os formatos que podem ser selecionados são os seguintes:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagem

Nesta versão do AppAssure, os relatórios incluem agora as unidades de medida, o que torna mais fácil determinar se uma coluna é representada em GB, TB ou segundos.

Usar a barra de ferramentas de relatórios

A barra de ferramentas disponível para todos os relatórios permite imprimir e salvar de duas maneiras diferentes. A tabela a seguir descreve as opções de imprimir e salvar.

Tabela 115. Ícones da barra de ferramentas de relatórios

Ícone	Descrição
	Imprimir o relatório
	Imprimir a página atual
	Exportar um relatório e salvá-lo no disco

Para obter informações sobre como gerar um relatório, consulte Gerar um relatório sobre um Core ou agente. Para obter informações sobre como gerar um relatório para vários cores no Central Management Console, consulte Gerar um relatório no Central Management Console. Para obter informações sobre como gerar relatórios de cluster, consulte Visualizar um relatório de cluster ou nó.

Noções básicas sobre relatórios de conformidade

Os relatórios de conformidade estão disponíveis para o AppAssure Core e o AppAssure Agent. Eles fornecem uma maneira de visualizar o status dos trabalhos realizados por um core ou agente selecionado. Os trabalhos com falha aparecem em texto em vermelho. As informações do Relatório de conformidade do Core que não estão associadas a um agente aparecem em branco.

Os detalhes sobre os trabalhos são apresentados em uma visualização de coluna que inclui as seguintes categorias:

- Core
- Agente protegido
- Tipo
- Resumo
- Status
- Erro
- Hora inicial
- Hora final
- Hora
- Trabalho total

Para obter informações sobre como gerar um relatório, consulte Gerar um relatório sobre um Core ou agente.

Noções básicas sobre relatórios de falha

Os relatórios de falha são subconjuntos dos relatórios de conformidade e estão disponíveis para AppAssure Cores e AppAssure Agents. Os relatórios de falha incluem apenas os trabalhos com falha relacionados em relatórios de conformidade, compilando-os em um único relatório que pode ser impresso e exportado.

Os detalhes sobre os erros são apresentados em uma visualização de coluna com as seguintes categorias:

- Core
- Agente
- Tipo
- Resumo
- Erro
- Hora inicial
- Hora final
- Tempo decorrido
- Trabalho total

Para obter informações sobre como gerar um relatório, consulte Gerar um relatório sobre um Core ou agente.

Noções básicas sobre o relatório resumido

O relatório resumido inclui informações sobre os repositórios no AppAssure Core selecionado e os agentes protegidos por esse Core. As informações aparecem como dois resumos dentro de um relatório. Para obter informações sobre como gerar um relatório resumido, consulte Gerar um relatório sobre um Core ou agente.

Resumo de repositórios

A parte Repositórios do Relatório resumido inclui dados dos repositórios localizados no AppAssure Core selecionado. Os detalhes sobre os repositórios são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Caminho de dados
- Caminho de metadados
- Espaço alocado
- Espaço usado
- Espaço livre
- Taxa de compressão/deduplicação

NOTA: Os espaços alocado, usado e livre são representados em unidades de medida. As medidas são em GB, TB ou segundos.

Resumo de agentes

A seção Agentes do relatório resumido inclui dados de todas as máquinas protegidas pelo AppAssure Core selecionado.

Os detalhes sobre cada máquina protegida são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Volumes protegidos
- Espaço total protegido
- Espaço protegido atual
- Taxa de alteração por dia (Média | Mediana)
- Estatística dos trabalhos (Aprovada | Com falha | Cancelada)

Gerar um relatório sobre um Core ou agente

Conclua as etapas do procedimento a seguir para gerar um relatório sobre um AppAssure Core ou uma máquina protegida.

Para gerar um relatório sobre um Core ou máquina protegida

1. Navegue até o AppAssure Core Console e selecione o Core ou a máquina protegida para o qual deseja executar o relatório.
2. Clique na guia Ferramentas.
3. Na guia Ferramentas, expanda **Relatórios** na área de navegação à esquerda.
4. Na área de navegação à esquerda, selecione o relatório que deseja executar. Os relatórios disponíveis dependem da seleção feita na Etapa 1 e estão descritos na tabela a seguir.

   Tabela 116. Relatórios disponíveis

Máquina	Relatórios disponíveis
Core	Relatório de conformidade
	Relatório resumido
	Relatório de falhas
Agente	Relatório de conformidade
	Relatório de falhas

5. No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

   NOTA: Não há dados disponíveis anteriores ao horário em que o Core ou o AppAssure Agent foram implantados na máquina protegida.

6. No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.
7. Para um Relatório resumido, marque a caixa de seleção **A todo o momento** se quiser que a Hora inicial e a Hora final se estendam pela duração do Core.
8. Para um Relatório de conformidade ou de falha, use a lista suspensa Cores de destino para selecionar o Core do qual deseja visualizar dados.
9. Clique em **Gerar relatório**.

Após a geração do relatório, você pode usar a barra de ferramentas para imprimir ou exportar o relatório. Para obter mais informações sobre a barra de ferramentas, consulte Usar a barra de ferramentas de relatórios.

Noções básicas sobre os relatórios do Central Management Console no Core

O AppAssure permite gerar e visualizar informações de conformidade, erro e resumo de vários AppAssure Cores. Os detalhes sobre os Cores são apresentados em visualizações de coluna com as mesmas categorias descritas nas seções Noções básicas sobre relatórios de conformidade, Noções básicas sobre relatórios de falha e Noções básicas sobre o relatório resumido.

Para obter informações sobre como gerar um relatório de vários cores, consulte Gerar um relatório no Central Management Console.

Gerar um relatório no Central Management Console

Execute o procedimento a seguir para gerar um relatório para vários AppAssure Cores no Central Management Console.

Para gerar um relatório no Central Management Console

1. Na tela Bem-Vindo do Central Management Console, clique no menu suspenso no canto superior direito.
2. No menu suspenso, clique em **Relatórios** e selecione uma das seguintes opções:
   - Relatório de conformidade
   - Relatório resumido
   - Relatório de falhas
3. Na área de navegação à esquerda, selecione o AppAssure Core ou Cores para o(s) qual(is) deseja executar o relatório.
4. No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

   NOTA: Não há dados disponíveis anteriores ao horário em que os Cores foram implementados.

5. No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.
6. Clique em **Gerar relatório**.

   Após a geração do relatório, você pode usar a barra de ferramentas para imprimir ou exportar o relatório. Para obter mais informações sobre a barra de ferramentas, consulte Usar a barra de ferramentas de relatórios.

14

Restaurar dados

Este capítulo descreve como restaurar dados armazenados em cópias de segurança. Ele inclui as seguintes seções:

- Restaurar dados de pontos de recuperação
- Restaurar volumes a partir de um ponto de recuperação
- Restaurar um diretório ou arquivo usando o Windows Explorer
- Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

O AppAssure Core pode restaurar instantaneamente dados ou recuperar máquinas para máquinas físicas ou virtuais a partir dos pontos de recuperação. Os pontos de recuperação contêm snapshots de volume de agentes capturados no nível do bloco. Esses snapshots reconhecem o aplicativo, ou seja, todas as transações abertas e os registros de transações contínuas são concluídos e os caches são descarregados em disco antes da criação do snapshot. O uso de snapshots que reconhecem aplicativos em conjunto com o Verified Recovery permite que o Core realize vários tipos de recuperações, incluindo:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados usando Live Recovery
- Recuperação de volumes de dados para Microsoft Exchange Server e Microsoft SQL Server, usando Live Recovery
- Bare metal restore, usando o Universal Recovery
- Bare metal restore para hardware diferente, usando o Universal Recovery
- Exportação ad hoc e contínua para máquinas virtuais

Restaurar dados de pontos de recuperação

O AppAssure protege seus dados em máquinas com Windows e Linux. As cópias de segurança de máquinas agente protegidas são salvas no AppAssure Core como pontos de recuperação. Use esses pontos de recuperação para restaurar seus dados usando um dos três métodos disponíveis.

No AppAssure Core Console, é possível restaurar volumes inteiros a partir de um ponto de recuperação de um volume que não é do sistema, substituindo os volumes na máquina de destino. É possível fazer isso em máquinas com Windows ou Linux. Para obter mais informações, consulte Restaurar volumes a partir de um ponto de recuperação.

Também é possível restaurar volumes inteiros em máquinas com Linux a partir de pontos de recuperação usando a linha de comando do agente Linux. Para obter mais informações sobre como usar o utilitário aamount da linha de comando, consulte Restaurar volumes em uma máquina Linux usando a linha de comando.

Não é possível restaurar um volume que contenha o sistema operacional diretamente de um ponto de recuperação, porque a máquina para a qual você está restaurando está usando o sistema operacional e os drivers que estão incluídos no processo de restauração. Se você deseja restaurar a partir de um ponto de recuperação em agente um volume do sistema (por exemplo, a unidade C da máquina do Agent), realize uma bare metal restore (BMR). Isso envolve a criação de uma imagem inicializável a partir do ponto de recuperação, incluindo o sistema operacional e os arquivos de configuração, além dos dados, e o início da máquina de destino a partir dessa imagem inicializável para concluir a restauração. A imagem inicializável é diferente se a máquina que você deseja restaurar usa um sistema operacional Windows ou Linux.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Windows, consulte Realizar uma bare metal restore em máquinas Windows.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Linux, consulte Realizar uma bare metal restore em máquinas Windows.

Finalmente, em contraste com a restauração de volumes inteiros, é possível montar um ponto de recuperação a partir de uma máquina com Windows e navegar pelas pastas e arquivos individuais para recuperar apenas um conjunto específico de arquivos. Para obter mais informações, consulte Restaurar um diretório ou arquivo usando o Windows Explorer. Se for preciso fazer isso e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

Os tópicos desta seção descrevem informações sobre como restaurar dados em máquinas físicas. Para obter mais informações sobre a exportação de dados protegidos de máquinas com Windows para máquinas virtuais, consulte Exportar dados protegidos de máquinas Windows para máquinas virtuais.

NOTA: Ao recuperar dados em máquinas com Windows, se o volume que você está restaurando está com a deduplicação de dados do Windows ativada, será preciso ter certeza que a deduplicação também está ativada no server do Core.

O AppAssure suporta o Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 para transferências normais (de base e incrementais), bem como para restauração de dados, bare metal restore e exportações virtuais.

Para obter mais informações sobre os tipos de volumes suportados e não suportados para cópia de segurança e recuperação, consulte Limitações de suporte para volumes dinâmicos e básicos.

Restaurar volumes a partir de um ponto de recuperação

É possível restaurar volumes em uma máquina protegida a partir dos pontos de recuperação armazenados no AppAssure Core. No AppAssure 5.4 e posterior, esse processo usa o Assistente de restauração de máquinas.

NOTA: Em versões anteriores, esse processo era conhecido como realizar uma reversão.

O AppAssure suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas com Windows 8, Windows 8.1, Windows Server 2012 e Windows 2012 R2 que usam o Windows Recovery Environment (Windows RE).

É possível iniciar uma restauração a partir de qualquer local no AppAssure Core Console clicando no ícone **Restaurar** na barra de botões do AppAssure. Ao iniciar uma restauração dessa maneira, é preciso especificar qual das máquinas protegidas no Core você deseja restaurar e, depois, explorar até o volume que deseja restaurar.

Ou explore na UI do Core Console em uma máquina específica, expanda os pontos de recuperação para os volumes dessa máquina e, no ponto de recuperação adequado, selecione **Restaurar**. Se uma restauração for iniciada dessa maneira, siga este procedimento começando com a Etapa 5.

Se você deseja restaurar um ponto de recuperação em uma máquina com Linux, primeiro desmonte o disco no qual vai restaurar os dados.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema, ou restaurar a partir de um ponto de recuperação utilizando um CD de inicialização, você deve realizar uma Bare Metal Restore (BMR). Para obter informações sobre a BMR, consulte Noções básicas sobre bare metal restores em máquinas Windows, e para obter informações de pré-requisitos para sistemas operacionais Windows ou Linux, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente. É possível acessar as funções da BMR a partir do Core Console conforme descrito no roteiro para cada sistema operacional. Também é possível realizar uma BMR a partir do assistente de Restauração de máquinas. Esse procedimento irá direcioná-lo ao ponto adequado no assistente para o procedimento Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

Execute o procedimento abaixo para restaurar volumes em um ponto de recuperação.

Para restaurar volumes em um ponto de recuperação

1 Para restaurar um volume em uma máquina protegida no ícone Restaurar, navegue até o Core Console e clique em **Restaurar** na barra de botões do AppAssure.

O Assistente de restauração de máquinas é exibido.

2 Na página Máquinas protegidas, selecione a máquina protegida da qual deseja restaurar os dados e clique em **Avançar**.

> **NOTA:** A máquina protegida deve ter o software Agent instalado e deve ter pontos de recuperação a partir dos quais você realizará a operação de restauração.

Aparece a página Pontos de recuperação.

3 Na lista de pontos de recuperação, procure o snapshot que deseja restaurar da máquina agente.

- Se necessário, use os botões de navegação na parte inferior da página para exibir pontos de recuperação adicionais.
- Como opção, se quiser limitar a quantidade de pontos de recuperação que aparecem na página Pontos de recuperação do assistente, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação.

4 Clique em qualquer ponto de recuperação para selecioná-lo e em **Avançar**.

Aparece a página Destino.

5 Na página Destino, escolha a máquina para a qual deseja restaurar os dados da seguinte forma:

- Se você deseja restaurar os dados a partir do ponto de recuperação selecionado para a mesma máquina agente (por exemplo, Machine1), e se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, confirme se a máquina de destino (Machine1) está selecionada e clique em **Avançar**.

  A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Se você deseja restaurar os dados a partir do ponto de recuperação selecionado em uma máquina protegida diferente (por exemplo, substituir o conteúdo da Machine2 pelos dados da Machine1), selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, selecione a máquina de destino (por exemplo, Machine2) na lista e clique em **Avançar**.

  A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Se você deseja restaurar a partir do ponto de recuperação selecionado na mesma máquina ou em uma máquina diferente usando um CD de inicialização, isso é considerado uma bare metal restore (BMR). Para obter informações sobre a BMR, consulte Noções básicas sobre bare metal restores em máquinas Windows.

  > **NOTA:** A realização de uma BMR tem requisitos específicos, com base no sistema operacional da máquina do agente que você deseja restaurar. Para entender esses pré-requisitos, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente.

  Se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de restauração de máquinas, clique em **Avançar** e vá para a Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

- Se você já criou o CD de inicialização e a máquina de destino foi iniciada utilizando-o, vá para Etapa 8 do tópico Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

- Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema (por exemplo, a unidade C da máquina agente chamada Machine1), isso também é considerado uma BMR. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em Avançar e vá para a Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

  - Se você já criou o CD de inicialização, vá para a Etapa 6.

6 Inicie a máquina que você deseja restaurar utilizando o CD de inicialização. Para obter mais informações para BMR em uma máquina com Windows, consulte Carregar o CD de inicialização e inicializar a máquina de destino, e para BMR em uma máquina com Linux, consulte Carregar o Live DVD e iniciar a máquina de destino.

7 De volta ao server do Core, na página Destino do assistente de Restauração de máquinas, selecione **Já possuo um CD de inicialização executando na máquina de destino** e insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

Tabela 117. Informações da máquina

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8 Clique em **Avançar**.

Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida.

Para concluir sua BMR a partir do assistente de Restauração de máquinas, vá para Etapa 8 do tópico Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

NOTA: Embora o AppAssure suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado no Windows 8/2012, que fornece suporte nativo ao formato ReFS, caso contrário, a funcionalidade será limitada e operações que envolvem tarefas como a montagem de uma imagem de volume não funcionarão. O AppAssure Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Para obter mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*.

9 Na página Mapeamento de volume, para cada volume no ponto de recuperação que você deseja restaurar, selecione o volume de destino apropriado. Se você não deseja restaurar um volume, na coluna Volumes de destino, selecione **Não restaurar**.

10 Selecione **Exibir opções avançadas** e faça o seguinte:

- Para restaurar em máquinas com Windows, se quiser usar o Live Recovery, selecione **Live Recovery**.

Usando a tecnologia de recuperação instantânea Live Recovery no AppAssure, é possível recuperar ou restaurar instantaneamente os dados em suas máquinas físicas ou virtuais a partir de pontos de recuperação armazenados de máquinas com Windows, incluindo espaços de armazenamento do Microsoft Windows. O Live Recovery não está disponível para máquinas com Linux.

- Se deseja forçar a desmontagem, selecione **Forçar desmontagem**.

  Se você não forçar uma desmontagem antes de restaurar os dados, a restauração pode falhar com um erro de volume em uso.

11 Se os volumes que você deseja restaurar contiverem bancos de dados do SQL ou Microsoft Exchange, na página Desmontar bancos de dados, será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**. Depois, clique em **Concluir**.

12 Clique em **OK** para confirmar a mensagem de status de que o processo de restauração foi iniciado.

13 Como opção, para monitorar o progresso de sua ação de restauração, no Core Console, clique em **Eventos**. Para obter mais informações, consulte Visualizar tarefas, alertas e eventos.

Restaurar um diretório ou arquivo usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows. Isso pode ser útil quando você quiser distribuir apenas uma parte de um ponto de recuperação para seus usuários.

Ao copiar arquivos e diretórios, as permissões de acesso do usuário que está realizando a operação de cópia são utilizadas e aplicadas aos diretórios e arquivos colados. Se você quiser restaurar diretórios e arquivos para seus usuários e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

Para restaurar um diretório ou arquivo usando o Windows Explorer

1 Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.

2 No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.

3 No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar**.

Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows e, ao mesmo tempo, preservar as permissões de acesso dos arquivos.

Por exemplo, se precisar restaurar uma pasta acessada somente por usuários específicos em um server de arquivos, você pode usar os comandos **Copiar** e **Colar com permissões** para garantir que os arquivos restaurados

retenham as permissões que restringem o acesso. Dessa forma, é possível evitar ter que aplicar manualmente as permissões aos diretórios e arquivos restaurados.

NOTA: O comando Colar com permissões é instalado com o AppAssure Core e o software Agent. Não está disponível no Local Mount Utility.

Para restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

1. Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.
2. No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.
3. No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar com permissões**.

   NOTA: Nessa etapa, se o comando **Colar com permissões** estiver desabilitado no menu do botão direito, o Windows Explorer não terá conhecimento dos arquivos que você deseja copiar. Repita a Etapa 2 para habilitar o comando **Colar com permissões** no menu do botão direito.

15

Noções básicas sobre bare metal restores em máquinas Windows

Este capítulo descreve como restaurar completamente uma máquina protegida Windows a partir de hardware semelhante ou diferente. Os seguintes tópicos estão incluídos:

- Realizar uma bare metal restore em máquinas Windows
- Gerenciar uma imagem de inicialização do Windows
- Iniciar uma bare metal restore para Windows
- Verificar uma bare metal restore

Os servers, se estiverem operando como esperado, realizam as tarefas que estão configurados para fazer. É somente quando eles falham que as coisas mudam. Quando ocorre um evento catastrófico, deixando um server inoperante, medidas imediatas são necessárias para restaurar a funcionalidade total da máquina.

O AppAssure fornece a capacidade de realizar uma bare metal restore (BMR) em suas máquinas com Windows ou Linux. A BMR é um processo que restaura a configuração completa do software de um sistema específico. A operação de restauração recupera não só os dados do server, mas também reformata o disco rígido e reinstala o sistema operacional e todos os aplicativos de software. Para realizar uma BMR, especifique um ponto de recuperação de uma máquina protegida e reverta (realize uma restauração) para a máquina física ou virtual designada. Se estiver realizando uma restauração em um volume do sistema, isso é considerado uma BMR. Se estiver realizando uma restauração e for necessário um CD de inicialização, isso também é considerado uma BMR. Outras circunstâncias em que você pode decidir realizar uma bare metal restore incluem atualização de hardware ou substituição do server. Em ambos esses casos, você realiza uma restauração a partir de um ponto de recuperação para o hardware atualizado ou substituído.

O AppAssure oferece suporte aos sistemas operacionais Windows 8, 8.1 e Windows Server 2012, 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System).

NOTA: A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão.

Atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em um Windows 8, Windows 8.1, Windows Server 2012 ou uma máquina com Windows Server 2012 R2, desde que esses sistemas operacionais ofereçam suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O AppAssure Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

Apenas os sistemas operacionais Linux suportados estão disponíveis para proteção ou recuperação. Eles incluem Ubuntu, Red Hat Enterprise Linux, CentOS e SUSE Linux Enterprise Server (SLES). Para obter mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*.

É possível realizar uma BMR em máquinas físicas ou virtuais. Um benefício adicional é que o AppAssure permite realizar uma BMR quer o hardware seja *semelhante*, quer *diferente*. Realizar uma BMR no AppAssure separa o sistema operacional de uma plataforma específica, proporcionando portabilidade.

Exemplos de realização de uma BMR para hardwares semelhantes incluem a substituição do disco rígido do sistema existente ou troca de server com falha por uma máquina idêntica.

Exemplos de realização de uma BMR para hardwares diferentes incluem a restauração de um sistema com falha com um server produzido por um fabricante diferente ou com configuração diferente. Esse processo envolve a criação de uma imagem de CD de inicialização, gravação da imagem em disco, inicialização do server de destino a partir da imagem de inicialização, conexão com a instância do console de recuperação, mapeamento dos volumes, início da recuperação e monitoramento do processo. Depois que a bare metal restore for concluída, você poderá continuar com a tarefa de carregar o sistema operacional e os aplicativos de software no server restaurado, seguida pelo estabelecimento de definições exclusivas necessárias para sua configuração.

A bare metal restore é usada não apenas em cenários de recuperação após desastres, mas também para migração de dados ao atualizar ou substituir servers.

Embora a BMR seja suportada para máquinas virtuais, também é interessante notar que é mais fácil realizar uma exportação virtual para uma VM do que realizar uma BMR em uma máquina física. Para obter mais informações sobre como realizar uma exportação de VM para máquinas virtuais, consulte o procedimento adequado para a VM suportada.

- Para obter mais informações sobre como realizar uma exportação de VM usando ESXi, consulte Exportar dados para uma máquina virtual ESXi.
- Para obter mais informações sobre como realizar uma exportação de VM usando VMware Workstation, consulte Exportar dados para uma máquina virtual VMWare Workstation.
- Para obter mais informações sobre como realizar uma exportação de VM usando Hyper-V, consulte Exportar dados para uma máquina virtual Hyper-V.
- Para obter mais informações sobre como realizar uma exportação de VM usando VirtualBox, consulte Exportar dados para uma máquina virtual VirtualBox.
- Para obter mais informações sobre como realizar uma exportação de VM de uma máquina Linux protegida, consulte Exportar dados para uma máquina virtual VirtualBox baseada em Linux.

Para realizar uma BMR em uma máquina com Windows, consulte o roteiro específico para Windows, incluindo os pré-requisitos. Para obter mais informações, consulte Realizar uma bare metal restore em máquinas Windows.

Também é possível realizar uma BMR a partir do assistente de Restauração de máquinas. Para fazer isso, inicie com o procedimento Restaurar volumes a partir de um ponto de recuperação e, quando for direcionado nesse procedimento, vá até Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

Para realizar uma BMR em uma máquina com Linux, consulte o roteiro específico para Linux, incluindo os pré-requisitos. Além de realizar uma BMR usando o utilitário de linha de comando aamount, agora ela pode ser realizada de dentro da UI do Core Console. O roteiro leva em conta ambas as abordagens.

Realizar uma bare metal restore em máquinas Windows

Para realizar uma bare metal restore em máquinas com Windows, realize as tarefas a seguir.

- **Gerenciar uma imagem de inicialização do Windows**. Essa imagem ISO do CD de inicialização será usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciar uma imagem de inicialização do Windows.
    - Se você precisar de mídia física para iniciar a máquina de destino, precisará **transferir a imagem ISO do CD de inicialização para a mídia**. Consulte Transferir a imagem ISO do CD de inicialização para a mídia.
    - Em todos os casos, será preciso **carregar a imagem de inicialização no servidor de destino e iniciar o servidor** a partir da imagem de inicialização. Consulte Carregar o CD de inicialização e inicializar a máquina de destino.
- **Iniciar uma bare metal restore para Windows**. Depois que a máquina de destino é iniciada a partir do CD de inicialização, é possível iniciar a BMR. Consulte Iniciar uma bare metal restore para Windows.

    - Será preciso **iniciar uma restauração a partir de um ponto de recuperação do Core**. Consulte Selecionar um ponto de recuperação e iniciar a BMR.
    - Será preciso **mapear os volumes**. Consulte Mapear volumes para uma bare metal restore.
    - Se a restauração for em hardware diferente e o armazenamento e drivers de rede necessário não estiverem presentes no CD de inicialização, talvez seja necessário carregar os drivers a partir de um dispositivo de mídia portátil. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.
    - Se a restauração for em hardware diferente e todos os drivers necessários estiverem presentes no CD de inicialização, será necessário **injetar drivers nos dispositivos de hardware** que não estavam na configuração anterior, mas estão incluídos no sistema que substitui o server. Para obter mais informações, consulte Injetar drivers no servidor de destino.
- **Realização de uma BMR a partir do assistente de Restauração de máquinas**. De forma opcional, os processos para gerenciamento de uma imagem de inicialização do Windows e para iniciar a BMR, incluindo todas as subtarefas, podem ser realizados a partir do assistente de Restauração de máquinas. Para obter informações sobre iniciar o assistente, consulte as etapas 1 até 5 do Restaurar volumes a partir de um ponto de recuperação, e depois consulte Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.
- **Confirmação de um bare metal restore**. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Verificar uma bare metal restore.
    - É possível **monitorar o progresso de sua restauração**. Consulte Visualizar o progresso da recuperação.
    - Depois de concluída, você poderá **iniciar o servidor restaurado**. Consulte Inicializar um servidor de destino restaurado
    - **Solucionar problemas do processo de BMR**. Consulte Solucionar problemas de conexão com o Universal Recovery Console e Reparar problemas de inicialização.

Pré-requisitos para realizar uma bare metal restore em uma máquina Windows

Antes de iniciar o processo de realização de uma bare metal restore de uma máquina com Windows, é preciso garantir que as seguintes condições e critérios estejam presentes:

- **Cópias de segurança da máquina que você deseja restaurar.** É preciso ter um AppAssure Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar
- **Hardware para restaurar (novo ou antigo, similar ou não).** A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*.
- **Software e mídia de imagem.** É preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO. Se gerenciar máquinas remotamente usando software de computação de rede virtual, como o UltraVNC, você precisará ter também o VNC Viewer.
- **Drivers do adaptador de rede e de armazenamento compatíveis.** Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatível com Windows 7 PE (32 bits) e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- **Partições e espaço de armazenamento, conforme apropriado.** Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- **Partições compatíveis.** Os sistemas operacionais Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 que são inicializados a partir de partições FAT32 EFI que estão disponíveis para proteção ou recuperação, da mesma forma que os volumes Resilient File System (ReFS). As partições UEFI são tratadas como simples volumes FAT32. Transferências incrementais são totalmente suportadas e protegidas. O AppAssure fornece suporte de sistemas UEFI para BMR, incluindo discos GPT de particionamento automático.

Gerenciar uma imagem de inicialização do Windows

A bare metal restore para Windows exige uma imagem de inicialização chamada de CD de inicialização, criada pela definição de parâmetros no AppAssure Core Console. Essa imagem é adaptada às suas necessidades específicas. Use a imagem para iniciar a máquina de destino do Windows. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Windows a partir da imagem de inicialização.

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Windows.

Para gerenciar uma imagem de inicialização do Windows, você pode realizar as seguintes tarefas:

- Criar uma imagem ISO de um CD de inicialização para Windows
- Definir os parâmetros da imagem ISO do CD de inicialização
- Transferir a imagem ISO do CD de inicialização para a mídia
- Carregar o CD de inicialização e inicializar a máquina de destino

NOTA: Esse processo descreve como gerenciar uma imagem do CD de inicialização da caixa de diálogo Criar CD de inicialização. Também é possível realizar essas etapas a partir de um assistente de Restauração de máquinas, começando da página CD de Inicialização do assistente. Acesse isso quando especificar **Recuperar em qualquer máquina de destino usando um CD de inicialização** a partir da página Destino do assistente.

Para obter instruções passo a passo para gerenciar uma imagem de inicialização do Windows a partir do assistente de Restauração de máquinas como parte de uma bare metal restore, consulte Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina.

Criar uma imagem ISO de um CD de inicialização para Windows

A primeira etapa ao realizar uma bare metal restore (BMR) de uma máquina com Windows é criar o arquivo do CD de inicialização no AppAssure Core Console. Trata-se de uma imagem ISO inicializável que contém a interface do Universal Recovery Console (URC) do AppAssure, um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do AppAssure Core.

A imagem ISO do CD de inicialização criada é adaptada à máquina que está sendo restaurada e, portanto, deve conter os drivers corretos de rede e de armazenamento em massa. Se for prevista a restauração em hardware diferente da máquina em que o ponto de recuperação se originou, inclua o controlador de armazenamento e outros drivers no CD de inicialização. Para obter informações sobre como injetar esses drivers no CD de inicialização, consulte Injetar drivers em um CD de inicialização.

NOTA: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais, incluindo Windows. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Gerenciar uma imagem de inicialização do Windows.

Para criar uma imagem ISO de um CD de inicialização

1. No AppAssure Core Console em que o server que você precisa restaurar está protegido, selecione o Core e clique na guia Ferramentas.
2. Clique em **CDs de inicialização**.

3 Selecione **Ações** e clique em **Criar CD de inicialização**.

A caixa de diálogo Criar CD de inicialização é exibida. Use os procedimentos a seguir para concluir a caixa de diálogo.

Definir os parâmetros da imagem ISO do CD de inicialização

Depois de abrir a caixa de diálogo Criar CD de inicialização, vários parâmetros podem ser necessários. Com base nas particularidades de sua situação, realize as tarefas a seguir, conforme necessário, para definir as propriedades de uma imagem ISO do CD de inicialização a ser usada em uma bare metal restore.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Nomear o arquivo do CD de inicialização e definir o caminho

Execute a etapa a seguir para dar um nome ao arquivo do CD de inicialização e definir o caminho onde a imagem ISO será armazenada.

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Para dar um nome ao arquivo do CD de inicialização e definir o caminho

- Na caixa de diálogo Criar CD de inicialização, em Opções de saída, na caixa de texto Caminho de saída, insira o caminho onde deseja armazenar a imagem ISO do CD de inicialização no server do Core.

  Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, defina o caminho conforme necessário; por exemplo, D:\filename.iso.

  NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

Criar conexões

Execute as seguintes etapas para criar as conexões.

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Para criar conexões

1 Em Opções de conexão, realize um dos procedimentos a seguir:

   - Para obter o endereço IP dinamicamente usando o protocolo DHCP (Dynamic Host Configuration Protocol), selecione **Obter o endereço IP automaticamente**.
   - Como opção, a fim de especificar um endereço IP estático para o console de recuperação, selecione **Use o seguinte endereço IP** e insira o endereço IP, a máscara de sub-rede, o gateway padrão e o server DNS nos campos apropriados. É preciso especificar todos esses quatro campos.

2 Se necessário, em Opções de UltraVNC, selecione **Adicionar UltraVNC** e insira a Senha de UltraVNC e a Porta de UltraVNC.

As definições de UltraVNC permitem gerenciar remotamente o console de recuperação enquanto ele está em uso.

NOTA: Essa etapa é opcional. Se você precisar de acesso remoto ao console de recuperação, precisará configurar e usar o UltraVNC. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

Especificar um ambiente de recuperação

A imagem do CD de inicialização deverá ser criada para que o CD de inicialização (físico ou virtual) seja montável no hardware que você está restaurando. Você deve especificar a arquitetura mais bem adequada para essa máquina.

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Conclua a seguinte etapa para especificar um ambiente de recuperação

- No Ambiente de Recuperação, selecione a partir das opções de notificação conforme descrito na tabela a seguir.

Tabela 118. Opções do ambiente de recuperação

Opção	Descrição
OS Windows de 64 bits	Para restaurar em qualquer máquina com Windows e arquitetura de 64 bits, incluindo máquinas com uma BIOS UEFI
OS Windows de 32 bits	Para restaurar em qualquer máquina com arquitetura de 32 bits (x86)

Injetar drivers em um CD de inicialização

A imagem de CD de inicialização exige que os drivers de armazenamento reconheçam as unidades de server e os drivers do adaptador de rede a fim de se comunicarem com o AppAssure Core pela rede.

Um conjunto genérico de drivers do controlador de armazenamento e de adaptador de rede do Windows 7 PE de 32 bits é incluído automaticamente ao gerar um CD de inicialização para Windows. Isso atenderá aos requisitos de sistemas Dell mais recentes. Sistemas de outros fabricantes ou sistemas Dell mais antigos podem exigir uma injeção de drivers de controlador de armazenamento e de adaptador de rede ao criar o CD de inicialização. Se você descobrir que o CD de inicialização criado não contém os drivers necessários para executar a restauração, também poderá carregá-los na máquina de destino usando o URC. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.

Ao criar o CD de inicialização, a injeção de drivers é usada para facilitar a interoperabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no server de destino.

Os dados restaurados a partir do ponto de recuperação incluem drivers para o hardware usado anteriormente. Se for feita uma bare metal restore para um hardware diferente, será preciso injetar também drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados para a unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que o OS possa interagir com seu novo hardware.

Para obter mais informações, consulte Injetar drivers no servidor de destino.

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Execute as etapas a seguir para injetar drivers do controlador de armazenamento e do adaptador de rede em um CD de inicialização.

Para injetar drivers em um CD de inicialização

1 Baixe os drivers no website do fabricante do server e descompacte-os.

2 Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).

3 Na caixa de diálogo Criar CD de inicialização, no painel Drivers, clique em **Adicionar um driver**.

4 Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.

Os drivers injetados aparecem em destaque no painel Drivers.

5 Repita a Etapa 3 e a Etapa 4, conforme o caso, até que todos os drivers tenham sido injetados.

Criar a imagem ISO do CD de inicialização

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Execute a etapa a seguir para criar a imagem ISO do CD de inicialização.

Para criar uma imagem ISO de um CD de inicialização

- Depois de ter dado nome ao arquivo do CD de inicialização e especificado o caminho, criado uma conexão e, opcionalmente, injetado os drivers, na tela Criar CD de inicialização, clique em **Criar CD de inicialização**.

  A imagem ISO é então criada e salva com o nome do arquivo fornecido.

Visualizar o progresso da criação da imagem ISO

Essa tarefa é uma etapa no processo de Definir os parâmetros da imagem ISO do CD de inicialização. Faz parte do processo de Criar uma imagem ISO de um CD de inicialização para Windows.

Execute a etapa a seguir para visualizar o progresso de criação da imagem ISO.

Para visualizar o progresso de criação da imagem ISO

- Selecione a guia Eventos e, em seguida, em Tarefas, é possível monitorar o progresso da construção da imagem ISO. Para obter mais informações sobre o monitoramento de eventos do AppAssure, consulte Visualizar tarefas, alertas e eventos.

  Quando a criação da imagem ISO estiver concluída, ela aparecerá na página CDs de inicialização, acessível no menu Ferramentas.

Acessar a imagem ISO

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Gerenciar uma imagem de inicialização do Windows.

Execute a etapa a seguir para acessar a imagem ISO.

Para acessar a imagem ISO

- Para acessar a imagem ISO, navegue até o caminho de saída especificado ou clique no link para baixar a imagem em um local do qual é possível carregá-la para o novo sistema; por exemplo, uma unidade de rede.

Transferir a imagem ISO do CD de inicialização para a mídia

Quando você cria o arquivo de CD de inicialização, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de montar essa imagem como unidade no server no qual está realizando uma bare metal restore.

É possível gravar a imagem ISO do CD de inicialização em mídia de CD ou DVD acessível na inicialização do sistema.

Se a máquina for iniciada do CD de inicialização, o Universal Recovery Console será iniciado automaticamente.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições dessa VM para iniciar essa unidade.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Gerenciar uma imagem de inicialização do Windows.

Carregar o CD de inicialização e inicializar a máquina de destino

Depois de criar a imagem do CD de inicialização, é preciso inicializar o server de destino com o CD de inicialização recém-criado.

NOTA: Se o CD de inicialização tiver sido criado usando DHCP, será preciso capturar o endereço IP e a senha.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Gerenciar uma imagem de inicialização do Windows.

Para carregar um CD de inicialização e iniciar a máquina de destino

1. Navegue até o novo server e carregue a imagem do CD de inicialização a partir do local apropriado. Especifique se o server inicializará a partir da imagem de CD de inicialização.
2. Inicie a máquina, o que irá carregar o seguinte:
   - Windows 7 PE
   - Software AppAssure Agent

   O AppAssure Universal Recovery Console é iniciado e exibe o endereço IP e a senha de autenticação da máquina.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com o CD de inicialização. Anote o endereço IP exibido no painel Definições de adaptadores de rede e a senha de autenticação exibida no painel Autenticação. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.
3. Caso queira alterar o endereço IP, selecione-o e clique em **Alterar**.

   NOTA: Se um endereço IP tiver sido especificado na caixa de diálogo Criar CD de inicialização, o Universal Recovery Console o usará e exibirá na tela de definições do adaptador de rede.

Depois de iniciada com o CD de inicialização, essa máquina está pronta para o usuário se conectar a ela a partir do Core para dar início ao processo de bare metal restore.

Gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de Máquina

Restaurar volumes a partir de um ponto de recuperação utilizando um CD de inicialização ou restaurar um volume de sistema é considerado uma realização de uma bare metal restore. Antes de realizar uma BMR, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina Windows ou Pré-requisitos para realizar uma bare metal restore em máquinas Linux, conforme adequado. Se desejar iniciar sua BMR em uma máquina com Windows a partir do Core Console, consulte Realizar uma bare metal restore em máquinas Windows.

Se desejar iniciar sua BMR a partir do assistente de Restauração de máquinas, na página Destino desse assistente, selecione a opção **Recuperar em qualquer máquina de destino usando um CD de inicialização**, e siga este procedimento. O gerenciamento de uma imagem de inicialização do Windows por meio do assistente inclui iniciar a criação do CD de inicialização, a definição do caminho para a imagem na máquina do Core, a seleção do ambiente de recuperação adequado para o hardware que você deseja restaurar, a definição, de forma opcional, dos parâmetros de conexão para o agente restaurado para utilizar a rede ou UltraVNC, a inserção, de forma opcional, de drivers para hardware que você deseja restaurar e a transferência, de forma opcional, da imagem de inicialização para mídias físicas. Esse processo também inclui inicializar a máquina na qual você deseja restaurar os dados a partir do CD; conexão com o Universal Recovery Console; mapeamento de volumes; e inicialização da bare metal restore a partir do ponto de recuperação selecionado no core.

NOTA: Esse processo descreve como gerenciar uma imagem do CD de inicialização do assistente de Restauração de máquinas como parte do processo para realizar uma BMR utilizando esse assistente. Também é possível gerenciar uma imagem de inicialização da caixa de diálogo Criar CD de inicialização. Para obter informações sobre o gerenciamento de uma imagem do CD de inicialização fora do assistente de Restauração de máquinas, consulte Gerenciar uma imagem de inicialização do Windows.

Para gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de máquinas

1 Na página CD de inicialização, faça o seguinte:

   a No campo de texto **Caminho de saída**, digite o caminho onde a imagem ISO do CD de inicialização deve ser armazenada.

   Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, defina o caminho conforme necessário; por exemplo, D:\filename.iso.

   NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

   b Em **Ambiente,** selecione a arquitetura mais adequada ao hardware que você está restaurando:

   - Para restaurar em qualquer máquina com Windows e arquitetura de 64 bits, selecione **Windows 8 de 64 bits (necessário para máquinas configuradas com uma bios UEFI)**.
   - Para restaurar em qualquer máquina com arquitetura de 32 bits (x86), selecione **Windows 7 32 bits**.

2 Como opção, para definir os parâmetros de rede para o agente restaurado ou para usar UltraVNC, selecione **Exibir opções avançadas** e faça um dos seguintes:

   - Para estabelecer uma conexão de rede para a máquina restaurada, selecione **Use o seguinte endereço IP**, como descrito na tabela a seguir.

Tabela 119. Opções de conexão de rede

Opção	Descrição
Endereço IP	Especifique um endereço IP ou nome de host da máquina restaurada.
Máscara de sub-rede	Especifique a máscara de sub-rede da máquina restaurada.
Gateway padrão	Especifique o gateway padrão da máquina restaurada.
DNS Server	Especifique o server de nome de domínio da máquina restaurada.

- Para definir as informações de UltraVNC, selecione **Adicionar UltraVNC**, como descrito na tabela a seguir.

  Use essa opção se você precisar de acesso remoto ao console de recuperação. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado

Tabela 120. Conexão UltraVNC

Opção	Descrição
Senha	Especifique uma senha para essa conexão UltraVNC.
Porta	Especifique uma porta para essa conexão UltraVNC. A porta padrão é 5900.

3 Quando estiver satisfeito com suas seleções na página CD de inicialização, clique em **Avançar**.

4 Como opção, na página Injeção de drivers, para injetar um driver, faça o seguinte:

  a Selecione **Adicionar um arquivo de drivers**

  b Navegue até um arquivo ZIP que contém o arquivo, selecione o arquivo ZIP e clique em **Abrir**.

  O arquivo é carregado e aparece na página Injeção de drivers.

  c Depois, clique em **Avançar**.

5 Na página Imagem ISO, é possível ver o status enquanto a imagem ISO do CD de inicialização é criada. Quando o CD de inicialização for bem-sucedido, clique em **Avançar**.

A página Conexão é exibida.

6 Nesse ponto, você quer iniciar a máquina agente para a qual deseja restaurar os dados a partir do CD de inicialização.

- Se você puder inicializar a máquina agente de uma imagem ISO do CD de inicialização, faça-o agora.
- Caso contrário, copie a imagem ISO para a mídia física (CD ou DVD), coloque o disco na máquina agente, configure a máquina para carregar a partir do CD de inicialização e reinicie a partir desse CD.

  NOTA: Talvez seja necessário alterar as definições de BIOS da máquina agente para garantir que o volume carregado primeiro seja o CD de inicialização.

  A máquina agente, quando iniciada a partir do CD de inicialização, exibe a interface do Universal Recovery Console (URC). Esse ambiente é usado para restaurar a unidade do sistema ou volumes selecionados diretamente do AppAssure Core. Observe o endereço IP e as credenciais da chave de autenticação no URC, que são atualizados cada vez que é feita uma inicialização a partir do CD de inicialização.

7 De volta ao Core Console na página Conexão, insira as informações de autenticação a partir da instância de URC da máquina que você deseja restaurar, como segue:

  a Na caixa de texto Endereço IP, insira o endereço IP da máquina na qual está restaurando a partir de um ponto de recuperação.

  b Na caixa de texto Chave de autenticação, insira as informações do URC.

c Depois, clique em **Avançar**.

A página Mapeamento de disco é exibida.

8 Caso queira mapear volumes automaticamente, faça o seguinte. Caso queira mapear volumes automaticamente, vá para Etapa 9.

a Selecione **Mapeamento de volume automático**.

b Na área Mapeamento de volume automático, à esquerda, selecione os volumes que deseja restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

c No lado direito, selecione o disco de destino para a restauração.

d Clique em **Avançar** e vá para Etapa 10.

9 Caso queira mapear volumes manualmente, faça o seguinte:

a Selecione **Mapeamento de volume manual**.

b Na área Mapeamento de volume manual, na lista suspensa Volumes de destino de cada volume, selecione os volumes que deseja restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

c Quando estiver satisfeito, clique em **Concluir**.

CUIDADO: Se você selecionar Concluir, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

O Assistente de restauração de máquinas fecha e os dados são restaurados dos volumes selecionados do ponto de recuperação na máquina de destino.

Vá para a Etapa 13.

10 Na página Visualização de mapeamento de disco, revise os parâmetros das ações de restauração selecionadas. Para realizar a restauração, clique em **Concluir**.

CUIDADO: Se você selecionar Concluir, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

11 Se os volumes que deseja restaurar contiverem bancos de dados do SQL ou Microsoft Exchange, e se você estiver realizando uma Live Restore, na página Desmontar bancos de dados, será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**. Depois, clique em **Concluir**.

12 Clique em **OK** para confirmar a mensagem de status de que o processo de restauração foi iniciado.

13 Como opção, para monitorar o progresso de sua ação de restauração, no Core Console, clique em **Eventos**. Para obter mais informações, consulte Visualizar tarefas, alertas e eventos.

Iniciar uma bare metal restore para Windows

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Windows, certas condições devem ser satisfeitas.

Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina Windows.

A máquina com Windows de destino da BMR deve ser iniciada usando a imagem do CD de inicialização. Para obter mais informações, consulte Gerenciar uma imagem de inicialização do Windows.

A primeira etapa é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida no Universal Recovery Console.

A seguir, você precisa mapear as unidades e iniciar a restauração.

O ponto de recuperação inclui drivers do hardware anterior. Se for feita uma restauração para um hardware diferente, será preciso injetar drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados na unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que OS possa interagir com seu novo hardware.

Para iniciar uma BMR no AppAssure Core Console, realize as seguintes tarefas.

- Selecionar um ponto de recuperação e iniciar a BMR
- Mapear volumes para uma bare metal restore
- Carregar drivers usando o Universal Recovery Console
- Injetar drivers no servidor de destino

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Windows.

Selecionar um ponto de recuperação e iniciar a BMR

Depois que o Universal Recovery Console estiver acessível na máquina em que você deseja realizar uma BMR, será preciso selecionar o ponto de recuperação que deseja restaurar. Navegue até o Core Console para selecionar que ponto de recuperação você deseja carregar e designar o console de recuperação como o destino para os dados restaurados.

NOTA: Essa etapa é necessária para realizar BMR em todas as máquinas com Windows e opcional para executar BMR em máquinas com Linux.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Iniciar uma bare metal restore para Windows.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Execute as etapas deste procedimento para selecionar um ponto de recuperação no Core e restaurar na máquina de destino física ou virtual de BMR.

Para selecionar um ponto de recuperação e iniciar a BMR

1. Navegue até o AppAssure Core Console e, na lista de máquinas protegidas, clique no nome do server protegido em que deseja executar a bare metal restore.

   A guia Resumo da máquina selecionada é exibida.

2. Clique na guia Pontos de recuperação.

3 Na lista de pontos de recuperação, clique no símbolo de maior que (>) para expandir o ponto de recuperação que deseja restaurar.

4 Nos detalhes expandidos desse ponto de recuperação, no menu Ações, clique em **Restaurar**.

O Assistente de restauração de máquinas é exibido.

5 Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.

6 Selecione **Eu já tenho um CD de inicialização em execução na máquina de destino.**

Os campos de autenticação ficam acessíveis.

7 Insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

Tabela 121. Informações da máquina de destino

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8 Clique em **Avançar**.

Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida. Nesse caso, sua próxima etapa é mapear volumes.

NOTA: Embora o AppAssure suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2, quem fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O AppAssure Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Para obter mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*.

Mapear volumes para uma bare metal restore

Depois de se conectar ao Universal Recovery Console, você precisará mapear volumes entre aqueles relacionados no ponto de recuperação e os volumes existentes no hardware de destino para realizar a restauração.

O AppAssure tenta mapear volumes automaticamente. Se você aceitar o mapeamento padrão, o disco na máquina de destino será limpo e reparticionado e quaisquer dados anteriores serão excluídos. O alinhamento é realizado na ordem em que os volumes estão relacionados no ponto de recuperação e os volumes são alocados aos discos de forma adequada de acordo com o tamanho, e assim por diante. Supondo que haja espaço suficiente na unidade de destino, nenhum particionamento será necessário ao utilizar o alinhamento automático do disco. Um disco pode ser usado em diversos volumes. Se você mapear manualmente as unidades, observe que não poderá usar o mesmo disco duas vezes.

Para o mapeamento manual, é preciso ter a nova máquina corretamente formatada antes de restaurá-la. A máquina de destino deve ter uma partição separada para cada volume no ponto de recuperação, incluindo o volume reservado do sistema. Para obter mais informações, consulte Iniciar uma bare metal restore para Windows.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Iniciar uma bare metal restore para Windows.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Iniciar uma bare metal restore para Linux.

Execute as etapas deste procedimento para mapear um volume.

Para mapear volumes para uma bare metal restore

1 Caso queira mapear volumes automaticamente, faça o seguinte. Caso queira mapear volumes automaticamente, vá para a Etapa 2

   a Na página Mapeamento de disco do Assistente de restauração de máquinas, selecione a guia Mapear volumes automaticamente.

   b Na área Mapeamento de disco, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.

   > **NOTA:** Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume C:\).

   c Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção sob o volume de origem. Pelo menos um volume deve ser selecionado para realizar a BMR.

   d Se o disco de destino automaticamente mapeado for o volume de destino correto, selecione **Disco de destino** e confirme se todos os volumes adequados estão selecionados.

   e Clique em **Restaurar** e vá para a Etapa 3.

2 Caso queira mapear volumes manualmente, faça o seguinte:

   a Na página Mapeamento de disco do Assistente de restauração de máquinas, selecione a guia Mapear volumes manualmente.

   > **NOTA:** Se não existirem volumes na unidade da máquina na qual você está realizando uma BMR, não será possível ver essa guia ou mapear manualmente os volumes.

   b Na área Mapeamento de volume, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.

   c Em Destino, a partir do menu suspenso, selecione o destino apropriado que é o volume de destino para realizar a bare metal restore do ponto de recuperação selecionado e clique em **Restaurar**.

3 Na caixa de diálogo de confirmação, revise o mapeamento da origem do ponto de recuperação e do volume de destino da restauração. Para realizar a restauração, clique em **Começar a restauração**.

> **CUIDADO: Se você selecionar Começar a restauração, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos por conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.**

Carregar drivers usando o Universal Recovery Console

Ao criar um CD de inicialização, você pode adicionar drivers necessários à imagem ISO. Depois de inicializar a máquina de destino, você também pode carregar drivers de armazenamento ou de rede de dentro do Universal Recovery Console (URC). Esse recurso permite adicionar os drivers esquecidos que não foram incluídos na imagem ISO, mas são necessários para uma bare metal restore bem-sucedida.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Iniciar uma bare metal restore para Windows.

Execute as etapas do procedimento a seguir para carregar drivers usando o URC.

Para carregar drivers usando o Universal Recovery Console

1. Em uma máquina conectada à Internet, baixe e salve os drivers necessários para um dispositivo de mídia portátil, como uma unidade USB.
2. Remova a mídia da máquina conectada e insira-a no server de destino de inicialização.
3. No URC do server de destino, na guia Console, clique em **Carregar driver**.
4. Na janela Selecionar driver, navegue até o local do driver, selecione-o e clique em **Abrir**.
5. Repita conforme necessário para cada driver que você deseja carregar.

Injetar drivers no servidor de destino

Se você estiver restaurando em um hardware diferente, precisará injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers se eles não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino depois que o sistema for reiniciado após o processo de restauração.

Se você não tem certeza de quais drivers são necessários para o server de destino, clique na guia Informações do sistema do Universal Recovery Console. Essa guia mostra todos os tipos de hardware e de dispositivos do sistema do server de destino para o qual você deseja restaurar.

NOTA: O server de destino contém automaticamente alguns drivers genéricos do Windows 7 PE de 32 bits que funcionarão em alguns sistemas.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Iniciar uma bare metal restore para Windows.

Execute a tarefa a seguir para injetar drivers em seu server de destino.

Para injetar drivers em seu server de destino

1. Baixe os drivers no website do fabricante do server e descompacte-os.
2. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip) e copie-o para o server de destino.
3. No Universal Recovery Console, clique em **Injeção de drivers.**
4. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado e selecione-o.
5. Se você clicou em Injeção de drivers na etapa 3, clique em **Adicionar driver**. Se você clicou em Carregar driver na etapa 3, clique em **Abrir**.

   Os drivers selecionados serão injetados e carregados no sistema operacional depois que o server de destino for reiniciado.
6. Repita da Etapa 3 à Etapa 5, conforme o caso, até que todos os drivers tenham sido injetados.

Verificar uma bare metal restore

Depois de realizar uma bare metal restore, você poderá confirmar o progresso da restauração. Quando a ação for concluída com sucesso, você poderá iniciar o server restaurado. Algumas etapas de resolução de problemas são incluídas se houver dificuldades para se conectar ao Universal Recovery Console a fim de concluir a restauração e para reparar problemas de inicialização com a máquina restaurada.

Você pode realizar as seguintes tarefas:

- Visualizar o progresso da recuperação
- Inicializar um servidor de destino restaurado
- Solucionar problemas de conexão com o Universal Recovery Console
- Reparar problemas de inicialização

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Windows.

Visualizar o progresso da recuperação

Execute as etapas deste procedimento para visualizar o progresso da restauração de dados de um ponto de recuperação (incluindo bare metal restore) iniciado no AppAssure Core Console.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Verificar uma bare metal restore.

Para visualizar o progresso da recuperação

1. Depois de iniciar o processo de restauração de dados de um ponto de recuperação, enquanto a tarefa estiver em andamento, você pode visualizar seu progresso no menu suspenso Tarefas em execução no Core Console.
2. É possível visualizar informações detalhadas na guia Eventos. Para obter mais informações sobre o monitoramento de eventos do AppAssure, consulte Visualizar tarefas, alertas e eventos.

Inicializar um servidor de destino restaurado

Execute as etapas deste procedimento para iniciar o server de destino restaurado.

NOTA: Antes de iniciar o server de destino restaurado, confirme se a recuperação foi bem-sucedida. Para obter mais informações, consulte Visualizar o progresso da recuperação.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Verificar uma bare metal restore.

Para iniciar um server de destino restaurado

1. Navegue de volta ao servidor de destino e confirme se o AppAssure Universal Recovery Console está ativo.
2. Ejete o CD de inicialização (ou desconecte a mídia física com a imagem do CD de inicialização) do server restaurado.
3. No Universal Recovery Console, na guia Console, clique em **Reinicializar**.
4. Especifique para iniciar o sistema operacional normalmente.
5. Efetue login na máquina. O sistema deve ser restaurado ao seu estado capturado no ponto de recuperação.

Solucionar problemas de conexão com o Universal Recovery Console

Encontramos a seguir as etapas da solução de problemas de conexão com a imagem do CD de inicialização como parte do processo de Selecionar um ponto de recuperação e iniciar a BMR.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Verificar uma bare metal restore.

Se um erro for exibido indicando que o Core não pôde se conectar ao server remoto, existem várias causas possíveis.

- Confirme se o endereço IP e a senha atual exibidos no URC são idênticos às informações inseridas na caixa de diálogo Instância do console de recuperação.
- Para alcançar o server no qual irá restaurar dados, o Core deve ser capaz de identificar o server na rede. Para determinar se isso é possível, você pode abrir um prompt de comando no Core e fazer um ping do

endereço IP do server de BMR de destino. Também é possível abrir um prompt de comando no server de destino e fazer um ping para o endereço IP do AppAssure Core.

- Confirme se as definições do adaptador de rede são compatíveis entre o Core e o server de BMR de destino.

Reparar problemas de inicialização

Execute as etapas deste procedimento para reparar problemas de inicialização. Lembre-se de que, se você tiver restaurado em um hardware diferente, precisará ter injetado o driver do controlador de armazenamento, RAID, AHCI, chipset e outros drivers, se eles já não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino. Para obter mais informações, consulte Injetar drivers no servidor de destino.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Windows. Faz parte do processo de Verificar uma bare metal restore.

Execute o procedimento a seguir para reparar problemas de inicialização no seu server de destino.

Para reparar problemas de inicialização

1 Abra o Universal Recovery Console recarregando o CD de inicialização.

2 No Universal Recovery Console, clique em **Injeção de drivers.**

3 Na caixa de diálogo Injeção de drivers, clique em **Reparar problemas de inicialização**.

Os parâmetros de inicialização no registro de inicialização do server de destino são reparados automaticamente.

4 No Universal Recovery Console, clique em **Reinicializar.**

16

Retenção e arquivamento

Este capítulo descreve como gerenciar dados antigos com políticas de retenção e, em seguida, arquivá-los para armazenamento de longo prazo. Ele inclui as seguintes seções:

- Gerenciar políticas de retenção
- Noções básicas sobre arquivos
- Arquivar na nuvem

Snapshots de cópia de segurança periódicas de todas as máquinas protegidas se acumulam no Core ao longo do tempo. As políticas de retenção são usadas para reter snapshots de cópia de segurança por períodos de tempo mais longos e para ajudar a gerenciar esses snapshots de cópia de segurança. Quando os dados antigos atingem seu limite predeterminado (por exemplo, um ano), você pode excluir os dados ou arquivá-los em um de vários locais, incluindo uma conta na nuvem. Os tópicos a seguir descrevem como definir políticas de retenção e como arquivar dados de uma máquina protegida.

Gerenciar políticas de retenção

A política de retenção é imposta pelo processo noturno de rollup que ajuda no processo de envelhecimento e exclusão das cópias de segurança antigas. Para obter informações sobre a configuração de políticas de retenção, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Configurar as definições da política de retenção padrão do Core

A política de retenção do Core especifica por quanto tempo os pontos de recuperação de uma máquina de Agent são armazenados no repositório. Essa política de retenção é imposta pelo processo de rollup, que é executado como um dos componentes da execução de trabalhos noturnos. Nesse momento, os pontos de recuperação além da idade especificada na política de retenção são submetidos a um "rollup" (combinados) em menos pontos de recuperação, que abrangem um período de tempo menos granular. Aplicar a política de retenção todas as noites resulta no rollup contínuo de cópias de segurança antigas. Com o tempo, os pontos de recuperação mais antigos são excluídos, com base nos requisitos especificados nessa política de retenção.

Diferentes definições de retenção podem ser configuradas para cores de origem e de destino.

NOTA: Esse tópico é específico para personalizar as definições de política de retenção no AppAssure Core. Ao salvar definições de política de retenção personalizadas no Core, você estabelece as definições de política de retenção padrão que podem ser aplicadas a todas as máquinas protegidas por esse Core. Para obter mais informações sobre a personalização das definições da política de retenção para máquinas protegidas individuais, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Para configurar as definições da política de retenção padrão do Core

1 Navegue até o AppAssure Core Console, clique na guia Configuração e depois em **Política de retenção**.

Aparece a tela Política de retenção, exibindo as opções de política de retenção do Core.

2 Especifique a definição principal que determina por quanto tempo os snapshots de cópia de segurança inicial são retidos e depois passe a definir um conjunto de requisitos de rollup em cascata que determina os intervalos nos quais os pontos de recuperação devem passar por rollup.

As opções da política de retenção são descritas na tabela a seguir.

Tabela 122.

Caixa de texto	Descrição
Manter todos os pontos de recuperação por *n* [*período de retenção*]	Especifica o período de retenção para os pontos de recuperação. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por hora por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção com a definição principal para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por dia por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *4* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por semana por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* semanas. Você pode selecionar dentre: Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por mês por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 meses*. Você pode selecionar dentre: Meses ou Anos
…e depois manter um Ponto de recuperação por ano por *n* [*período de retenção*]	Insira um número para representar o período de retenção e a seguir selecione o período de tempo. Você pode selecionar dentre: Anos

A caixa de texto Ponto de recuperação mais novo exibe o ponto de recuperação mais recente. O ponto de recuperação mais antigo será determinado pelas definições da política de retenção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por *3 dias*.

…e depois manter um Ponto de recuperação por hora por *3 dias*

…e depois manter um Ponto de recuperação por dia por *4 dias*

…e depois manter um Ponto de recuperação por semana por *3 semanas*

…e depois manter um Ponto de recuperação por mês por *2 meses*

…e depois manter um Ponto de recuperação por ano por *1 ano*

O Ponto de recuperação mais novo é definido para o dia, mês e ano atuais.

Neste exemplo, o ponto de recuperação mais antigo teria 1 ano, 4 meses e 6 dias.

3 Em Definições, no campo de texto **Número de rollups simultâneos**, insira um valor numérico.

Essa configuração determina o número de operações de rollup que podem ser realizadas ao mesmo tempo. Definir o número acima de 1 resultará em menos tempo para concluir o processo de rollup, mas colocará uma carga mais pesada no Core enquanto os rollups ocorrem.

> **NOTA:** Como regra geral, defina esse valor em 1. Se as operações de rollup demorarem muito, incremente em um dígito, e verifique o desempenho do sistema para garantir que a alteração é construtiva em seu ambiente.

4 Clique em **Aplicar**.

A política de retenção definida será aplicada durante o rollup noturno.

Também será possível aplicar essas definições ao especificar a política de retenção para qualquer máquina agente individual. Para obter mais informações sobre a definição de políticas de retenção para uma máquina agente, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Personalizar as definições de política de retenção de uma máquina protegida

A política de retenção de uma máquina especifica por quanto tempo os pontos de recuperação são armazenados no repositório. Normalmente, cada agente usa a política de retenção padrão estabelecida para o core, a menos que você especifique uma política de retenção personalizada, conforme descrito neste procedimento.

A partir da versão 5.4.1, o AppAssure inclui a capacidade de definir políticas de retenção discrepantes entre um agente no Core de origem e o agente replicado correspondente no Core de destino.

Use este procedimento para definir uma política de retenção personalizada para um agente, incluindo um agente replicado.

> **NOTA:** Em atualizações de ambiente do AppAssure versão 5.3.x para a versão 5.4.1 ou superior, se você quiser personalizar uma política de retenção para qualquer agente replicado, primeiramente precisará atualizar os Cores de origem e de destino para 5.4.1 e, em seguida, executar o trabalho de verificação de integridade em cada repositório nesse Core de destino. A conclusão deste trabalho tende a levar um bom tempo, com base no tamanho de seu repositório e no sistema de armazenamento subjacente. Para obter mais informações sobre este trabalho, consulte Sobre o trabalho de verificação de integridade do repositório. Para obter mais informações sobre como executar este trabalho, consulte Executar o trabalho de verificação de integridade em um repositório.

Essa tarefa também é uma das etapas do Modificar definições de nó de cluster.

Para personalizar as definições de política de retenção de uma máquina protegida

1 No AppAssure Core Console, navegue até a máquina que deseja modificar.

2 Clique na guia Configuração.

A página Definições é exibida.

3 No painel Trabalhos noturnos, clique em **Alterar**.

A caixa de diálogo Trabalhos noturnos é exibida.

4 Para especificar os intervalos de tempo a reter os dados de cópia de segurança, conforme necessário, selecione a opção **Rollup** e clique em **Definições**.

É exibida a caixa de diálogo Configuração da política de retenção.

5 Se você estiver personalizando as definições de políticas de retenção para um agente replicado e receber uma notificação de cautela para a verificação de integridade que está executando em seu repositório, prossiga com esta etapa. De outra forma, vá para Etapa 6.

a Se você está preparado para executar este trabalho, clique em **Verificar integridade**

b Clique em **Sim** para confirmar o trabalho de verificação de integridade.

CUIDADO: Esse processo pode levar um bom tempo, com base no tamanho de seu repositório. Durante este tempo, você não poderá realizar nenhuma outra ação (Snapshots, replicação, exportação virtual e assim por diante) no repositório. Para obter mais informações sobre este trabalho, consulte Sobre o trabalho de verificação de integridade do repositório.

- Depois que o trabalho de Verificação da integridade concluir todos as sub-rotinas com sucesso, retorna para este procedimento e continua coma próxima etapa.

6 Na caixa de diálogo Configuração, realize um dos procedimentos a seguir:

- Para definir uma política de retenção personalizada para este agente, selecione a opção **Usar a política de retenção personalizada** e, em seguida, clique em **Salvar**. A política padrão é aplicada a este agente.
- Para definir uma política de retenção personalizada para este agente, selecione a opção **Usar a política de retenção personalizada** e, em seguida, continue na próxima etapa.

7 Insira a programação personalizada para reter os pontos de recuperação, conforme descrito na tabela a seguir.

Tabela 123.

Caixa de texto	Descrição
Manter todos os pontos de recuperação por *n* [*período de retenção*]	Especifica o período de retenção para os pontos de recuperação. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* dias. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por hora por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção com a definição principal para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 dias*. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por dia por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *4 dias*. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por semana por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3 semanas*. Você pode selecionar dentre: Semanas, Meses e Anos

Tabela 123.

Caixa de texto	Descrição
…e depois manter um Ponto de recuperação por mês por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 meses*. Você pode selecionar dentre: Meses e Anos
…e depois manter um Ponto de recuperação por ano por *n* [*período de retenção*]	Insira um número para representar o período de retenção e a seguir selecione o período de tempo. Você pode selecionar dentre: Anos

A caixa de texto Ponto de recuperação mais novo exibe o ponto de recuperação mais recente. O ponto de recuperação mais antigo será determinado pelas definições da política de retenção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por *3 dias*.

…e depois manter um Ponto de recuperação por hora por *3 dias*

…e depois manter um Ponto de recuperação por dia por *4 dias*

…e depois manter um Ponto de recuperação por semana por *3 semanas*

…e depois manter um Ponto de recuperação por mês por *2 meses*

…e depois manter um Ponto de recuperação por ano por *1 ano*

O Ponto de recuperação mais novo é definido para o dia, mês e ano atuais.

Neste exemplo, o ponto de recuperação mais antigo teria 1 ano, 4 meses e 6 dias.

8 Clique em **Salvar**.

Noções básicas sobre arquivos

As políticas de retenção impõem períodos em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada desses backups, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivo do AppAssure é usado para oferecer suporte à retenção estendida de dados compatíveis e não compatíveis. Também é usado para executar propagação de dados de replicação para um core de réplica remota.

Criar um arquivo

Execute as etapas deste procedimento para criar um arquivo.

Para criar um arquivo

1 Navegue até o AppAssure Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Criar**.

O assistente Adicionar arquivo é aberto.

3 Na página Criar do assistente Adicionar Arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de Localização:

- Local

- Rede
- Nuvem

4 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa 3.

Tabela 124.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Avançar**.

6 Na página Máquinas do assistente, selecione quais máquinas protegidas ou máquinas contêm os pontos de recuperação que deseja arquivar.

7 Clique em **Avançar**.

8 Na página Opções, insira as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar o arquivo efetuando uma das seguintes ações: • Selecione **Destino Inteiro** para reservar todo o espaço disponível no caminho fornecido em Etapa 4. (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, use as setas para cima e para baixo para inserir uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. **NOTA:** Os arquivos da nuvem do Amazon são automaticamente divididos em segmentos de 50 GB. Os arquivos da nuvem Microsoft Azure são automaticamente divididos em segmentos de 200 GB.

Caixa de texto	Descrição
Reciclar ação	Selecione uma das seguintes opções de ação de reciclagem: • **Não reutilizar.** Não substitui ou apaga nenhum dado arquivado existente no local. Se o local não estiver vazio, a gravação do arquivo falhará. • **Substituir este Core.** Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo. • **Incremental.** Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Comentários	Insira qualquer informação adicional necessária para o arquivo. O comentário será exibido se você importar o arquivo mais tarde.
Usar formato compatível	Selecione essa opção para arquivar seus dados em um formato compatível com versões antigas dos cores. NOTA: O novo formato oferece melhor desempenho, contudo, não é compatível com os cores mais antigos.

9 Clique em **Avançar**.

10 Na página Intervalo de data, insira a Data de início e a Data de expiração dos pontos de recuperação a serem arquivados.

- Para inserir uma hora, clique na hora exibida (padrão, 8h) para revelar as barras deslizantes para selecionar horas e minutos.
- Para inserir uma data, clique na caixa de texto para revelar o calendário, e depois clique no dia de sua preferência.

11 Clique em **Concluir**.

Definir um arquivo programado

O recurso Arquivo agendado permite que você defina uma hora para que um arquivo de uma máquina selecionada seja automaticamente criado e salvo em um local especificado. Isso abriga situações em que você deseje arquivos frequentes de uma máquina a serem salvos, sem a inconveniência de precisar criar os arquivos manualmente. Execute as etapas do procedimento a seguir para programar o arquivamento automático agendado.

Definir um arquivo agendado

1 Navegue até o AppAssure Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo Agendado, clique em **Adicionar**.

O assistente Adicionar arquivo é aberto.

4 Na página Local do assistente Adicionar arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de localização:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa 4.

Tabela 125.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Define o caminho do local onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Define o caminho do local onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Estabelece credenciais de logon para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Estabelece credenciais de logon para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Avançar**.

7 Na página Máquinas do assistente, selecione quais máquinas protegidas contêm os pontos de recuperação que deseja arquivar.

8 Clique em **Avançar**.

9 Na página Opções, selecione uma das seguintes Ações de reciclagem na lista suspensa:

- **Substituir este Core.** Substitui quaisquer dados arquivados existentes pertencentes a este core, porém deixa os dados de outros cores intactos.
- **Apagar completamente.** Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.
- **Incremental.** Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.

10 Na página Programar, selecione uma das seguintes opções de Enviar frequência de dados:

- Diariamente
- Semanalmente
- Mensalmente

11 Insira as informações descritas na tabela a seguir dependendo de sua seleção do Etapa 10.

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

12 Para pausar o arquivamento para retomar posteriormente, selecione **Pausa inicial do arquivamento**.

> **NOTA:** Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

13 Clique em **Concluir**.

Pausar ou retomar um arquivo programado

Pode haver vezes que deseje pausar um trabalho de arquivo agendado, como quando precisar alterar o local do arquivo de destino. Além disso, se escolheu pausar inicialmente o arquivamento quando realizou o procedimento Definir um arquivo programado, você provavelmente desejará retomar o arquivo agendado no futuro. Execute as etapas do procedimento a seguir para pausar ou retomar o arquivo agendado.

Pausar ou retomar o arquivamento automático

1 Navegue até o AppAssure Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo agendado, realize um dos procedimentos a seguir:

- Selecione o arquivo de preferência, e depois clique em uma das seguintes ações disponíveis:
  - Pause
  - Resume
- Ao lado do arquivo de preferência, clique no menu suspenso e em uma das seguintes ações disponíveis, conforme adequado:
  - Pause
  - Resume

O status do arquivo é exibido na coluna Programar.

Editar um arquivo programado

AppAssure permite que você altere os detalhes de um arquivo agendado. Para editar um arquivo agendado, execute as etapas do procedimento a seguir.

Editar um arquivo de programação

1 Navegue até o AppAssure Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo agendado, clique no menu suspenso ao lado do arquivo que você deseja alterar, e depois clique em **Editar**.

O assistente Adicionar arquivo é aberto.

4 Na página Local do assistente Adicionar arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de localização:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa 4.

Tabela 126.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Avançar**.

7 Na página Máquinas do assistente, selecione quais máquinas protegidas contêm os pontos de recuperação que deseja arquivar.

8 Clique em **Avançar**.

9 Na página Programar, selecione uma das seguintes opções de Enviar frequência de dados:

- Diariamente
- Semanalmente
- Mensalmente

10 Insira as informações descritas na tabela a seguir dependendo de sua seleção do Etapa 9.

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

11 Para pausar o arquivamento para retomar posteriormente, selecione **Pausa inicial do arquivamento**.

NOTA: Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

12 Clique em **Concluir**.

Verificar um arquivo

É possível fazer uma varredura de um arquivo para integridade estrutural realizando uma verificação do arquivo. Isso verifica a presença de todos os arquivos necessários dentro do arquivo. Para realizar uma verificação do arquivo, execute as etapas do procedimento a seguir.

Para verificar um arquivo

1 Navegue até o AppAssure Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Verificar arquivo**.

3 A caixa de diálogo Verificar arquivo é exibida.

4 Para **Tipo de localização**, selecione uma das seguintes opções na lista suspensa:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo como descrito na tabela a seguir, com base no tipo de local que você selecionou na Etapa 4.

Tabela 127.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Para realizar também uma verificação da integridade da estrutura, selecione **Integridade da estrutura**.

7 Clique em **Verificar arquivo**.

Importar um arquivo

Quando desejar recuperar dados arquivados, é preciso importar o arquivo inteiro a um local especificado. Depois, você poderá procurar os dados. Para importar um arquivo, execute as etapas do procedimento a seguir.

Para importar um arquivo

1 Navegue até o AppAssure Core Console e selecione a guia Ferramentas.

2 Na opção Arquivo, clique em **Importar**.

3 Para **Tipo de localização**, selecione uma das seguintes opções na lista suspensa:

- Local
- Rede
- Nuvem

4 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou na Etapa 3.

Tabela 128.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Verificar arquivo** para validar a existência do arquivo a ser importado.

6 Na caixa de diálogo, verifique o nome do core de origem exibido na lista suspensa do Core.

7 Selecione os agentes a serem importados do arquivo.

8 Selecione o repositório no qual os dados arquivados serão salvos.

NOTA: O repositório selecionado deve ser o mesmo repositório em que todos os atuais pontos de recuperação para o agente selecionado são armazenados.

9 Clique em **Restaurar** para importar o arquivo.

Arquivar na nuvem

Quando os dados atingirem o final de um período de retenção, você pode desejar ampliar essa retenção criando um arquivo dos dados antigos. Quando você arquiva dados, há sempre uma dúvida de onde armazená-los. O AppAssure permite que você carregue seus arquivos a uma variedade de provedores de nuvem diretamente do Core Console. As nuvens compatíveis incluem Microsoft Azure, Amazon, Rackspace e qualquer provedor baseado em OpenStack.

Exportar um arquivo a uma nuvem utilizando o AppAssure envolve os seguintes procedimentos:

- **Adicione sua conta em nuvem ao AppAssure Core Console.** Para obter mais informações, consulte Adicionar uma conta de nuvem.
- **Arquive seus dados e exporte-os para sua conta em nuvem.** Para obter mais informações, consulte Criar um arquivo.
- **Retomar dados arquivados importando-os do local da nuvem.** Para obter mais informações, consulte Importar um arquivo.

17

Gerenciar contas de nuvem

Este capítulo descreve como definir links para contas existentes de provedores de armazenamento em nuvem e como gerenciar essas contas para uso com o AppAssure. Por exemplo, você pode arquivar os dados do AppAssure na nuvem ou importar dados arquivados da nuvem. Este capítulo inclui as seguintes seções:

- Adicionar uma conta de nuvem
- Editar uma conta de nuvem
- Configurar as definições da conta de nuvem
- Remover uma conta de nuvem

O AppAssure permite arquivar dados em diversos provedores de nuvem ou importar dados arquivados armazenados em uma conta de nuvem. As nuvens compatíveis incluem Microsoft Azure, Amazon, Rackspace e qualquer provedor baseado em OpenStack.

Você pode adicionar uma conta de nuvem existente ao AppAssure Core Console. Depois de adicionada, você pode editar as informações, configurar as opções de conexão da conta ou removê-la do AppAssure.

Adicionar uma conta de nuvem

Antes que possa exportar seus dados arquivados para uma nuvem, você deve adicionar as informações da conta em seu provedor da nuvem ao AppAssure Core Console. Para adicionar uma conta em nuvem, execute as etapas do procedimento a seguir.

Adicionar uma conta em nuvem

1 No AppAssure Core Console, clique na guia Ferramentas.

2 No menu à esquerda, clique em **Nuvens**.

3 Na página Nuvens, clique em **Adicionar nova conta**.

A caixa de diálogo Adicionar nova conta é aberta.

4 Selecione um provedor de nuvem compatível da lista suspensa Tipo de nuvem.

5 Insira os detalhes descritos na tabela a seguir com base no tipo de nuvem selecionado no Etapa 4.

Tabela 129. Detalhes da conta de nuvem

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Nome da conta de armazenamento	Insira o nome de sua conta de armazenamento do Microsoft Azure.
	Chave de acesso	Insira a chave de acesso para sua conta.
	Nome de exibição	Crie um nome de exibição para essa conta no AppAssure; por exemplo, Microsoft Azure 1.

Tipo de nuvem	Caixa de texto	Descrição
Amazon S3	Chave de acesso	Insira a chave de acesso para sua conta em nuvem da Amazon.
	Chave secreta	Insira a chave secreta para esta conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure. Por exemplo, Amazon 1.
Fornecido pelo OpenStack	Nome de usuário	Insira o nome de usuário para sua conta em nuvem baseada no OpenStack.
	Chave API	Insira a chave API para sua conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure. Por exemplo, OpenStack 1.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta.
Rackspace Cloud Block Storage	Nome de usuário	Insira o nome de usuário para sua conta em nuvem do Rackspace.
	Chave API	Insira a chave API para esta conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure. Por exemplo, Rackspace 1.

6 Clique em **Adicionar**.

A caixa de diálogo fecha, e sua conta aparece na página Nuvens do Core Console.

Editar uma conta de nuvem

Se for necessário alterar as informações para se conectar à sua conta em nuvem, por exemplo, para atualizar a senha ou editar o nome de exibição, é possível fazer isso na guia Ferramentas do Core Console. Execute as etapas do procedimento a seguir para editar uma conta em nuvem.

Editar uma conta em nuvem

1 No AppAssure Core Console, clique na guia Ferramentas.

2 No menu à esquerda, clique em **Nuvens**.

3 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Editar**.

A janela Editar conta é aberta.

4 Edite os detalhes conforme necessário e clique em **Salvar**.

NOTA: Não é possível editar o tipo de nuvem.

Configurar as definições da conta de nuvem

As definições de configuração em nuvem permitem que você determine a quantidade de vezes que AppAssure deve tentar se conectar à sua conta em nuvem, e quanto tempo deve passar para essas tentativas antes que o tempo delas acabe. Execute as etapas do procedimento a seguir para configurar as definições da conexão para sua conta em nuvem.

Configurar definições da conta em nuvem

1 No AppAssure Core Console, clique na guia Configuração.

2 No menu à esquerda, clique em **Configurações**.

3 Na página Configurações, role para baixo até Configuração da nuvem.

4 Clique no menu suspenso ao lado da conta em nuvem que você desejar configurar, e depois realize os passos a seguir:

- Clique em **Editar**.

  A caixa de diálogo Configuração da nuvem é exibida.

  a Use as setas para cima e para baixo para editar as seguintes opções:

  - **Tempo limite de solicitação.** Exibido em minutos e segundos, ele determina a quantidade de tempo que AppAssure deve passar em uma única tentativa para se conectar à conta em nuvem quando houver um atraso. As tentativas de conexão irão parar depois da quantidade de tempo inserida.
  - **Tentar a contagem novamente.** Determina a quantidade de tentativas que AppAssure deve realizar antes de determinar que a conta em nuvem não possa ser atingida.
  - **Tamanho da memória intermediária de gravação.** Determina o tamanho da memória intermediária reservada para gravar dados arquivados na nuvem.
  - **Tamanho da memória intermediária de leitura.** Determina o tamanho do bloqueio reservado para ler dados arquivados da nuvem.

  b Clique em **Avançar**.

- Clique em **Redefinir**.

  Volta a configuração às seguintes definições padrão:

  - **Tempo limite de solicitação:** 01:30 (minutos e segundos)
  - **Tentar a contagem novamente:** 3 (tentativas)

Remover uma conta de nuvem

Se você interromper seu serviço em nuvem, ou decidir parar de usá-lo em um Core específico, você pode desejar remover sua conta em nuvem do Core Console. Execute as etapas do procedimento a seguir para remover uma conta em nuvem.

Remover uma conta em nuvem

1 No AppAssure Core Console, clique na guia Ferramentas.

2 No menu à esquerda, clique em **Nuvens**.

3 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Remover**.

4 Na janela Excluir conta, clique em **Sim** para confirmar que deseja remover a conta.

5 Se a conta em nuvem estiver atualmente em uso, uma segunda janela pergunta se você ainda deseja removê-la. Clique em **Sim** para confirmar.

> **NOTA:** Remover uma conta atualmente em uso faz com que todos os trabalhos de arquivamento para esta conta falhem.

18

Trabalhar com máquinas Linux

Este capítulo descreve como proteger, configurar e gerenciar máquinas Linux protegidas em seu ambiente do AppAssure. Ele inclui as seguintes seções:

- Trabalhar com pontos de recuperação do Linux
- Exportar dados para uma máquina virtual VirtualBox baseada em Linux
- Restaurar volumes em uma máquina Linux usando a linha de comando
- Realizar uma bare metal restore em máquinas Linux
- Gerenciar uma imagem de inicialização do Linux
- Gerenciar partições Linux
- Iniciar uma bare metal restore para Linux
- Confirmar a bare metal restore na linha de comando

O software AppAssure Agent é compatível com vários sistemas operacionais baseados em Linux (para mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*). O AppAssure Core é compatível apenas com máquinas Windows. Embora seja possível gerenciar máquinas Linux protegidas no AppAssure Core Console, vários procedimentos para máquinas Linux têm etapas que diferem dos procedimentos equivalentes no Windows. Além disso, você pode executar algumas ações diretamente em uma máquina Linux protegida usando o utilitário de linha de comando aamount.

Trabalhar com pontos de recuperação do Linux

A maneira recomendada e compatível de montar e desmontar pontos de recuperação em uma máquina Linux protegida é usar o utilitário aamount. Para obter mais informações, consulte os procedimentos a seguir:

- Montar um volume de ponto de recuperação em máquina Linux
- Desmontar um ponto de recuperação em uma máquina Linux

Esses procedimentos tratam especificamente do uso de aamount para montar e desmontar pontos de recuperação do Linux. Para gerenciar pontos de recuperação do Linux de outras maneiras, consulte Gerenciar snapshots e pontos de recuperação, pois todas as outras atividades de gerenciamento podem ser realizadas no Core Console.

Montar um volume de ponto de recuperação em máquina Linux

Usando o utilitário aamount no AppAssure, é possível montar remotamente um volume de um ponto de recuperação como um volume local em uma máquina Linux.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

Para montar um volume de ponto de recuperação em máquina com Linux

1. Crie um novo diretório para montar o ponto de recuperação (por exemplo, pode usar o comando `mkdir`).
2. Confirme se o diretório existe (por exemplo, usando o comando `ls`).
3. Execute o utilitário, do AppAssure, aamount como raiz ou como superusuário, por exemplo:

   ```
   sudo aamount
   ```

4. No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

   ```
   lm
   ```

5. Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure Core.
6. Insira as credenciais de login do server do Core, ou seja, o nome de usuário e a senha.

   Será exibida uma lista das máquinas que estão protegidas pelo servidor AppAssure. Cada máquina é identificada por: número de item de linha, host/endereço IP e número de ID da máquina.

   Por exemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f
7. Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

   ```
   lr <line_number_of_machine
   ```

   NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

   É exibida uma lista com os pontos de recuperação de base e incrementais da máquina. Essa lista inclui o número do item de linha, o carimbo de data e hora, o local do volume, o tamanho do ponto de recuperação e número de ID do volume, que termina com um número de sequência para identificar o ponto de recuperação.

   Por exemplo, 293cc667-44b4-48ab-91d8-44bc74252a4f:2
8. Insira o seguinte comando para selecionar e montar o ponto de recuperação especificado no ponto/caminho de montagem especificado.

   ```
   m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
   ```

   O sinalizador no comando determina como montar o ponto de recuperação. Você pode usar uma das opções a seguir:

   - [r] - montar apenas leitura (padrão). Este sinalizador permite montar um ponto de recuperação, mas não alterá-lo.
   - [w] - montar gravável. Este sinalizador permite montar um ponto de recuperação e alterá-lo.
   - [v] - montar com gravações anteriores. O sinalizador "v" permite montar o ponto de recuperação e incluir alterações que tenham sido feitas durante a montagem gravável anterior mas não estejam presentes no ponto de recuperação.
   - [n] - não montar nbd em <path>. Um nbd (dispositivo de bloco de rede) estabelece uma conexão de socket entre o Core e a máquina protegida quando você realiza uma montagem local. Este sinalizador permite montar o ponto de recuperação sem montar o nbd, o que é útil caso você queira verificar manualmente o sistema de arquivos do ponto de recuperação.

   NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha da máquina (da saída de lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido do caminho, como neste exemplo: m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>. Por exemplo, se a saída de `lm` relacionar três máquinas protegidas e você inserir o comando `lr` para o número 2 e montar o volume b do ponto de recuperação 23 em /tmp/mount_dir, o comando será:
   `m 2 23 b /tmp/mount_dir`

9 Para confirmar se a montagem foi bem-sucedida, insira o seguinte comando, que deve listar o volume remoto anexado:

```
l
```

Desmontar um ponto de recuperação em uma máquina Linux

Complete as etapas neste procedimento para desmontar um ponto de recuperação em uma máquina Linux.

Para desmontar um ponto de recuperação em máquina com Linux

1 Execute o utilitário, do AppAssure, aamount como raiz ou como superusuário, por exemplo:

```
sudo aamount
```

2 No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

```
lm
```

3 Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure Core.

4 Insira as credenciais de login (nome de usuário e a senha) do server do Core.

Será exibida uma lista das máquinas que estão protegidas pelo servidor AppAssure.

5 Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

```
lr <line_number_of_machine
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma lista exibe e inclui os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim, que identifica o ponto de recuperação.

Por exemplo, 293cc667-44b4-48ab-91d8-44bc74252a4f:2

6 Execute o comando `l ou list` para obter uma lista dos dispositivos Network Block Device (NBD). Se você montar um ponto de recuperação, receberá um caminho para o NBD-device depois de executar o comando `l ou list`.

7 Insira o seguinte comando para desmontar um ponto de recuperação:

```
unmount <path_of_nbd-device>
```

8 Execute o comando `l ou list` para garantir que a desmontagem do ponto de recuperação foi bem-sucedida.

Exportar dados para uma máquina virtual VirtualBox baseada em Linux

Com o AppAssure, você pode exportar dados para uma máquina virtual (VM) baseada em Windows ou Linux usando o VirtualBox. Uma exportação inclui todas as informações de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos para a programação de proteção da sua máquina.

NOTA: O Virtual Box Versão 4.2.18 ou superior é suportado. A exportação para uma VM VirtualBox baseada em Linux requer uma conexão SSH do Core para a máquina Linux.

NOTA: Para exportar para uma VM VirtualBox baseada em Windows, consulte Exportar dados para uma máquina virtual VirtualBox.

CUIDADO: O AppAssure não permite exportar máquinas que têm partições estendidas.

Realizar uma exportação única de VirtualBox

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

Para realizar uma exportação única para o VirtualBox

1. No AppAssure Core Console, navegue até a máquina com Linux que deseja exportar.
2. Na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar** e depois selecione **Única**.

   O Assistente de exportação é exibido na página Máquinas protegidas.
3. Selecione uma máquina para exportar e depois clique em **Avançar**.
4. Na página Pontos de recuperação, selecione o ponto de recuperação que deseja exportar e clique em **Avançar**.
5. Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.
6. Na página Opções de máquina virtual, selecione **Máquina remota do Linux**.
7. Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 130. Definições da máquina Linux remota

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Porta	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA:** Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Na página Volumes, selecione os volumes de dados a exportar e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua de VirtualBox (Standby virtual)

Conclua as etapas deste procedimento para criar um Standby virtual e realizar uma exportação contínua para VirtualBox.

Para realizar uma exportação contínua de VirtualBox (Standby virtual)

1 No AppAssure Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar para a máquina virtual, selecione **VirtualBox**.

3 Na página Opções de máquina virtual, selecione **Máquina remota do Linux**.

4 Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 131. Definições da máquina Linux remota

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Porta	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA:** Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

5 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

6 Clique em **Avançar**.

7 Na página Volumes, selecione os volumes de dados a exportar e clique em **Avançar**.

8 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Restaurar volumes em uma máquina Linux usando a linha de comando

No AppAssure, é possível restaurar volumes em suas máquinas Linux protegidas usando o utilitário de linha de comando aamount.

NOTA: Esse processo antes era chamado de reversão.

Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

A restauração de volumes também é suportada em suas máquinas protegidas no AppAssure Core Console. Consulte Restaurar volumes a partir de um ponto de recuperação para obter mais informações.

CUIDADO: Para restaurar a partição de sistema ou raiz (/) ou todo o sistema operacional, consulte Realizar uma bare metal restore em máquinas Linux.

Para restaurar volumes em uma máquina com Linux usando a linha de comando

1 Execute o utilitário AppAssure aamount como raiz, por exemplo:

```
sudo aamount
```

2 No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

```
lm
```

3 Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure Core.

4 Insira as credenciais de login desse server, ou seja, o nome de usuário e a senha.

Aparece uma lista que mostra as máquinas protegidas por esse server AppAssure. Ela relaciona as máquinas agente encontradas por número de item de linha, host/endereço IP e número de ID da máquina (por exemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f).

5 Insira o seguinte comando para relacionar os pontos de recuperação atualmente montados para a máquina especificada:

```
lr <machine_line_item_number>
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma exibição em lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim (por exemplo,
”293cc667-44b4-48ab-91d8-44bc74252a4f:2”), que identifica o ponto de recuperação.

6 Insira o seguinte comando para selecionar um ponto de recuperação a restaurar:

```
r <volume_recovery_point_ID_number> <caminho>
```

Esse comando restaura a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho para a restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

> **NOTA:** Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha de agente/máquina (da saída lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido pelo caminho, como, r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <caminho>. Nesse comando, <caminho> é o descritor de arquivo do volume real.
>
> Por exemplo, se a saída `lm` relacionar três máquinas agente e você inserir o comando `lr` para o número `2`, e quiser restaurar o ponto de recuperação `23` do volume `b` no volume montado no diretório `/mnt/data`, o comando será:
>
> ```
> r2 23 b /mnt/data
> ```
>
> É possível restaurar para /, mas apenas ao realizar uma Bare Metal Restore ao ser inicializado com um Live DVD. Para obter mais informações, consulte Iniciar uma bare metal restore para Linux.

7 Quando solicitado a continuar, insira `y`, para Sim.

Depois que a restauração continuar, uma série de mensagens será exibida para notificá-lo sobre o status.

8 Após a restauração bem-sucedida, o utilitário aamount montará e reanexará automaticamente o módulo do kernel ao volume restaurado se o destino antes estava protegido e montado. Caso contrário, será necessário montar o volume restaurado no disco local e, em seguida, confirmar se os arquivos estão restaurados (por exemplo, é possível usar o comando `sudo mount` e depois o comando `ls`.)

Realizar uma bare metal restore em máquinas Linux

No AppAssure é possível realizar uma bare metal restore (BMR) em uma máquina com Linux, incluindo uma restauração do volume do sistema. Ao restaurar uma máquina com Linux, você irá reverter para o ponto de recuperação do volume de inicialização. A funcionalidade de BMR é suportada usando o utilitário de linha de comando aamount e de dentro da UI do Core Console.

△ **CUIDADO: Antes de iniciar o processo de BMR, certifique-se de que a máquina Linux que você deseja restaurar não inclui uma partição de inicialização EXT2. Uma BMR realizada em uma máquina com esse tipo de partição resulta em uma máquina não inicializável. Para realizar uma BMR nesse caso, você teria que converter as partições EXT2 para EXT3 ou EXT4 antes de começar a proteger e criar cópias de segurança da máquina.**

CUIDADO: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o AppAssure gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a criação de um snapshot incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.

Para realizar uma bare metal restore em máquinas com Linux, realize as tarefas a seguir.

- **Gerenciamento de uma imagem de inicialização do Linux**. Essa imagem ISO do DVD de inicialização Linux Live é usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciar uma imagem de inicialização do Linux.
  - Se você precisar de mídia física para iniciar a máquina Linux de destino, precisará transferir a imagem ISO para a mídia. Consulte Transferir a imagem ISO do Live DVD para a mídia.
  - Em todos os casos, será preciso carregar a imagem de inicialização no server de destino e iniciar o server da imagem de inicialização. Consulte Carregar o Live DVD e iniciar a máquina de destino.
- **Gerenciamento de partições**. Pode ser necessário criar ou montar as partições antes de realizar uma BMR em uma máquina com Linux. Consulte Gerenciar partições Linux.
  - O sistema Linux no qual você está realizando uma BMR deve ter as mesmas partições dos volumes de origem no ponto de recuperação. Talvez seja necessário criar partições adicionais no sistema de destino. Consulte Criar partições na unidade de destino.
  - Se estiver sendo feita uma BMR manual, será preciso primeiro montar partições. Consulte Montar partições a partir da linha de comando. As etapas para montar partições estão incluídas no processo de realização da BMR na linha de comando. Consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

    Se você usar particionamento automático para BMR no Core Console, não precisará montar partições. O AppAssure restaurará as mesmas partições incluídas nos pontos de recuperação que estão sendo restaurados.
- **Iniciar uma bare metal restore para Linux**. Depois que a máquina de destino é iniciada da imagem de inicialização do Live DVD, é possível iniciar a BMR. As tarefas exigidas dependem de se isso será feito na interface com o usuário do AppAssure ou na linha de comando usando o utilitário aamount. Consulte Iniciar uma bare metal restore para Linux.
  - Se for usado o Core Console, será preciso iniciar uma restauração em um ponto de recuperação do Core. Consulte Selecionar um ponto de recuperação e iniciar a BMR.
  - Se for usado o Core Console, será preciso mapear os volumes na UI. Consulte Mapear volumes para uma bare metal restore.
  - Como opção, ao restaurar da linha de comando, você poderá iniciar o utilitário de tela para melhorar sua capacidade de rolar e ver os comandos no console do terminal. Para obter mais informações, consulte Iniciar o utilitário Screen.

    - Se usar aamount, todas as tarefas serão realizadas na linha de comando. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.
- **Confirmação de um bare metal restore**. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmar a bare metal restore na linha de comando.
    - É possível monitorar o progresso de sua restauração. Consulte Visualizar o progresso da recuperação.
    - Depois de concluída, você pode iniciar o server restaurado. Consulte Inicializar um servidor de destino restaurado.
    - Solucionar problemas do processo de BMR. Consulte Solucionar problemas de conexão com o Universal Recovery Console e Reparar problemas de inicialização.

Pré-requisitos para realizar uma bare metal restore em máquinas Linux

Antes de iniciar o processo de realização de uma bare metal restore em uma máquina com Linux, é preciso garantir que as seguintes condições e critérios estejam presentes:

- **Cópias de segurança da máquina que você deseja restaurar.** É preciso ter um AppAssure Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar.
- **Hardware para restaurar (novo ou antigo, similar ou não).** A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o *Guia de instalação e atualização do Dell AppAssure*.
- **Imagem de inicialização do Live DVD**. Obtenha a imagem ISO do Linux Live DVD, que inclui uma versão inicializável do Linux. Baixe-o do Portal de licenças do Dell AppAssure em https://licenseportal.com. Se houver problemas para baixar o Live DVD, entre em contato com o suporte do Dell AppAssure.
- **Software e mídia de imagem.** Se usar mídia física, é preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO.
- **Drivers do adaptador de rede e de armazenamento compatíveis.** Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- **Partições e espaço de armazenamento, conforme apropriado.** Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- **Restaurar caminho.** Identifique o caminho da restauração, que é o caminho do descritor de arquivo de dispositivo. Para identificar o caminho do descritor de arquivo de dispositivo, use o comando `fdisk` de uma janela de terminal.

Gerenciar uma imagem de inicialização do Linux

Uma bare metal restore para Linux exige uma imagem de inicialização do Live DVD, que pode ser baixada do Portal de licenças do Dell AppAssure. Use essa imagem para iniciar a máquina de destino com Linux. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Linux a partir da imagem de inicialização.

NOTA: O Live DVD era conhecido anteriormente como Live CD.

Você pode realizar as seguintes tarefas:

- Baixar uma imagem ISO de inicialização para Linux
- Transferir a imagem ISO do Live DVD para a mídia
- Carregar o Live DVD e iniciar a máquina de destino

O gerenciamento de uma imagem de inicialização do Linux é uma etapa do Realizar uma bare metal restore em máquinas Linux.

Baixar uma imagem ISO de inicialização para Linux

A primeira etapa ao realizar uma bare metal restore (BMR) em uma máquina com Linux é baixar a imagem ISO do Live DVD para Linux do Portal de licenças do Dell AppAssure. O Live DVD funciona com todos os sistemas de arquivo Linux suportados pelo AppAssure, e inclui uma versão inicializável do Linux, um utilitário de tela e a interface do Universal Recovery Console (URC) do AppAssure. O Universal Recovery Console do AppAssure é um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do AppAssure Core.

NOTA: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

É preciso baixar a imagem ISO do Live DVD que corresponde à sua versão do AppAssure. A versão atual do Live DVD está disponível no Portal de licenças do Dell AppAssure em https://licenseportal.com. Se precisar de uma versão diferente, entre em contato com o Suporte do Dell AppAssure.

NOTA: Para obter mais informações sobre o Portal de licenças do Dell AppAssure, consulte o *Dell AppAssure Guia do usuário do Portal de licenças do*.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Execute as etapas deste procedimento para baixar a imagem ISO do Live DVD.

Para baixar uma imagem ISO de inicialização para Linux

1. Efetue login no Portal de licenças do Dell AppAssure em https://licenseportal.com.
2. Acesse a área **Downloads**.
3. Role para baixo até Aplicativos com base em Linux e, na seção do Live DVD para Linux, clique em **Baixar**.
4. Salve a imagem ISO do Live DVD. Se você estiver restaurando uma máquina virtual, poderá salvá-la em um local de rede e definir a VM para iniciar da unidade de CD ou DVD associada à imagem ISO.
5. Se a restauração for de uma máquina física, grave a imagem ISO do CD de inicialização em um CD ou DVD a partir do qual a máquina de destino pode ser iniciada. Para obter mais informações, consulte Transferir a imagem ISO do Live DVD para a mídia.

Transferir a imagem ISO do Live DVD para a mídia

Quando você baixa o arquivo do Live DVD para Linux, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de inicializar a máquina Linux de destino com a imagem do Live DVD.

É possível gravar a imagem ISO do CD de inicialização em mídia de CD ou DVD.

Se a máquina for iniciada do Live DVD, o Universal Recovery Console será iniciado automaticamente.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições dessa VM para iniciar essa unidade.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Carregar o Live DVD e iniciar a máquina de destino

Depois de obter a imagem ISO do Live DVD, é preciso iniciar a máquina Linux com o Live DVD recém-criado.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Para carregar um Live DVD e iniciar a máquina de destino

1. Navegue até o novo server e carregue a imagem do Live DVD a partir do local apropriado. Especifique se o server será iniciado da imagem do Live DVD.
2. Inicie a máquina.

   É exibida uma tela de abertura do AppAssure e uma janela de terminal se abre, exibindo o endereço IP e a senha de autenticação da máquina.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com a imagem do Live DVD.
3. Anote o endereço IP e a senha de autenticação exibidos na tela de introdução. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.

Depois que a máquina de destino com Linux é iniciada com o Live DVD, essa máquina fica pronta para o usuário se conectar a ela a partir do Core para iniciar o processo de bare metal restore. É possível realizar esse processo usando um de dois métodos:

- Ativação de uma restauração a partir do AppAssure Core Console. Para obter mais informações, consulte Iniciar uma bare metal restore para Linux.
- Ativação de uma restauração a partir da linha de comando usando o utilitário aamount. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Gerenciar partições Linux

Ao realizar uma BMR, a unidade de destino na qual você restaurará os dados deve ter as mesmas partições do ponto de recuperação que está sendo restaurado. Talvez seja necessário criar partições para atender a esse requisito.

É possível iniciar a restauração na linha de comando usando o utilitário aamount ou no AppAssure Core Console. Se a restauração for feita usando a interface com o usuário, primeiro será preciso montar as partições.

Você pode realizar as seguintes tarefas:

- Criar partições na unidade de destino
- Formatar partições na unidade de destino
- Montar partições a partir da linha de comando

O gerenciamento de partições no Linux é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

Criar partições na unidade de destino

Muitas vezes, ao fazer uma BMR, a unidade de destino é um novo volume que pode ser composto de uma única partição. A unidade na máquina de destino deve ter a mesma tabela de partições do ponto de recuperação, incluindo o tamanho dos volumes. Se a unidade de destino não contiver as mesmas partições, será preciso criá-las antes de realizar a bare metal restore. Use o utilitário fdisk para criar partições na unidade de destino iguais às partições na unidade de origem.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar partições Linux.

Para criar partições na unidade de destino

1 Como opção, você pode iniciar o utilitário Screen. Depois de iniciado, ele permanece ativo até que você reinicialize a máquina.

> **NOTA:** Para obter mais informações, consulte Iniciar o utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que o volume que você deseja particionar é /dev/sda. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
sudo fdisk /dev/sda
```

4 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
n
```

5 Para criar uma nova partição primária, insira o seguinte comando e pressione **Enter**:

```
p
```

6 Para especificar o número de partição, insira-o e pressione **Enter**. Por exemplo, para especificar a partição 1, digite 1 e, em seguida, pressione **Enter**.

7 Para usar o primeiro setor, 2048, pressione **Enter**.

8 Aloque uma quantidade adequada para a partição de inicialização, inserindo o sinal de mais e a quantidade de alocação e pressionando **Enter**.

Por exemplo, para alocar 500 M para a partição de inicialização, digite o seguinte e pressione **Enter**:

```
+500M
```

9 Para alternar um sinalizador inicializável para a partição de inicialização (para tornar a partição inicializável), digite o seguinte comando e pressione **Enter**:

```
a
```

10 Para atribuir um sinalizador inicializável à partição adequada, digite o número da partição e pressione **Enter**. Por exemplo, para atribuir um sinalizador inicializável para a partição 1, digite 1 e pressione **Enter**.

11 Para salvar todas as alterações no utilitário fdisk, digite o seguinte comando e pressione **Enter**:

```
w
```

Formatar partições na unidade de destino

Depois de criar partições em um novo volume na unidade de destino, você deverá formatá-las antes que elas sejam montadas. Se essa situação se aplicar a você, siga este procedimento para formatar partições em formatos Ext3, Ext4 ou XFS.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar partições Linux.

Para formatar partições na unidade de destino

1 Como opção, você pode iniciar o utilitário Screen. Depois de iniciado, ele permanece ativo até que você reinicialize a máquina.

> **NOTA:** Para obter mais informações, consulte Iniciar o utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que a partição que você deseja formatar é /dev/sda1. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Selecione um dos seguintes comandos dependendo do formato que você deseja utilizar a partição de destino:

- Para formatar uma partição no formato Ext3, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext3 /dev/sda1
  ```

- Para formatar uma partição no formato Ext4, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext4 /dev/sda1
  ```

- Para formatar uma partição no formato xfs, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.xfs /dev/sda1
  ```

A partição selecionada é formatada de acordo.

4 De forma opcional, se você precisar formatar outras partições, repita esse procedimento.

Montar partições a partir da linha de comando

Se for feita uma BMR usando o AppAssure Core Console, será preciso primeiro montar as partições adequadas na máquina de destino. Realize isso na linha de comando do Universal Recovery Console.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar partições Linux.

Execute as etapas deste procedimento para montar partições na máquina com Linux antes de fazer uma restauração.

Para montar partições a partir da linha de comando

1. Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

   ```
   sudo fdisk -l
   ```

   Uma lista com todos os volumes é exibida.

2. Formate todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

3. Monte todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

   ```
   mount /dev/sda1 /mnt
   ```

4. Repita a Etapa 3 conforme necessário até ter montado todos os volumes necessários.

Depois que os volumes estiverem montados, é possível fazer uma restauração para a máquina com Linux de destino a partir do AppAssure Core Console. Consulte Iniciar uma bare metal restore para Linux.

Iniciar uma bare metal restore para Linux

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Linux, certas condições devem ser satisfeitas.

Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma bare metal restore em máquinas Linux.

A máquina com Linux de destino da BMR deve ser iniciada usando a imagem de inicialização do Live DVD. Para obter mais informações, consulte Gerenciar uma imagem de inicialização do Linux.

O número de volumes na máquina com Linux a ser restaurada deve corresponder ao número de volumes no ponto de recuperação. Também é preciso decidir se deseja restaurar a partir do AppAssure Core Console ou da linha de comando usando aamount. Para obter mais informações, consulte Gerenciar partições Linux.

Se a restauração for feita a partir da UI do Core Console, a primeira etapa para iniciar a BMR é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida a partir do Universal Recovery Console. A seguir, você precisa mapear as unidades e iniciar a restauração.

Para iniciar uma BMR no AppAssure Core Console, realize as seguintes tarefas.

- Selecionar um ponto de recuperação e iniciar a BMR
- Mapear volumes para uma bare metal restore

Se a restauração for feita da linha de comando usando o utilitário aamount, primeiro será preciso definir os privilégios apropriados, montar volumes, executar o aamount, obter informações sobre o Core na lista de máquinas, conectar-se ao core, obter uma lista de pontos de recuperação, selecionar o ponto de recuperação do qual deseja reverter em bare metal restore e iniciar a restauração.

Como opção, você pode iniciar o utilitário Screen.

Para iniciar uma BMR na linha de comando, realize as tarefas a seguir.

- Iniciar o utilitário Screen
- Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Linux.

Iniciar o utilitário Screen

O Live DVD inclui o utilitário Screen, disponível ao inicializar a partir do Live DVD no Universal Recovery Console. O Screen permite aos usuários gerenciar vários shells simultaneamente em uma única sessão Secure Shell (SSH) ou janela de console. Isso permite realizar uma tarefa em uma janela de terminal (como confirmar volumes montados) e, enquanto isso é executado, abrir ou alternar para outra instância de shell e realizar outra tarefa (como executar o utilitário aamount).

O utilitário Screen também tem seu próprio buffer de rolagem para trás, o que permite rolar a tela para ver maiores quantidades de dados, como a lista de pontos de recuperação.

NOTA: O utilitário Screen é fornecido para sua conveniência; seu uso é opcional.

O utilitário Screen inicia na máquina inicializada com o Live DVD por padrão. Contudo, se você fechou esse aplicativo, é preciso iniciar o utilitário Screen a partir do Live DVD usando o procedimento abaixo.

Para iniciar o utilitário Screen

- Se a máquina foi inicializada a partir do Live DVD, na janela do terminal, digite **screen** e pressione **Enter**.

  O utilitário Screen é iniciado.

Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Depois que a imagem ISO do Live DVD estiver acessível na máquina na qual você deseja realizar uma BMR e o número e tamanho dos volumes forem correspondentes entre a máquina de destino e o ponto de recuperação no qual deseja executar a bare metal restore, será possível iniciar essa restauração na linha de comando usando o utilitário aamount.

Se desejar realizar uma BMR usando a UI do AppAssure Core Console, consulte Selecionar um ponto de recuperação e iniciar a BMR.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Execute as etapas deste procedimento para selecionar um ponto de recuperação no Core para reverter para a máquina de destino física ou virtual da BMR.

Para realizar uma bare metal restore em uma máquina com Linux usando a linha de comando

1 Para executar o utilitário AppAssure aamount como raiz, digite o seguinte comando e pressione **Enter**:

```
sudo aamount
```

2 Para relacionar as máquinas protegidas, digite o seguinte comando e pressione **Enter**:

```
lm
```

3 Quando solicitado, insira as informações de conexão do AppAssure Core, como descrito na tabela a seguir, e pressione **Enter** após cada comando obrigatório:

Tabela 132. Informações de conexão do AppAssure Core

Caixa de texto	Descrição	Obrigatório
Endereço IP do AppAssure Core ou nome de host	O endereço IP ou nome de host do AppAssure Core.	Sim
Domínio	O domínio do AppAssure Core. Opcional.	Não
Usuário	O nome de usuário de um usuário administrativo no Core	Sim
Senha	A senha usada para conectar o usuário administrativo ao Core.	Sim

Aparece uma lista que mostra as máquinas protegidas pelo AppAssure Core. Ela relaciona as máquinas encontradas por número de item de linha, nome de exibição do host ou endereço IP e número de ID da máquina.

4 Para relacionar os pontos de recuperação da máquina que você deseja restaurar, digite o comando Relacionar os pontos de recuperação usando a seguinte sintaxe e pressione **Enter**:

```
lr <machine_line_item_number>
```

NOTA: Você também pode inserir o número de ID da máquina nesse comando em vez do número do item de linha.

Uma lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui:

- Número de item de linha
- Carimbo de data e hora
- Uma lista de volumes com letras dentro do ponto de recuperação
- Localização do volume
- Tamanho do ponto de recuperação
- Um número de ID do volume que inclui um número de sequência no fim, identificando o ponto de recuperação

5 Para selecionar o ponto de recuperação de uma restauração, insira o seguinte comando e pressione **Enter**:

```
r <recovery_point_ID_number> <caminho>
```

CUIDADO: É preciso garantir que o volume do sistema não esteja montado.

NOTA: Se a máquina foi iniciada do Live DVD, o volume do sistema não estará montado.

Esse comando reverte a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

> **NOTA:** Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, use o número de linha de agente/máquina (da saída `lm`), seguido do número da linha do ponto de recuperação e da letra de volume (da lista de volumes com letras dentro do ponto de recuperação), seguidos pelo caminho. Por exemplo:
>
> `r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <caminho>`
>
> Por exemplo, digite:
>
> `r 1 24 a /dev/sda1`
>
> Nesse comando, *<caminho>* é o descritor de arquivo do volume real.

6 Quando solicitado a continuar, insira **y**, para Sim, e pressione **Enter**.

Depois que a restauração iniciar, uma série de mensagens será exibida para notificá-lo do status de conclusão da restauração.

> **NOTA:** Se você receber uma mensagem de exceção, os detalhes sobre essa exceção poderão ser encontrados no arquivo aamount.log. O arquivo aamount.log encontra-se em /var/log/appassure.

7 Depois de uma restauração bem-sucedida, saia do aamount digitando `exit` e pressione **Enter**.

8 A próxima etapa é confirmar a restauração. Para obter mais informações, consulte Confirmar a bare metal restore na linha de comando.

Confirmar a bare metal restore na linha de comando

A Dell recomenda realizar as seguintes etapas para confirmar se uma bare metal restore foi concluída na linha de comando.

- Realizar uma verificação do sistema de arquivos no volume restaurado
- Usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

Realizar uma verificação do sistema de arquivos no volume restaurado

Depois de executar uma bare metal restore na linha de comando, você deve realizar uma verificação do sistema de arquivos no volume restaurado para garantir que os dados restaurados do ponto de recuperação não foram corrompidos.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a bare metal restore na linha de comando.

Realize a tarefa abaixo para realizar uma verificação do sistema de arquivos no volume restaurado.

Para realizar uma verificação do sistema de arquivos no volume restaurado

1 Na linha de comando do Universal Recovery Console da máquina com Linux que você restaurou, para confirmar se as partições adequadas estão montadas, digite o seguinte comando e pressione **Enter**:

`df`

2 Se o volume restaurado não estiver montado, vá para a Etapa 3. Se o volume restaurado estiver montado, desmonte-o digitando o seguinte comando e pressionando **Enter**:

```
umount <volume>
```

3 Execute uma verificação do sistema de arquivos nos volumes restaurados digitando o seguinte comando e pressionando Enter:

```
fsck -f <volume>
```

Se o retorno do fsck for limpo, o sistema de arquivos estará confirmado.

4 Monte os volumes adequados novamente digitando o seguinte comando no formato `mount <volume> <pasta>` e depois pressione **Enter**.

Por exemplo, se o caminho do volume for prod/sda1 e a pasta que você deseja montar for mnt, digite o seguinte e pressione **Enter**:

```
mount /dev/sda1 /mnt
```

Usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Depois de executar uma verificação limpa do sistema de arquivos no volume restaurado, crie partições inicializáveis.

O GNU Grand Unified Bootloader (GRUB) é um carregador de inicialização que permite aos administradores configurar qual sistema operacional ou configuração de kernel específica será utilizado para iniciar o sistema. Após uma BMR, o arquivo de configuração do GRUB deve ser modificado para que a máquina use o identificador universal exclusivo (UUID) apropriado para o volume raiz. Antes dessa etapa, é preciso montar os volumes raiz e de inicialização e verificar os UUIDs de cada um. Isso garante que você consiga inicializar a partir da partição.

NOTA: Este procedimento aplica-se a máquinas Linux que usam GRUB1 ou GRUB2. Ao usar este procedimento, certifique-se de que a partição de inicialização está íntegra e protegida.

CUIDADO: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o AppAssure gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a criação de um snapshot incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a bare metal restore na linha de comando.

Realize a tarefa abaixo para criar partições inicializáveis usando a linha de comando.

Para usar a linha de comando para tornar uma máquina Linux restaurada inicializável

1 É preciso montar o volume raiz primeiro e, depois, o volume de inicialização. Monte cada volume restaurado usando os seguintes comandos:

a Para montar o volume raiz, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[root]> /mnt
```

Por exemplo, se /dev/sda2 for o volume raiz, digite **mount /dev/sda2 /mnt** e pressione **Enter**.

b Para montar o volume de inicialização, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[boot]> /mnt/boot
```

Por exemplo, se /dev/sda1 for o volume de inicialização, digite **mount /dev/sda1 /mnt/boot** e pressione **Enter**.

NOTA: Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.

2 Se o tamanho do volume estiver aumentando — ou seja, se o volume de destino na nova máquina Linux for maior do que o volume no ponto de recuperação — será preciso excluir os arquivos de dados de mapa de bits existentes.

3 Obtenha o identificador universal exclusivo (UUID) dos novos volumes usando o comando `blkid`. Digite o seguinte comando e pressione **Enter**:

```
blkid [volume]
```

NOTA: Também é possível usar o comando `ls -l /dev/disk/by-uuid`.

4 Obtenha o UUID antigo da partição ou partições no arquivo `/etc/fstab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/fstab
```

5 Obtenha o UUID antigo das partições no arquivo `/etc/mtab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/mtab
```

6 Se a BMR estiver sendo realizada em um disco novo na máquina de destino, comente a partição de swap em fstab no seu volume raiz.

7 A modificação dos caminhos fstab e mtab deve ocorrer no volume restaurado e não no Live DVD. Não há necessidade de modificar os caminhos do Live DVD. Prepare a instalação do Grand Unified Bootloader (GRUB) digitando os seguintes comandos. Depois de cada comando, pressione **Enter**:

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

8 Localize o arquivo `grub.conf` em seu volume montado e abra-o usando um editor de texto.

A localização do grub.conf varia dependendo das versões do OS e do GRUB instalado. As localizações mais prováveis incluem **<root path>/boot/grub/grub.conf**, **<root path>/boot/grub/grub.cfg** ou **<root path>/etc/grub.conf**.

9 No grub.conf, localize todas as linhas que contêm “root=<root device uuid>” e substitua-o pelo UUID correto do volume raiz. Também é possível usar o caminho do dispositivo raiz. Como nos exemplos acima, se o caminho do dispositivo raiz for /dev/sda2, altere todas as instâncias para root=/dev/sda2.

10 Realize um dos procedimentos a seguir:

- Se não estiver usando LVM, remova todas as entradas "rd_LVM_LV=" do arquivo grub.conf, salve o arquivo e saia do editor de texto.
- Se estiver usando LVM, insira o nome do dispositivo. Por exemplo:

  ```
  root=/dev/mapper/vg_TEST-root
  rd_LVM_LV=vg_TEST/sqp_1rd_LVM_LV=vg_TEST/root
  ```

11 Altere o diretório raiz digitando o seguinte comando e pressionando **Enter**:

```
chroot /mnt /bin/bash
```

12 Se estiver usando o SLES, instale o GRUB digitando os seguintes comandos, pressionando **Enter** depois de cada um:

```
grub-install --recheck /dev/sda
```

```
grub-install /dev/sda
```

13 Para distribuições Linux que não sejam o SLES, instale o GRUB digitando o seguinte comando e pressionando **Enter**:

```
grub-install/dev/sda
```

> **NOTA:** Se for instalar em SUSE, ao instalar o GRUB, não serão necessários parâmetros. Por exemplo, o comando para instalar o GRUB em SUSE é simplesmente grub-install. Depois, pressione **Enter**.

14 Quando concluir a instalação, execute uma das atualizações a seguir:

- Para SLES:

```
grub-install.unsupported --recheck /dev/sda
grub-install.unsupported /dev/sda
update-grub
```

> **NOTA:** Se o comando `update-grub` não existir na sua distribuição Linux, ignore essa opção.

- Para outras distribuições:

```
grub-install /dev/sda
update-grub
```

> **NOTA:** Se o comando `update-grub` não existir na sua distribuição Linux, ignore essa opção.

15 Remova o disco do Live DVD da unidade de CD-ROM ou DVD e reinicie a máquina com Linux.

19

Noções básicas do Local Mount Utility

Este capítulo descreve como baixar, instalar e usar o Local Mount Utility (LMU) para montar e explorar pontos de recuperação em uma máquina que não hospeda o AppAssure Core. Os seguintes tópicos estão incluídos:

- Baixar o Local Mount Utility
- Instalar o Local Mount Utility
- Usando o Local Mount Utility
- Usar opções do AppAssure Core e de máquina protegida

O LMU é um aplicativo que pode ser obtido por download e permite montar um ponto de recuperação em um AppAssure Core remoto a partir de qualquer máquina. O utilitário leve inclui os drivers *aavdisk* e *aavstor*, mas não é executado como um serviço. Quando o utilitário é instalado, por padrão, ele é instalado no diretório C:\Program Files\AppRecovery\Local Mount Utility, e um atalho aparece na área de trabalho da máquina.

Embora o utilitário tenha sido projetado para acesso remoto a uma máquina AppAssure Core, também é possível instalar o LMU na mesma máquina de um AppAssure Core. Quando executado em um Core, o aplicativo reconhece e exibe todas as montagens desse Core, incluindo montagens realizadas por meio do AppAssure Core Console. Da mesma forma, as montagens realizadas no LMU também aparecem no console.

Quando está instalado em uma máquina Core, o LMU fornece acesso ao Mailbox Restore, o aplicativo do Dell AppAssure usado para restaurar armazenamentos de dados e itens do Microsoft Exchange. Para obter mais informações sobre o Mailbox Restore, consulte o *Guia do usuário do Mailbox Restore for Microsoft Exchange do Dell AppAssure*.

Baixar o Local Mount Utility

Há duas maneiras baixar o Local Mount Utility. É possível baixar a versão do instalador da Web do software diretamente do AppAssure Core Console, que é prático se você estiver instalando o LMU no Core. Também é possível baixar os arquivos do instalador executável de 32 bits ou de 64 bits para o LMU do Portal de licenças do Dell AppAssure.

Esta seção inclui os seguintes tópicos:

- Baixar o LMU do AppAssure Core Console
- Baixar o LMU do Portal de licenças do Dell AppAssure

Baixar o LMU do AppAssure Core Console

Conclua as seguintes etapas para baixar o Local Mount Utility a partir do AppAssure Core Console.

Para baixar o Local Mount Utility a partir do AppAssure Core Console

1. Na máquina em que você deseja instalar o LMU, acesse o AppAssure Core Console inserindo a URL do console no seu navegador e fazendo login com o seu nome de usuário e senha.
2. No AppAssure Core Console, clique na guia Ferramentas.
3. Na guia Ferramentas, clique em **Downloads.**
4. Em Local Mount Utility, clique no link **Baixar instalador da web**.

5 Na janela Abrindo LocalMountUtility-Web.exe, clique em **Salvar arquivo.**

O arquivo é salvo na pasta local Downloads. Em alguns navegadores, a pasta é aberta automaticamente ou uma mensagem pop-up oferece a opção de executar a instalação.

Baixar o LMU do Portal de licenças do Dell AppAssure

Se você já tiver registrado o software AppAssure Core no Portal de licenças do Dell AppAssure, pode efetuar login no Portal de licenças em https://licenseportal.com e baixar o software LMU para a máquina em que deseja instalá-lo.

NOTA: Para obter mais informações sobre o Portal de licenças do Dell AppAssure, incluindo como obter uma chave de licença ou registrar-se e criar uma conta do Portal de licenças, consulte o *Guia do usuário do portal de licenças do Dell AppAssure*.

Conclua as etapas a seguir para baixar o Local Mount Utility e instalá-lo a partir do Portal de Licenças do Dell AppAssure.

Para baixar o Local Mount Utility a partir do Portal de Licenças do Dell AppAssure

1 Na máquina em que você deseja instalar o LMU, efetue login no Portal de licenças do Dell AppAssure em https://licenseportal.com.

2 Acesse a área **Downloads**.

3 Role para baixo na lista de Aplicativos baseados no Windows. Na seção do Local Mount Utility, com base na arquitetura da máquina em que você está instalando o utilitário (sistemas de 64 bits ou de 32 bits na arquitetura de x86), clique em **Baixar.**

4 Salve o instalador executável no local adequado (por exemplo, Downloads).

Instalar o Local Mount Utility

O Local Mount Utility pode ser instalado usando o instalador da Web ou um arquivo de instalação executável específico da arquitetura da máquina em que ele está sendo instalado. O processo é o mesmo, não importa o instalador usado. Siga o procedimento abaixo para instalar o Local Mount Utility.

Para instalar o Local Mount Utility

1 Na máquina em que você deseja instalar o LMU, localize o arquivo de instalação executável.

Se tiver baixado o instalador a partir do Core, o arquivo de instalação usa o instalador da Web, que se chama LocalMountUtility-Web.exe. Se você tiver baixado do Portal de licenças, o nome do instalador inclui a arquitetura do seu sistema operacional, por exemplo, LocalMountUtility-X32.exe ou LocalMountUtility-X64.exe.

2 Ative do programa instalador usando um dos métodos a seguir.

- Na pasta Downloads, clique com o botão direito no arquivo executável e clique em **Abrir**.
- Ou, se o navegador da Web abrir uma mensagem após o download com a opção de executar o arquivo executável, clique em **Executar**.

Dependendo da configuração da sua máquina, a janela Controle da Conta do Usuário ou a janela Abrir Arquivo - Aviso de Segurança pode aparecer.

3 Se a janela Controle da Conta do Usuário ou a janela Abrir Arquivo - Aviso de Segurança aparecer, clique em **Sim** ou **Executar** para permitir que o programa faça alterações na máquina.

4 Na caixa de diálogo Instalação, no campo de idioma, selecione o idioma adequado e clique em **OK**.

O instalador prepara a instalação.

5 Escolha uma das seguintes opções:

- Se a máquina tiver uma versão antiga do software AppAssure Local Mount Utility instalada, uma mensagem será exibida perguntando se você deseja fazer a atualização para a versão atual.

  a Clique em **Sim.**

  O AppAssure Local Mount Utility Installation Wizard é aberto e a página de progresso do assistente aparece. O aplicativo é transferido por download para a pasta de destino. O progresso é exibido na barra de progresso. Ao terminar, o assistente avança automaticamente para a página Concluído.

  b Vá para Etapa 10.

- Se essa for a primeira vez que o software AppAssure LMU está sendo instalado na máquina, siga para Etapa 6.

6 Na página Bem-Vindo do Assistente de Instalação do AppAssure Local Mount Utility, clique em **Avançar** para ir à página Acordo de Licença.

7 Na página Acordo de licença, selecione **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.

8 Na página Pré-requisito, instale os pré-requisitos necessários e, em seguida, clique em **Avançar**.

9 Na página Opções de instalação, realize as tarefas a seguir:

a Selecione uma pasta de destino para o LMU clicando no **ícone da pasta**.

> **NOTA:** A pasta de destino padrão é
>
> `C:\Program Files\AppRecovery\LocalMountUtility`.

b Opcionalmente, para instalar também o Mailbox Restore, selecione **Mailbox Restore**.

> **CUIDADO: Se você já instalou o Mailbox Restore nesta máquina com sua instalação do AppAssure Core, desmarque essa opção para que você não o instale de novo.**

c Selecione se você deseja (ou não) **permitir que o Local Mount Utility envie automaticamente informações de diagnóstico e uso para a Dell.**

d Clique em **Instalar**.

A página Progresso do assistente aparece, e o aplicativo é transferido por download para a pasta de destino. O progresso é exibido na barra de progresso. Ao terminar, o assistente avança automaticamente para a página Concluído.

10 Na página Concluído, clique em **Concluir** para fechar o assistente.

Usando o Local Mount Utility

O LMU permite montar, explorar e desmontar os pontos de recuperação de qualquer Core adicionado ao utilitário. Não há um limite para o número de Cores que podem ser adicionados. Para obter mais informações sobre o uso do LMU, consulte os seguintes procedimentos:

- Adicionar uma máquina Core ao Local Mount Utility
- Montar um ponto de recuperação usando o Local Mount Utility
- Usar o Local Mount Utility para explorar um ponto de recuperação montado
- Usar o Local Mount Utility para desmontar um ponto de recuperação

Adicionar uma máquina Core ao Local Mount Utility

Para montar um ponto de recuperação, é necessário adicionar uma máquina Core ao LMU. Não há limite ao número de Cores que podem ser adicionados.

Execute o procedimento a seguir para configurar o LMU adicionando um core.

Para adicionar um core ao Local Mount Utility

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.

2 Se a janela Controle da conta do usuário aparecer, clique em **Sim** para permitir que o programa faça alterações na máquina.

3 No canto superior esquerdo da janela AppAssure Local Mount Utility, clique em **Adicionar core**.

4 Na caixa de diálogo Adicionar Core, insira as credenciais solicitadas, descritas na tabela a seguir.

Tabela 133. Credenciais do AppAssure Core

Opção	Descrição
Nome do host	O nome do Core a partir do qual você deseja montar pontos de recuperação. NOTA: Se você estiver instalando o LMU em um core, o LMU adicionará a máquina localhost automaticamente.
Porta	O número da porta usada para se comunicar com o Core. O número de porta padrão é 8006.
Use minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core forem iguais às credenciais do Windows.
Use credenciais específicas	Selecione essa opção se as credenciais que você usa para acessar o Core forem diferentes das credenciais do Windows.
Nome de usuário	O nome de usuário utilizado para acessar a máquina do Core. NOTA: Essa opção fica disponível apenas se você opta por usar credenciais específicas.
Senha	A senha usada para acessar a máquina do Core. NOTA: Essa opção fica disponível apenas se você opta por usar credenciais específicas.

5 Clique em **Conectar.**

6 Se você estiver adicionando vários cores, repita as etapas de Etapa 3 a Etapa 5 conforme a necessidade.

Montar um ponto de recuperação usando o Local Mount Utility

Antes de montar um ponto de recuperação, o Local Mount Utility (LMU) precisa se conectar ao Core no qual o ponto de recuperação está armazenado. Como descrito no procedimento Adicionar uma máquina Core ao Local Mount Utility, o número de cores que podem ser adicionados ao LMU é ilimitado; no entanto, o aplicativo pode ser conectado somente a um core por vez. Por exemplo, se você montar um ponto de recuperação de uma máquina protegida por um Core e depois montar um ponto de recuperação de outra máquina protegida por um Core diferente, o LMU automaticamente se desconectará do primeiro Core para estabelecer uma conexão com o segundo Core.

Realize o procedimento a seguir para montar um ponto de recuperação em um core remoto usando o LMU.

Para montar um ponto de recuperação usando o Local Mount Utility

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.

2 Na janela principal do AppAssure Local Mount Utility, expanda o Core na árvore de navegação para revelar as máquinas protegidas.

3 Na árvore de navegação, selecione a máquina protegida a partir da qual deseja montar um ponto de recuperação.

Os pontos de recuperação aparecem no frame principal.

4 Expanda o ponto de recuperação que você deseja montar para revelar volumes de disco individuais ou bancos de dados.

5 Clique com o botão direito no ponto de recuperação que você deseja montar e selecione uma das opções a seguir:

- Montagem
- Montagem gravável
- Montagem com gravações anteriores
- Montagem avançada

a Se você tiver selecionado Montagem avançada, na janela Montagem avançada, execute as opções descritas na tabela a seguir.

Tabela 134. Opções de Montagem avançada

Opção	Descrição
Caminho de ponto de montagem	Clique no botão **Procurar** para selecionar um caminho para os pontos de recuperação diferente do caminho padrão do ponto de montagem.
Tipo de montagem	Selecione uma das opções a seguir: • Montagem de apenas leitura • Montagem gravável • Montagem de apenas leitura com gravações anteriores

b Clique em **Montagem**.

O LMU abre automaticamente a pasta que contém o ponto de recuperação montado.

NOTA: Se for selecionado um ponto de recuperação que já está montado, a caixa de diálogo Montando perguntará se deve desmontar o ponto de recuperação.

Usar o Local Mount Utility para explorar um ponto de recuperação montado

Execute o procedimento a seguir para explorar um ponto de recuperação que permaneceu montado desde uma sessão anterior.

NOTA: Esse procedimento não é necessário se você estiver explorando um ponto de recuperação imediatamente após a montagem dele, visto que a pasta que contém o ponto de recuperação é aberta automaticamente após a conclusão do procedimento de montagem.

Para explorar um ponto de recuperação montado usando o Local Mount Utility

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.

2 Na tela principal do Local Mount Recovery, clique em **Montagens ativas.**

A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.

3 Clique em **Explorar** ao lado do ponto de recuperação a partir do qual deseja fazer a recuperação a fim de abrir a pasta de volumes deduplicados.

Usar o Local Mount Utility para desmontar um ponto de recuperação

Execute o procedimento a seguir para desmontar um ponto de recuperação em um core remoto usando o LMU.

Para desmontar um ponto de recuperação usando o Local Mount Utility

1. Na máquina em que o LMU está instalado, clique duas vezes no ícone do Local Mount Utility no desktop para iniciar o programa.
2. Na tela principal do Local Mount Recovery, clique em **Montagens ativas.**

   A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.
3. Realize um dos procedimentos a seguir:
   - Para desmontar um ponto de recuperação, selecione um ponto que deseja desmontar e, em seguida, clique em **Desmontar**.
   - Para desmontar todos os pontos de recuperação montados, clique em **Desmontar tudo** e, em seguida, clique em **Sim** na caixa de diálogo Desmontar tudo para confirmar.
4. Para fechar a janela Montagens ativas, clique no X no canto superior direito.
5. Para minimizar o aplicativo LMU, clique no X no canto superior direito da janela do Local Mount Utility.
6. Para fechar o aplicativo LMU, clique com o botão direito do mouse no AppAssure ícone do Local Mount Utility no menu da bandeja do LMU e selecione **Sair**.

Usar o menu de bandeja do Local Mount Utility

O menu da bandeja do LMU está localizado na barra de tarefas da área de trabalho. Clique com o botão direito do mouse no ícone para revelar as opções descritas na tabela a seguir:

Tabela 135. Opções do menu de bandeja

Opção	Descrição
Buscar pontos de recuperação	Abre a janela principal do LMU.
Montagens ativas	Abre a caixa de diálogo Montagens ativas no alto da janela principal do LMU.
Opções	Abre a caixa de diálogo Opções no alto da janela principal do LMU. Na caixa de diálogo Opções, você pode alterar o diretório do ponto de montagem Padrão e as credenciais do Core padrão para a interface de usuário do LMU.
Sobre	Revela as informações de aplicação de licença do Local Mount Utility.
Sair	Fecha o aplicativo LMU. **NOTA:** Ao clicar no X no canto superior da janela principal do LMU, o aplicativo é minimizado para a bandeja, em vez de ser fechado.

Usar opções do AppAssure Core e de máquina protegida

Clicando com o botão direito do mouse no AppAssure Core ou em uma máquina protegida na tela principal do LMU, você pode acessar certas opções, descritas nos tópicos a seguir:

- Acessar opções de localhost
- Acesso às opções de Core remotoAcessar opções de máquina protegida

Acessar opções de localhost

Conclua as etapas deste procedimento para acessar as opções de localhost.

Para acessar as opções de localhost

- Clique com o botão direito do mouse no AppAssure Core ou em uma máquina protegida e depois clique em **Reconectar ao Core**.

  As informações do Core são atualizadas com, por exemplo, as máquinas protegidas adicionadas recentemente.

Acesso às opções de Core remoto

Execute as etapas deste procedimento para acessar as opções de core remoto.

Para acessar as opções de core remoto

- Clique com o botão direito do mouse no AppAssure Core ou na máquina protegida e selecione uma das opções de Core remoto, descritas na tabela a seguir.

  Tabela 136. Opções de Core remoto

Opção	Descrição
Reconectar ao core	Atualiza as informações do Core, como as máquinas protegidas adicionadas recentemente.
Remover core	Exclui o Core do Local Mount Utility.
Editar core	Abre a janela Editar Core, onde é possível alterar o nome de host, a porta e as credenciais.

Acessar opções de máquina protegida

Conclua as etapas deste procedimento para acessar as opções de máquina protegida.

Para acessar as opções de máquina protegida

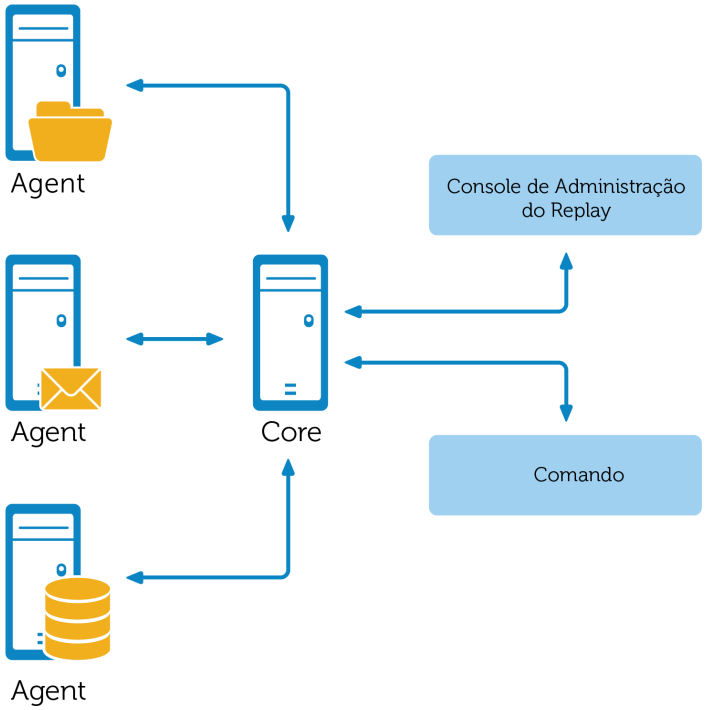
- Clique com o botão direito do mouse na máquina protegida do AppAssure e depois clique em **Atualizar pontos de recuperação**.

  A lista de pontos de recuperação da máquina protegida selecionada é atualizada.

Noções básicas do utilitário AppAssure Command Line Management

O produto de recuperação após desastres e cópia de segurança AppAssure consiste em vários componentes de software, incluindo AppAssure Agent, AppAssure Core e o utilitário AppAssure Command Line Management. O AppAssure Agent é responsável por snapshots de volume e pela rápida transferência de dados para o Core. O AppAssure Core, por sua vez, armazena os snapshots junto com uma vasta gama de recursos aprimorados, como bare metal restore (BMR) para hardwares diferentes, Standby virtual e replicação, entre outros. Para fornecer acesso a terceiros para o gerenciamento da funcionalidade do sistema, o AppAssure inclui uma ferramenta de linha de comando chamada AppAssure Command Line Management (aacmd). Ela permite utilizar scripts para as funções de gerenciamento do AppAssure Core.

Figura 9.



O AppAssure Command Line Management é uma ferramenta que suporta linha de comando do Windows que permite aos usuários interagirem com o AppAssure servidor do Core. Ele oferece algumas das mesmas funcionalidades fornecidas pelo elemento da GUI no AppAssure Core Console. Por exemplo, a ferramenta AppAssure Command Line Management pode montar pontos de recuperação ou forçar um snapshot.

O utilitário AppAssure Command Line Management é incorporado em todas as instalações do AppAssure Core. Para abrir o utilitário AppAssure Command Line Management, vá até o local das pastas instaladas do AppAssure e clique duas vezes no arquivo `aacmd.exe`.

No Modo de linha de comando, sinalizadores de ação podem ser passados para a ferramenta AppAssure Command Line Management por meio de uma seleção de qualificadores e opções do comando para realizar funções limitadas de gerenciamento.

Esta seção inclui os seguintes tópicos:

- Comandos
- Localização

Comandos

Esta seção descreve os comandos e as opções disponíveis para a ferramenta AppAssure Command Line Management. Os seguintes comandos estão disponíveis para uso:

- Archive
- CancelActiveJobs
- CreateRepository
- Dismount
- Force
- ForceAttach
- ForceChecksum
- ForceLogTruncation
- ForceMount
- ForceReplication
- ForceRollup
- Help
- List
- Mount
- Pause [snapshot | vmexport | replication]
- Protect
- ProtectCluster
- RemoveAgent
- RemovePoints
- RestoreArchive
- Resume [snapshot | vmexport | replication]
- StartExport
- UpdateRepository
- Version

Archive

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do AppAssure suporta retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou no local de rede especificando o parâmetro `-path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
/archive -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address] -path [location] -startdate [time string] -
enddate [time string] -archiveusername [name] -archivepassword [password] -comment
[text]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Archive`:

Tabela 137. Opções do comando Archive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Arquivar todos os pontos de recuperação para todas as máquinas protegidas no Core.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem arquivados. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por espaços.
`-path`	O caminho é colocado onde estão os dados arquivados; por exemplo: d:\work\archive ou caminho de rede \\NomedoServidor\Compartilhamento.
`-startdate`	Iniciar a data selecionando pontos de recuperação pela data de criação. Os valores devem ser informados entre aspas duplas.
`-enddate`	Opcional. Data final para selecionar os pontos de recuperação pela data de criação. Os valores devem ser informados entre aspas duplas. O sistema de tempo atual é usado por padrão.
`-archiveusername`	Opcional. Nome de usuário da máquina remota. Necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Senha para a máquina remota. Necessário para caminho de rede apenas.
`-comment`	Opcional. O texto de comentário deve ser informado entre aspas duplas; por exemplo: `-comment "comentário vem aqui..."`.

Exemplos:

Arquivar todos os pontos de recuperação com datas de criação de 04/30/2012 14h55min para todas as máquinas no Core:

```
>aacmd /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
d:\work\archive -startdate "04/30/2012 02:55 PM" -all
```

Arquivar pontos de recuperação que entram num intervalo de datas para duas máquinas protegidas:

```
>aacmd /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate
"04/30/2012 14:55" -enddate "05/31/2012 11:00"
```

CancelActiveJobs

Use o comando `CancelActiveJobs` para cancelar a execução de todos os trabalhos em andamento de um tipo específico, como transferência e replicação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type filter]]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `CancelActiveJobs`:

Tabela 138. Opções do comando CancelActiveJobs

Opção	Descrição
`-?`	Exibir ajuda sobre o comando.
`-core`	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, são usadas as credenciais para o usuário registrado.
`-protectedserver`	Determinar a máquina protegida na qual os trabalhos serão cancelados.
`-all`	Selecionar e cancelar eventos de tipo específico em todos os servidores protegidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de trabalho. Os valores disponíveis são: • 'transfer' (transferência de dados) • 'repository' (manutenção de repositório) • 'replication' (replicações locais e remotas) • 'backup' (cópia de segurança e restaurar) • 'bootcdbuilder' (criar CDs de inicialização) • 'diagnostics' (logs para fazer upload) • 'exchange' (verificação de arquivos do Exchange Server) • 'export' (exportação do ponto de recuperação) • 'pushinstall' (implementar agentes) • 'rollback' (reversão de ponto de recuperação) • 'rollup' (rollups de ponto de recuperação) • 'sqlattach' (verificações da capacidade de anexação do agente) • 'mount' (montar repositório) Como padrão, todos os trabalhos do tipo especificado são cancelados.

Exemplo:

Cancelar todos os trabalhos de transferência no Core 10.10.10.10:

```
>aacmd /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -jobtype transfer
```

CreateRepository

Use o comando `CreateRepository` para criar um novo repositório numa máquina local, assim como numa localização partilhada.

Forma de uso

A forma de uso do comando, enquanto cria um repositório num espaço local, é a seguinte:

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

A forma de uso do comando, enquanto cria um repositório num local partilhado, é a seguinte:

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time\ -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `CreateRepository`:

Tabela 139. Opções do comando CreateRepository

Opção	Descrição
`-?`	Exibir ajuda sobre o comando.
`-core`	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Determinar a máquina protegida na qual os trabalhos serão cancelados.
`-all`	Selecionar e cancelar eventos de tipo específico em todos os servidores protegidos.
`-name`	Nome do repositório.
`-size`	Tamanho do local de armazenamento do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb, e Pb.
`-datapath`	Para espaço local, somente. Determinar o caminho de dados do local de armazenamento do repositório.
`-metadatapath`	Para espaço local, somente. Determinar o caminho de metadados do local de armazenamento do repositório.
`-uncpath`	Para local partilhado, somente. Determinar os caminhos de dados e metadados do local de armazenamento do repositório.
`-shareusername`	Para local partilhado, somente. Determina o nome de usuário para o local de compartilhamento.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.

Tabela 139. Opções do comando CreateRepository

Opção	Descrição
-comment	Opcional. Descrição do repositório.
-concurrentoperations	Opcional. O número máximo de operações pode estar pendente de uma só vez. Valor pelo padrão: 64.

Exemplos:

Criar repositório em um espaço local:

```
>aacmd /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd
```

Criar repositório em um local partilhado:

```
>aacmd /createrepository -name "Repository 1" -size 200 Gb -uncpath
\\share\repository -shareusername login -sharepassword pass123 -comment "First
repository." -concurrentoperations 8 -core 10.10.10.10:8006 -user administrator
-password 23WE@#$sdd
```

Dismount

Use o comando Dismount para desmontar um ponto de recuperação especificado pelo comando Path, desmontar pontos para o agente selecionado pelo parâmetro -protectedserver, ou desmontar todos os pontos de recuperação (-all).

Forma de uso

A forma de uso do comando é a seguinte:

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all |
-protectedserver [name | IP address] | -path [location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Dismount:

Tabela 140. Opções do comando Dismount

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-all	Desmontar todos os pontos de recuperação montados.
-protectedserver	Desmontar todos os pontos de recuperação montados para o agente atual.
-path	Desmontar ponto de montagem selecionado.

Exemplo:

Desmontar um ponto de recuperação que foi montado na pasta c:\mountedrecoverypoint:

```
>aacmd /dismount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
c:\mountedRecoveryPoint
```

Force

O comando `Force` força um snapshot do servidor protegido especificado. Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]]
-core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Force`:

Tabela 141. Opções do comando Force

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-force`	Opcional. Tipo de snapshot para criar. Valores disponíveis: 'snapshot' (snapshot incremental) e 'base' (imagem base do snapshot). Por padrão, um snapshot incremental é realizado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Forçar snapshots para todas as máquinas no Core.
`-protectedserver`	Forçar um snapshot numa máquina protegida específica.

Exemplo:

Forçar snapshots para todas as máquinas no Core:

```
>aacmd /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
all
```

ForceAttach

O comando `ForceAttach` permite que você force uma verificação de capacidade de anexação do banco de dados SQL. Ao forçar uma verificação de capacidade de anexação, a transferência começa imediatamente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forceattach -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ForceAttach`:

Tabela 142. Opções do comando ForceAttach

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Opcional. Máquina protegida na qual a verificação de capacidade de anexação será realizada.
`-rpn`	Opcional. O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
`-time`	Opcional. Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar verificações de capacidade de anexação para pontos de recuperação com números 5 e 7:

```
>aacmd /forceattach -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

O comando `ForceChecksum` permite forçar uma verificação de integridade de bancos de dados de mensagem do Exchange (MDBs) presentes no ponto ou pontos de recuperação especificados. Quando você força uma verificação de soma de verificação, o comando inicia imediatamente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forcechecksum -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ForceChecksum`:

Tabela 143. Opções do comando ForceChecksum

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Opcional. Máquina protegida na qual a verificação de soma de verificação será realizada.
`-rpn`	Opcional. O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
`-time`	Opcional. Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar uma verificação de soma de verificação nos pontos de recuperação com números 5 e 7:

```
>aacmd /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

Forçar truncamento de log permite que você execute este trabalho de uma vez, sob demanda. Ele imediatamente trunca os logs para o agente SQL Server da máquina especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ForceLogTruncation`:

Tabela 144. Opções do comando ForceLogTruncation

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Opcional. Máquina protegida na qual o truncamento de arquivo log será realizado.

Exemplo:

Forçar truncamento de log para um servidor protegido:

```
>aacmd /forcelogtruncation -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.20.20
```

ForceMount

Usar o comando `ForceMount` para conduzir uma verificação única de capacidade de montagem do ponto de recuperação. Isso determina se o ponto de recuperação especificado ou os pontos de recuperação podem ou não ser montados e usados para restaurar dados da cópia de segurança. Você deve listar um ou mais pontos de recuperação específicos sobre os quais conduzir a verificação ou um intervalo de tempo durante o qual foram criados os pontos de recuperação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forcemount -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ForceMount`:

Tabela 145. Opções do comando ForceMount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Tabela 145. Opções do comando ForceMount

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-protectedserver	Opcional. Máquina protegida na qual o truncamento de arquivo log será realizado.
-rpn	Opcional. O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
-time	Opcional. Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar verificações de montabilidade para pontos de recuperação com números 5 e 7:

```
>aacmd /forcemount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication

Usar o comando `ForceReplication` para forçar uma transferência única de dados replicados do core de origem para o core de destino. Você pode replicar um servidores protegido específico ou replicar todos os servidores protegidos. Os servidores protegidos devem ser imediatamente configurados para replicação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -
targetcore [host name] -all | -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ForceReplication`:

Tabela 146. Opções do comando ForceReplication

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
-targetcore	O nome do host do core de destino no qual a replicação deverá ser forçada.

Tabela 146. Opções do comando ForceReplication

Opção	Descrição
-protectedserver	Opcional. Máquina protegida na qual o truncamento de arquivo log será realizado.
-all	Forçar replicação para todas as máquinas sendo replicadas no core de destino.

Exemplo:

Forçar replicação para um servidor protegido num core de destino específico:

```
>aacmd /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

Usar o comando ForceRollup para forçar o rollup dos pontos de recuperação de uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando ForceRollup:

Tabela 147. Opções do comando ForceRollup

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
-protectedserver	Opcional. Máquina protegida na qual o truncamento de arquivo log será realizado.

Exemplo:

Forçar rollup para o agente 10.10.10.1 no Core:

```
>aacmd /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.1
```

Help

O comando Help exibe uma lista de comandos disponíveis e suas definições. Também fornece detalhes dos direitos autorais e da versão.

Forma de uso

A forma de uso do comando é a seguinte:

```
/help
```

Exemplo:

Solicitar o comando linha de ajuda:

```
>aacmd /help
```

List

O comando `List` retorna informações sobre todos os pontos de recuperação, os trabalhos ativos, os trabalhos concluídos, trabalhos com falha, pontos de recuperação inválidos (com falha), pontos de recuperação válidos (aprovados), montagens, servidores protegidos, volumes, servidores virtualizados, volumes desprotegidos, clusters, grupos de proteção, bancos de dados SQL, bancos de dados do Exchange, servidores replicados e repositórios para o agente especificado ou lista de servidores atualmente protegidos pelo Core. Os registros mais recentes retornados por padrão: Você pode listar todos os registros ou quantos registros serão exibidos usando um parâmetro numérico. Esse parâmetro deve conter a letra ***l*** para os pontos de recuperação mais recentes e ***f*** para o primeiro ponto de recuperação. Cada ponto de recuperação tem seu próprio número, que o administrador pode usar para a montagem.

Forma de uso

A forma de uso do comando é a seguinte:

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs |
completed jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters |
protectiongroups | sqldatabases | exchangemailstores | replicatedservers |
repositories] -protectedserver [name | IP address] -core [host name] -user [user
name] -password [password] -number [all | l<number> | f<number> | <number>] -jobtype
```

Opções do comando

A seguinte tabela descreve as opções disponíveis para o comando `List`:

Tabela 148. Opções do comando List

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-list`	Selecione uma das opções a seguir: • todos os pontos de recuperação (‘rps’) • pontos de recuperação válidos (‘passed’) • pontos de recuperação inválidos (‘failed’) • montagens (‘mounts’) • volumes protegidos ('volumes') • volumes desprotegidos ('unprotectedvolumes') • máquinas protegidas ('protectedservers') • trabalhos ativos ('activejobs') • trabalhos com falha ('failedjobs') • trabalhos concluídos ('completedjobs') • servidores virtualizados ('virtualizedservers') • clusters ('clusters') • grupos de proteção ('protectiongroups') • Bancos de dados do SQL Server ('sqldatabases') • Bancos de dados do MS Exchange ('exchangemailstores') • servidores replicados ('replicatedservers') • repositórios (‘repositories’)
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Para exibição de trabalhos, somente. Exibir todos os eventos de um tipo específico (ativo/com falha/concluído) no servidor do core.
`-protectedserver`	Máquina protegida com pontos de recuperação para exibir.

Tabela 148. Opções do comando List

Opção	Descrição
-number	Opcional. Número de itens de dados para exibir. Use os especificadores a seguir: 'rps', 'activejobs', 'completedjobs', 'failedjobs'. Os valores disponíveis são: • all (buscar todos os itens de dados) • l[number] ou [number] (busca os ## itens de dados do topo) • f[number] (busca os primeiros ## itens de dados) Somente tem efeito quando exibir pontos de recuperação e trabalhos.
-jobtype	Opcional. Filtrar saída pelo tipo de trabalho. Valores disponíveis incluem: • 'transfer' (transferência de dados) • 'repository' (manutenção de repositório) • 'replication' (replicações locais e remotas) • 'backup' (cópia de segurança e restaurar) • 'bootcdbuilder' (criar CDs de inicialização) • 'diagnostics' (logs para fazer upload) • 'exchange' (verificação de arquivos do Exchange Server) • 'export' (exportar o ponto de recuperação) • 'pushinstall' (implementar agentes) • 'rollback' (reversão de ponto de recuperação) • 'rollup' (rollups de máquina protegida) • 'sqlattach' (verificações da capacidade de anexação do agente) • 'mount' (montar repositório)

Exemplos:

Listar os 30 mais recentes pontos de recuperação:

```
>aacmd /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.5.22 -number l30
```

Ver todos os trabalhos com falha de transferência de dados realizados por uma máquina protegida:

```
>aacmd /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.5.22 -number all -jobtype transfer
```

Mount

O comando Mount monta um snapshot de uma ou mais unidades. Você pode especificar se a montagem deve ler, escrever ou ser apenas leitura com gravações anteriores. A seleção padrão é apenas leitura.

Forma de uso

A forma de uso do comando é a seguinte:

```
/mount -core [host name] -user [user name] -password [password] -protectedserver
[name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives
[drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -
time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Mount`:

Tabela 149. Opções do comando Mount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida com ponto ou pontos de recuperação a serem montados.
`-mounttype`	Opcional. Especifica um modo de montagem. Valores disponíveis são `'read' (apenas leitura)`, `'readOnlyWithPreviousWrites'` (apenas leitura com gravações anteriores), `'write'` (gravável). O modo padrão é `read-only`.
`-volumes`	Opcional. Lista de nomes de volumes a serem montados. Se não especificado, todos os volumes serão montados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo: "c:" "d:". Não use barras nos nomes dos volumes.
`-path`	Caminho para uma pasta no core servidor na qual o ponto de recuperação deve ser montado. Se esse não existir, uma pasta será automaticamente criada.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação para montagem (use o comando `/list rps` para obter os números). Para especificar muitos pontos de recuperação com um único comando, usar vários números separados por espaços. Neste caso, os dados de cada ponto de recuperação serão armazenados em uma pasta child separada. Nota: se nenhuma opção -time ou -rpn for especificada, então o ponto de recuperação mais recente que passou com êxito na verificação de integridade será montado.
`-time`	Opcional. Determinar ponto ou pontos de recuperação a serem selecionados para montagem. Valores disponíveis incluem: 'latest', 'passed', tempo exato no formato “mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC. Se nenhuma opção -time ou -rpn for especificada, então, o ponto de recuperação mais recente que passou com êxito na verificação de integridade será montado.
`-localdrive`	Opcional. Realizar montagem no disco de usuário no PC local.

Exemplos:

Montar os mais recentes pontos de recuperação contendo volumes “c:\” e “d:\” no modo apenas leitura:

```
>aacmd /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes
"c:" "d:"
```

Montar pontos de recuperação com números 2 e 7:

```
>aacmd /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

Pause [snapshot | vmexport | replication]

Um administrador pode pausar snapshots, exportar para máquinas virtuais ou replicar para um Core. O comando `Pause` aceita três parâmetros: `snapshot`, `vmexport` e `replication`. Somente um parâmetro pode ser especificado. Um snapshot pode ser pausado até um determinado momento, caso um parâmetro de tempo seja especificado.

Um usuário pode pausar uma replicação de três maneiras:

- Em um Core de origem para todos os Agents (`-[outgoing]`).

  O administrador precisa especificar o nome da máquina remota com o emparelhamento de replicação de saída para pausar a replicação de saída no core de origem:

  ```
  >aacmd /Pause replication /o 10.10.12.10
  ```

- No Core de origem para um único Agent (`-protectedserver`):

  ```
  >aacmd /Pause replication /protectedserver 10.10.12.97
  ```

- No Core de destino (`-incoming`).

  Se o Core local é um Core de destino, o administrador pode pausar a replicação especificando o core de origem usando o parâmetro incoming:

  ```
  >aacmd /Pause replication /i 10.10.12.25
  ```

Forma de uso

A forma de uso do comando é a seguinte:

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name]
-password [password] -all | -protectedserver [name | IP address] -incoming [host
name] | outgoing [host name] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Pause`:

Tabela 150. Opções do comando Pause

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-pause`	[`snapshots`], [`replication`] ou [`vmexport`].
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Pausar todos os agentes do Core selecionado.
`-protectedserver`	Pausar o servidor protegido atual.
`-incoming`	Nome do host do core remoto que replica para o core da máquina.
`-outgoing`	Nome do host do core de destino remoto no qual os dados são replicados.
`-time`	O horário no formato “Dia-Horas-Minutos” em que os snapshots serão retomados (somente para pausas de snapshots).

Exemplos:

Pausar a criação de snapshots para um servidor protegido específico:

```
>aacmd /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.10.4
```

Pausar a criação de snapshots para uma máquina protegida e retomar depois de três dias, 20 horas e 50 minutos:

```
>aacmd /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.10.4 -time 3-20-50
```

Pausar exportação para máquina virtual para cada máquina protegida no core:

```
>aacmd /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$sdd -
all
```

Pausar replicação de saída no core de uma máquina protegida específica:

```
>aacmd /pause replication –core 10.10.10.10 -user administrator -password 23WE@#$sdd
–protectedserver 10.10.1.76
```

Pausar replicação de saída para todas as máquinas protegidas no core de destino:

```
>aacmd /pause replication -core 10.10.10.10 -user administrator -password -
23WE@#$sdd –outgoing 10.10.1.63
```

Pausar replicação de entrada para todas as máquinas do core de destino:

```
>aacmd /pause replication –core 10.10.10.10 -user administrator -password 23WE@#$sdd
–incoming 10.10.1.82
```

Protect

O comando `Protect` adiciona um servidor sob proteção por um Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/protect -core [host name] -user [user name] -password [password] -repository [name]
-agentname [name | IP address] -agentusername [user name] -agentpassword [password]
-agentport [port] -volumes [volume names]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Protect`:

Tabela 151. Opções do comando Protect

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Tabela 151. Opções do comando Protect

Opção	Descrição
-repository	Nome do repositório do Core onde os dados da máquina protegida deverão ser armazenados. O nome deve ser informado entre aspas duplas.
-agentname	O nome ou endereço IP do servidor que deseja proteger.
-agentusername	Nome de usuário do servidor a ser protegido.
-agentpassword	Senha do servidor a ser protegido.
-agentport	Número da porta do servidor protegido.
-volumes	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes; por exemplo: “c:” “d:”.

Exemplo:

Proteger volumes específicos de um servidor com o Core:

```
>aacmd /protect -core 10.10.10.10 -username administrator -password 23WE@#$sdd -repository "Repository 1" -agentname 10.10.9.120 -agentport 5002 -agentusername administrator agentpassword 12345 -volumes "c:" "d:"
```

ProtectCluster

O comando `ProtectCluster` adiciona um cluster sob proteção por um Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `ProtectCluster`:

Tabela 152. Opções do comando ProtectCluster

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-repository	Nome do repositório do Core onde os dados da máquina protegida deverão ser armazenados. O nome deve ser informado entre aspas duplas.
-clustername	O nome ou endereço IP do cluster que deseja proteger.

Tabela 152. Opções do comando ProtectCluster

Opção	Descrição
-clusterusername	Nome de usuário para o cluster a ser protegido.
-clusterpassword	Senha do cluster a ser protegido.
-clusterport	Número da porta do cluster do servidor protegido.
-clustervolumes	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes; por exemplo: “c:” “d:”.
-clusternodes	Lista dos nós de cluster e os volumes que você deseja proteger em cada nó.

Exemplo:

Proteger volumes específicos de um cluster do servidor com o Core:

```
>aacmd /protectcluster -core 10.10.10.10 -username administrator -password
23WE@#$sdd -repository “Repository 1” -clustername 10.10.8.150 -clusterport 8006 -
clusterusername clusterAdmin clusterpassword password -volumes
“C:\ClusterStorage\Volume1” -clusternodes nodeName 10.10.8.150 volumes “c:” nodeName
10.10.8.151 volumes “c:”
```

RemoveAgent

O comando RemoveAgent permite remover uma máquina protegida da proteção de um Core e, como opção, excluir os pontos de recuperação da máquina removida. Se você não excluir os pontos de recuperação, o AppAssure irá retê-los e rotulá-los como uma máquina apenas de pontos de recuperação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removeagent -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -deleterecoverypoints
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando RemoveAgent:

Tabela 153. Opções do comando RemoveAgent

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-protectedserver	O nome ou endereço IP do servidor a ser removido da proteção.
-deleterecoverypoints	Opcional. Exclui todos os pontos de recuperação da máquina a ser removida.

Exemplo:

Remover uma máquina da proteção e excluir os pontos de recuperação associados:

```
>aacmd /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemovePoints

O comando `RemovePoints` permite excluir pontos de recuperação específicos de uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removepoints -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `RemovePoints`:

Tabela 154. Opções do comando RemovePoints

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou endereço IP do servidor cujos pontos de recuperação você deseja excluir
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser excluído (use o comando `/list rps` para obter os números). Especifique vários números separados por espaço para excluir múltiplos pontos de recuperação com um único comando.
`-time`	Opcional. Determina quais pontos de recuperação serão excluídos até o momento da criação. Especifique o tempo exato no formato "mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembre-se de especificar os valores de data e hora do fuso horário definido no seu PC.

Exemplo:

Excluir os pontos de recuperação com números 5 e 7:

```
>aacmd /removepoints -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

RestoreArchive

Este comando restaura um arquivo a partir de um arquivo local ou partes e coloca os dados restaurados em um repositório específico.

Forma de uso

A forma de uso do comando é a seguinte:

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword [password] -path [location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `RestoreArchive`:

Tabela 155. Opções do comando RestoreArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Restaurar dados para todas as máquinas protegidas dos arquivos compactados.
`-protectedserver`	Máquina protegida com pontos de recuperação para restauro. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por espaços.
`-repository`	Nome do repositório do Core onde os pontos de recuperação restaurados deverão ser colocados. O nome deve ser informado entre aspas duplas.
`-archiveusername`	Opcional. Nome de usuário da máquina remota. Necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Senha para a máquina remota. Necessário para caminho de rede apenas.
`-path`	Local dos dados arquivados a serem restaurados; por exemplo: d:\work\archive ou network path \\servidor\compartilhamento.

Exemplos:

Restaurar dados arquivados para todos os servidores protegidos:

```
>aacmd /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -all -repository repository1 -path d:\work\archive
```

Restaurar dados arquivados para os servidores protegidos específicos:

```
>aacmd /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -protectedserver “10.10.20.30” “20.10.10.5” -repository repository1 -path d:\work\archive
```

Resume [snapshot | vmexport | replication]

O administrador pode retomar snapshots, exportar para uma máquina virtual e replicar. Você precisa especificar sua necessidade de retomar com um parâmetro. Os seguintes parâmetros são válidos: `snapshot`, `vmexport` e `replication`. Consulte Pause [snapshot | vmexport | replication] para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name]
-password [password] -all | -protectedserver [name | IP address] -incoming [host
name] | outgoing [host name] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Resume`:

Tabela 156. Opções do comando Resume

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-restore`	[`snapshots`], [`replication`] ou [`vmexport`].
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Retomar todos os agentes do Core selecionado.
`-protectedserver`	Retomar o servidor protegido atual.
`-incoming`	Nome do host do core remoto que replica para o core da máquina.
`-outgoing`	Nome do host do core de destino remoto no qual os dados são replicados.

Exemplos:

Retomar snapshots para os servidores protegidos específicos:

```
>aacmd /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.10.4
```

Retomar exportação para máquina virtual para todas as máquinas protegidas no core:

```
>aacmd /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
all
```

Retomar replicação de saída no core de uma máquina protegida específica:

```
>aacmd /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.1.76
```

Retomar replicação de saída para todas as máquinas protegidas no core de destino:

```
>aacmd /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -outgoing 10.10.1.63
```

Retomar replicação de entrada para todas as máquinas do core de destino:

```
>aacmd /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -incoming 10.10.1.82
```

StartExport

O comando `StartExport` força uma exportação única de dados de sua máquina protegida para um servidor virtual. Você pode exportar para ESXi, VMware Workstation, Hyper-V ou VirtualBox da máquina virtual. Se exportar ESXi, você deve especificar se o disco de aprovisionamento é thick ou thin.

Forma de uso

A forma de uso do comando é a seguinte:

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user
name] -password [password] -protectedserver [name | IP address] -volumes [volume
names] -rpn [recovery point number | numbers] | -time [time string] -vmname [virtual
machine name] -hostname [virtual host name] -hostport [virtual hostport number] -
hostusername [virtual host user name] -hostpassword [virtual host password] [-ram
[total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping
[automatic | manual | withvm] -targetpath [location] -pathusername [user name] -
pathpassword [password] [-uselocalmachine]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `StartExport`:

Tabela 157. Opções do comando StartExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-exporttype`	Realizar exportação de dados do servidor protegido para um servidor ESXi ('esxi'), servidor VMware Workstation ('vm'), servidor Hyper-V ('hyperv') ou servidor VirtualBox ('vb').
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não especificado, todos os volumes serão exportados. Os valores devem ser informados entre aspas duplas e separados por espaços; por exemplo: “c:” “d:”. Não use barras nos nomes dos volumes.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação para exportar (use o comando Get-RecoveryPoints para obter os números). Se nenhuma opção ‘time’ ou ‘rpn’ for especificada, então, o ponto de recuperação mais recente é exportado.
`-time`	Opcional. Determinar ponto ou pontos de recuperação a serem selecionados para exportação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo definidos no seu PC. Nota: se nenhuma opção ‘time’ ou ‘rpn’ for especificada, então, o ponto de recuperação mais recente é exportado.

Tabela 157. Opções do comando StartExport

Opção	Descrição
-vmname	Exportação ESXi/VMware Workstation, somente. Nome do Windows da máquina virtual.
-hostname	Exportação ESXi/Hyper-V, somente. Nome do host do servidor virtual.
-linuxhostname	Exportação VirtualBox, somente. Nome do host do servidor virtual.
-hostport	Exportação ESXi/Hyper-V, somente. Número da porta do servidor virtual.
-hostusername	Exportação ESXi/Hyper-V, somente. Nome de usuário do host de servidor virtual.
-hostpassword	Exportação ESXi/Hyper-V, somente. Senha para o host do servidor virtual.
-ram	Exportação ESXi/Hyper-V, somente. Alocar uma quantidade específica de RAM no servidor virtual.
-usesourceram	Exportação ESXi/Hyper-V, somente. Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto tiver na máquina de origem protegida.
-diskprovisioning	Exportação ESXi, somente. Opcional. A quantidade de espaço em disco a ser alocada na máquina virtual. Especificar 'grosso' para fazer o disco virtual tão grande como a unidade original no servidor protegido ou 'fino' para alocar a quantidade de espaço em disco ocupado na unidade original + alguns megabytes extras. A seleção padrão é aprovisionamento 'fino'.
-diskmapping	Exportação ESXi, somente. Opcional. Valores disponíveis: 'auto', 'manual', 'withvm'. O valor padrão é automapeamento.
-targetpath	VMware Workstation ou exportação VirtualBox, somente. Caminho local ou da rede (ou caminho do Linux para exportação VirtualBox somente) para a pasta onde os arquivos da máquina virtual devem ser armazenados.
-pathusername	Exportação VMware workstation, somente. Nome de usuário da máquina de rede. Somente obrigatório quando você especifica um caminho de rede em -targetpath.
-pathpassword	Exportação VMware workstation, somente. Senha para a máquina da rede. Somente obrigatório quando você especifica um caminho de rede em -targetpath.
-uselocalmachine	Exportação Hyper-V, somente. Opcional. Conectar ao server Hyper-V local. Neste caso, as opções 'hostname', 'hostport', 'hostusername' e 'hostpassword' são ignoradas.

Exemplos:

Exportar dados para uma máquina virtual ESXi com um nome específico e a mesma quantidade de RAM e tamanho do disco como o server de origem protegido:

```
>aacmd /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -
hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -
diskprovisioning thick
```

Criar um arquivo de máquina VMware Workstation na unidade local com dados protegidos do ponto de recuperação #4:

```
>aacmd /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -
targetpath c:\virtualmachines -ram 4096
```

Criar arquivos de máquina Hyper-V a serem arquivados numa máquina remota:

```
>aacmd /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-
Bobby\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -
hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository

O comando `UpdateRepository` adiciona um local de armazenamento novo a um repositório existente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path] -metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -sharepassword [share password] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `UpdateRepository`:

Tabela 158. Opções do comando UpdateRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-name`	Nome do repositório.
`-size`	Tamanho do local de armazenamento do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb, e Pb.
`-datapath`	Para espaço local, somente. Determinar o caminho de dados do local de armazenamento do repositório.
`-metadatapath`	Para espaço local, somente. Determinar o caminho de metadados do local de armazenamento do repositório.
`-uncpath`	Para local partilhado, somente. Determinar os caminhos de dados e metadados do local de armazenamento do repositório.
`-shareusername`	Para local partilhado, somente. Determina o nome de usuário para o local de compartilhamento.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Exemplos:

Criar um novo local de armazenamento no repositório local:

```
>aacmd /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

Criar um local de armazenamento no local partilhado:

```
>aacmd /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

Version

O comando `Version` exibe informações sobre a versão do software AppAssure instalado no servidor especificado. Se você não especificar um Core ou server protegido, serão retornadas informações relacionadas ao Core no qual você está trabalhando no momento.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[version | ver] -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Version`:

Tabela 159. Opções do comando Version

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Opcional. A máquina protegida cujas informações de versão você deseja visualizar. Se você não especificar uma máquina protegida, serão retornadas informações sobre a máquina Core na qual você está trabalhando no momento.

Exemplo:

Exibir informações sobre a versão do AppAssure instalada no AppAssure Core atual:

```
>aacmd.exe /version
```

Localização

Quando é executado na mesma máquina em que o AppAssure Core está instalado, o utilitário AppAssure Command Line Management usa como idioma de exibição o idioma configurado para o AppAssure Core. Nesta versão, os idiomas compatíveis são inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (Brasil) e espanhol.

Se o AppAssure Command Line Management estiver instalado em uma máquina separada, inglês é o único idioma compatível.

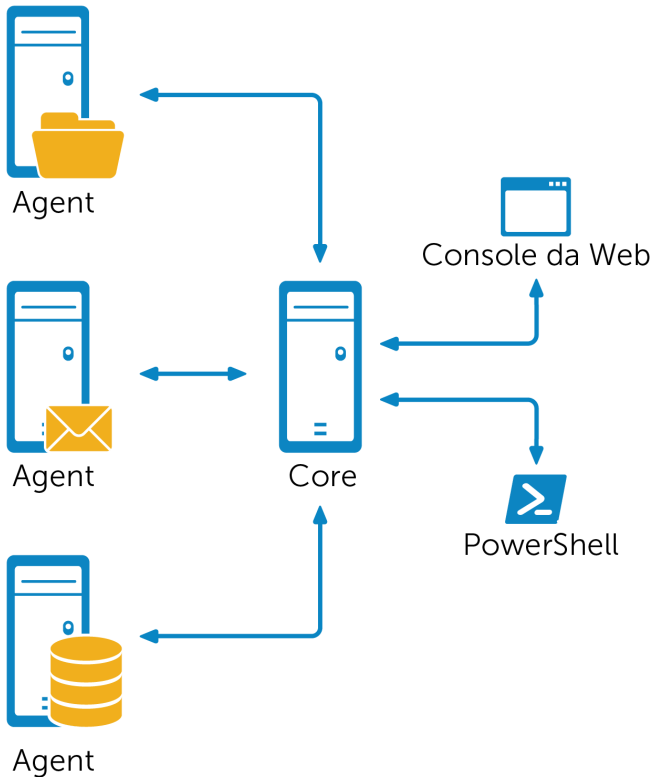
B

Noções básicas do módulo AppAssure PowerShell

O produto de recuperação após desastres e cópia de segurança AppAssure consiste em vários componentes de software, incluindo AppAssure Agent, AppAssure Core e o Módulo AppAssure PowerShell.

- O AppAssure Agent é responsável por capturar snapshots de volume e pela rápida transferência de dados para o AppAssure Core.
- O AppAssure Core armazena dados de snapshot de máquinas protegidas pelo software Agent e oferece outros recursos aprimorados, como restauração integral para hardware diferente, exportação virtual e replicação.
- O Módulo AppAssure PowerShell é um utilitário do Windows que permite que os usuários interajam com o AppAssure Core Server por meio do uso de scripts PowerShell. Esse módulo oferece algumas das mesmas funcionalidades fornecidas pela interface gráfica de usuário do AppAssure Core Console. Por exemplo, o Módulo AppAssure PowerShell pode montar pontos de recuperação do AppAssure ou forçar um snapshot de uma máquina protegida.

Figura 10. PowerShell interage com o AppAssure Core



O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. Esta seção descreve o módulo AppAssure PowerShell e os cmdlets que podem ser usados por administradores para criar scripts que realizam certas funções sem interação com a interface gráfica de usuário do AppAssure Core.

Esta seção inclui os seguintes tópicos:

- Pré-requisitos para usar o PowerShell
- Trabalhar com comandos e cmdlets

NOTA: Você também pode executar scripts PowerShell como pré-scripts e pós-scripts. Para obter mais informações e exemplos de scripts, consulte Estender trabalhos do AppAssure usando scripts.

Pré-requisitos para usar o PowerShell

Para usar o módulo AppAssure PowerShell, é preciso instalar o Windows PowerShell 2.0 ou posterior. Devido a novos recursos introduzidos no PowerShell 3.0, incluindo acesso mais fácil a propriedades de objeto, acesso a PowerShell Web e suporte a chamadas REST, a Dell recomenda usar o PowerShell 3.0 ou posterior.

NOTA: Certifique-se de colocar o arquivo powershell.exe.config no diretório base do PowerShell. Por exemplo, C:\WindowsPowerShell\powershell.exe.config

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

Iniciar o PowerShell e importar o módulo

Diferentemente de outros módulos do sistema, o módulo AppAssure PowerShell não é carregado por padrão. Em cada sessão, você pode abrir o Windows PowerShell com privilégios administrativos e importar o módulo. Siga as instruções descritas neste procedimento para iniciar o PowerShell e importar o módulo AppAssure PowerShell.

Para iniciar o PowerShell e importar o módulo AppAssure PowerShell

1. Abra um prompt de comando elevado do Windows PowerShell. Por exemplo, digite Windows PowerShell no menu Iniciar e, no aplicativo Windows PowerShell resultante, clique com o botão direito e selecione **Executar como administrador**.

   O Windows PowerShell é aberto em uma nova janela de comando.

2. Digite o seguinte comando e pressione Enter:

   ```
   Importar-Módulo “AppAssurePowerShellModule”
   ```

   O módulo AppAssure PowerShell é importado para a sessão atual. Você pode começar a executar cmdlets na janela de comando atual.

Trabalhar com comandos e cmdlets

Cmdlets são comandos especializados em um script Windows PowerShell que realizam uma única função. Um cmdlet geralmente é representado por um par verbo-substantivo. O resultado retornado por um cmdlet é um objeto.

Você pode usar pipelines com comandos PowerShell, o que permite que a saída de um cmdlet seja usada como entrada de outro cmdlet. Um exemplo simples é solicitar a lista de comandos no módulo AppAssure PowerShell e classificar a lista por nome. O script de exemplo para isso seria:

```
Get-Command -module appassurepowershellmodule | sort-object name
```

Obter ajuda e exemplos de cmdlet

Depois de abrir o PowerShell e importar o módulo AppAssure PowerShell, você pode solicitar mais informações a qualquer momento usando o cmdlet Get-Help <command_name>. Por exemplo, para obter informações sobre o cmdlet de exportação de máquina virtual, digite o cmdlet a seguir e pressione Enter:

```
Get-Help Start-VMExport
```

O objeto retornado inclui o nome do comando, a sinopse, a sintaxe e as opções que podem ser usadas.

Outro método para obter ajuda sobre um cmdlet específico é digitar o nome do comando seguido de `-?`. Por exemplo:

```
Start-VMExport -?
```

Para solicitar exemplos de um cmdlet, execute o comando a seguir:

```
>Get-Help Start-VMExport -examples
```

Cmdlets do módulo AppAssure PowerShell

Esta seção descreve os cmdlets e as opções disponíveis no módulo AppAssure PowerShell. Os cmdlets disponíveis são listados na tabela a seguir.

Tabela 160. Cmdlets no módulo AppAssure PowerShell

Nome do cmdlet	Descrição
Get-ActiveJobs	Recuperar uma coleção de trabalhos ativos
Get-Clusters	Recuperar uma coleção de clusters protegidos
Get-CompletedJobs	Recuperar uma coleção de trabalhos concluídos
Get-ExchangeMailStores	Recuperar uma coleção de armazenamentos de e-mail do Exchange
Get-Failed	Obter informações sobre pontos de recuperação com falha
Get-FailedJobs	Recuperar uma coleção de trabalhos com falha
Get-Mounts	Exibir todos os pontos de recuperação montados
Get-Passed	Obter informações sobre pontos de recuperação aprovados
Get-ProtectedServers	Obter informações sobre servidores protegidos
Get-ProtectionGroups	Recuperar uma coleção de grupos de proteção
Get-RecoveryPoints	Obter informações sobre pontos de recuperação
Get-ReplicatedServers	Obter informações sobre servidores replicados
Get-Repositories	Obter informações sobre repositórios
Get-SqlDatabases	Recuperar uma coleção de bancos de dados SQL
Get-UnprotectedVolumes	Recuperar uma coleção de volumes não protegidos

Tabela 160. Cmdlets no módulo AppAssure PowerShell

Nome do cmdlet	Descrição
Get-VirtualizedServers	Obter informações sobre servidores virtualizados
Get-Volumes	Obter informações sobre volumes
New-Base	Forçar snapshot de imagem de base
New-Mount	Montar pontos de recuperação
New-Repository	Criar novo repositório
New-Snapshot	Forçar snapshot
Push-Replication	Forçar replicação
Push-Rollup	Forçar rollup
Remove-Mount	Desmontar ponto de recuperação
Remove-Mounts	Desmontar todos os pontos de recuperação montados
Resume-Replication	Retomar replicação
Resume-Snapshot	Retomar snapshot
Resume-VMExport	Retomar exportação de máquina virtual
Start-Archive	Arquivar pontos de recuperação
Start-AttachabilityCheck	Forçar verificação de capacidade de anexação em bancos de dados MS SQL protegidos
Start-EsxiExport	Forçar exportação para um servidor ESXi
Start-HypervExport	Forçar exportação para um servidor Hyper-V
Start-LogTruncation	Forçar truncamento de log
Start-MountabilityCheck	Forçar verificação de capacidade de montagem em armazenamentos de e-mail do Exchange protegidos
Start-Protect	Colocar um servidor sob proteção
Start-ProtectCluster	Colocar um cluster sob proteção
Start-RestoreArchive	Restaurar arquivo com pontos de recuperação
Start-VBExport	Forçar exportação para um servidor VirtualBox
Start-VMExport	Forçar exportação para um servidor VMWare Workstation
Stop-ActiveJobs	Cancelar trabalhos ativos
Suspend-Replication	Pausar replicação
Suspend-Snapshot	Pausar snapshot
Suspend-VMExport	Pausar exportação de máquina virtual
Update-Repository	Adicionar extensão a repositório

Get-ActiveJobs

O comando `Get-ActiveJobs` retorna todos os trabalhos ativos do Core. O parâmetro `--jobtype` pode ser usado para observar tarefas específicas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ActiveJobs`:

Tabela 161. Opções do comando Get-ActiveJobs

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `"transfer"` (transferência de dados), `"repository"` (manutenção do repositório), `"replication"` (replicações locais e remotas), `"backup"` (cópia de segurança e restauração), `"bootcdbuilder"` (criar CDs de inicialização), `"diagnostics"` (carregar logs), `"exchange"` (verificação de arquivos do Exchange Server), `"export"` (exportação de pontos de recuperação), `"pushinstall"` (implantar agentes), `"rollback"` (restaurar de um ponto de recuperação), `"rollup"` (rollups de ponto de recuperação), `"sqlattach"` (verificações de capacidade de anexação de agente) e `"mount"` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs -all
```

Get-Clusters

O comando `Get-Clusters` retorna informações sobre os clusters do servidor protegidos no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Clusters`:

Tabela 162. Opções do comando Get-Clusters

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Mostrar uma lista de clusters do servidor protegidos no Core local:

```
>Get-Clusters
```

Get-CompletedJobs

O comando `Get-CompletedJobs` retorna uma lista de trabalhos concluídos no Core. O parâmetro `--jobtype` pode ser usado para observar tarefas específicas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-CompletedJobs`:

Tabela 163. Opções do comando Get-CompletedJobs

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `"transfer"` (transferência de dados), `"repository"` (manutenção do repositório), `"replication"` (replicações locais e remotas), `"backup"` (cópia de segurança e restauração), `"bootcdbuilder"` (criar CDs de inicialização), `"diagnostics"` (carregar logs), `"exchange"` (verificação de arquivos do Exchange Server), `"export"` (exportação de pontos de recuperação), `"pushinstall"` (implantar agentes), `"rollback"` (restaurar de um ponto de recuperação), `"rollup"` (rollups de ponto de recuperação), `"sqlattach"` (verificações de capacidade de anexação de agente) e `"mount"` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-CompletedJobs -all
```

Listar todas as tarefas de criação de repositório concluídas no Core local:

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

O comando `Get-ExchangeMailStores` retorna informações sobre armazenamentos de e-mail em servidores Exchange protegidos pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ExchangeMailStores`:

Tabela 164. Opções do comando Get-ExchangeMailStores

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Mostra a lista de armazenamentos de e-mail do servidor Exchange do Core local:

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

O comando `Get-Failed` retorna informações sobre pontos de recuperação com falha no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Failed -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Failed`:

Tabela 165. Opções do comando Get-Failed

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 165. Opções do comando Get-Failed

Opção	Descrição
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
-number	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.

Exemplo:

Mostra uma lista de todos os pontos de recuperação com falha:

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

O comando `Get-FailedJobs` retorna todos os trabalhos com falha do Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-FailedJobs`:

Tabela 166. Opções do comando Get-FailedJobs

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
-all	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.

Tabela 166. Opções do comando Get-FailedJobs

Opção	Descrição
-number	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
-jobtype	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: "transfer" (transferência de dados), "repository" (manutenção do repositório), "replication" (replicações locais e remotas), "backup" (cópia de segurança e restauração), "bootcdbuilder" (criar CDs de inicialização), "diagnostics" (carregar logs), "exchange" (verificação de arquivos do Exchange Server), "export" (exportação de pontos de recuperação), "pushinstall" (implantar agentes), "rollback" (restaurar de um ponto de recuperação), "rollup" (rollups de ponto de recuperação), "sqlattach" (verificações de capacidade de anexação de agente) e "mount" (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
-time	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Mostra uma lista de todos os trabalhos com falha no Core local:

```
>Get-FailedJobs -all
```

Listar todas as tarefas de criação de cópia de segurança que falharam no local Core:

```
>Get-FailedJobs -type backup
```

Get-Mounts

O comando `Get-Mounts` retorna todos os pontos de recuperação montados no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver
[server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Mounts`:

Tabela 167. Opções do comando Get-Mounts

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Exibir todos os pontos de recuperação montados:

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.5.22
```

Get-Passed

O comando `Get-Passed` retorna informações sobre pontos de recuperação que foram aprovados em verificações no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver
[server name or IP address] -number [all | f[number] |l[number] | number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Passed`:

Tabela 168. Opções do comando Get-Passed

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os pontos de recuperação no Core local que foram aprovados em verificações:

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

O comando `Get-ProtectedServers` retorna informações sobre máquinas protegidas no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ProtectedServers`:

Tabela 169. Opções do comando Get-ProtectedServers

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todas as máquinas protegidas atualmente no Core local:

```
>Get-ProtectedServers
```

Get-ProtectionGroups

O comando `Get-ProtectionGroups` retorna informações sobre grupos de proteção no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ProtectionGroups`:

Tabela 170. Opções do comando Get-ProtectionGroups

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista grupos de proteção no Core local:

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-RecoveryPoints

O comando `Get-RecoveryPoints` retorna informações sobre pontos de recuperação de máquinas protegidas no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-RecoveryPoints`:

Tabela 171. Opções do comando Get-RecoveryPoints

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Tabela 171. Opções do comando Get-RecoveryPoints

Opção	Descrição
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
-number	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.

Exemplo:

Lista pontos de recuperação de máquinas protegidas no Core local:

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

O comando `Get-ReplicatedServers` retorna informações sobre máquinas replicadas no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ReplicatedServers`:

Tabela 172. Opções do comando Get-ReplicatedServers

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os servidores replicados no Core local:

```
>Get-ReplicatedServers
```

Get-Repositories

O comando `Get-Repositories` retorna informações sobre repositórios no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Repositories`:

Tabela 173. Opções do comando Get-Repositories

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista repositórios no Core local:

```
>Get-Repositories
```

Get-SqlDatabases

O comando `Get-SqlDatabases` retorna uma lista de bancos de dados SQL da máquina protegida especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-SqlDatabases`:

Tabela 174. Opções do comando Get-SqlDatabases

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os trabalhos de bancos de dados SQL no Core local:

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

O comando `Get-UnprotectedVolumes` retorna informações sobre volumes que estão disponíveis para proteção, mas não estão protegidos atualmente no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-UnprotectedVolumes`:

Tabela 175. Opções do comando Get-UnprotectedVolumes

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os volumes disponíveis para proteção (mas que não estão protegidos) na máquina de agente especificada:

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

O comando `Get-VirtualizedServers` retorna informações sobre servidores virtualizados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-VirtualizedServers`:

Tabela 176. Opções do comando Get-VirtualizedServers

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os servidores virtualizados no Core local:

```
>Get-VirtualizedServers
```

Get-Volumes

O comando `Get-Volumes` retorna informações sobre volumes em uma máquina especificada que é protegida pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Volumes -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Volumes`:

Tabela 177. Opções do comando Get-Volumes

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os volumes na máquina especificada:

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

O comando `New-Base` força uma nova imagem de base resultando em uma transferência de dados da máquina atualmente protegida. Ao forçar uma imagem de base, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-Base`:

Tabela 178. Opções do comando New-Base

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Imagem de base para todos os agentes.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Tabela 178. Opções do comando New-Base

Opção	Descrição
-protectedserver	Forçar para o nome da máquina protegida atual.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Forçar imagem de base para todas as máquinas protegidas:

```
>New-Base -all
```

New-Mount

O comando New-Mount monta um snapshot de uma ou mais unidades.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Mount -core [host name] -user [user name] -password [password]
-protectedserver [machine name] -mounttype [read | write |
readonlywithpreviouswrites] -drives [drive names] -path [location] -time [MM/DD/YYYY
hh:mm:ss tt | passed | latest] -rpn [number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando New-Mount:

Tabela 179. Opções do comando New-Mount

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-protectedserver	O nome da máquina ou endereço IP do servidor protegido (depende de como a máquina específica foi protegida).
-time	Opcional. O timestamp do ponto de recuperação a ser montado. Ele deve estar no formato especificado pelo OS do computador em questão. O administrador é capaz de obter o ponto de recuperação mais recente especificando o último ponto de recuperação ou o mais recentemente verificado pelo valor de parâmetro aprovado. Como padrão, a opção de último horário é escolhida.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-path	Caminho na máquina Core para a qual os pontos de recuperação serão montados.
-mounttype	Opcional. Especifica um modo de montagem. As opções disponíveis são "read", "readOnlyWithPreviousWrites" (apenas leitura com gravações anteriores) e "write" (gravável). O modo padrão é read-only.

Tabela 179. Opções do comando New-Mount

Opção	Descrição
-volumes	Opcional. Lista separada por espaços dos nomes de volumes a serem montados. Se o nome do volume contém espaços ou caracteres especiais, ele precisa ser especificado usando aspas duplas. Se não especificado, todos os volumes serão montados.
-drivers	Opcional. Lista separada por vírgulas dos nomes de volumes a serem montados. Se não especificado, todos os volumes serão montados. NOTA: Esta opção é obsoleta, use "-volumes" em vez dela.
-rpn	Opcional. Número do ponto de recuperação para a montagem. Você pode conseguir isso usando o comando get-mounts. Especifique diversos números para o parâmetro rpn para montar diferentes pontos com um único comando. NOTA: Se você definir uma matriz de pontos para montar, cada ponto estará localizado em um diretório subordinado separado. O nome descreve o horário em que o ponto de recuperação foi criado. Quando você chamar a função de desmontar, todos os diretórios subordinados serão removidos. Você deve remover o diretório principal manualmente.

Exemplo:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c
"d, ko"
```

Montar uma matriz de pontos de recuperação:

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path "D:/Folder for mount"
```

Montar um ponto de recuperação com certo horário de criação:

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012
11:46 AM"
```

New-Repository

O comando New-Repository cria um novo repositório no AppAssure Core. O tamanho especificado deve estar entre 250 Mb e 16 Tb.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath
[location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando New-Repository:

Tabela 180. Opções do comando New-Repository

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 180. Opções do comando New-Repository

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-name	Nome do repositório.
-size	Tamanho da extensão do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb e Pb.
-datapath	Para espaço local, somente. Determina o caminho de dados da extensão de repositório.
-metadatapath	Para espaço local, somente. Determina o caminho de metadados da extensão de repositório.
-uncpath	Para local partilhado, somente. Determina os caminhos de dados e metadados da extensão de repositório.
-shareusername	Para local partilhado, somente. Determinar login para local partilhado.
-sharepassword	Para local partilhado, somente. Determinar senha para local partilhado.
-comment	Opcional. Descrição do repositório.
-concurrent Operations	Opcional. O número máximo de operações pode estar pendente de uma só vez. Valor pelo padrão: 64.

Exemplo:

Criar um novo repositório do tamanho mínimo na unidade local E:

```
>New-Repository –name Repository2 -size 250Mb -datapath e:\Repository\Data -
metadatapath e:\Repository\Metadata
```

New-Snapshot

O comando New-Snapshot força um snapshot resultando em uma transferência de dados da máquina atualmente protegida. Ao forçar um snapshot, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user
name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando New-Snapshot:

Tabela 181. Opções do comando New-Snapshot

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Forçar todas as máquinas protegidas.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 181. Opções do comando New-Snapshot

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Forçar para o nome da máquina protegida atual.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Forçar um snapshot de todas as máquinas protegidas:

```
>New-Snapshot -all
```

Push-Replication

O comando Push-Replication força a replicação de uma ou mais máquinas protegidas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Push-Replication -core [host name] -user [user name] -password [password]
-targetcore [host name] -all | -protectedserver [machine name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Push-Replication:

Tabela 182. Opções do comando Push-Replication

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Forçar replicação para todas as máquinas sendo replicadas no Core de destino.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Nome da máquina protegida no Core de destino contra a qual a replicação será forçada.
-user	Opcional. Login para a máquina de host do Core remoto. Se você especificar um login, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Enviar replicação para uma única máquina protegida:

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

Enviar replicação para todas as máquinas protegidas:

```
>Push-Replication -all
```

Push-Rollup

O comando `Push-Rollup` força o rollup de uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
Push-Rollup -core [host name] -user [user name] -password [password]
-protectedserver [machine name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Push-Rollup`:

Tabela 183. Opções do comando Push-Rollup

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Forçar todas as máquinas protegidas.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Forçar para o nome da máquina protegida atual.
`-user`	Opcional. Login para a máquina de host do Core remoto. Se você especificar um login, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Enviar rollup para uma única máquina protegida:

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Enviar rollup para todas as máquinas protegidas:

```
>Push-Rollup -all
```

Remove-Mount

O comando `Remove-Mount` desmonta um ponto de recuperação montado especificado por `/Path`. Desmonta pontos para a máquina selecionada usando o parâmetro `-protectedserver`, ou desmonta pontos para todos os pontos de recuperação montados usando o parâmetro `--all`.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Mount -core [host name] -user [user name] -password [password]
[-protectedserver [machine name] | -path [mount path]]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Remove-Mount`:

Tabela 184. Opções do comando Remove-Mount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Desmontar todos os pontos de recuperação montados.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-path`	Desmontar ponto de montagem selecionado.
`-protectedserver`	Desmontar todos os pontos de recuperação montados para a máquina protegida atual.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Desmontar o ponto de recuperação especificado pelo caminho:

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -path
C:\mountedRecoveryPoint
```

Remove-Mounts

O comando `Remove-Mounts` desmonta todos os pontos de recuperação montados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Remove-Mounts`:

Tabela 185. Opções do comando Remove-Mounts

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 185. Opções do comando Remove-Mounts

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Desmontar todos os pontos de recuperação no Core especificado:

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Resume-Replication

O comando Resume-Replication permite que você retome a replicação. Consulte Suspend-Replication para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-Replication -core [host name] -user [user name] -password [password] -all |
-protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host
name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Resume-Replication:

Tabela 186. Opções do comando Resume-Replication

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-all	Todos os servidores protegidos.
-protectedserver	Retomar a replicação da máquina especificada.
-incoming	Nome do host do Core remoto que replica para a máquina Core. A replicação de todas as máquinas protegidas no Core remoto é retomada.
-outgoing	Nome de host do Core de destino remoto no qual os dados são replicados. A replicação de todas as máquinas protegidas no Core remoto é retomada.

Exemplo:

Retomar replicação da máquina protegida com o IP 10.10.10.4 para o Core local:

```
>Resume-Replication -protectedserver 10.10.10.4
```

Resume-Snapshot

Um administrador é capaz de retomar snapshots, exportar para máquinas virtuais e realizar replicações. Consulte Start-VMExport para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Resume-Snapshot`:

Tabela 187. Opções do comando Resume-Snapshot

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Todos os servidores protegidos.
`-protectedserver`	Retoma o snapshot da máquina especificada.

Exemplo:

Retomar snapshots da máquina protegida com o IP 10.10.10.4 para o Core local:

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VMExport

O comando `Resume-VMExport` permite que um administrador exporte para máquinas virtuais. Consulte Suspend-VMExport para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Resume-VMExport`:

Tabela 188. Opções do comando Resume-VMExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Todos os servidores protegidos.
`-protectedserver`	Retoma o snapshot da máquina especificada.

Exemplo:

Retomar a exportação para uma máquina virtual em cada máquina protegida no Core local:

```
>Resume-VMExport -all
```

Start-Archive

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do AppAssure é usado para suportar a retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou local de rede especificando o comando `/Path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or
[IP]] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-Archive`:

Tabela 189. Opções do comando Start-Archive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-path`	Caminho até o local. Exemplo de caminho: **D:\work\archive** ou caminho de rede: **'\\NomedoServidor\Compartilhamento'**.
`-all`	Arquivar os pontos de recuperação para todas as máquinas no Core.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 189. Opções do comando Start-Archive

Opção	Descrição
-startdate	Data inicial dos pontos de recuperação criados no período. Ela deve estar no formato especificado pelo OS do computador em questão.
-enddate	Data final do período. O padrão é a data atual.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Arquiva pontos de recuperação para a máquina especificada.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-archiveusername	Opcional. Necessário para caminho de rede apenas.
-archivepassword	Opcional. Necessário para caminho de rede apenas.
-comment	Opcional. Exemplo: `-comment 'Before install new application'`.

Exemplo:

Arquivar todos os pontos de recuperação para todas as máquinas no Core:

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

O comando `Start-AttachabilityCheck` força uma verificação de capacidade de anexação em todos os SQL Server databases protegidos pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time
string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-AttachabilityCheck`:

Tabela 190. Opções do comando Start-AttachabilityCheck

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	A máquina protegida na qual será realizada a verificação de capacidade de anexação do SQL.

Tabela 190. Opções do comando Start-AttachabilityCheck

Opção	Descrição
-rpn	Opcional. O número sequencial de um ponto de recuperação no qual deverá ser realizada a verificação de capacidade de anexação do SQL. Use o comando -GetRecoveryPoints para obter números de pontos de recuperação. Você pode especificar vários números separados por espaços para realizar verificações em vários pontos de recuperação com um único comando. NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será usado para a verificação de capacidade de anexação.
-time	Opcional. Determina o ponto de recuperação a ser selecionado para a verificação de capacidade de anexação do SQL. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.

Exemplo:

Realizar uma verificação de capacidade de anexação do SQL no ponto de recuperação mais recente para o servidor SQL protegido especificado:

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-EsxiExport

O comando Start-EsxiExport inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor ESX(i).

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; o nome de host e porta do host de servidor Linux; e o caminho para a pasta local, de rede ou de Linux na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-EsxiExport -core [host name] -user [user name] -password [password]
-protectedserver [machine name | IP address] -volumes [volume names] -rpn [number |
numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual host port number] -hostusername [virtual host user
name] hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram]
-diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Start-EsxiExport:

Tabela 191. Opções do comando Start-EsxiExport

Opção	Descrição
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Máquina protegida com pontos de recuperação a serem exportados.
-volumes	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras no final dos nomes de volumes. Por exemplo, especifique "C:" e não "C:/"
-rpn	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando -GetRecoveryPoints para obter números de pontos de recuperação.) NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
-time	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
-vmname	Nome do Windows da máquina virtual.
-hostname	O nome do host do servidor virtual.
-hostport	O número da porta do servidor virtual.
-hostusername	O nome de usuário para o host do servidor virtual.
-hostpassword	A senha para o host do servidor virtual.
-ram	Alocar uma quantidade específica de RAM no servidor virtual.
-usesourceram	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
-diskprovisioning	Opcional. A quantidade de espaço em disco que será alocada na máquina virtual. Especifique "thick" para fazer o disco virtual ter o mesmo tamanho da unidade original no server protegido, ou "thin" para alocar a quantidade de espaço em disco efetivamente ocupada na unidade original mais algum espaço extra em megabytes. Por padrão, o provisionamento "thin" é selecionado.
-diskmapping	Opcional. Selecione "auto", "manual" ou "withvm". O automapeamento está ativado por padrão.

Start-HypervExport

O comando Start-HypervExport inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor Hyper-V.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-HypervExport -core [host name] -user [user name] -password [password]
-protectedserver [[machine name] or [IP address]] -volumes [volume names] -rpn
[number | numbers] | -time [time string] [-vmname [uselocalmachine] | -hostname
[virtual host name] -hostport [virtual host port number] -hostusername [virtual host
user name] -hostpassword [virtual host password] -vmlocation [location]] [-ram
[total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-HypervExport`:

Tabela 192. Opções do comando Start-HypervExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras no final dos nomes de volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `-GetRecoveryPoints` para obter números de pontos de recuperação.) **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-vmname`	Nome do Windows da máquina virtual.
`-uselocalmachine`	Opcional. Conectar ao servidor Hyper-V local. Quando este parâmetro é usado, as seguintes opções são ignoradas: hostname, host port, host username, host password.
`-hostname`	O nome do host do servidor virtual.
`-hostport`	O número da porta do servidor virtual.
`-hostusername`	O nome de usuário para o host do servidor virtual.
`-hostpassword`	A senha para o host do servidor virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.

Tabela 192. Opções do comando Start-HypervExport

Opção	Descrição
-diskprovisioning	Opcional. A quantidade de espaço em disco que será alocada na máquina virtual. Especifique "thick" para fazer o disco virtual ter o mesmo tamanho da unidade original no server protegido, ou "thin" para alocar a quantidade de espaço em disco efetivamente ocupada na unidade original mais algum espaço extra em megabytes. Por padrão, o provisionamento "thin" é selecionado.
-diskmapping	Opcional. Selecione "auto", "manual" ou "withvm". O automapeamento está ativado por padrão.
-diskformat	Opcional. Especificar o formato de disco apropriado dentre as opções VHD ou VHDX. VHD é usado por padrão caso não seja especificado.

Start-LogTruncation

O comando `Start-LogTruncation` força o truncamento de log no SQL Server ou servidor Microsoft Exchange protegido especificado.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-LogTruncation -core [host name] -user [user name] -password [password]
-protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-LogTruncation`:

Tabela 193. Opções do comando Start-LogTruncation

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Arquivo de pontos de recuperação para a máquina especificada.
-target	Especificar o tipo de truncamento de log ("sql" ou "exchange"). Se não for especificado, os logs de todos os bancos de dados serão truncados.

Exemplo:

Truncar logs de SQL:

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Truncar logs de servidor Exchange: todos os pontos de recuperação de todas as máquinas no Core:

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

O comando `Start-MountabilityCheck` força uma verificação de capacidade de montagem em armazenamentos de e-mail do Microsoft Exchange protegidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password]
-protectedserver [[machine name] or [IP address]] -rpn [number | numbers] |
-time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-MountabilityCheck`:

Tabela 194. Opções do comando Start-MountabilityCheck

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Arquivo de pontos de recuperação para a máquina especificada.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `-GetRecoveryPoints` para obter números de pontos de recuperação.) **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.

Exemplo:

Iniciar uma verificação de capacidade de montagem em todos os pontos de recuperação para todas as máquinas no Core:

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

O comando `Start-Protect` permite que um administrador adicione um servidor sob proteção por um Core.

Forma de uso

```
Start-Protect -core [host name] -user [user name] -password [password] -repository
[repository name] -agent [name | IP address] -agentusername [user name]
-agentpassword [password] -agentport [port] -volumes [volume names]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-Protect`:

Tabela 195. Opções do comando Start-Protect

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida estão armazenados.
`-agentname`	Nome da máquina protegida ou endereço IP.
`-agentusername`	Login do servidor a ser protegido.
`-agentpassword`	Senha do servidor a ser protegido.
`-agentport`	Número da porta do servidor protegido.
`-volumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes. Por exemplo, "**c:**" ou **“d:”**.

Exemplo:

Colocar os volumes de um servidor sob proteção:

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername
administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

O comando `Start-ProtectCluster` permite que um administrador adicione um cluster do servidor sob a proteção de um Core.

Forma de uso

O uso do comando é o seguinte:

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -
repository [repository name] -clustername [name | IP address] -clusterusername [user
name for cluster] -clusterpassword [password for cluster] -clusterport [port] -
clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-ProtectCluster`:

Tabela 196. Opções do comando Start-ProtectCluster

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida estão armazenados. O nome deve ser informado entre aspas duplas.
`-clustername`	O nome do cluster a ser protegido.
`-clusterusername`	Nome de usuário para o cluster a ser protegido.
`-clusterpassword`	Senha do cluster a ser protegido.
`-clusterport`	Número de porta do cluster a ser protegido.
`-clustervolumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes. Por exemplo, "c:", "d".
`-clusternodes`	Lista de nós de cluster com volumes a serem protegidos. Primeiro especifique o rótulo "nodename" e, em seguida, digite o nome do nó. Em seguida, especifique o rótulo "volumes" e digite uma lista de volumes para o nó. Por exemplo: `“nodename”, “10.10.10.10”, “volumes”, “c:”, “e:”, “nodename”, “10.10.10.11,” “volumes”, “c:”`

Exemplo:

Colocar os volumes de um servidor sob proteção:

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120
-clusterusername administrator -clusterpassword 12345 -clusterport 5002
-clustervolumes "c:" "d:" -clusternodes nodename 10.10.10.10 volumes “c:” “e:”
```

Start-RestoreArchive

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do AppAssure é usado para suportar a retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou local de rede especificando o comando `/Path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-RestoreArchive –path -repository [-all] | -protectedserver [machine name] or
[IP]] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-RestoreArchive`:

Tabela 197. Opções do comando Start-RestoreArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-path`	Caminho até o local. Exemplo de caminho: **D:\work\archive** ou caminho de rede: **'\\NomedoServidor\Compartilhamento'**.
`-repository`	Repositório do Core para a máquina não protegida.
`-all`	Arquivar os pontos de recuperação para todas as máquinas no Core.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Arquivo de pontos de recuperação para a máquina especificada.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-archiveusername`	Opcional. Necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Necessário para caminho de rede apenas.

Exemplo:

Arquivar todos os pontos de recuperação para todas as máquinas no Core:

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-VBExport

O comando `start-VBExport` inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor Oracle VirtualBox.

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; o nome de host e porta do host de servidor Linux; e o caminho para a pasta local, de rede ou de Linux na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-VBExport -core -user [user name] -password [password] -protectedserver
[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath
[location] pathusername [user name] - pathpassword [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-VBExport`:

Tabela 198. Opções do comando Start-VBExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras no final dos nomes de volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `Get-RecoveryPoints` para obter números de pontos de recuperação.) **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-vmname`	Nome do Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
`-linuxhostname`	Nome de host do servidor Linux VirtualBox.
`-hostport`	Porta do servidor Linux VirtualBox.
`-targetpath`	Caminho local, de rede ou de Linux para a pasta em que os arquivos da máquina virtual devem ser armazenados.
`-pathusername`	Nome de usuário da máquina de rede. Somente necessário quando você especifica um caminho de rede no parâmetro `-targetpath`.
`-pathpassword`	Senha para a máquina da rede. Somente necessário quando você especifica um caminho de rede no parâmetro `-targetpath`.
`-accountusername`	Opcional. Use caso possa especificar uma conta de usuário para registrar a máquina virtual exportada. Apenas para máquina local ou de rede.
`-accountpassword`	Opcional. Use apenas quando você especificar uma conta de usuário para registrar a máquina virtual exportada usando o parâmetro `-accountusername`. Apenas para máquina local ou de rede.

Exemplo:

Exportar todos os volumes do último ponto de recuperação na máquina 10.10.12.97 para uma VM chamada NewVirtualBoxVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram
usesourceram -targetpath D:/exports
```

Start-VMExport

O comando `start-VMExport` inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor VMware Workstation.

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; e o caminho para a pasta local ou de rede na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-VMExport -core -user [user name] -password [password] -protectedserver
[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostnme [linux hostname] -hostport [linux port] -targetpath
[location] pathusername [user name] - pathpassword [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-VMExport`:

Tabela 199. Opções do comando Start-VMExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras no final dos nomes de volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `Get-RecoveryPoints` para obter números de pontos de recuperação.) **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o horário exato no formato "MM/DD/YYYY hh:mm tt" (por exemplo: "04/24/2015 09:00 AM")." Especifique os valores de data e de hora do fuso horário definido na sua máquina local. **NOTA:** Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-vmname`	Nome do Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.

Tabela 199. Opções do comando Start-VMExport

Opção	Descrição
-usesourceram	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
-targetpath	Caminho local, de rede ou de Linux para a pasta em que os arquivos da máquina virtual devem ser armazenados.
-pathusername	Nome de usuário da máquina de rede. Somente necessário quando você especifica um caminho de rede no parâmetro -targetpath.
-pathpassword	Senha para a máquina da rede. Somente necessário quando você especifica um caminho de rede no parâmetro -targetpath.
-version	Opcional. Use caso possa especificar uma conta de usuário para registrar a máquina virtual exportada. Apenas para máquina local ou de rede.
-version	Versão do VMware Tools a ser usada. As versões válidas são: 7, 8, 9 e 10.

Exemplo:

Exportar todos os volumes do último ponto de recuperação na máquina 10.10.12.97 para uma VM chamada NewVMwareVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath D:/exports
```

Suspend-Replication

O comando Suspend-Replication permite que um administrador pause uma replicação.

Um usuário pode pausar uma replicação de três maneiras:

- Pausar a replicação no Core mestre de todas as máquinas protegidas (parâmetro -outgoing)

  O administrador precisa especificar o nome da máquina remota com o emparelhamento de replicação de saída para pausar a replicação de saída no Core mestre.

  ```
  >Suspend-replication -outgoing 10.10.12.10
  ```

- Pausar a replicação no Core mestre de uma única máquina protegida (parâmetro -protectedserver)

  ```
  >Suspend-replication -protectedserver 10.10.12.97
  ```

- Pausar replicação no Core de destino (--incoming parameter)

  Se o Core local é um Core de destino, o administrador pode pausar a replicação especificando o Core mestre usando o parâmetro -incoming.

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Suspend-Replication:

Tabela 200. Opções do comando Suspend-Replication

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Pausa todas as máquinas protegidas no Core selecionado.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-pause	[snapshots], [replication] ou [vmexport].

Tabela 200. Opções do comando Suspend-Replication

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Pausar o servidor protegido atual.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-incoming	Nome do host do Core remoto que replica para a máquina Core. A replicação de todas as máquinas protegidas no Core remoto é suspensa.
-outgoing	Nome de host do Core de destino remoto no qual os dados são replicados. A replicação de todas as máquinas protegidas no Core remoto é suspensa.

Exemplo:

Pausar uma replicação de saída no Core remoto com o endereço IP: 10.10.1.15, para a máquina protegida única com o endereço IP: 10.10.1.76:

```
>Suspend-replication –core 10.10.1.15 –protectedserver 10.10.1.76
```

Pausar a replicação de saída no Core local para o destino remoto com o endereço IP: 10.10.1.63 para todas as máquinas protegidas:

```
>Suspend-replication –outgoing 10.10.1.63
```

Pausar replicação de entrada a partir de 10.10.1.82 no Core remoto com o endereço IP: 10.10.1.15 (o administrador é capaz de pausar uma replicação de entrada somente para toda a máquina):

```
>Suspend-replication –core 10.10.1.15 –incoming 10.10.1.82
```

Stop-ActiveJobs

O comando `Stop-ActiveJobs` cancela trabalhos ativos em uma máquina protegida especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
Stop-ActiveJobs [-protectedserver [machine name | IP address] | -core [host name]]
-user [user name] -password [password] -jobtype [jobtype]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Stop-ActiveJobs`:

Tabela 201. Opções do comando Stop-ActiveJobs

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Selecionar e cancelar eventos do tipo especificado em todas as máquinas protegidas.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Tabela 201. Opções do comando Stop-ActiveJobs

Opção	Descrição
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Determina a máquina protegida na qual os trabalhos serão cancelados.
-jobtype	Opcional. Especifica o filtro do tipo de trabalho. Os valores disponíveis são: "transfer" (transferência de dados), "repository" (manutenção do repositório), "replication" (replicações locais e remotas), "backup" (cópia de segurança e restauração), "bootcdbuilder" (criar CDs de inicialização), "diagnostics" (carregar logs), "exchange" (verificação de arquivos do Exchange Server), "export" (exportação de ponto de recuperação), "pushinstall" (implementar software Agent em máquinas protegidas), “rollback" (restaurar dados de um ponto de recuperação), "rollup" (rollups de ponto de recuperação), "sqlattach" (verificações de capacidade de anexação de agente), "mount" (não repositório). Como padrão, todos os trabalhos do tipo especificado são cancelados.

Exemplo:

Interromper o trabalho de transferência na máquina protegida:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

Interromper todos os trabalhos para uma máquina protegida específica:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Snapshot

O comando `Suspend-Snapshot` permite que um administrador pause snapshot.

Forma de uso

A forma de uso do comando é a seguinte:

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |
-protectedserver [name | IP address] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Suspend-Snapshot`:

Tabela 202. Opções do comando Suspend-Snapshot

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Pausa todas as máquinas protegidas no Core selecionado.

Tabela 202. Opções do comando Suspend-Snapshot

Opção	Descrição
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-time	O horário no formato "Dia-Horas-Minutos" em que os snapshots serão retomados (somente para pausas de snapshots).

Exemplo:

Pausar snapshots da máquina protegida com o IP 10.10.10.4 para o Core local, com retomada em um determinado horário:

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VMExport

O comando Suspend-VMExport permite que um administrador pause exportações para máquinas virtuais.

Forma de uso

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando Suspend-VMExport:

Tabela 203. Opções do comando Suspend-VMExport

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-all	Pausa todas as máquinas protegidas no Core selecionado.
-protectedserver	Pausar o servidor protegido atual.

Exemplo:

Suspender a exportação de VM da máquina protegida com IP 10.10.10.4 para o Core local:

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

O comando `Update-Repository` adiciona uma extensão a um repositório existente. O tamanho especificado deve estar entre 250 Mb e 16 Tb.

Forma de uso

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user
name] -sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Update-Repository`:

Tabela 204. Opções do comando Update-Repository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-name`	Nome do repositório.
`-size`	Tamanho da extensão do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb e Pb.
`-datapath`	Para espaço local, somente. Determina o caminho de dados da extensão de repositório.
`-metadatapath`	Para espaço local, somente. Determina o caminho de metadados da extensão de repositório.
`-uncpath`	Para local partilhado, somente. Determina os caminhos de dados e metadados da extensão de repositório.
`-shareusername`	Para local partilhado, somente. Determinar login para local partilhado.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.

Exemplo:

Adicionar ao repositório uma extensão do tamanho mínimo:

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -
metadatapath C:\repository\Metadata
```

Localização

Quando é executado na mesma máquina em que o AppAssure Core está instalado, o módulo AppAssure PowerShell usa como idioma de exibição o idioma definido para o AppAssure Core. Nesta versão, os idiomas compatíveis são inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (Brasil) e espanhol.

Se o módulo AppAssure PowerShell estiver instalado em uma máquina separada, o idioma inglês é o único compatível.

Qualificadores

A tabela a seguir descreve os qualificadores disponíveis para o Módulo AppAssure PowerShell.

Tabela 205.

Qualificador	Forma de uso
`-core <AppAssure Core Name>`	Nome do host do Core. Padrão: `Localhost`
`-ProtectedServer <Protected Server Name>`	Nome do host/endereço IP do AppAssure Agent. Padrão: `Localhost` no caso de múltiplos servidores protegidos, caso contrário o único servidor protegido.
`-Mode <READ, READWRITE, WRITE>`	Modo de montagem do ponto de recuperação. Padrão: `Read`.
`-Volumes <Snapshot Volume Letter>`	Letra do volume do snapshot do AppAssure Agent. Padrão: `All`.
`-User <User Name>`	Nome de usuário usado para se conectar ao AppAssure Core. Normalmente é o usuário de serviço.
`-Domain <Domain Name>`	Domínio ao qual pertence o usuário definido em /User.
`-Password <Password>`	Senha do usuário definido em `/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	Por exemplo: `C:\AppAssureMount`.

C

Estender trabalhos do AppAssure usando scripts

O AppAssure permite aos administradores automatizar a administração e o gerenciamento de recursos em determinadas ocorrências pela execução de comandos e scripts. O software AppAssure suporta o uso de script de PowerShell para Windows e script de Bourne Shell para Linux.

Os trabalhos do Core são criados automaticamente quando você inicia operações no AppAssure Core, como replicação, exportação virtual ou snapshot de cópia de segurança. Você pode estender esses trabalhos executando um script antes ou depois deles. Esses scripts são chamados de pré-script e pós-script.

Esta seção descreve os scripts que podem ser usados por administradores em ocorrências designadas no AppAssure para Windows e Linux.

△ **CUIDADO: Os exemplos de script PowerShell e Bourne oferecidos neste documento funcionarão quando forem executados conforme projetado por administradores qualificados. Tome cuidado ao modificar scripts de funcionamento para manter versões de trabalho. Qualquer modificação nos exemplos de script incluídos aqui ou qualquer script que você criar são considerados como uma personalização, que normalmente não é coberta pelo Atendimento ao Cliente.**

Esta seção inclui os seguintes tópicos:

- Usar scripts PowerShell no AppAssure
- Parâmetros de entrada do PowerShell Scripting
- Exemplos de scripts PowerShell
- Usar scripts Bourne Shell no AppAssure
- Parâmetros de entrada para scripts do Bourne Shell
- Exemplos de scripts do Bourne Shell
- Exemplos de scripts PowerShell

Usar scripts PowerShell no AppAssure

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O AppAssure inclui kits abrangentes de desenvolvimento de software cliente (SDKs) para PowerShell Scripting que permitem aos usuários administrativos executar scripts PowerShell fornecidos pelo usuário em ocorrências designadas; por exemplo, antes ou depois de um snapshot, de verificações de capacidade de anexação e montabilidade, e assim por diante. Os administradores podem executar scripts a partir do AppAssure Core e da máquina protegida. Os scripts podem aceitar parâmetros e a saída de um script é gravada nos arquivos de log do Core e da máquina protegida.

ⓘ **NOTA:** Para trabalhos noturnos, preserve um arquivo de script e o parâmetro de entrada *JobType* para distinguir entre trabalhos noturnos.

Os arquivos de script estão localizados na pasta %ALLUSERSPROFILE%\AppRecovery\Scripts.

- No Windows 7, o caminho para localizar a pasta %ALLUSERSPROFILE% é: C:\ProgramData.

- No Windows 2003, o caminho para localizar a pasta é: Documents and Settings\All Users\Application Data\.

NOTA: É necessário que o Windows PowerShell esteja instalado e configurado antes de executar scripts do AppAssure.

Para obter mais informações sobre como usar scripts do PowerShell, consulte Exemplos de scripts PowerShell, Parâmetros de entrada do PowerShell Scripting, Parâmetros de entrada para scripts do Bourne Shell e Exemplos de scripts do Bourne Shell.

Pré-requisitos para PowerShell Scripting

Antes de executar scripts do PowerShell no AppAssure, é preciso instalar o Windows PowerShell 2.0 ou posterior. Devido a novos recursos introduzidos no PowerShell 3.0, incluindo acesso mais fácil a propriedades de objeto, acesso a PowerShell Web e suporte a chamadas REST, a Dell recomenda usar o PowerShell 3.0 ou posterior.

NOTA: Coloque o arquivo powershell.exe.config no diretório base do PowerShell. Por exemplo, C:\WindowsPowerShell\powershell.exe.config.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

Teste dos scripts do PowerShell

Se desejar testar os scripts que pretende executar, poderá fazê-lo usando o editor gráfico do PowerShell, o *powershell_is*. Também é preciso adicionar o arquivo de configuração, *powershell_ise.exe.config* na mesma pasta do arquivo de configuração, *powershell.exe.config*.

NOTA: O arquivo de configuração, *powershell_ise.exe.config*, deve ter o mesmo conteúdo do arquivo *powershell.exe.config*.

CUIDADO: Se o script pré-PowerShell ou pós-PowerShell falhar, o trabalho também falhará.

Localização

Quando é executado na mesma máquina em que o AppAssure Core está instalado, o módulo AppAssure PowerShell usa como idioma de exibição o idioma definido para o AppAssure Core. Nesta versão, os idiomas compatíveis são inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (Brasil) e espanhol.

Se o módulo AppAssure PowerShell estiver instalado em uma máquina separada, o idioma inglês é o único compatível.

Qualificadores

A tabela a seguir descreve os qualificadores disponíveis para o módulo AppAssure PowerShell.

Tabela 206. Qualificadores do módulo AppAssure PowerShell

Qualificador	Forma de uso
`-core <AppAssure Core Name>`	Nome do host do Core. Padrão: `Localhost`
`-ProtectedServer <Protected Server Name>`	Nome do host/endereço IP do AppAssure Agent. Padrão: `Localhost` no caso de múltiplos servidores protegidos, caso contrário o único servidor protegido.
`-Mode <READ, READWRITE, WRITE>`	Modo de montagem do ponto de recuperação. Padrão: `Read`.
`-Volumes <Snapshot Volume Letter>`	Letra do volume do snapshot do AppAssure Agent. Padrão: `All`.
`-User <User Name>`	Nome de usuário usado para conectar ao AppAssure Core, que é geralmente o usuário do serviço.
`-Domain <Domain Name>`	Domínio ao qual pertence o usuário definido em /User.
`-Password <Password>`	Senha do usuário definido em `/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	Por exemplo: `C:\AppAssureMount`.

Parâmetros de entrada do PowerShell Scripting

Todos os parâmetros de entrada disponíveis são usados em scripts de exemplo. Os parâmetros estão descritos nas tabelas a seguir.

NOTA: Os arquivos de script devem possuir o mesmo nome dos arquivos de script de exemplo.

AgentProtectionStorageConfiguration (espaço de nomes Replay.Common.Contracts.Agents)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentProtectionStorageConfiguration.

Tabela 207. Objetos para o parâmetro AgentProtectionStorageConfiguration

Método	Descrição
public Guid RepositoryId { get; set; }	Obtém ou define o ID do repositório onde os pontos de recuperação do Agent estão armazenados.
public string EncryptionKeyId { get; set; }	Obtém ou define o ID da chave de criptografia dos pontos de recuperação do Agent. Uma cadeia de caracteres vazia significa nenhuma criptografia.

AgentTransferConfiguration (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentTransferConfiguration.

Tabela 208. Objetos para o parâmetro AgentTransferConfiguration

Método	Descrição
public uint MaxConcurrentStreams { get; set; }	Obtém ou define o número máximo de conexões TCP simultâneas que o Core estabelece com o Agent para transferência de dados.
public uint MaxTransferQueueDepth { get; set; }	Quando um intervalo de blocos é lido de um fluxo de transferência, esse intervalo é colocado em uma fila de produtor ou consumidor, onde um thread de consumidor o lê e grava no objeto epoch. Se o repositório grava mais lentamente do que a rede lê, essa fila fica cheia. O ponto em que a fila está cheia e a leitura é interrompida é a extensão máxima da fila de transferência.
public uint MaxConcurrentWrites { get; set; }	Obtém ou define o número máximo de operações de gravação de blocos pendentes em um epoch em qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que uma das gravações pendentes seja concluída.
public ulong MaxSegmentSize { get; set; }	Obtém ou define o número máximo de blocos contíguos que serão transferidos em uma única solicitação. Dependendo do teste, valores mais altos ou mais baixos podem ser ideais.
public Priority Priority { get; set; }	Obtém ou define a prioridade da solicitação de transferência.
public int MaxRetries { get; set; }	Obtém ou define o número máximo de vezes que uma transferência com falha deve ser tentada novamente antes de ser considerada como falha.
public Guid ProviderId{ get; set; }	Obtém ou define o GUID do provedor de VSS que será usado para snapshots neste host. Os administradores em geral aceitam o padrão.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Obtém ou define o conjunto de IDs de gravação do VSS, os quais devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome do gravador.
public ushort TransferDataServerPort { get; set; }	Obtém ou define um valor que contém a porta TCP através da qual as conexões serão aceitas do Core para a transferência real de dados do Agent para o Core. O Agent tenta escutar essa porta, mas se ela estiver em uso, ele poderá usar uma porta diferente. O Core deve usar o número de porta especificado nas propriedades BlockHashesUri e BlockDataUri do objeto VolumeSnapshotInfo para cada volume expandido.
public TimeSpan SnapshotTimeout { get; set; }	Obtém ou define o tempo de espera para que uma operação de snapshot do VSS seja concluída antes que ela seja abandonada e expire.

Tabela 208. Objetos para o parâmetro AgentTransferConfiguration

Método	Descrição
public TimeSpan TransferTimeout { get; set; }	Obtém ou define o tempo de espera para contatos adicionais do Core antes de abandonar o snapshot.
public TimeSpan NetworkReadTimeout { get; set; }	Obtém ou define o tempo limite para operações de leitura de rede relacionadas a essa transferência.
public TimeSpan NetworkWriteTimeout { get; set; }	Obtém ou define o tempo limite para operações de gravação de rede relacionadas a essa transferência.

BackgroundJobRequest (espaço de nomes Replay.Core.Contracts.BackgroundJobs)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro BackgroundJobRequest.

Tabela 209. Objetos para o parâmetro BackgroundJobRequest

Método	Descrição
public Guid AgentId { get; set; }	Obtém ou define o ID do Agent.
public bool IsNightlyJob { get; set; }	Obtém ou define o valor que indica se o trabalho em segundo plano é um trabalho noturno.
public virtual bool InvolvesAgentId(Guid agentId)	Determina o valor que indica se o Agent concreto está envolvido no trabalho.

ChecksumCheckJobRequest (espaço de nomes Replay.Core.Contracts.Exchange.ChecksumChecks)

Herda seus valores do parâmetro DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (espaço de nomes Replay.Core.Contracts.Exchange)

Herda seus valores do parâmetro, BackgroundJobRequest.

ExportJobRequest (espaço de nomes Replay.Core.Contracts.Export)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro ExportJobRequest.

Tabela 210. Objetos para o parâmetro ExportJobRequest

Método	Descrição
public uint RamInMegabytes { get; set; }	Obtém ou define o tamanho da memória para a VM exportada. Defina como zero (0) para usar o tamanho da memória da máquina de origem.
public VirtualMachineLocation Location { get; set; }	Obtém ou define o local de destino dessa exportação. Trata-se de uma classe de base abstrata.

Tabela 210. Objetos para o parâmetro ExportJobRequest

Método	Descrição
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Obtém ou define as imagens de volume a incluir na exportação da VM.
public ExportJobPriority Priority { get; set; }	Obtém ou define a prioridade da solicitação de exportação.

NightlyAttachabilityJobRequest (espaço de nomes Replay.Core.Contracts.Sql)

Herda seus valores do parâmetro, BackgroundJobRequest.

RollupJobRequest (espaço de nomes Replay.Core.Contracts.Rollup)

Herda seus valores do parâmetro, BackgroundJobRequest.

TakeSnapshotResponse (espaço de nomes Replay.Agent.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TakeSnapshotResponse.

Tabela 211. Objetos para o parâmetro TakeSnapshotResponse

Método	Descrição
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

TransferJobRequest (espaço de nomes Replay.Core.Contracts.Transfer)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferJobRequest.

Tabela 212. Objetos para o parâmetro TransferJobRequest

Método	Descrição
public VolumeNameCollection VolumeNames { get; set; }	Obtém ou define o conjunto de nomes para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • **GuidName.** O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • **DisplayName.** O nome de exibição do volume.

Tabela 212. Objetos para o parâmetro TransferJobRequest

Método	Descrição
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. Os valores disponíveis são: • Unknown • Copy • Full
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento.
public string Key { get; set; }	Gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a imagem de base foi forçada ou não.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o trabalho é truncamento de log ou não.

TransferPrescriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPrescript.

Tabela 213. Objetos para o parâmetro TransferPrescript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • **GuidName**. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • **DisplayName**. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full

Tabela 213. Objetos para o parâmetro TransferPrescript

Método	Descrição

public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
	AgentTransferConfiguration é um objeto que terá os seguintes dados:
	• **MaxConcurrentStreams**. O número máximo de conexões TCP simultâneas que o Core estabelecerá com o agente para transferir dados
	• **MaxTransferQueueDepth**. O número máximo de extensões de bloco que podem ser enfileiradas para gravação
	• **MaxConcurrentWrites**. O número máximo de operações de gravação de bloco pendentes em uma época a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado.
	• **MaxSegmentSize**. O número máximo de blocos contíguos que serão transferidos em uma única solicitação
	• **Priority**. Um objeto que terá os seguintes dados:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (which is equal to One)
	  • Lowest (which is equal to Ten)
	  • Default (which is equal to Five)
	• MaxRetries. O número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha
	• **UseDefaultMaxRetries**. Um valor indicando que o número máximo de tentativas é o valor padrão
	• **ProviderId**. O GUID do provedor de VSS que será usado para snapshots nesse host. Os usuários geralmente usam a definição padrão.

Tabela 213. Objetos para o parâmetro TransferPrescript

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• **ExcludedWriterIds**. Conjunto de IDs de gravador de VSS que devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome real do gravador. • **TransferDataServerPort**. Um valor contendo a porta TCP em que serão aceitas conexões do Core para a transferência efetiva de dados do agente para o Core. • **SnapshotTimeout**. Tempo de espera para que uma operação de snapshot de VSS seja concluída antes que ela seja abandonada e expire. • **TransferTimeout**. Tempo de espera por contatos adicionais do Core antes de abandonar o snapshot. • **NetworkReadTimeout**. O tempo limite para operações de leitura de rede relacionadas a essa transferência. • **NetworkWriteTimeout**. O tempo limite para operações de gravação de rede relacionadas a essa transferência. • **InitialQueueSize**. O tamanho da fila inicial de solicitações. • **MinVolumeFreeSpacePercents**. Quantidade mínima de espaço livre em um volume, expressa como uma porcentagem. • **MaxChangeLogsSizePercents**. Tamanho máximo dos registros de alterações de driver como parte da capacidade do volume, expresso como uma porcentagem. • **EnableVerification**. Um valor que indica se a verificação de diagnóstico de cada bloco enviado ao Core deve ser realizada.
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o “número de epoch” atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

TransferPostscriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript.

Tabela 214. Objetos para o parâmetro TransferPostscript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • **GuidName.** O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • **DisplayName**. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full

Tabela 214. Objetos para o parâmetro TransferPostscript

Método	Descrição

public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
	AgentTransferConfiguration é um objeto que terá os seguintes dados:
	• **MaxConcurrentStreams**. O número máximo de conexões TCP simultâneas que o Core estabelecerá com o agente para transferir dados
	• **MaxTransferQueueDepth**. O número máximo de extensões de bloco que podem ser enfileiradas para gravação
	• **MaxConcurrentWrites**. O número máximo de operações de gravação de bloco pendentes em uma época a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado.
	• **MaxSegmentSize**. O número máximo de blocos contíguos que serão transferidos em uma única solicitação
	• **Priority**. Um objeto que tem os seguintes dados:
	  • “Indefinido
	  • “Um
	  • “Dois
	  • “Três
	  • “Quatro
	  • “Cinco
	  • “Seis
	  • “Sete
	  • “Oito
	  • “Nove
	  • “Dez
	  • “Mais alto (é igual a Um)
	  • “Mais baixo (igual a Dez)
	  • “Padrão (igual a Cinco)
	• **MaxRetries**. O número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha
	• **UseDefaultMaxRetries**. Um valor indicando que o número máximo de tentativas é o valor padrão
	• **ProviderId**. O GUID do provedor de VSS que será usado para snapshots nesse host. Os administradores em geral aceitam o padrão.

Tabela 214. Objetos para o parâmetro TransferPostscript

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• **ExcludedWriterIds**. Conjunto de IDs de gravador de VSS que devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome real do gravador. • **TransferDataServerPort**. Um valor contendo a porta TCP em que serão aceitas conexões do Core para a transferência efetiva de dados do agente para o Core. • **SnapshotTimeout**. Tempo de espera para que uma operação de snapshot de VSS seja concluída antes que ela seja abandonada e expire. • **TransferTimeout**. Tempo de espera por contatos adicionais do Core antes de abandonar o snapshot. • **NetworkReadTimeout**. O tempo limite para operações de leitura de rede relacionadas a essa transferência. • **NetworkWriteTimeout**. O tempo limite para operações de gravação de rede relacionadas a essa transferência. • **InitialQueueSize**. O tamanho da fila inicial de solicitações. • **MinVolumeFreeSpacePercents**. Quantidade mínima de espaço livre em um volume, expressa como uma porcentagem. • **MaxChangeLogsSizePercents**. Tamanho máximo dos registros de alterações de driver como parte da capacidade do volume, expresso como uma porcentagem. • **EnableVerification**. Um valor que indica se a verificação de diagnóstico de cada bloco enviado ao Core deve ser realizada.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento O objeto AgentProtectionStorageConfiguration contém os seguintes dados: • **RepositoryId**. Nome do repositório onde os pontos de recuperação desse agente serão armazenados • **EncryptionKeyId**. O ID da chave de criptografia para os pontos de recuperação desse agente. Uma cadeia de caracteres vazia significa nenhuma criptografia
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.

Tabela 214. Objetos para o parâmetro TransferPostscript

Método	Descrição
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

VirtualMachineLocation (espaço de nomes Replay.Common.Contracts.Virtualization)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VirtualMachineLocation.

Tabela 215. Objetos para o parâmetro VirtualMachineLocation

Método	Descrição
public string Description { get; set;}	Obtém ou define uma descrição desse local legível para humanos.
public string Method { get; set;}	Obtém ou define o nome da VM.

VolumeImageIdsCollection (espaço de nomes Replay.Core.Contracts.RecoveryPoints)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<string>.

VolumeName (espaço de nomes Replay.Common.Contracts.Metadata.Storage)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeName.

Tabela 216. Objetos para o parâmetro VolumeName

Método	Descrição
public string GuidName { get; set;}	Obtém ou define o ID do volume.
public string DisplayName { get; set;}	Obtém ou define o nome do volume.

Tabela 216. Objetos para o parâmetro VolumeName

Método	Descrição
public string UrlEncode()	Obtém uma versão do nome codificada como URL que pode ser passada adequadamente em uma URL. NOTA: Existe um problema conhecido no .NET 4.0 WCF (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312) que impede os caracteres de escape de caminho de funcionar corretamente em um modelo de URI. Visto que o nome do volume contém '\' e '?', substitua os caracteres especiais '\' e '?' por outros caracteres especiais.
public string GetMountName()	Retorna um nome para esse volume que é válido para a imagem do volume de montagem em alguma pasta.

VolumeNameCollection (espaço de nomes eplay.Common.Contracts.Metadata.Storage)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<VolumeName>.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeNameCollection.

Tabela 217. Objetos para o parâmetro VolumeNameCollection

Método	Descrição
public override bool Equals(object obj)	Determina se essa instância e um objeto especificado, que também deve ser um objeto VolumeNameCollection, têm o mesmo valor. (Substitui Object.Equals(Object).)
public override int GetHashCode()	Retorna o código hash de VolumeNameCollection. (Substitui Object.GetHashCode().)

VolumeSnapshotInfo (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeSnapshotInfo.

Tabela 218. Objetos para o parâmetro VolumeSnapshotInfo

Método	Descrição
public Uri BlockHashesUri { get; set;}	Obtém ou define o URI em que os hashes MD5 dos blocos de volume podem ser lidos.
public Uri BlockDataUri { get; set;}	Obtém ou define o URI em que os blocos de dados de volume podem ser lidos.

VolumeSnapshotInfoDictionary (espaço de nomes Replay.Common.Contracts.Transfer)

Herda seus valores do parâmetro System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Exemplos de scripts PowerShell

Os exemplos de scripts a seguir são fornecidos para auxiliar os usuários administrativos na execução de scripts PowerShell. Os scripts de amostra incluem:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

PreTransferScript.ps1

O PreTransferScript é executado na máquina protegida antes da transferência de um snapshot.

Amostra de PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];

# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {

     echo 'TransferPrescriptParameterObject parameter is null'
}
else {

     echo
     'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguratio
     n

     echo 'StorageConfiguration:'
     $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

O PostTransferScript é executado na máquina protegida após a transferência de um snapshot.

Amostra de PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];

# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {

     echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames

          echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType

     echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage

     echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation

}
```

PreExportScript.ps1

O PreExportScript é executado no Core antes de qualquer trabalho de exportação.

Amostra de PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
```

```
if($ExportJobRequestObject -eq $null) {
     echo 'ExportJobRequestObject parameter is null'
}
else {
     echo 'Location:' $ExportJobRequestObject.Location
     echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

PostExportScript.ps1

O PostExportScript é executado no Core após qualquer trabalho de exportação.

NOTA: Não há parâmetros de entrada para o PostExportScript quando usado para executar uma vez na máquina protegida exportada após a inicialização inicial. A máquina protegida regular deve conter esse script na pasta de scripts PowerShell como PostExportScript.ps1.

Amostra de PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
     echo 'ExportJobRequestObject parameter is null'
}
else {
     echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
     echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

O PreNightlyJobScript é executado antes de cada trabalho noturno no lado do Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PreNightlyJobScript

```
# receiving parameters from Nightlyjob
```

```
param([System.String]$JobClassMethod, [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

            if($NightlyAttachabilityJobRequestObject -eq $null) {

                  echo 'NightlyAttachabilityJobRequestObject parameter is null';

            }

            else {

                  echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;

                  echo 'IsNightlyJob:'
                  $NightlyAttachabilityJobRequestObject.IsNightlyJob;

            }

            break;

      }

# working with Rollup Job
   RollupJob {

      $RollupJobRequestObject = $RollupJobRequest -as
      [Replay.Core.Contracts.Rollup.RollupJobRequest];

      echo 'Rollup job results:';

            if($RollupJobRequestObject -eq $null) {

                        echo 'RollupJobRequestObject parameter is null';

            }

            else {

                  echo 'SimultaneousJobsCount:'
                  $RollupJobRequestObject.SimultaneousJobsCount;

                        echo 'AgentId:' $RollupJobRequestObject.AgentId;

                        echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;

            }

            $AgentsCollection = $Agents -as
            "System.Collections.Generic.List``1[System.Guid]"
```

```
            if($AgentsCollection -eq $null) {
                  echo 'AgentsCollection parameter is null';
            }
            else {
                  echo 'Agents GUIDs:'
                  foreach ($a in $AgentsCollection) {
                        echo $a
            }
      }
      break;
   }
# working with Checksum Check Job
      ChecksumCheckJob {
            $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
            [Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
            echo 'Exchange checksumcheck job results:';
            if($ChecksumCheckJobRequestObject -eq $null) {
                  echo 'ChecksumCheckJobRequestObject parameter is null';
      }
      else {
                  echo 'RecoveryPointId:'
                  $ChecksumCheckJobRequestObject.RecoveryPointId;
                  echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                  echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
            }
            break;
      }
# working with Log Truncation Job
   TransferJob {
      $TransferJobRequestObject = $TransferJobRequest -as
      [Replay.Core.Contracts.Transfer.TransferJobRequest];
      echo 'Transfer job results:';
      if($TransferJobRequestObject -eq $null) {
                  echo 'TransferJobRequestObject parameter is null';
      }
      else {
                  echo 'TransferConfiguration:'
                  $TransferJobRequestObject.TransferConfiguration;
                  echo 'StorageConfiguration:'
                  $TransferJobRequestObject.StorageConfiguration;
            }
            echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
```

```
            break;
      }
}
```

PostNightlyJobScript.ps1

O PostNightlyJobScript é executado após cada trabalho noturno no Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod, [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore,
[object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

      if($NightlyAttachabilityJobRequestObject -eq $null) {

            echo 'NightlyAttachabilityJobRequestObject parameter is null';

      }

      else {

            echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;

            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;

      }

      break;
   }

# working with Rollup Job
   RollupJob {

      $RollupJobRequestObject = $RollupJobRequest -as
      [Replay.Core.Contracts.Rollup.RollupJobRequest];
```

```
      echo 'Rollup job results:';
      if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
      }
      else {
            echo 'SimultaneousJobsCount:'
            $RollupJobRequestObject.SimultaneousJobsCount;
            echo 'AgentId:' $RollupJobRequestObject.AgentId;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
      }
      $AgentsCollection = $Agents -as
      "System.Collections.Generic.List``1[System.Guid]"
      if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
      }
      else {
      echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                  echo $a
                  }
            }
            break;
      }
# working with Checksum Check Job
   ChecksumCheckJob {
      $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
      [Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
      echo 'Exchange checksumcheck job results:';
      if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
      }
      else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
      }
      break;
   }
# working with Log Truncation Job
   TransferJob {
      $TransferJobRequestObject = $TransferJobRequest -as
      [Replay.Core.Contracts.Transfer.TransferJobRequest];
```

```
      echo 'Transfer job results:';
      if($TransferJobRequestObject -eq $null) {
            echo 'TransferJobRequestObject parameter is null';
      }
      else {
             echo 'TransferConfiguration:'
            $TransferJobRequestObject.TransferConfiguration;
            echo 'StorageConfiguration:'
            $TransferJobRequestObject.StorageConfiguration;
      }
      echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
      $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
      [Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
      if($TakeSnapshotResponseObject -eq $null) {
            echo 'TakeSnapshotResponseObject parameter is null';
      }
      else {
            echo 'ID of this transfer session:' $TakeSnapshotResponseObject.Id;
            echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
      }
      break;
   }
}
```

Usar scripts Bourne Shell no AppAssure

Bourne shell (sh) é uma linguagem de shell ou intérprete de linha de comando para sistemas operacionais baseados em Unix. Bourne Shell é usado no AppAssure com Linux para personalizar ambientes e especificar que certas operações ocorram em uma sequência predeterminada. .sh é a extensão de arquivo e convenção de nomenclatura para arquivos Bourne shell.

Bourne Again Shell (BASH) é uma linguagem de shell semelhante que implementa a mesma gramática, parâmetro e expansão de variável, redireção e citação. BASH também usa a extensão de arquivo .sh. As informações fornecidas aqui também se aplicam ao BASH.

Usando os ganchos de script pré e pós-transferência e de exportação, é possível executar operações do sistema antes e depois de uma transferência ou exportação. Por exemplo, você talvez queira desativar certo cronjob enquanto a transferência está ocorrendo e ativá-lo assim que ela for concluída. Em outro exemplo, pode ser necessário executar comandos para liberar dados específicos do aplicativo para o disco. O conteúdo é gravado em um arquivo temporário e executado usando exec. O script é executado usando o intérprete definido na sua primeira linha, como, por exemplo, `(#!/usr/bin/env bash)`. Se o intérprete especificado não estiver disponível, o script usará o shell padrão definido na variável de ambiente $SHELL.

Você pode substituir e usar qualquer intérprete. Por exemplo, na linha `#!` do script, você pode substituir "bash" por "zsh" (Z shell), "tcsh" (tee shell) e assim por diante, segundo sua preferência.

É possível adicionar objetos disponíveis do parâmetro TransferPrescript ou adicionar seus próprios comandos aos scripts PreTransferScript.sh e PostTransfer.sh para personalizá-los.

Esta seção descreve os scripts que podem ser usados por administradores em ocorrências designadas no AppAssure para Windows e Linux. Os seguintes tópicos estão incluídos:

- Parâmetros de entrada para scripts do Bourne Shell
- Exemplos de scripts do Bourne Shell

Pré-requisitos para scripts do Bourne Shell

Todos os scripts devem ter o nome PreTransferScript.sh, PostTransfer.sh e PostExportScript.sh. Todos os scripts também precisam residir no diretório `/opt/appassure/scripts/`.

Testar os scripts do Bourne Shell

É possível testar os scripts que deseja executar usando o editor de arquivos de script (.sh).

NOTA: Se os scripts pré-Bourne Shell ou pós-Bourne Shell falharem, o trabalho também falhará. Há informações sobre o trabalho disponíveis no arquivo /var/log/appassure/appassure.log.

Os scripts bem-sucedidos retornam o código de saída 0.

Parâmetros de entrada para scripts do Bourne Shell

Os parâmetros dos scripts do Bourne Shell no AppAssure são descritos nas tabelas a seguir.

TransferPrescriptParameters_VolumeNames

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPrescript.

Tabela 219. Objetos de TransferPrescript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • **GuidName**. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • **DisplayName**. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.

Tabela 219. Objetos de TransferPrescript

Método	Descrição
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

TransferPostscriptParameter

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript.

Tabela 220. Objetos de TransferPostscript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • **GuidName**. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • **DisplayName**. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

Exemplos de scripts do Bourne Shell

Esta seção descreve os exemplos de scripts de Bourne Shell disponíveis para execução por usuários administrativos em máquinas protegidas.

△ **CUIDADO: Os exemplos de script Bourne fornecidos neste documento funcionarão quando forem executados conforme projetado por administradores qualificados. Tome cuidado ao modificar scripts de funcionamento para manter versões de trabalho. Qualquer modificação nos exemplos de script incluídos aqui ou qualquer script que você criar são considerados como uma personalização, que normalmente não é coberta pelo Atendimento ao Cliente.**

Os exemplos de scripts para máquinas protegidas incluem:

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

ⓘ **NOTA:** Máquinas protegidas usam o comando de shell "exec" para iniciar o script. Para indicar qual intérprete deve executar o script, defina essa informação na primeira linha do script. Se você não especificar o intérprete, o shell padrão interpretará o script. Se você optar por algo diferente do shell padrão, precisará garantir que o intérprete especificado esteja disponível em todas as máquinas protegidas.

PreTransferScript.sh

O PreTransferScript é executado na máquina protegida antes da transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PreTransferScript

```
#!/bin/bash
echo
"TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyTyp
e
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImag
e
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncat
ion
TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_Latest
EpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

O PostTransferScript é executado na máquina protegida após a transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PostTransferScript

```
#!/bin/bash
echo
"TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyT
ype
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseIm
age
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTrunc
ation
TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_Late
stEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

O PostExportScript é executado na máquina protegida após a transferência.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)ExportScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

D

Noções básicas das APIs do AppAssure

O propósito desta seção é fornecer uma introdução e visão geral das APIs REST do AppAssure, seu uso e sua função.

As APIs de serviço da Web do AppAssure são RESTful e permitem automatizar e personalizar certas funções e tarefas na solução de software AppAssure para ajudá-lo a atingir os seus objetivos comerciais.

Este documento descreve as referências de API do AppAssure Core e do Agent e lista os contratos de serviço e URI de cada categoria.

Consulte uma das seções a seguir para obter informações sobre os contratos de serviço incluídos nos conjuntos de cliente de Core e Agent:

- Usar a API do AppAssure Core
- Uso da API AppAssure Agent

Público-alvo

As APIs do AppAssure são destinadas a desenvolvedores que desejem integrar e estender o AppAssure em seus aplicativos e a administradores que desejem criar scripts de interações com o AppAssure Core Server.

Leitura adicional recomendada

- *Guia de instalação e atualização do Dell AppAssure*. Esse guia apresenta uma visão geral da arquitetura e recursos do AppAssure e descreve as etapas e as instruções necessárias para instalar os componentes do AppAssure, bem como para migrar do Replay para o AppAssure.

O guia está disponível para download em https://support.software.dell.com/appassure/5.4.3/release-notes-guides/.

Trabalhar com APIs REST do AppAssure

As APIs do AppAssure são APIs em estilo REST, o que significa que usam solicitações HTTP para fornecer acesso a recursos (entidades de dados) por meio de caminhos de URI. As APIs do AppAssure usam métodos HTTP padrão, como GET, PUT, POST e DELETE. Como as APIs REST são baseadas em padrões abertos, você pode usar qualquer idioma ou ferramenta com suporte a chamadas HTTP.

Há duas maneiras para desenvolvedores e administradores de aplicativos trabalharem com as APIs do AppAssure. São elas:

- Empregar C# ou outra linguagem .NET para usar diretamente os arquivos DLL de cliente .NET do AppAssure.
- Comunicar-se diretamente com o terminal HTTP para gerar seu próprio XML.

Recomendamos a primeira abordagem. Os DLLs de cliente encontram-se no diretório de instalação do AppAssure Core. O método para chamar as APIs do AppAssure é consistente com a maneira de consumir qualquer serviço WCF do .NET 4.0.

O DLL principal é Core.Client.dll. Você pode usar Core.Contracts.dll, Agent.Contracts.dll e qualquer outro *.Contract.dll conforme necessário para auxiliar no que você está tentando fazer com o AppAssure.

Usar a API do AppAssure Core

As referências da API do AppAssure Core são agrupadas de acordo com as seguintes categorias e interfaces de serviço. Clique em uma categoria para exibir mais informações sobre as operações de serviço disponíveis para uma interface específica.

Os contratos de serviço contidos no conjunto de cliente do Core são descritos nas tabelas a seguir:

Tabela 1. Contratos de serviço do Core

Contrato de serviço	URI	Descrição
IAgentDiagnosticsManagement	agentdiag/	Replay.Core.Contracts.Agents.IAgentDiagnosticsManagement
IAgentsGroupsManagement	agentGroups/	Interface implementada pelo serviço de grupos, que executa ações no Core relacionado ao grupo.
IAgentsManagement	agents/	Interface implementada pelo serviço de agentes, que realiza ações no Core relacionado ao agente.
IApplianceEventsManagement	events/appliance/	Expõe os eventos de appliance para o Core.
IApplicationIdManagement	id/	Expõe o ID exclusivo do aplicativo.
IAutoUpdateManagement	autoupdate/	Replay.Core.Contracts.AutomaticUpdate.IAutoUpdateManagement
IBackgroundJobManagement	jobmgr/	Interface de contrato WCF que é implementada por uma classe que implementa a interface de gerenciamento sobre o gerenciador de trabalho de segundo plano.
IBackupManagement	backup/	Interface implementada pelo serviço de gerenciamento de backup do Core, que é usada para criar uma cópia de segurança e restaurar um Core local.
IBootCdBuilderManagement	bootcdbuilder/	Replay.Core.Contracts.BootCdBuilder.IBootCdBuilderManagement
ICloudManagement	cloud/	Expõe a API de gerenciamento de nuvem.
IClustersManagement	clusters/	Expõe a API de gerenciamento de cluster.
ICoreBackupRestoreManagement	corebackuprestore/	Interface que é implementada pelo serviço de gerenciamento de cópia de segurança e restauração de configuração do Core, usada para criar uma cópia de segurança e restaurar a configuração do Core.
ICoreCallbackManagement	corecallback/	Interface que é implementada pelo serviço de gerenciamento de retorno de chamada do Core, que é usada por agentes remotos.
ICoreDiagnosticsManagement	corediag/	Replay.Core.Contracts.Diagnostics.ICoreDiagnosticsManagement
ICoreMetadataManagement	metadata/	Interface que é implementada pelo serviço de metadados do Core, que mantém, armazena em cache e retorna metadados do Core.
ICoreSettingsManagement	settings/	Permite consultar e ajustar diversas definições do Core.

Tabela 1. Contratos de serviço do Core

Contrato de serviço	URI	Descrição
IDatabaseStorageManagement	databaseStorage/	Interface para comunicação e configuração de armazenamento de banco de dados persistente, que é usada para eventos e registra o armazenamento de informações.
IDiagnosticsManagement	diag/	Replay.Common.Contracts.Diagnostics.IDiagnosticsManagement
IEmailsManagement	emailsmgr/	Interface de contrato WCF para gerenciamento de e-mail.
IEncryptionKeyManagement	encryption/	Gerenciamento de chaves de criptografia, que é usado com repositórios e serviços dependentes.
IEventsManagement	events/	Expõe os eventos e alertas no Core.
IExchangeManagement	exchange/	Expõe o gerenciamento do MS Exchange no Core.
IExportQueueManagement	export/queue/	API RESTful da fila de exportação.
IExportSchedulerManagement	export/schedule/	API RESTful do programador de exportação.
IHyperVAgentManagement	hypervagent/	Replay.Common.Contracts.Virtualization.IHyperVAgentManagement
IIsoDatabaseManagement	bootcdbuilder/	Replay.Core.Contracts.BootCdBuilder.IIsoDatabaseManagement
ILicenseManagement	license/	Interface que é implementada pelo serviço de gerenciamento de licença do Core, que fornece informações e funcionalidade sobre licenças.
ILocalizationManagement	localization/	Interface que é implementada pelo serviço de localização comum com uma configuração persistente, que mantém, define e obtém a cultura atual do produto.
ILocalMountManagement	mounts/	Interface que é implementada pelo serviço de gerenciamento de montagens locais, usada para montar e desmontar imagens de volume no Core local.
ILoggingManagement	logs/	Replay.Core.Contracts.Logging.ILoggingManagement
ILogTruncationManagement	logtruncation/	Interface que é implementada pelo serviço de gerenciamento de truncamento de log do Core, que fornece a funcionalidade de truncamento de log.
INightlyJobsManagement	nightlyJobs/	API RESTful para trabalhos noturnos.
IProtectedItemsManagement	protectedItems/	Expõe itens protegidos, como agentes, clusters, nós de cluster e grupos, como uma árvore.
IPushInstallCommunication	pushinstallcomm/	API usada internamente para comunicação entre o Core e agente PushInstall. NOTA: Não use esta API diretamente.
IPushInstallManagement	pushinstall/	Interface que implementa a capacidade de instalar um agente em uma máquina remota. A instalação por push é uma funcionalidade que permite que o usuário inicie e controle instalações de agente em ambientes remotos em uma rede.

Tabela 1. Contratos de serviço do Core

Contrato de serviço	URI	Descrição
IRecoveryPointsManagement	recoveryPoints/	Interface que é implementada pelo serviço de gerenciamento de pontos de recuperação, que expõe informações sobre pontos de recuperação para clientes REST.
IRemoteMountManagement	remoteMounts/	Interface que é implementada pelo serviço de gerenciamento de montagens remotas, usada para desconectar imagens do volume montadas em máquinas remotas.
IReplayEngineManagement	replayEngine/	Interface que é implementada pelo serviço de gerenciamento do mecanismo Replay, que é usada para configurar e monitorar o mecanismo Replay.
IReplicationCommunication	replicationcomms/	API usada internamente para comunicação entre Cores para replicação. NOTA: Não use esta API diretamente.
IReplicationManagement	replication/	API para configuração, gerenciamento e monitoramento de replicação.
IReportingManagement	report/	Interface implementada pelo serviço de gerenciamento de relatórios do Core, que fornece funcionalidade de relatórios.
IRepositoryManagement	reposManagement/	Interface implementada pelo serviço de gerenciamento de repositório, que lida com as operações do Core relacionadas aos repositórios.
IRollbackManagement	rollback/	Interface implementada pelo serviço de reversão do core, que fornece funcionalidades do mecanismo Replay para restaurar a partir de um ponto de recuperação.
IRollupManagement	rollup/	Interface implementada pelo serviço de gerenciamento de rollup do core, que fornece a funcionalidade de rollup do mecanismo Replay.
ISeedDriveManagement	seedDrive/	Interface implementada pelo serviço de gerenciamento de unidade de propagação, que fornece funcionalidade de cópia e consumo do mecanismo Replay.
IServiceHostManagement	servicehost/	Interface implementada por uma classe que fornece uma interface de gerenciamento para o IServiceHost.
ISqlManagement	sql/	Interface implementada pelo serviço de gerenciamento de SQL do Core, que fornece verificações de capacidade de anexação e outras funcionalidades de gerenciamento de SQL específicas do Core
IStatusSummaryManagement	status/	Expõe informações resumidas de status sobre vários serviços no core que são usados para exibir ícones de status nas guias da GUI.
ITransferQueueManagement	xfer/queue/	API RESTful para a fila de transferência.
ITransferSchedulerManagement	xfer/schedule/	API RESTful para o programador de transferência.
IUtilitiesManagement	utilities/	API para diversos auxiliares.

Tabela 1. Contratos de serviço do Core

Contrato de serviço	URI	Descrição
IVirtualDiskManagement	vhd/	Replay.Common.Contracts.Virtualization.IVirtualDiskManagement
IWhiteLabelingManagement	whitelabeling/	Expõe as cadeias de caracteres personalizáveis.

IAgentDiagnosticsManagement

Esta seção descreve as operações de serviço disponíveis para IAgentDiagnosticsManagement em agentdiag/. São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ExecuteRemoteCommand
- GetLog
- RestartService
- UploadLogSessions

ExecuteRemoteCommand

Executa um comando remoto arbitrário.

URI: agentdiag/{agentId}/command/

Método HTTP: POST

GetLog

Obtém todo o conteúdo do arquivo replay.log.

URI: agentdiag/{agentId}/log/

Método HTTP: GET

RestartService

Interrompe, força o encerramento (se necessário) e reinicia o serviço.

URI: agentdiag/{agentId}/service/

Método HTTP: DELETE

UploadLogSessions

Carrega a sessão de log atual no Gibraltar (http://www.gibraltarsoftware.com/).

URI: agentdiag/{agentId}/log/

Método HTTP: POST

IAgentsGroupsManagement

Esta seção descreve as operações de serviço disponíveis para IAgentsGroupsManagement em agentGroups/. O contrato de serviço IAgentsGroupsManagement é a interface que é implementada pelo serviço de grupos, que realiza ações no Core relacionadas ao grupo.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddAgent
- AddGroup
- ChangeName
- GetGroups
- RemoveAgent
- RemoveGroup

AddAgent

Adiciona um agente protegido ao grupo.

URI: agentGroups/{groupId}/{agentId}

Método HTTP: POST

AddGroup

Adiciona um novo grupo.

URI: agentGroups/

Método HTTP: POST

ChangeName

Altera o nome do grupo.

URI: agentGroups/{groupId}/{newName}

Método HTTP: PUT

GetGroups

Obtém uma lista de todos os grupos que o Core conhece.

URI: agentGroups/

Método HTTP: GET

RemoveAgent

Remove um agente do grupo.

URI: agentGroups/{groupId}/{agentId}

Método HTTP: DELETE

RemoveGroup

Remove o grupo do Core.

URI: agentId}agentGroups/{groupId}

Método HTTP: DELETE

IAgentsManagement

Esta seção descreve as operações de serviço disponíveis para IAgentsManagement em agents/. O contrato de serviço IAgentsManagement é a interface implementada pelo serviço de agentes, que realiza ações no Core relacionadas ao agente.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddAgent
- AddAgents
- AddAgentWithVolumeGroupsValidation
- ChangeAgentDescriptor
- ChangeDisplayName
- ChangeHostName
- ChangePort
- CheckAgentPairing
- DeleteAgent
- DeleteAgents
- FindAgentById
- ForceAgentMetadataRefresh
- GetAgentDetails
- GetAgentInfo
- GetAgentInfoSummaries
- GetAgentMetadata
- GetAgentMetadataById
- GetAgentMetadataCredentials
- GetAgents
- GetAgentSummaryInfo
- GetAgentSummaryMetadatadata/sum
- GetAgentVolumeGroupsAvailableForProtection
- GetAgentVolumesAvailableForProtection
- GetCachedAgentMetadataById
- GetCachedAgentSummaryMetadataById
- GetPairingSettings
- GetProtectedAgents
- GetProtectedAgentsSummaries

- GetRecoveryPointsOnlyAgents
- GetRecoveryPointsOnlyAgentsSummaries
- GetReplicatedAgents
- GetReplicatedAgentsSummaries
- GetWriters
- IsClusterAddress
- RepairPairing
- SetAgentMetadataCredentials
- SetReplicatedAgentRepository
- ValidateAgentCreationParameters
- ValidateAgentCreationParametersForDeploy
- ValidateAgentProtectionAbility
- VerifyAgentVolumesAreNotInConflictWithRepositoryPaths
- VerifyConnect

AddAgent

Adiciona um agente que não está protegido atualmente, pareia com o agente e grava as informações de configuração de proteção.

URI: agents/new

Método HTTP: POST

AddAgents

Adiciona os agentes especificados que não estão protegidos atualmente. O software pareia com os agentes e grava sua configuração de proteção.

URI: agents/newagents

Método HTTP: POST

AddAgentWithVolumeGroupsValidation

Adiciona um agente que não está protegido atualmente, pareia com o agente, grava as informações de configuração de proteção e depois valida os grupos de proteção.

URI: agents/newWithValidGroups

Método HTTP: POST

ChangeAgentDescriptor

Altera o descritor que é usado para um agente existente, permitindo que o Core use um novo URI e novas credenciais especificadas pelo originador da chamada.

URI: agents/{agentId}/descriptor

Método HTTP: POST

ChangeDisplayName

Altera o nome de exibição usado pela GUI para um agente específico.

URI: agents/{agentId}/changeDisplayName/{newDisplayName}

Método HTTP: POST

ChangeHostName

Altera o nome de host usado para conectar a um agente específico.

URI: agents/{agentId}/changeHostName/{newHostName}

Método HTTP: POST

ChangePort

Altera a porta usada para conectar a um agente específico.

URI: agents/{agentId}/port

Método HTTP: POST

CheckAgentPairing

Conecta a um agente especificado no descritor (que provavelmente não é protegido atualmente pelo Core) e verifica se o agente está pareado ao Core ou a qualquer Core.

URI: agents/query/checkpairing

Método HTTP: PUT

DeleteAgent

Exclui um agente do Core; opcionalmente, exclui os pontos de recuperação do agente e também desabilita os volumes.

URI: agents/{agentId}/delete

Método HTTP: POST

DeleteAgents

Exclui agentes do core; opcionalmente, exclui os pontos de recuperação do agente e também desabilita os volumes.

URI: agents/delete

Método HTTP: POST

FindAgentById

Localiza informações sobre um agente protegido, caso existam.

URI: agents/find/{agentId}

Método HTTP: GET

ForceAgentMetadataRefresh

Força uma atualização de metadados para um agente com um ID especificado.

URI: agents/{agentId}/metadata/refresh

Método HTTP: POST

GetAgentDetails

Obtém todas as informações necessárias para exibir a página Detalhes do agente na GUI.

URI: agents/{agentId}/details

Método HTTP: GET

GetAgentInfo

Obtém informações sobre o agente protegido.

URI: agents/{agentId}/info

Método HTTP: GET

GetAgentInfoSummaries

Obtém uma lista de contratos de dados de resumo de informações para cada agente (protegido, replicado e somente replay). Esse é um método extremamente leve, que não realiza chamadas REST relacionadas a metadados e fornece informações muito limitadas.

URI: agents/infosummaries

Método HTTP: GET

GetAgentMetadata

Conecta a um agente (que provavelmente não é protegido atualmente pelo Core) especificado no descritor e solicita os metadados do agente.

URI: agents/query/metadata

Método HTTP: PUT

GetAgentMetadataById

Obtém os metadados mais recentes relativos a um agente protegido.

URI: agents/{agentId}/metadata

Método HTTP: GET

GetAgentMetadataCredentials

Obtém credenciais que são usadas para recuperar os metadados do agente com um ID específico.

URI: agents/{agentId}/metadata/credentials

Método HTTP: GET

GetAgents

Obtém uma lista de todos os agentes que o Core conhece.

URI: agents/

Método HTTP: GET

GetAgentSummaryInfo

Obtém informações resumidas sobre o agente, incluindo metadados resumidos, alertas associados recentes e pontos de recuperação recentes.

URI: agents/{agentId}/summaryInfo

Método HTTP: GET

GetAgentSummaryMetadataById

Obtém os metadados resumidos mais recentes relativos a um agente protegido pelo Core.

URI: agents/{agentId}/metadata/summary

Método HTTP: GET

GetAgentSummaryMetadatadata/sum

Conecta a um agente (que provavelmente não está sendo protegido pelo Core) especificado no descritor e solicita os metadados resumidos do agente.

URI: agents/query/summarymetadata

Método HTTP: PUT

GetAgentVolumeGroupsAvailableForProtection

Conecta a um agente (que provavelmente não está sendo protegido pelo Core) especificado no descritor e solicita a lista de volumes disponíveis para proteção e agrupados para refletir dependências de proteção. É possível que um agente e um Core sejam instalados na mesma máquina; portanto, a lista resultante não conteria volumes que contêm dados de repositório de Core ou diretórios de metadados. Em casos regulares, essa lista seria idêntica à lista de volumes retornada nos metadados.

URI: agents/query/availableGroups

Método HTTP: PUT

GetAgentVolumesAvailableForProtection

Conecta a um agente especificado no descritor (que provavelmente não está sendo protegido por este core) e solicita a lista de volumes disponíveis para proteção. É possível que um agente e um Core sejam instalados na mesma máquina; portanto, a lista resultante não conteria volumes que contêm dados de repositório de Core ou diretórios de metadados. Em casos regulares, essa lista seria idêntica à lista de volumes retornada nos metadados.

URI: agents/query/availablevolumes

Método HTTP: PUT

GetCachedAgentMetadataById

Obtém metadados armazenados em cache relativos a um agente protegido pelo Replay.

URI: agents/{agentId}/cachedmetadata

Método HTTP: GET

GetCachedAgentSummaryMetadataById

Obtém metadados resumidos armazenados em cache relativos a um agente protegido pelo Replay.

URI: agents/{agentId}/cachedmetadata/summary

Método HTTP: GET

GetPairingSettings

Conecta a um agente especificado no descritor (que provavelmente não está sendo protegido por esse Core) e solicita as informações de emparelhamento do agente.

URI: agents/query/pairing

Método HTTP: PUT

GetProtectedAgents

Obtém uma lista de agentes protegidos que o Core conhece.

URI: agents/protected

Método HTTP: GET

GetProtectedAgentsSummaries

Obtém uma lista de resumos de agentes protegidos que o Core conhece.

URI: agents/protectedSummaries

Método HTTP: GET

GetRecoveryPointsOnlyAgents

Obtém uma lista de pontos de recuperação somente de agente.

URI: agents/recoveryPointsOnly

Método HTTP: GET

GetRecoveryPointsOnlyAgentsSummaries

Obtém uma lista resumida de pontos de recuperação somente de agente.

URI: agents/recoveryPointsOnlySummaries

Método HTTP: GET

GetReplicatedAgents

Obtém uma lista de agentes replicados que o Core conhece.

URI: agents/replicated

Método HTTP: GET

GetReplicatedAgentsSummaries

Obtém uma lista de resumos de agentes replicados que o Core conhece.

URI: agents/replicatedSummaries

Método HTTP: GET

GetWriters

Obtém informações detalhadas sobre gravadores VSS instalados no agente.

URI: agents/{agentId}/writers

Método HTTP: GET

IsClusterAddress

Confirma se o endereço fornecido é um cluster.

URI: agents/verifyClusterAddress

Método HTTP: POST

RepairPairing

Tenta restabelecer o emparelhamento com um agente já protegido pelo Core, possivelmente usando credenciais novas.

URI: agents/pairing/repair

Método HTTP: POST

SetAgentMetadataCredentials

Define as credenciais usadas para recuperação de metadados do agente com o ID especificado.

URI: agents/{agentId}/metadata/credentials

Método HTTP: POST

SetReplicatedAgentRepository

Atribui um repositório a um agente que foi adicionado à replicação.

URI: agents/{agentId}/changeRepository/{repositoryId}

Método HTTP: POST

ValidateAgentCreationParameters

Valida parâmetros de criação de agente.

URI: agents/validateAgentCreationParameters

Método HTTP: POST

ValidateAgentCreationParametersForDeploy

Valida parâmetros de criação de agente para implementação.

URI: agents/validateAgentCreationParametersForDeploy

Método HTTP: POST

ValidateAgentProtectionAbility

Confirma se é possível proteger o Agent.

URI: agents/validateAgentProtectionAbility

Método HTTP: POST

VerifyAgentVolumesAreNotInConflictWithRepositoryPaths

Confirma se os volumes selecionados para proteção não estão em estado de conflito com qualquer dos caminhos de repositório especificados no ambiente do agente.

URI: agents/verifyVolumesConflictState

Método HTTP: POST

VerifyConnect

Tenta conectar ao agente e, em seguida, retorna o ID.

URI: agents/verifyConnection/?useNtlm={useNtlm}

Método HTTP: POST

IApplianceEventsManagement

Esta seção descreve as operações de serviço disponíveis para IApplianceEventsManagement em events/appliance/. O contrato de serviço IApplianceEventsManagement expõe os eventos de appliance para o Core.

São fornecidos o URI e o método HTTP da operação de serviço:

- SendApplianceEvent

SendApplianceEvent

Publica o evento aprovado.

URI: events/appliance/raise

Método HTTP: POST

IApplicationIdManagement

Esta seção descreve as operações de serviço disponíveis para IApplicationIdManagement em id/. O contrato de serviço IApplicationIdManagement expõe o ID exclusivo do aplicativo.

São fornecidos o URI e o método HTTP da operação de serviço:

- SendApplianceEvent

GetId

Obtém o ID do Core.

URI: id/

Método HTTP: GET

IAutoUpdateManagement

Esta seção descreve as operações de serviço disponíveis para IAutoUpdateManagement em autoupdate/.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CheckUpdates
- ForceUpgrade
- GetConfiguration
- GetState
- IsCoreServiceStarting
- SetConfiguration

CheckUpdates

Verifica se há atualizações.
URI: autoupdate/checkForUpdates
Método HTTP: GET

ForceUpgrade

Define a configuração de AutoUpdate.
URI: autoupdate/forceUpgrade
Método HTTP: POST

GetConfiguration

Define a configuração de AutoUpdate.
URI: autoupdate/config
Método HTTP: GET

GetState

Executa uma atualização.
URI: autoupdate/updateState
Método HTTP: GET

IsCoreServiceStarting

Retorna o valor "True" quando é determinado que o serviço Core foi reiniciado.
URI: autoupdate/isCoreServiceRestarting
Método HTTP: GET

SetConfiguration

Obtém o status de atualização atual.
URI: autoupdate/config
Método HTTP: PUT

IBackgroundJobManagement

Esta seção descreve as operações de serviço disponíveis para IBackgroundJobManagement em jobmgr/.

O contrato de serviço IBackgroundJobManagement é a interface de contrato WCF implementada por uma classe que implementa a interface de gerenciamento sobre o gerenciador de trabalho de segundo plano.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CancelChildJob
- CancelJob
- GetBackgroundJobsConfiguration
- GetJob
- GetJobs
- GetJobsByPage
- GetJobsCount
- ResetBackgroundJobSettings
- UpdateBackgroundJobSettings

CancelChildJob

Cancela o trabalho subordinado.
URI: jobmgr/jobs/{parentJobId}/childJobs/{childJobId}

Método HTTP: DELETE

CancelJob

Cancela o trabalho.
URI: jobmgr/jobs/{jobId}

Método HTTP: DELETE

GetBackgroundJobsConfiguration

Obtém a configuração de trabalhos de segundo plano.
URI: jobmgr/config
Método HTTP: GET

GetJob

Obtém o trabalho especificado.
URI: jobmgr/jobs/{jobId}
Método HTTP: GET

GetJobs

Obtém todos os trabalhos que passam pelo filtro especificado na memória e no banco de dados.
URI: jobmgr/jobs/all
Método HTTP: PUT

GetJobsByPage

Obtém a lista atual de trabalhos que passam pelo filtro especificado, que então são apresentados em uma grade paginada para facilitar a visualização.

URI: jobmgr/jobs/paged/{jobsPerPage}/{page}

Método HTTP: PUT

GetJobsCount

Obtém o número atual de trabalhos que passam pelo filtro especificado na memória e no banco de dados.

URI: jobmgr/jobs/count

Método HTTP: PUT

ResetBackgroundJobSettings

Redefine o trabalho de segundo plano para a definição padrão.

URI: jobmgr/resetSettings

Método HTTP: PUT

UpdateBackgroundJobSettings

Realiza uma atualização das definições de trabalho de segundo plano.

URI: jobmgr/settings

Método HTTP: PUT

IBackupManagement

Esta seção descreve as operações de serviço disponíveis para IBackupManagement em backup/.

O contrato de serviço IBackupManagement é a interface implementada pelo serviço de gerenciamento de cópia de segurança do Core, que é usada para criar uma cópia de segurança e restaurar um Core local.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- DeleteScheduledBackup
- GetBackupAgentRecoveryPointsInfo
- GetBackupAgentRecoveryPointsInfoByCore
- GetBackupManifest
- GetBackupManifests
- GetScheduledBackups
- GetWaitingJobs
- PauseScheduledBackup
- ResumeScheduledBackup
- SaveScheduledBackupSettings
- StartBackup
- StartCheckBackup
- StartRestore
- UpdateBackup

- UpdateRestore
- VerifyBackupLocation
- VerifyRestoreContent
- VerifyRestoreLocation

DeleteScheduledBackup

Exclui arquivos programados.
URI: backup/deleteScheduledBackups
Método HTTP: DELETE

GetBackupAgentRecoveryPointsInfo

Obtém os metadados de uma cópia de segurança de agente existente por agendId.
URI: backup/metadataByCore/agents/{agentId}
Método HTTP: POST

GetBackupAgentRecoveryPointsInfoByCore

Obtém os metadados de uma cópia de segurança de agente existente por agendId e coreId.
URI: backup/metadataByCore/{requestedCoreId}/agents/{agentId}
Método HTTP: POST

GetBackupManifest

Obtém os metadados de uma cópia de segurança do Core existente por coreId.
URI: backup/metadataByCore/{requestedCoreId}
Método HTTP: POST

GetBackupManifests

Obtém todos os metadados de uma cópia de segurança existente.
URI: backup/metadataAll
Método HTTP: POST

GetScheduledBackups

Recupera as definições de todas as cópias de segurança programadas.
URI: backup/scheduledBackups
Método HTTP: GET

GetWaitingJobs

Obtém uma lista de trabalhos de cópia de segurança e restauração em espera.
URI: backup/waiting
Método HTTP: GET

PauseScheduledBackup

Pausa arquivos programados.

URI: backup/pauseScheduledBackups
Método HTTP: POST

ResumeScheduledBackup

Retoma arquivos programados.
URI: backup/resumeScheduledBackups
Método HTTP: POST

SaveScheduledBackupSettings

Salva arquivos programados.
URI: backup/saveScheduledBackupSettings
Método HTTP: POST

StartBackup

Inicia uma cópia de segurança.
URI: backup/backup
Método HTTP: POST

StartCheckBackup

Inicia a verificação de uma cópia de segurança.
URI: backup/checkBackup
Método HTTP: POST

StartRestore

Inicia uma restauração.
URI: backup/restore
Método HTTP: POST

UpdateBackup

Atualiza a solicitação de trabalho de uma cópia de segurança existente.
URI: backup/backup/update/{jobId}
Método HTTP: POST

UpdateRestore

Atualiza a solicitação de trabalho de uma restauração existente.
URI: backup/restore/update/{jobId}
Método HTTP: POST

VerifyBackupLocation

Confirma se o caminho do sistema de arquivos correto foi especificado como local da cópia de segurança e se a cópia de segurança pode ser colocada nesse caminho.
URI: backup/verifyBackupLocation
Método HTTP: POST

VerifyRestoreContent

Confirma se o conteúdo da cópia de segurança não está em estado de conflito com máquinas atualmente protegidas.

URI: backup/verifyRestoreContent

Método HTTP: POST

VerifyRestoreLocation

Confirma se o trabalho de cópia de segurança foi concluído para o local e o Core especificados.

URI: backup/verifyCanStartRestore

Método HTTP: POST

IBootCdBuilderManagement

Esta seção descreve as operações de serviço disponíveis para IBootCdBuilderManagement em bootcdbuilder/.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetDefaultOutputPath
- StartBuildingIso
- ValidateDriverPackages
- VerifyBuildingIsoParameters

GetDefaultOutputPath

Obtém o caminho padrão no qual a imagem ISO resultante será colocada, caso o caminho de saída não tenha sido especificado explicitamente.

URI: bootcdbuilder/defaults

Método HTTP: GET

StartBuildingIso

Inicia uma nova tarefa de criação de imagem ISO.

URI: bootcdbuilder/start

Método HTTP: POST

ValidateDriverPackages

Realiza a validação dos pacotes de driver especificados.

URI: bootcdbuilder/validate

Método HTTP: POST

VerifyBuildingIsoParameters

Confirma se os parâmetros ISO estão construídos corretamente.

URI: bootcdbuilder/verify

Método HTTP: POST

ICloudManagement

Esta seção descreve as operações de serviço disponíveis para ICloudManagement em cloud/. O contrato de serviço ICloudManagement expõe a API de gerenciamento de nuvem.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddConfigurationAccount
- DeleteConfigurationAccount
- GetCloudConfiguration
- GetConfigurationAccount
- IsConfigurationAccountUsed
- ListFiles
- ListFolders
- ListItems
- SetCloudConfiguration
- StartDownload
- StartUpload
- UpdateConfigurationAccount
- VerifyConnect

AddConfigurationAccount

Adiciona uma conta à configuração de nuvem.

URI: cloud/configurationAccount

Método HTTP: POST

DeleteConfigurationAccount

Exclui uma conta existente da configuração de nuvem.

URI: cloud/configurationAccount/{accountId}

Método HTTP: DELETE

GetCloudConfiguration

Obtém a configuração de nuvem.

URI: cloud/config

Método HTTP: GET

GetConfigurationAccount

Obtém uma conta existente da configuração de nuvem.

URI: cloud/configurationAccount/{accountId}

Método HTTP: GET

IsConfigurationAccountUsed

Verifica se uma conta de nuvem é usada, por exemplo, para arquivo programado.

URI: cloud/isConfigurationAccountUsed/{accountId}

Método HTTP: GET

ListContainers

Obtém contêineres de nuvem.

URI: cloud/containers?accountId={0}

Método HTTP: GET

ListFiles

Obtém arquivos de nuvem.

URI: cloud/items

Método HTTP: PUT

ListFolders

Obtém pastas de nuvem.

URI: cloud/items

Método HTTP: PUT

ListItems

Obtém arquivos e pastas de nuvem.

URI: cloud/items

Método HTTP: PUT

SetCloudConfiguration

Define a configuração de nuvem.

URI: cloud/config

Método HTTP: PUT

StartDownload

Inicia um download.

URI: cloud/download

Método HTTP: PUT

StartUpload

Inicia um upload.

URI: cloud/upload

Método HTTP: PUT

UpdateConfigurationAccount

Edita uma conta existente de configuração de nuvem.

URI: cloud/configurationAccount

Método HTTP: PUT

VerifyConnect

Confirma a disponibilidade da nuvem.

URI: cloud/verifyConnect

Método HTTP: GET

IClustersManagement

Esta seção descreve as operações de serviço disponíveis para IClustersManagement em clusters/. O contrato de serviço IClustersManagement expõe a API de gerenciamento de cluster.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddClusterAgent
- AddClusterNodeAgent
- ConvertAgentToClusterNode
- ConvertClusterNodeToAgent
- GetClusterNodes
- GetRecommendedClusterRepositoryIds
- GetReplicatedClusterNodes

AddClusterAgent

Adiciona um nó de cluster a um cluster existente.

URI: clusters/new

Método HTTP: PUT

AddClusterNodeAgent

Adiciona um nó de cluster a um cluster existente.

URI: clusters/{clusterId}/nodes/new

Método HTTP: POST

ConvertAgentToClusterNode

Converte um agente regular em nó de cluster.

URI: clusters/{agentId}/convertToNode

Método HTTP: POST

ConvertClusterNodeToAgent

Converte um nó de cluster em agente regular.

URI: clusters/{clusterNodeId}/convertToAgent

Método HTTP: POST

GetClusterNodes

Obtém uma lista de nós de cluster de um agente de cluster especificado.

URI: clusters/clusterNodes/{clusterAgentId}

Método HTTP: GET

GetRecommendedClusterRepositoryIds

Obtém uma lista de IDs de repositório de uso recomendado para nós de cluster.

URI: clusters/recommendedRepositories/{clusterAgentId}

Método HTTP: GET

GetReplicatedClusterNodes

Obtém uma lista de nós de cluster replicados de um agente de cluster especificado.

URI: clusters/replicatedClusterNodes/{clusterAgentId}

Método HTTP: GET

ICoreBackupRestoreManagement

Esta seção descreve as operações de serviço disponíveis para ICoreBackupRestoreManagement em corebackuprestore/.

O contrato de serviço ICoreBackupRestoreManagement é a interface implementada pelo serviço de gerenciamento de cópia de segurança/restauração do Core, usada para criação de cópia de segurança e restauração das configurações do Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- BackupCoreConfiguration
- ReadRepositoriesFromBackupSettings
- RestoreCoreConfiguration
- RestoreCoreConfigurationWithRestart
- ValidateRepositoryDirectory

BackupCoreConfiguration

Cria uma cópia de segurança da configuração do Core.

URI: corebackuprestore/backup

Método HTTP: POST

ReadRepositoriesFromBackupSettings

Realiza a validação de caminhos de repositório no arquivo de configuração de cópia de segurança. Retorna um dicionário.

URI: corebackuprestore/validatexml

Método HTTP: POST

RestoreCoreConfiguration

Realiza a restauração da configuração do Core.

URI: corebackuprestore/restore

Método HTTP: POST

RestoreCoreConfigurationWithRestart

Realiza a restauração da configuração do Core. O serviço Core será reiniciado para aplicar as novas configurações.

URI: corebackuprestore/restoreWithRestart

Método HTTP: POST

ValidateRepositoryDirectory

Realiza a validação do caminho de diretório do repositório. Quando o caminho é confirmado, o valor "True" é retornado.

URI: corebackuprestore/validatedirectory

Método HTTP: POST

ICoreCallbackManagement

Esta seção descreve as operações de serviço disponíveis para ICoreCallbackManagement em corecallback/.

O contrato de serviço ICoreCallbackManagement é a interface implementada pelo serviço de gerenciamento de retorno de chamada do Core, usada para ser chamada pelo agente remoto.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ProcessAgentProtectionRequest
- VerifyConnect

ProcessAgentProtectionRequest

O método é chamado pelo agente de ativação pós-falha para realizar emparelhamento remoto. Esse método é apenas para uso interno.

URI: corecallback/agentprotectionrequest

Método HTTP: POST

VerifyConnect

Chamado por um agente para confirmar a conectividade com esse Core.

URI: corecallback/connect

Método HTTP: GET

ICoreDiagnosticsManagement

Esta seção descreve as operações de serviço disponíveis para ICoreDiagnosticsManagement em corediag/.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CollectServerLogs
- GetAggregateStatus
- GetDiskSubsystemStatus
- GetServerLogs
- GetServerLogsInfo
- GetSystemHWStatus
- StartGatheringDiagnosticInfo
- UploadLogSessions

CollectServerLogs

Começa a coletar logs de servidor por meio de um trabalho de segundo plano.

URI: corediag/collectLogs

Método HTTP: POST

GetAggregateStatus

Obtém o status do sistema agregado de um provedor AMC.

URI: corediag/systemAggregateStatus

Método HTTP: GET

GetDiskSubsystemStatus

Obtém o status do subsistema de disco de um provedor AMC.

URI: corediag/diskSubsystemStatus

Método HTTP: GET

GetServerLogs

Obtém todo o conteúdo dos arquivos de log de servidor arquivados.

URI: corediag/serverLogs/

Método HTTP: GET

GetServerLogsInfo

Obtém o nome e a data e hora de criação em UTC do arquivo atual com os logs de servidor.

URI: corediag/serverLogsArchiveName

Método HTTP: GET

GetSystemHWStatus

Obtém o status do hardware do sistema de um provedor AMC.

URI: corediag/systemHWStatus

Método HTTP: GET

StartGatheringDiagnosticInfo

Começa a coletar informações de diagnóstico por meio de um trabalho de segundo plano e, em seguida, retorna a seguinte resposta: StartGatheringDiagnosticInformationResponse.

URI: corediag/diagnostic-info/

Método HTTP: POST

UploadLogSessions

Carrega os logs atuais do Core e de todos os agentes protegidos que estejam online no Gibraltar (http://www.gibraltarsoftware.com/) por meio de um trabalho de segundo plano. Nada é retornado.

URI: corediag/logs/

Método HTTP: POST

ICoreMetadataManagement

Esta seção descreve as operações de serviço disponíveis para ICoreMetadataManagement em metadata/.

O contrato de serviço ICoreMetadataManagement é a interface implementada pelo serviço de metadados do Core, que mantém, armazena em cache e retorna metadados do Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetCached
- GetCachedSummary
- GetCurrent
- GetCurrentSummary
- GetStartupGuideFinished
- SetStartupGuideFinished

GetCached

Obtém metadados do Core armazenados em cache.

URI: metadata/cached

Método HTTP: GET

GetCachedSummary

Obtém metadados resumidos do Core armazenados em cache.

URI: metadata/cachedsummary

Método HTTP: GET

GetCurrent

Obtém os metadados atuais do Core.

URI: metadata/

Método HTTP: GET

GetCurrentSummary

Obtém os metadados resumidos atuais do Core.
URI: metadata/summary
Método HTTP: GET

GetStartupGuideFinished

Obtém o valor que indica se o guia de inicialização deve ser mostrado.
URI: metadata/getStartupGuideFinished
Método HTTP: GET

SetStartupGuideFinished

Obtém o valor que indica se o assistente de configuração deve ser mostrado durante a inicialização.
URI: metadata/setStartupGuideFinished/{finished}
Método HTTP: POST

ICoreSettingsManagement

Esta seção descreve as operações de serviço disponíveis para ICoreSettingsManagement em settings/.

O contrato de serviço ICoreSettingsManagement permite consultar e definir diversas definições do Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetClientTimeout
- GetCoreInstallPath
- GetCoreSettings
- SetClientTimeout
- SetCoreSettings

GetClientTimeout

Obtém as definições de tempo limite que são usadas em comunicação REST e de socket.

URI: settings/clientTimeout

Método HTTP: GET

GetCoreInstallPath

Obtém o caminho do diretório onde estão localizados os instaladores do Agent e do Local Mount Utility.
URI: settings/installersPath
Método HTTP: GET

GetCoreSettings

Obtém as definições globais gerais do Core, como, por exemplo, definições de tempo limite e nome de exibição.
URI: settings/core
Método HTTP: GET

SetClientTimeout

Aplica definições de tempo limite que são usadas em comunicação REST e de socket.

URI: settings/clientTimeout

Método HTTP: PUT

SetCoreSettings

Aplica definições globais gerais do Core, como, por exemplo, definições de tempo limite e nome de exibição.

URI: settings/core

Método HTTP: PUT

IDatabaseStorageManagement

Esta seção descreve as operações de serviço disponíveis para IDatabaseStorageManagement em databaseStorage/.

O contrato de serviço IDatabaseStorageManagement é a interface para comunicação e configuração do armazenamento de banco de dados persistente usado para armazenamento de informações sobre eventos e relatórios.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetDatabaseStorageConfiguration
- GetDefaultDatabaseStorageConfiguration
- SetDatabaseStorageConfiguration
- TestConnection

GetDatabaseStorageConfiguration

Obtém a configuração do armazenamento em banco de dados (como, por exemplo, definições de conexão ao servidor de banco de dados, período de retenção de dados no banco de dados, tempo limite de conexão).

URI: databaseStorage/configuration

Método HTTP: GET

GetDefaultDatabaseStorageConfiguration

Obtém a configuração padrão de armazenamento em banco de dados.

URI: databaseStorage/defaults

Método HTTP: GET

SetDatabaseStorageConfiguration

Define a configuração de armazenamento em banco de dados (como, por exemplo, definições de conexão ao servidor de banco de dados, período de retenção de dados no banco de dados, tempo limite de conexão).

URI: databaseStorage/configuration

Método HTTP: PUT

TestConnection

Testa a conexão com a instância de armazenamento em banco de dados usando as definições de conexão especificadas.

URI: databaseStorage/connection

Método HTTP: POST

IDiagnosticsManagement

Esta seção descreve as operações de serviço disponíveis para IDiagnosticsManagement em diag/.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ExecuteRemoteCommand
- GetLog
- GetLogSession
- ReadFile
- RestartService
- UploadLogSessions

ExecuteRemoteCommand

Executa um comando remoto arbitrário.

URI: diag/command/

Método HTTP: POST

GetLog

Obtém todo o conteúdo do arquivo replay.log.

URI: diag/log/

Método HTTP: GET

GetLogSession

Empacota a sessão de log atual e a retorna como um fluxo de bytes. O conteúdo do fluxo é um Gibraltar (arquivo .glp).

URI: diag/logSession/

Método HTTP: GET

ReadFile

Lê um arquivo no sistema de arquivos local e o envia por fluxo de dados de volta ao cliente.

URI: diag/files/?q={path}

Método HTTP: GET

RestartService

Interrompe, força o encerramento (se necessário) e reinicia o serviço.

URI: diag/service/

Método HTTP: DELETE

UploadLogSessions

Carrega a sessão de log atual na estrutura de logs do Gibraltar (http://www.gibraltarsoftware.com/).
URI: diag/logSession/
Método HTTP: POST

IEmailsManagement

Esta seção descreve as operações de serviço disponíveis para IEmailsManagement em emailsmgr/.

O contrato IEmailsManagementservice é a interface de contrato WCF para o gerenciamento de e-mails.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetSmtpServerSettings
- IsConfigured
- SendTestEmail
- SetSmtpServerSettings

GetSmtpServerSettings

Retorna as definições de server de SMTP da configuração do serviço de e-mail.
URI: emailsmgr/settings
Método HTTP: GET

IsConfigured

Indica se as definições de server de SMTP foram definidas pelo usuário.
URI: emailsmgr/settings/check
Método HTTP: GET

SendTestEmail

Gera e envia um e-mail de teste usando a configuração de e-mail especificada.
URI: emailsmgr/config/test
Método HTTP: PUT

SetSmtpServerSettings

Define as definições de server de SMTP na configuração do serviço de e-mail.
URI: emailsmgr/settings
Método HTTP: PUT

IEncryptionKeyManagement

Esta seção descreve as operações de serviço disponíveis para IEncryptionKeyManagement em encryption/.

O contrato de serviço IEncryptionKeyManagement é o gerenciamento de chave de criptografia usado em conjunto com os repositórios e serviços dependentes.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ChangeKeyStatusToReplication
- ChangeKeyStatusToUniversal
- ChangePassphrase
- Create
- DeleteKey
- Export
- GetFilteredKeys
- GetKeys
- Import
- LockKey
- SerializedExport
- SerializedImport
- UnlockKey
- UpdateDescription

ChangeKeyStatusToReplication

Altera o status da chave para "Chave de replicação". Retorna informações atualizadas sobre a chave.
URI: encryption/changeKeyStatusToReplication/{keyId}
Método HTTP: POST

ChangeKeyStatusToUniversal

Altera o status da chave para "Chave universal". Retorna informações atualizadas sobre a chave.
URI: encryption/changeKeyStatusToUniversal
Método HTTP: POST

ChangePassphrase

Altera a frase de acesso da chave especificada.
URI: encryption/passphrase
Método HTTP: POST

Create

Cria uma nova chave com o nome e frase de acesso especificados.
URI: encryption/
Método HTTP: POST

DeleteKey

Exclui uma chave de criptografia ou emite uma exceção se a chave selecionada for usada.

URI: encryption/delete/{keyId}
Método HTTP: DELETE

Export

Exporta uma chave.
URI: encryption/{keyId}
Método HTTP: GET

GetFilteredKeys

Obtém a lista filtrada de chaves de criptografia. Passa o tipo das chaves como parâmetro.
URI: encryption/
Método HTTP: GET

GetKeys

Obtém a lista de chaves de criptografia.
URI: encryption/
Método HTTP: GET

Import

Importa uma chave exportada. Retorna informações sobre a chave importada.
URI: encryption/import
Método HTTP: POST

LockKey

Bloqueia a chave especificada. Retorna informações atualizadas sobre a chave.
URI: encryption/lock/{keyId}
Método HTTP: POST

SerializedExport

Retorna uma representação binária serializada de uma chave de criptografia com base no ID de chave fornecido.
URI: encryption/{keyId}/serialized
Método HTTP: GET

SerializedImport

Importa uma chave de criptografia com base na representação binária serializada fornecida. Retorna informações sobre a chave importada.
URI: encryption/serimport
Método HTTP: POST

UnlockKey

Desbloqueia a chave especificada. Retorna informações atualizadas sobre a chave.
URI: encryption/unlock
Método HTTP: POST

UpdateDescription

Atualiza o nome e o comentário de uma chave existente. Retorna informações atualizadas sobre a chave.

URI: encryption/{keyId}

Método HTTP: PUT

IEventsManagement

Esta seção descreve as operações de serviço disponíveis para IEventsManagement em events/. O contrato de serviço IEventsManagement expõe os eventos e alertas no Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- DismissAllAgentAlerts
- DismissAllCoreAlerts
- DismissEvent
- GetAgentAlertsByPage
- GetAgentAlertsCount
- GetAgentAlertsSettings
- GetAgentEventsByPage
- GetAgentEventsCount
- GetAllAgentAlerts
- GetAllAgentEvents
- GetAllCoreAlerts
- GetAllCoreEvents
- GetCachedEventsByDate
- GetConfiguration
- GetCoreAlertsByPage
- GetCoreAlertsCount
- GetCoreEventsByPage
- GetCoreEventsCount
- GetDetailsForEvent
- GetEventsByDate
- GetEventTypes
- SendTestEmail
- SetAgentAlertsSettings
- SetConfiguration

DismissAllAgentAlerts

Obtém as informações resumidas de todos os alertas associados ao agente especificado. Observe que essa lista pode ser muito extensa.

URI: events/agents/{agentId}/all

Método HTTP: DELETE

DismissAllCoreAlerts

Marca todos os alertas do Core como lidos, retirando-os da lista de alertas.

URI: events/core/all

Método HTTP: DELETE

DismissEvent

Marca um evento como lido, retirando-o da lista de eventos.

URI: events/event/{eventId}

Método HTTP: DELETE

GetAgentAlertsByPage

Obtém informações resumidas sobre alertas de um ID de agente específico, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: events/agents/{agentId}/alerts/paged?max={max}&page={page}

Método HTTP: GET

GetAgentAlertsCount

Obtém a contagem de alertas não ignorados de um agente especificado.

URI: events/agents/{agentId}/alertsCount

Método HTTP: GET

GetAgentAlertsSettings

Retorna as definições de alerta do agente especificado, como, por exemplo, conteúdo de e-mail e definições de notificação.

URI: events/config/agents/{agentId}

Método HTTP: GET

GetAgentEventsByPage

Obtém informações resumidas sobre eventos para um determinado ID de agente, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: events/agents/{agentId}/paged?max={max}&page={page}

Método HTTP: GET

GetAgentEventsCount

Obtém a contagem de eventos do agente especificado.

URI: events/agents/{agentId}/eventsCount

Método HTTP: GET

GetAllAgentAlerts

Obtém as informações resumidas de todos os alertas associados ao agente especificado. Observe que essa lista pode ser muito extensa.

URI: events/agents/{agentId}/alerts/all

Método HTTP: GET

GetAllAgentEvents

Obtém as informações resumidas sobre todos os eventos associados ao agente especificado. Observe que essa lista pode ser muito extensa.

URI: events/agents/{agentId}/all

Método HTTP: GET

GetAllCoreAlerts

Obtém as informações resumidas sobre todos os alertas associados ao Core. Observe que essa lista pode ser muito extensa.

URI: events/core/alerts/all

Método HTTP: GET

GetAllCoreEvents

Obtém as informações resumidas sobre todos os eventos associados ao Core. Observe que essa lista pode ser muito extensa.

URI: events/core/all

Método HTTP: GET

GetCachedEventsByDate

Obtém as informações resumidas sobre todos os eventos armazenados em cache associados ao Core especificado, organizados por data.

URI: events/cachedEventsDateParam

Método HTTP: PUT

GetConfiguration

Retorna informações de configuração sobre eventos como conteúdo de e-mail e definições de notificação.

URI: events/config

Método HTTP: GET

GetCoreAlertsByPage

Obtém informações resumidas sobre eventos do Core, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: events/core/alerts/paged?max={max}&page={page}

Método HTTP: GET

GetCoreAlertsCount

Obtém a contagem de alertas não ignorados do Core.

URI: events/core/alertsCount

Método HTTP: GET

GetCoreEventsByPage

Obtém informações resumidas sobre eventos do Core, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: events/core/paged?max={max}&page={page}

Método HTTP: GET

GetCoreEventsCount

Obtém a contagem de eventos do Core.
URI: events/core/eventsCount
Método HTTP: GET

GetDetailsForEvent

Obtém os detalhes de um único evento.
URI: events/event/{eventId}
Método HTTP: GET

GetEventsByDate

Obtém as informações resumidas sobre todos os eventos associados ao Core especificado, organizadas por data.
URI: events/EventsDateRange
Método HTTP: PUT

GetEventTypes

Obtém a lista de todos os tipos possíveis de eventos, organizados em grupos.
URI: events/types
Método HTTP: GET

SendTestEmail

Gera e envia uma notificação de teste por e-mail com base na configuração de e-mail especificada.
URI: events/config/email/test
Método HTTP: PUT

SetAgentAlertsSettings

Ajusta as definições de alerta do agente especificado, como conteúdo de e-mail e definições de notificação.
URI: events/config/agents/{agentId}
Método HTTP: PUT

SetConfiguration

Define informações de configuração de eventos, como conteúdo de e-mail e definições de notificação.
URI: events/config
Método HTTP: PUT

IExchangeManagement

Esta seção descreve as operações de serviço disponíveis para IExchangeManagement em exchange/. O contrato de serviço IExchangeManagement expõe o gerenciamento do MS Exchange no Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ForceChecksumCheck
- ForceMountabilityCheck
- GetAgentExchangeServerSettings
- GetChecksumCheckQueueConfiguration
- GetChecksumCheckQueueContents
- GetChecksumCheckQueueEntry
- GetMountabilityQueueConfiguration
- GetMountabilityQueueContents
- GetMountabilityQueueEntry
- SetAgentExchangeServerSettings
- SetChecksumCheckConfiguration
- SetMountabilityConfiguration
- VerifyCredentials

ForceChecksumCheck

Força a verificação de soma de verificação do ponto de recuperação especificado.
URI: exchange/checksumcheck/{recoveryPointId}/force
Método HTTP: POST

ForceMountabilityCheck

Força a confirmação de capacidade de montagem do ponto de recuperação especificado.
URI: exchange/mountabilitycheck/{recoveryPointId}/force
Método HTTP: POST

GetAgentExchangeServerSettings

Obtém as definições de servidor do Exchange do agente.
URI: exchange/agents/{agentId}/exchangeSettings
Método HTTP: GET

GetChecksumCheckQueueConfiguration

Obtém a configuração da fila de verificação de soma de verificação.
URI: exchange/checksumcheckconfig
Método HTTP: GET

GetChecksumCheckQueueContents

Obtém o conteúdo da fila de verificação de soma de verificação.
URI: exchange/checksumcheckentries
Método HTTP: GET

GetChecksumCheckQueueEntry

Obtém as informações de uma entrada específica na fila de verificação de soma de verificação.
URI: exchange/checksumcheckentries/{entryid}
Método HTTP: GET

GetMountabilityQueueConfiguration

Obtém a configuração da fila de capacidade de montagem.
URI: exchange/mountabilityConfig
Método HTTP: GET

GetMountabilityQueueContents

Obtém o conteúdo da fila de montabilidade.
URI: exchange/mountabilityentries
Método HTTP: GET

GetMountabilityQueueEntry

Obtém as informações sobre uma entrada específica da fila de montabilidade.
URI: exchange/mountabilityentries/{entryid}
Método HTTP: GET

SetAgentExchangeServerSettings

Ajusta as definições de servidor do Exchange do agente.
URI: exchange/agents/{agentId}/exchangeSettings
Método HTTP: PUT

SetChecksumCheckConfiguration

Ajusta a configuração da fila de verificação de soma de verificação.
URI: exchange/checksumcheckconfig
Método HTTP: POST

SetMountabilityConfiguration

Ajusta a configuração da fila de montabilidade.
URI: exchange/mountabilityConfig
Método HTTP: POST

VerifyCredentials

Confirma as credenciais para a instância do Exchange. Emite uma exceção no caso de falha de validação.
URI: exchange/agent/{agentId}/verifyExchangeCredentials
Método HTTP: PUT

IExportQueueManagement

Esta seção descreve as operações de serviço disponíveis para IExportQueueManagement em export/queue/. O contrato de serviço IExportQueueManagement é uma API RESTful da fila de exportação.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CancelAllExports
- CancelExports
- GetConfiguration
- GetEntryInfo
- GetQueueContents
- SetConfiguration

CancelAllExports

Cancela todas as exportações na fila.
URI: export/queue/entries
Método HTTP: DELETE

CancelExports

Cancela as entradas da fila de exportação identificadas pelos IDs de exportação.
URI: export/queue/entries/cancel
Método HTTP: POST

GetConfiguration

Obtém a configuração da fila de exportação de VM.
URI: export/queue/config
Método HTTP: GET

GetEntryInfo

Obtém as informações de uma entrada específica na fila de exportação.
URI: export/queue/entries/{exportid}
Método HTTP: GET

GetQueueContents

Obtém o conteúdo da fila de exportação.
URI: export/queue/entries
Método HTTP: GET

SetConfiguration

Define a configuração da fila de exportação de VM.
URI: export/queue/config
Método HTTP: POST

IExportSchedulerManagement

Esta seção descreve as operações de serviço disponíveis para IExportSchedulerManagement em export/scheduler/. O contrato de serviço IExportSchedulerManagement é uma API RESTful do programador de exportação.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- DeleteAgentExportConfiguration
- DeleteEC2Credentials
- ForceExport
- GetAgentExportConfiguration
- GetAllAgentsExportConfiguration
- GetAllAgentsExportStatus
- GetAllAgentsExportStatusWithAdHoc
- GetAllEC2Credentials
- GetEC2Credentials
- GetEc2Environment
- GetFreeSpaceOnNetworkShare
- GetGroupAgentsExportStatus
- GetHyperVCapabilities
- GetVSphereServerInformation
- SetAgentExportConfiguration
- UpdateEC2Credentials
- ValidateEC2Credentials
- ValidateExportLocation
- ValidateHyperVCredentials
- ValidateHyperVDiskExists
- ValidateHyperVRoleIsInstalled
- ValidateHyperVUefiPartitionByAgentId
- ValidateHyperVUefiPartitionByRecoveryPointId
- ValidateRemoteLinuxMachineCredentials
- ValidateStoragePoolSettings
- ValidateSystemVolumeDiskLocation
- ValidateVirtualBoxInstalled
- ValidateVirtualBoxUefiPartition
- ValidateWindowsMachineCredentials

DeleteAgentExportConfiguration

Exclui a configuração de exportação do agente.

URI: export/schedule/{agentId}/pgs

Método HTTP: DELETE

DeleteEC2Credentials

Exclui uma credencial EC2.

URI: export/schedule/ec2/credentials/{key}

Método HTTP: DELETE

ForceExport

Inicia imediatamente a exportação de VM de um ponto de recuperação que corresponde ao agente especificado. O ponto de recuperação e o tipo de VM resultante (Workstation, EC2 ou ESXi) devem ser especificados na instância de solicitação.

URI: export/schedule/{agentId}/export

Método HTTP: POST

GetAgentExportConfiguration

Obtém a configuração de exportação do agente.

URI: export/schedule/{agentId}/pgs

Método HTTP: GET

GetAllAgentsExportConfiguration

Obtém a configuração de exportação de todos os agentes.

URI: export/schedule/agents/allExportConfig

Método HTTP: GET

GetAllAgentsExportStatus

Obtém um resumo do status de exportação de todos os agentes no Core para os quais o Standby virtual está ativado.

URI: export/schedule/agents/all

Método HTTP: GET

GetAllAgentsExportStatusWithAdHoc

Obtém um resumo do status de exportação de todos os agentes no Core. Inclui exportações Ad Hoc e exportações de Standby virtual.

URI: export/schedule/agents/alladhoc

Método HTTP: GET

GetAllEC2Credentials

Obtém todas as credenciais de EC2.

URI: export/schedule/ec2/credentials

Método HTTP: GET

GetEC2Credentials

Obtém credenciais de EC2 específicas.

URI: export/schedule/ec2/credentials/{key}

Método HTTP: GET

GetEc2Environment

Obtém informações sobre segurança de EC2 específicas de um ambiente cujo método está sendo chamado.

URI: export/schedule/ec2/environment/{credentialKey}

Método HTTP: GET

GetFreeSpaceOnNetworkShare

Valida um caminho de compartilhamento UNC.

URI: export/schedule/uncshare/validate

Método HTTP: POST

GetGroupAgentsExportStatus

Obtém um resumo do status de exportação de todos os agentes no grupo especificado para os quais o Standby virtual está ativado.

URI: export/schedule/groups/{groupId}/all

Método HTTP: GET

GetHyperVCapabilities

Obtém recursos de Hyper-V.

URI: export/schedule/hyperv/capabilities

Método HTTP: POST

GetVSphereServerInformation

Recupera os detalhes sobre um servidor VSphere para funcionalidade de UI.

URI: export/schedule/vsphere/info

Método HTTP: POST

SetAgentExportConfiguration

Define a configuração de exportação do agente.

URI: export/schedule/{agentId}/pgs

Método HTTP: PUT

UpdateEC2Credentials

Cria ou atualiza uma credencial de EC2.

URI: export/schedule/ec2/credentials

Método HTTP: POST

ValidateEC2Credentials

Valida uma credencial de EC2.

URI: export/schedule/ec2/validate

Método HTTP: POST

ValidateExportLocation

Valida o local de uma máquina virtual.
URI: export/schedule/vm/location/validate
Método HTTP: POST

ValidateHyperVCredentials

Valida uma credencial de Hyper-V.
URI: export/schedule/hyperv/credentials
Método HTTP: POST

ValidateHyperVDiskExists

Valida a existência de um disco Hyper-V.
URI: export/schedule/hyperv/location/{path}
Método HTTP: POST

ValidateHyperVRoleIsInstalled

Valida credenciais de Hyper-V.
URI: export/schedule/hyperv/role
Método HTTP: POST

ValidateHyperVUefiPartitionByAgentId

Valida se essa máquina possui partição UEFI por identificador de agente.
URI: export/schedule/hyperv/validateUefiByAgent/{agentId}
Método HTTP: POST

ValidateHyperVUefiPartitionByRecoveryPointId

Valida se essa máquina possui partição UEFI por identificador de ponto de recuperação.
URI: export/schedule/hyperv/validateUefiByRecoveryPoints/{recoveryPointId}
Método HTTP: POST

ValidateRemoteLinuxMachineCredentials

Valida credenciais de VirtualBox.
URI: export/schedule/vbox/credentials
Método HTTP: POST

ValidateStoragePoolSettings

Valida se o recurso de pool de armazenamento foi ativado na máquina protegida.
URI: export/schedule/storagepool/{agentId}
Método HTTP: POST

ValidateSystemVolumeDiskLocation

Valida o local de uma máquina virtual.

URI: export/schedule/systemvolume/location/validate
Método HTTP: POST

ValidateVirtualBoxInstalled

Valida se o VirtualBox está instalado na máquina local/remota.
URI: export/schedule/vbox/installed?isVirtualMachineUpdating={isVirtualMachineUpdating}
Método HTTP: POST

ValidateVirtualBoxUefiPartition

Valida se a configuração da VM de destino possui suporte de UEFI.
URI: export/schedule/vbox/uefi/validate/{agentId}/{recoveryPointId}
Método HTTP: PUT

ValidateWindowsMachineCredentials

Valida credenciais de Windows do VirtualBox.
URI: export/schedule/vbox/wincredentials/{path}/{userName}
Método HTTP: POST

IHyperVAgentManagement

Esta seção descreve as operações de serviço disponíveis para IHyperVAgentManagement em hypervagent/.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddDvdDrive
- AddIsoImage
- AddNetworkAdapter
- AttachVirtualDisk
- DeleteVirtualMachine
- DetachVirtualDisk
- EndSession
- GetAvailableVirtualNetworks
- GetMaximumProcessorCount
- GetOrCreateVirtualMachineAndAttach
- GetSnapshotsCount
- GetVirtualDisks
- GetVirtualMachineName
- InsertIntegrationServices
- PingSession
- RenameVirtualMachine
- SetProcessorCount
- SetRamMegabytes

- VerifyConnection

AddDvdDrive

Adiciona uma unidade de DVD à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/dvd
PUT

AddIsoImage

Adiciona uma imagem ISO a uma unidade de DVD. Cria a unidade de DVD, caso ela não exista.
URI: hypervagent/{virtualMachineId}/iso/{isoPath}
Método HTTP: PUT

AddNetworkAdapter

Adiciona um novo adaptador de rede à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/nic/{networkAdapterName}
Método HTTP: PUT

AttachVirtualDisk

Conecta um disco virtual à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/disks/{diskPath}/{storageController}
Método HTTP: PUT

DeleteVirtualMachine

Exclui a máquina virtual atual e desconecta-se dela.
URI: hypervagent/existent/{virtualMachineId}
Método HTTP: DELETE

DetachVirtualDisk

Desconecta um disco virtual da máquina virtual atual.
hypervagent/{virtualMachineId}/disks/{diskPath}
Método HTTP: DELETE

EndSession

Determina ao Hyper-V Agent que conclua a sessão com a máquina virtual.
URI: hypervagent/{virtualMachineId}/endsession
Método HTTP: DELETE

GetAvailableVirtualNetworks

Obtém uma lista de adaptadores de rede virtuais disponíveis para uma máquina virtual no servidor Hyper-V.
URI: hypervagent/{virtualMachineId}/availablevirtualnetworks
Método HTTP: GET

GetMaximumProcessorCount

Obtém o número máximo de CPUs virtuais que podem ser conectadas a uma máquina virtual.
URI: hypervagent/cpu/{operatingSystemFamily}
Método HTTP: GET

GetOrCreateVirtualMachineAndAttach

Obtém ou cria a máquina virtual especificada no parâmetro de solicitação.
URI: hypervagent/getOrCreate
Método HTTP: POST

GetSnapshotsCount

Obtém a contagem de snapshots da máquina virtual.
URI: hypervagent/{virtualMachineId}/getSnapshotsCount
Método HTTP: GET

GetVirtualDisks

Obtém uma lista de discos virtuais conectados à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/disks
Método HTTP: GET

GetVirtualMachineName

Obtém o nome da máquina virtual atual.
URI: hypervagent/{virtualMachineId}/name
Método HTTP: GET

InsertIntegrationServices

Monta o disco de instalação dos serviços de integração.
URI: hypervagent/{virtualMachineId}/integrationservices
Método HTTP: PUT

PingSession

Indica que a sessão ainda está em uso.
URI: hypervagent/{virtualMachineId}/pingSession
Método HTTP: PUT

RenameVirtualMachine

Altera o nome da máquina virtual atual.
URI: hypervagent/{virtualMachineId}/newname/{newVirtualMachineName}
Método HTTP: PUT

SetProcessorCount

Altera o número de CPUs virtuais na máquina virtual atual.

URI: hypervagent/{virtualMachineId}/cpu/{processorCount}
Método HTTP: PUT

SetRamMegabytes

Altera a quantidade de RAM na máquina virtual atual.
URI: hypervagent/{virtualMachineId}/ram/{ramValue}
Método HTTP: PUT

VerifyConnection

Confirma a conexão ao Hyper-V Agent em execução.
URI: hypervagent/connect
Método HTTP: GET

IIsoDatabaseManagement

Esta seção descreve as operações de serviço disponíveis para IIsoDatabaseManagement em bootcdbuilder/. São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- DeleteIsoEntry
- GetAllIsoEntries

DeleteIsoEntry

Solicita ao serviço que exclua uma entrada específica.
URI: bootcdbuilder/isos/{entryId}
Método HTTP: DELETE

GetAllIsoEntries

Retorna a lista completa de arquivos ISO criados anteriormente.
URI: bootcdbuilder/isos
Método HTTP: GET

ILicenseManagement

Esta seção descreve as operações de serviço disponíveis para ILicenseManagement em license/. O contrato de serviço ILicenseManagement é a interface implementada pelo serviço de gerenciamento de licença do Core, que fornece informações e funcionalidade de licença.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ChangeGroupKey
- ForcePhoneHome
- GetAgentLicenseInfo
- GetCoreLicenseInfo
- GetLicenseConstraintsInfo

- GetLicenseInfo
- GetLicenseStatesNotifications
- IsKeySpecifiedAndValid
- IsPhoneHomeEnable
- IsPhoneHomeInProgress

ChangeGroupKey

Obtém uma nova chave de grupo da UI, valida-a e retorna os resultados da validação.
URI: license/changeGroupKey/{groupKey}
Método HTTP: POST

ForcePhoneHome

Força uma conexão imediata ao Portal de licenças.
URI: license/phoneHome/force
Método HTTP: POST

GetAgentLicenseInfo

Obtém informações sobre aplicação de licença do agente especificado.
URI: license/agent/{agentId}
Método HTTP: GET

GetCoreLicenseInfo

Obtém informações sobre aplicação de licença do Core.
URI: license/core
Método HTTP: GET

GetLicenseConstraintsInfo

Obtém a descrição de todas as limitações ativadas.
URI: license/constraintsInfo
Método HTTP: GET

GetLicenseInfo

Obtém informações de aplicação de licença do Core e de todos os agentes.
URI: license/licenseInfo
Método HTTP: GET

GetLicenseStatesNotifications

Obtém informações sobre estados de licença do Core e de todos os agentes.
URI: license/licenseStatesNotifications
Método HTTP: GET

IsKeySpecifiedAndValid

Obtém o estado da chave.

URI: license/key

Método HTTP: GET

IsPhoneHomeEnable

Determina se a operação de verificação online (phone home) está ativada.

URI: license/phoneHome/isEnable

Método HTTP: GET

IsPhoneHomeInProgress

Determina se a operação de verificação online (phone home) está em progresso.

URI: license/phoneHome/isInProgress

Método HTTP: GET

ILocalizationManagement

Esta seção descreve as operações de serviço disponíveis para ILocalizationManagement em localization/.

O contrato de serviço ILocalizationManagement é a interface implementada pelo serviço de localização comum com uma configuração persistente, que mantém, define e obtém a cultura atual do produto.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetAvailableCultures
- GetCurrentCulture
- SetCurrentCulture

GetAvailableCultures

Obtém uma lista de todas as culturas de recurso disponíveis.

URI: localization/availableCultures

Método HTTP: GET

GetCurrentCulture

Obtém a cultura de recurso atual.

URI: localization/currentCulture

Método HTTP: GET

SetCurrentCulture

Define uma nova cultura para todos os recursos.

URI: localization/newCulture/{lcid}

Método HTTP: POST

ILocalMountManagement

Esta seção descreve as operações de serviço disponíveis para ILocalMountManagement em mounts/.

O contrato de serviço ILocalMountManagement é a interface implementada pelo serviço de gerenciamento de montagens locais, usada para montar e desmontar imagens de volume no Core local.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- Dismount
- DismountAll
- DismountAllAgent
- GetAgentMounts
- GetMountOptions
- GetMounts
- IsVolumeFileSystemCompatible
- StartMount
- VerifyVolumeImagesMountability

Dismount

Desmonta um volume montado.

URI: mounts/volume/{mountedVolumeName}

Método HTTP: DELETE

DismountAll

Desmonta todos os volumes montados.

URI: mounts/allvolumes

Método HTTP: DELETE

DismountAllAgent

Desmonta todos os volumes montados que vieram de um agente específico.

URI: mounts/agents/{agentId}/allvolumes

Método HTTP: DELETE

GetAgentMounts

Obtém a lista dos volumes montados atualmente que vieram de um agente específico.

URI: mounts/agents/{agentId}

Método HTTP: GET

GetMountOptions

Obtém opções de locais de montagem de pontos de recuperação.

URI: mounts/options

Método HTTP: GET

GetMounts

Obtém a lista dos volumes montados atualmente.

URI: mounts/

Método HTTP: GET

IsVolumeFileSystemCompatible

Confirma se o sistema de arquivos do volume é compatível com o sistema operacional atual.

URI: mounts/supportos/{volumeImageId}

Método HTTP: GET

StartMount

Inicia a montagem de um ponto de recuperação específico.

URI: mounts/

Método HTTP: POST

VerifyVolumeImagesMountability

Valida a montabilidade de imagens do volume.

URI: mounts/verifyVolumeImagesMountability

Método HTTP: POST

ILoggingManagement

Esta seção descreve as operações de serviço disponíveis para ILoggingManagement em logs/. O contrato de serviço ILoggingManagement representa Replay.Core.Contracts.Logging.ILoggingManagement.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AllRegisteredTraceLogs
- EnableTraceLog
- GetEnabledTraceLogs
- SetEnabledTraceLogs
- TraceLogSuggestions
- UnregisterTraceLogs

AllRegisteredTraceLogs

Obtém todas as entradas de logs de rastreamento registradas.

URI: logs/allRegisteredTraceLogs

Método HTTP: GET

EnableTraceLog

Ativa o log de rastreamento especificado.

URI: logs/enableTraceLog

Método HTTP: PUT

GetEnabledTraceLogs

Obtém entradas de logs de rastreamento ativados.

URI: logs/enabledTraceLogs

Método HTTP: GET

SetEnabledTraceLogs

Aplica um novo conjunto de logs de rastreamento ativados.

URI: logs/enableTraceLogs

Método HTTP: POST

TraceLogSuggestions

Obtém sugestões para ativar logs de rastreamento.

URI: logs/traceLogSuggestions

Método HTTP: GET

UnregisterTraceLogs

Cancela o registro de log de rastreamento por nome de filtro.

URI: logs/unregisterTraceLogs

Método HTTP: POST

ILogTruncationManagement

Esta seção descreve as operações de serviço disponíveis para ILogTruncationManagement em logtruncation/.

O contrato de serviço ILogTruncationManagement é a interface implementada pelo serviço de gerenciamento de truncamento de log do Core, que fornece a funcionalidade de truncamento de log.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ForceLogTruncation

ForceLogTruncation

Força um trabalho de truncamento de log no agente especificado.

URI: logtruncation/agents/{agentId}/force

Método HTTP: POST

INightlyJobsManagement

Esta seção descreve as operações de serviço disponíveis para INightlyJobsManagement em nightlyJobs/. O contrato de serviço INightlyJobsManagement é a API RESTful de trabalhos noturnos.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CancelNightlyJobs
- GetAgentJobConfiguration

- GetAgentNightlyJobs
- GetJobConfiguration
- GetNightlyJobsSettings
- GetNightlyJobsStatus
- SetAgentJobConfiguration
- SetAgentNightlyJobs
- SetJobConfiguration
- SetNightlyJobsSettings

CancelNightlyJobs

Cancela a execução de todos os trabalhos noturnos.
URI: nightlyJobs/
Método HTTP: DELETE

GetAgentJobConfiguration

Obtém a configuração do trabalho especificado do agente.
URI: nightlyJobs/jobConfiguration/{jobId}/{agentId}
Método HTTP: GET

GetAgentNightlyJobs

Obtém os trabalhos do agente especificado.
URI: nightlyJobs/config/{agentId}
Método HTTP: GET

GetJobConfiguration

Obtém a configuração do trabalho especificado.
URI: nightlyJobs/jobConfiguration/{jobId}
Método HTTP: GET

GetNightlyJobsSettings

Obtém as definições de trabalhos noturnos do Core.
URI: nightlyJobs/config
Método HTTP: GET

GetNightlyJobsStatus

Determina se há trabalhos noturnos em progresso e, em seguida, obtém o ID de transação dos trabalhos atualmente em execução.
URI: nightlyJobs/status
Método HTTP: GET

SetAgentJobConfiguration

Define a configuração de trabalho do agente especificado.

URI: nightlyJobs/jobConfiguration/{jobId}/{agentId}

Método HTTP: PUT

SetAgentNightlyJobs

Define os trabalhos noturnos ativados do agente.

URI: nightlyJobs/config/{agentId}

Método HTTP: PUT

SetJobConfiguration

Define a configuração de trabalho.

URI: nightlyJobs/jobConfiguration/{jobId}

Método HTTP: PUT

SetNightlyJobsSettings

Ajusta as definições de trabalhos noturnos do Core.

URI: nightlyJobs/config

Método HTTP: PUT

IProtectedItemsManagement

Esta seção descreve as operações de serviço disponíveis para IProtectedItemsManagement em protectedItems/.

O contrato de serviço IProtectedItemsManagement expõe itens protegidos, como agentes, clusters, nós de cluster e grupos, como uma árvore.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetProtectedItems

GetProtectedItems

Obtém a árvore de itens protegidos.

URI: protectedItems/allItems

Método HTTP: GET

IPushInstallCommunication

Esta seção descreve as operações de serviço disponíveis para IPushInstallCommunication em pushinstallcomm/.

O contrato de serviço IPushInstallCommunication é usado pelo Replay internamente para comunicação entre o Core e o agente PushInstall. Não use esta API diretamente.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetInstallationStatus
- SetInstallationProgress

GetInstallationStatus

Obtém o progresso da instalação do job subordinado de instalação por push.

URI: pushinstallcomm/status/jobs/{jobId}

Método HTTP: GET

SetInstallationProgress

Este método é chamado pela funcionalidade de instalação por push, que é usada para rastrear o progresso da instalação remota de agentes.

> **CUIDADO: Esse método é apenas para uso interno.**

URI: pushinstallcomm/setProgress/jobs/{jobId}/{messageType}/{progress}/{message}

Método HTTP: POST

IPushInstallManagement

Esta seção descreve as operações de serviço disponíveis para IPushInstallManagement em pushinstall/.

O contrato de serviço IPushInstallManagement é a interface que implementa a capacidade de instalar um agente em uma máquina remota. A instalação por push é uma funcionalidade que permite que o usuário inicie e controle instalações de agente em ambientes remotos em uma rede.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- DeployAgents
- GetAgentServiceState
- GetConfiguration
- GetDeployAgentVersion
- GetInstalledProducts
- IsRemoveAgentProductRequired
- SetConfiguration
- ValidateMachine

DeployAgents

Inicia a implantação de um ou mais agentes em máquinas remotas.

URI: pushinstall/deployAgents

Método HTTP: PUT

GetAgentServiceState

Verifica se o agente já está instalado na máquina remota.
URI: pushinstall/isPushInstallNeed
Método HTTP: POST

GetConfiguration

Obtém a configuração de PushInstall.
URI: pushinstall/config
Método HTTP: GET

GetDeployAgentVersion

Obtém a versão do Agent a ser implantado.
URI: pushinstall/deployAgentVersion
Método HTTP: GET

GetInstalledProducts

Verifica se há produtos já instalados.
URI: pushinstall/getInstalledProducts
Método HTTP: POST

IsRemoveAgentProductRequired

Verifica se é necessário remover o produto do Agent.
URI: pushinstall/isRemoveAgentProductRequired/{removeProductId}/{installedProductVersion}
Método HTTP: GET

SetConfiguration

Define a configuração de PushInstall.
URI: pushinstall/config
Método HTTP: PUT

ValidateMachine

Verifica a disponibilidade da máquina e as permissões do agente de instalação.
URI: pushinstall/validateMachine
Método HTTP: PUT

IRecoveryPointsManagement

Esta seção descreve as operações de serviço disponíveis para IRecoveryPointsManagement em recoveryPoints/.

O contrato de serviço IRecoveryPointsManagement é a interface implementada pelo serviço de gerenciamento de pontos de recuperação, que expõe informações sobre pontos de recuperação para clientes REST.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CheckAgentVolumeImages
- CheckAgentVolumeImagesSupport
- DeleteOrphanVolumeImagesChains
- DeleteRecoveryPointsChain
- DeleteRecoveryPointsForAgent
- DeleteRecoveryPointsRange
- DeleteVolumeImages
- DeleteVolumeImagesSupport
- ExportVolumeImagesTree
- GetAgentRecoveryPointCheckSettings
- GetAgentsRecoveryPointsInfo
- GetAllRecoveryPoints
- GetFilteredRecoveryPointsByPage
- GetImageRawData
- GetImageRawKeys
- GetImageRawKeysText
- GetMostRecentRecoveryPoints
- GetRecoveryPointDetails
- GetRecoveryPointLockedKeys
- GetRecoveryPoints
- GetRecoveryPointsByDateRange
- GetRecoveryPointsByPage
- GetRecoveryPointSummary
- GetVolumeImageDetails
- IsOrphanRecoveryPoint
- SetAgentRecoveryPointCheckSettings

CheckAgentVolumeImages

Inicia uma tarefa que realiza uma verificação de integridade de todos os pontos de recuperação do agente e tenta corrigir os erros encontrados.

URI: recoveryPoints/agents/checkVolumes

Método HTTP: POST

CheckAgentVolumeImagesSupport

Inicia uma tarefa que realiza uma verificação de integridade de todos os pontos de recuperação do agente e tenta corrigir os erros encontrados. Para fins de suporte. Use o símbolo "*" como máscara para pontos de recuperação e volumes.

URI:
recoveryPoints/agents/{agentId}/rps/{recoveryPointId}/volumes/{volumeImageId}/integritycheck/target={target}

Método HTTP: GET

DeleteOrphanVolumeImagesChains

Exclui cadeias de imagens de volume órfãs de um ponto de recuperação especificado.

Método HTTP: URI: recoveryPoints/rps/deleteOrphanVolumeImagesChains/{recoveryPointId}

POST

DeleteRecoveryPointsChain

Exclui todas as cadeias de imagem do volume que contêm imagens de volume de um determinado ponto de recuperação.

URI: recoveryPoints/rps/{recoveryPointId}

Método HTTP: DELETE

DeleteRecoveryPointsForAgent

Exclui todos os pontos de recuperação de um agente especificado.

URI: recoveryPoints/agents/{agentId}

Método HTTP: DELETE

DeleteRecoveryPointsRange

Exclui todos os pontos de recuperação do agente especificado em um período de tempo especificado.

URI: recoveryPoints/rps/deleteRecoveryPointsRange

Método HTTP: POST

DeleteVolumeImages

Exclui imagens de volume sem rollup do agente especificado. Para fins de depuração.

URI: recoveryPoints/agents/deleteVolumes

Método HTTP: DELETE

DeleteVolumeImagesSupport

Exclui imagens de volume sem rollup do agente especificado.

URI: recoveryPoints/agents/{agentId}/rps/{recoveryPointId}/volumes/{volumeImageId}

Método HTTP: GET

ExportVolumeImagesTree

Exporta a árvore de imagens de volume do agente para um arquivo de texto.

URI: recoveryPoints/agents/exportVolumeImagesTree

Método HTTP: PUT

GetAgentRecoveryPointCheckSettings

Obtém definições de verificação de ponto de recuperação do agente, incluindo trabalho noturno e verificações iniciadas manualmente.

URI: recoveryPoints/agents/{agentId}/integritycheck/settings

Método HTTP: GET

GetAgentsRecoveryPointsInfo

Obtém uma lista de todos os agentes com pontos de recuperação.

URI: recoveryPoints/agents/all

Método HTTP: GET

GetAllRecoveryPoints

Obtém as informações resumidas de todos os pontos de recuperação associados ao agente especificado. Observe que essa lista pode ser muito extensa.

URI: recoveryPoints/agents/{agentId}/all

Método HTTP: GET

GetFilteredRecoveryPointsByPage

Obtém informações resumidas sobre pontos de recuperação de um determinado ID de agente e filtro, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: recoveryPoints/agents/{agentId}/paged?max={max}&page={page}

Método HTTP: PUT

GetImageRawData

Obtém um fluxo de dados que consiste nos dados na imagem, com o deslocamento e comprimento especificados. Útil apenas para fins de diagnóstico.

URI: recoveryPoints/images/rawdata/{imageId}.rawdata?blockOffset={blockOffset}&blockLength={blockLength}

Método HTTP: GET

GetImageRawKeys

Obtém um fluxo de pares de deslocamento/chave, contendo deslocamentos de bloco na imagem e as chaves DVM do registro em cada deslocamento de bloco. Útil apenas para fins de diagnóstico.

URI: recoveryPoints/images/rawkeys/{imageId}.rawkeys

Método HTTP: GET

GetImageRawKeysText

Obtém um fluxo de pares de deslocamento/chave, contendo deslocamentos de bloco na imagem e as chaves DVM do registro em cada deslocamento de bloco. Útil apenas para fins de diagnóstico.

URI: recoveryPoints/images/rawkeys/{imageId}.textkeys

Método HTTP: GET

GetMostRecentRecoveryPoints

Obtém informações resumidas sobre o ponto de recuperação mais recente de cada agente especificado na solicitação.

URI: recoveryPoints/recent

Método HTTP: PUT

GetRecoveryPointDetails

Obtém informações detalhadas sobre um único ponto de recuperação.

URI: recoveryPoints/rps/{recoveryPointId}/details

Método HTTP: GET

GetRecoveryPointLockedKeys

Obtém uma lista de chaves de criptografia usadas por um ponto de recuperação que estão bloqueadas e precisam de uma frase de acesso para serem montadas.

URI: recoveryPoints/rps/{recoveryPointId}/lockedkeys

Método HTTP: GET

GetRecoveryPoints

Obtém as informações resumidas dos pontos de recuperação associados ao agente especificado que estão fora de um intervalo de data/hora de última modificação. Você também pode especificar um número máximo de pontos de recuperação a serem retornados com o intervalo especificado.

URI: recoveryPoints/agents/{agentId}/where?max={max}&olderThan={olderThan}&newerThan={newerThan}

Método HTTP: GET

GetRecoveryPointsByDateRange

Obtém as informações resumidas dos pontos de recuperação associados ao agente especificado que estão dentro de um intervalo de data/hora da última modificação. Você também pode especificar um número máximo de pontos de recuperação a serem retornados com o intervalo especificado.

URI: recoveryPoints/agents/{agentId}/daterange?max={max}&startDate={startDate}&endDate={endDate}

Método HTTP: GET

GetRecoveryPointsByPage

Obtém informações resumidas dos pontos de recuperação para um ID de agente específico, apresentando os resultados em uma grade paginada para facilitar a visualização.

URI: recoveryPoints/agents/{agentId}/paged?max={max}&page={page}

Método HTTP: GET

GetRecoveryPointSummary

Obtém informações detalhadas sobre um único ponto de recuperação.

URI: recoveryPoints/rps/{recoveryPointId}/summary

Método HTTP: GET

GetVolumeImageDetails

Obtém informações sobre uma única imagem do volume especificada pelo identificador exclusivo.

URI: recoveryPoints/images/{imageId}/'

Método HTTP: GET

IsOrphanRecoveryPoint

Verifica se o ponto de recuperação é órfão ou não.

URI: recoveryPoints/rps/{recoveryPointId}/isOrphan

Método HTTP: GET

SetAgentRecoveryPointCheckSettings

Ajusta as definições de verificação do ponto de recuperação do agente, incluindo trabalho noturno e verificações iniciadas manualmente.

URI: recoveryPoints/agents/{agentId}/integritycheck/settings

Método HTTP: PUT

IRemoteMountManagement

Esta seção descreve as operações de serviço disponíveis para IRemoteMountManagement em remoteMounts/.

O contrato de serviço IRemoteMountManagement é a interface implementada pelo serviço de gerenciamento de montagens remotas, usada para desconectar imagens do volume montadas em máquinas remotas.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddRemoteMount
- Disconnect
- DisconnectAll
- DisconnectAllForAgent
- GetAgentRemoteMounts
- GetRemoteMounts

AddRemoteMount

Adiciona informações sobre um ponto de montagem remoto.

URI: remoteMounts/addRemoteMount

Método HTTP: POST

Disconnect

Desconecta o ponto de montagem remoto.

URI: remoteMounts/disconnect/{remoteMountItemId}/mountType/{mountType}

Método HTTP: POST

DisconnectAll

Desconecta todos os pontos de montagem remotos.

URI: remoteMounts/disconnectAll

Método HTTP: POST

DisconnectAllForAgent

Desconecta todos os pontos de montagem remotos do agente especificado.

URI: remoteMounts/disconnectAllForAgent/{agentId}

Método HTTP: POST

GetAgentRemoteMounts

Obtém informações sobre pontos de montagem remotos do agente especificado.

URI: remoteMounts/getAgentRemoteMoutns/{agentId}

Método HTTP: POST

GetRemoteMounts

Obtém informações sobre pontos de montagem remotos.

URI: remoteMounts/remoteMountInfos

Método HTTP: POST

IReplayEngineManagement

Esta seção descreve as operações de serviço disponíveis para IReplayEngineManagement em replayEngine/.

O contrato de serviço IReplayEngineManagement é a interface implementada pelo serviço de gerenciamento do mecanismo Replay, usada para configurar e monitorar o mecanismo Replay.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CloseConnection
- GetConfiguration
- GetConnections
- SetConfiguration

CloseConnection

Força o fechamento de uma conexão existente ao mecanismo AppAssure.

URI: replayEngine/connections/{id}

Método HTTP: DELETE

GetConfiguration

Obtém a configuração atual do serviço do mecanismo Replay.

URI: replayEngine/config

Método HTTP: GET

GetConnections

Obtém uma lista de conexões ativas ao serviço do mecanismo Replay.

URI: replayEngine/connections

Método HTTP: GET

SetConfiguration

Define a configuração do serviço.

URI: replayEngine/config

Método HTTP: POST

IReplicationCommunication

Esta seção descreve as operações de serviço disponíveis para IReplicationCommunication em replicationcomms/.

O contrato de serviço IReplicationCommunication é usado pelo Replay internamente para comunicação entre Cores para replicação. Não use esta API diretamente.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddAgentsByDemand
- AddAgentsByRequest
- CancelRemoteMetadataUpdate
- CancelRemoteRollup
- CancelRemoteVolumeImagesDeletion
- CancelUploadFile
- ContinueUploadFile
- DeleteAgent
- DeletePairing
- DemandPairing
- EndCheck
- EndUploadFile
- EndVolumeImageReplicationSession
- EndVolumeImageReplicationSessionOld
- EndVolumeImageVerificationSession
- GetAgentRecoveryPointDetails
- GetAgentRecoveryPoints
- GetAgentRecoveryPointsCount
- GetAgentRepositoryRelationships
- GetAgents
- GetBasicReplicatedVolumeImagesInfo
- GetBasicReplicatedVolumeImagesInfoOld
- GetConsumedSeedDrives
- GetCoreId
- GetExchangeVersions
- GetFileInfoForExchangeDll
- GetMetadataUpdateProgress
- GetNextBlockMD5Digest
- GetNextBlockMD5Digest
- GetPairingStatus
- GetRemoteMasterCoresForDemand
- GetReplicatedAgents
- GetReplicatedAgentsRecoveryPointsInfo

- GetReplicatedAgentsStorageUsage
- GetRepositories
- GetRepositoryFreeSpaceForAgent
- GetRollupProgress
- GetVolumeImageBlockDigest
- GetVolumeImageBlockIndex
- GetVolumeImageDigest
- GetVolumeImageMD5CheckResult
- GetVolumeImagesDeletionProgress
- NegotiateMissingRecords
- NegotiateMissingRecordsOld
- NewVolumeImageMD5BlockCheck
- RequestPairing
- SelectRangeAgentRecoveryPoints
- StartHashVerificationJob
- StartMetadataUpdate
- StartMetadataUpdate
- StartMetadataUpdateJob
- StartNewUploadSession
- StartNewVolumeImageReplicationSession
- StartRemoteReplicationJob
- StartRollup
- StartRollupJob
- StartTransferJob
- StartVolumeImagesDeletion
- StartVolumeImagesDeletionJob
- StartVolumeImagesDeletionJobOld
- StartVolumeImagesDeletionOld
- StartVolumeImageVerificationSession
- SyncPairingStatus
- SyncRemoteReplicationJob
- TransferMissingRecords
- TransferMissingRecordsOld
- TransferUndiscoveredRecords
- TransferVolumeBlock
- UpdateIndex
- UpdateMasterStorageUsage
- UpdateReplicationStatus
- VerifyAddAgentsByDemand
- VerifyAddAgentsByRequest

- VerifyReplicationAbility
- VerifyReplicationCorePairingAbility

AddAgentsByDemand

Adiciona agentes por demanda a um Core servo remoto.
URI: replicationcomms/slave/agents/demand
Método HTTP: POST

AddAgentsByRequest

Adiciona agentes por solicitação a um servo remoto.
URI: replicationcomms/slave/agents/request
Método HTTP: POST

CancelRemoteMetadataUpdate

Cancela a fase de atualização de metadados do trabalho de replicação do agente replicado.
URI: replicationcomms/slave/agents/{agentId}/metadataUpdate
Método HTTP: DELETE

CancelRemoteRollup

Cancela a fase de rollup do trabalho de replicação do agente replicado.
URI: replicationcomms/slave/agents/{agentId}/rollup
Método HTTP: DELETE

CancelRemoteVolumeImagesDeletion

Cancela a fase de exclusão de imagens de volume do trabalho de replicação do agente replicado.
URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletion
Método HTTP: DELETE

CancelUploadFile

Cancela a sessão de upload atual.
URI: replicationcomms/slave/sessions/{uploadSessionId}/
Método HTTP: DELETE

ContinueUploadFile

Lê dados do Core servo na sessão de upload atual.
URI: replicationcomms/slave/sessions/{uploadSessionId}/data/{dataSize}
Método HTTP: POST

DeleteAgent

Exclui um agente replicado do Core servo, incluindo todos os seus pontos de recuperação.
URI: replicationcomms/slave/agents/{agentId}
Método HTTP: DELETE

DeletePairing

Remove o relacionamento de replicação com o Core mestre no lado do Core servo. O agente real replicado e protegido nos Cores mestre e servo permanece disponível.

URI: replicationcomms/slave/pairing?deleteRecoveryPoints={deleteRecoveryPoints}

Método HTTP: DELETE

DemandPairing

Demanda o estabelecimento de um relacionamento de emparelhamento com um Core remoto. As demandas são aceitas apenas se o originador da chamada realiza autenticação NTLM como membro do grupo de administradores. Este método redefine a conexão para estabelecer uma nova conexão protegida.

URI: replicationcomms/slave/pairing/demand

Método HTTP: POST

EndCheck

Cancela o contexto de verificação MD5 atual.

URI: replicationcomms/slave/contexts/{contextId}/

Método HTTP: POST

EndUploadFile

Encerra a sessão de upload atual e verifica o hash MD5 do arquivo recebido.

URI: replicationcomms/slave/sessions/{uploadSessionId}/

Método HTTP: POST

EndVolumeImageReplicationSession

Encerra a sessão de replicação da imagem do volume, opcionalmente confirmando a imagem do volume transferida.

URI: replicationcomms/slave/{agentId}/{jobId}/{sessionId}?commit={commit}

Método HTTP: DELETE

EndVolumeImageReplicationSessionOld

Encerra a sessão de replicação da imagem do volume, opcionalmente confirmando a imagem do volume transferida.

URI: replicationcomms/slave/sessions/{sessionId}?commit={commit}

Método HTTP: DELETE

EndVolumeImageVerificationSession

Encerra a sessão de verificação de integridade com um Core servo.

URI: replicationcomms/slave/check/session/{sessionId}/end?commit={commit}

Método HTTP: DELETE

GetAgentRecoveryPointDetails

Obtém os detalhes de um único ponto de recuperação replicado.

URI: replicationcomms/slave/agents/{agentId}/rps/{recoveryPointId}

Método HTTP: GET

GetAgentRecoveryPoints

Obtém os pontos de recuperação replicados do agente especificado.

URI: replicationcomms/slave/agents/{agentId}/rps

Método HTTP: GET

GetAgentRecoveryPointsCount

Obtém a contagem dos pontos de recuperação replicados do agente especificado.

URI: replicationcomms/slave/agents/{agentId}/rpsCount

Método HTTP: GET

GetAgentRepositoryRelationships

Obtém os repositórios dos agentes replicados.

URI: replicationcomms/slave/cores/agentRepositoryRelationships

Método HTTP: GET

GetAgents

Obtém a lista de todos os agentes. É necessário que haja um emparelhamento, e essa solicitação deve ser autenticada pelo certificado de cliente do Core mestre.

URI: replicationcomms/slave/agents

Método HTTP: GET

GetBasicReplicatedVolumeImagesInfo

Obtém os detalhes de todos os pontos de recuperação replicados do agente especificado.

URI: replicationcomms/slave/agents/{agentId}/replicatedVolumeImagesNew

Método HTTP: GET

GetBasicReplicatedVolumeImagesInfoOld

Obtém os detalhes de todos os pontos de recuperação replicados do agente especificado.

URI: replicationcomms/slave/agents/{agentId}/replicatedVolumeImages

Método HTTP: GET

GetConsumedSeedDrives

Obtém identificadores de unidades de propagação consumidas no Core para o agente especificado.

URI: replicationcomms/consumedSeedDrives/{agentId}

Método HTTP: GET

GetCoreId

Testa a conexão ao Core remoto e retorna o ID do Core. Se useCredentials for verdadeiro, a autenticação NTLM será usada; do contrário, será usada autenticação anônima.

URI: replicationcomms/slave/validate/?useCredentials={useCredentials}

Método HTTP: GET

GetExchangeVersions

Obtém as versões das DLLs do Exchange presentes no Core servo remoto.

URI: replicationcomms/slave/exchange

Método HTTP: GET

GetFileInfoForExchangeDll

Obtém informações sobre um arquivo DLL do Exchange especificado.

URI: replicationcomms/slave/exchange/dllinfo/{fileName}

Método HTTP: POST

GetMetadataUpdateProgress

Obtém o status do trabalho de atualização de metadados iniciado no Core mestre.

URI: replicationcomms/slave/agents/{agentId}/metadataUpdate/status

Método HTTP: GET

GetNextBlockMD5Digest

Obtém o resumo MD5 do bloco especificado.

URI: replicationcomms/slave/getBlockMD5/contextId/{contextId}/count/{blockCount}/md5/{blockMD5}

Método HTTP: POST

GetNextBlockMD5Digest

Obtém MD5 e tamanho da imagem do volume. Não chama uma nova verificação.

URI: replicationcomms/slave/getVolumeImageMD5/?volumeId={volumeId}

Método HTTP: GET

GetPairingStatus

Obtém o status do emparelhamento entre o Core originador da chamada e o Core servo remoto. O originador da chamada é identificado por seu certificado de cliente SSL. Este método está disponível para um Core remoto independentemente de ter sido pareado por solicitação ou ter ele próprio iniciado o emparelhamento.

URI: replicationcomms/slave/pairing/status

Método HTTP: GET

GetRemoteMasterCoresForDemand

Obtém informações sobre Cores mestres remotos para o Core servo atual. Usa autenticação NTLM.

URI: replicationcomms/slave/cores/masters

Método HTTP: GET

GetReplicatedAgents

Obtém a lista de agentes que o originador da chamada está replicando nesse Core servo. É necessário que haja um emparelhamento, e essa solicitação deve ser autenticada pelo certificado de cliente do Core mestre.

URI: replicationcomms/slave/agents

Método HTTP: GET

GetReplicatedAgentsRecoveryPointsInfo

Obtém a lista de agentes que possuem pontos de recuperação em um Core servo remoto.
URI: replicationcomms/slave/agents/rpsinfo
Método HTTP: GET

GetReplicatedAgentsStorageUsage

Obtém um resumo do uso de armazenamento pelos agentes replicados.
replicationcomms/slave/agents
Método HTTP: GET

GetRepositories

Obtém todos os repositórios. Com autenticação de certificado para os Cores já pareados.
URI: replicationcomms/slave/repositories
Método HTTP: GET

GetRepositoryFreeSpaceForAgent

Obtém o espaço livre no repositório remoto do agente.
URI: replicationcomms/slave/agents/{agentId}
Método HTTP: GET

GetRollupProgress

Obtém o status do trabalho de rollup iniciado no Core mestre.
replicationcomms/slave/agents/{agentId}/rollup/progress
Método HTTP: GET

GetVolumeImageBlockDigest

Obtém o resumo de bloco de imagem do volume do bloco especificado.
URI: replicationcomms/slave/check/session/{sessionId}/blockDigest
Método HTTP: POST

GetVolumeImageBlockIndex

Obtém os valores de índice de imagem do volume do bloco especificado.
URI: replicationcomms/slave/check/session/{sessionId}/index?block={blockNumber}
Método HTTP: GET

GetVolumeImageDigest

Obtém o resumo de imagem do volume para uma sessão de verificação de integridade especificada.
URI: replicationcomms/slave/check/session/{sessionId}/digest
Método HTTP: GET

GetVolumeImageMD5CheckResult

Obtém o resultado da verificação MD5 do volume atual para o contexto.

URI: replicationcomms/slave/checkResult/{contextId}/

Método HTTP: POST

GetVolumeImagesDeletionProgress

Obtém o status do trabalho de exclusão iniciado no Core mestre

URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletion/progress

Método HTTP: GET

NegotiateMissingRecords

Envia um fluxo de metadados de registro para a imagem que está sendo replicada e recebe de volta um fluxo de registros que estão ausentes no Core remoto.

URI: replicationcomms/slave/{agentId}/{jobId}/{sessionId}/records/keys

Método HTTP: POST

NegotiateMissingRecordsOld

Envia um fluxo de metadados de registro para a imagem que está sendo replicada e recebe de volta um fluxo de registros que estão ausentes no Core remoto.

URI: replicationcomms/slave/sessions/{sessionId}/records/keys

Método HTTP: POST

NewVolumeImageMD5BlockCheck

Inicia uma nova verificação MD5 e sessão de comparação mestre/servo de índices de registro de volume. Retorna contextId.

URI: replicationcomms/slave/volumeImageMD5BlockCheck/{volumeId}

Método HTTP: POST

RequestPairing

Envia a um servo remoto uma solicitação de autorização para replicar um ou mais agentes. A solicitação é avaliada por um operador humano e será aprovada ou negada em uma data posterior. Este método redefine a conexão para estabelecer uma nova conexão protegida.

URI: replicationcomms/slave/pairing/request

Método HTTP: POST

SelectRangeAgentRecoveryPoints

Seleciona o intervalo de pontos de recuperação replicados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/skipCount/{skipCount}/maxCount/{maxCount}/rps

Método HTTP: GET

StartHashVerificationJob

Inicia o trabalho de verificação de integridade para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/verification/{jobId}/start

Método HTTP: POST

StartMetadataUpdate

Inicia a atualização de metadados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/metadataUpdate

Método HTTP: POST

StartMetadataUpdateJob

Inicia o trabalho de atualização de metadados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/metadataUpdateJob

Método HTTP: POST

StartNewUploadSession

Inicia uma nova sessão de upload de arquivo.

URI: replicationcomms/slave/newsession/

Método HTTP: POST

StartNewVolumeImageReplicationSession

Inicia uma sessão de replicação com um Core servo.

URI: replicationcomms/slave/sessions/new

Método HTTP: POST

StartRemoteReplicationJob

Inicia um trabalho de replicação espelhado remoto em um Core servo.

URI: replicationcomms/slave/agents/replicationJob/start

Método HTTP: POST

StartRollup

Inicia o rollup no agente servo especificado com as células de granularidade (intervalos de tempo) especificadas.

URI: replicationcomms/slave/agents/{agentId}/rollup

Método HTTP: POST

StartRollupJob

Inicia o rollup no agente servo especificado com as células de granularidade (intervalos de tempo) especificadas.

URI: replicationcomms/slave/agents/{agentId}/rollupJob

Método HTTP: POST

StartTransferJob

Inicia um trabalho de transferência espelhado remoto em um Core servo.

URI: replicationcomms/slave/agents/{agentId}/transferJob/{jobId}

Método HTTP: POST

StartVolumeImagesDeletion

Inicia a exclusão de imagens de volume com os identificadores especificados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletionNew

Método HTTP: POST

StartVolumeImagesDeletionJob

Inicia o trabalho de exclusão de imagens de volume com os identificadores especificados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletionJobNew

Método HTTP: POST

StartVolumeImagesDeletionJobOld

Inicia o trabalho de exclusão de imagens de volume com os identificadores especificados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletionJob

Método HTTP: POST

StartVolumeImagesDeletionOld

Inicia a exclusão de imagens de volume com os identificadores especificados para o agente especificado.

URI: replicationcomms/slave/agents/{agentId}/volumeImagesDeletion

Método HTTP: POST

StartVolumeImageVerificationSession

Inicia uma sessão de verificação de integridade com um Core servo.

URI: replicationcomms/slave/check/{agentId}/{jobId}/session/start

Método HTTP: POST

SyncPairingStatus

Obtém o status do emparelhamento entre o Core originador da chamada e o Core servo remoto. O originador da chamada é identificado por seu certificado de cliente SSL. Este método está disponível para um Core remoto independentemente de ter sido pareado por solicitação ou de ter ele próprio iniciado o emparelhamento.

URI: replicationcomms/slave/pairing/sync

Método HTTP: POST

SyncRemoteReplicationJob

Sincroniza com um trabalho de replicação espelhado remoto em um Core servo.

URI: replicationcomms/slave/agents/replicationJob/sync

Método HTTP: POST

TransferMissingRecords

Envia ao Core servo um fluxo de registros brutos, cuja lista é determinada por NegotiateMissingRecords.

URI: replicationcomms/slave/{agentId}/{jobId}/{sessionId}/records/rawdata

Método HTTP: POST

TransferMissingRecordsOld

Envia ao Core servo um fluxo de registros brutos, cuja lista é determinada por NegotiateMissingRecords.

URI: replicationcomms/slave/sessions/{sessionId}/records/rawdata

Método HTTP: POST

TransferUndiscoveredRecords

Envia um fluxo de dados de registro para a imagem que está sendo verificada e recebe de volta um fluxo de metadados de registro que foram detectados como ausentes no Core remoto.

URI: replicationcomms/slave/check/session/{sessionId}/transferRecords

Método HTTP: POST

TransferVolumeBlock

Lê dados do agente na sessão de transmissão atual.

URI:
replicationcomms/slave/blockTransfer/contextId/{contextId}/blockCount/{blockCount}/offset/{offset}/size/{size}

Método HTTP: POST

UpdateIndex

Atualiza um índice de imagem do volume no Core remoto.

URI: replicationcomms/slave/check/session/{sessionId}/updateIndex

Método HTTP: POST

UpdateMasterStorageUsage

Fornece um resumo do uso de armazenamento no Core mestre para o Core servo. Isso existe principalmente para fornecer suporte aos requisitos de faturamento de MSP.

URI: replicationcomms/slave/storage

Método HTTP: PUT

UpdateReplicationStatus

Define o status de replicação no Core servo.

URI: replicationcomms/slave/agents/{agentId}/status

Método HTTP: PUT

VerifyAddAgentsByDemand

Confirma se agentes podem ser replicados sob demanda com segurança

URI: replicationcomms/slave/demand/agents/verify

Método HTTP: POST

VerifyAddAgentsByRequest

Confirma se agentes podem ser replicados por solicitação com segurança

URI: replicationcomms/slave/request/agents/verify

Método HTTP: POST

VerifyReplicationAbility

Confirma a capacidade de replicação.

URI: replicationcomms/slave/agents/{agentId}/replication/verifyStart

Método HTTP: GET

VerifyReplicationCorePairingAbility

Confirma a capacidade de emparelhamento.

URI: replicationcomms/slave/replication/verifyStart/?useCredentials={useCredentials}

Método HTTP: POST

IReplicationManagement

Esta seção descreve as operações de serviço disponíveis para IReplicationManagement em replication/.

O contrato de serviço IReplicationManagement é usado para configuração, gerenciamento e monitoramento de replicação.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddAgentsByDemand
- AddAgentsByRequest
- DeleteAgentFromMaster
- DeleteAgentFromSlave
- DeleteMasterCore
- DeletePairing
- DeleteSlaveCore
- DemandPairing
- ForceReplication
- GetAgentReplicationSettings
- GetAgentRepositoryRelationships
- GetCoreIdByDescriptor
- GetCoreIdByUrl
- GetCountRemoteAgentsRecoveryPoints
- GetPendingPairingRequest
- GetPendingPairingRequests
- GetCountRemoteAgentsRecoveryPoints
- GetPendingPairingRequest
- GetPendingPairingRequests
- GetRemoteAgentsRecoveryPoints
- GetRemoteCoreRepositories
- GetRemoteCoreRepositoriesForDemand
- GetRemoteCores
- GetRemoteMasterCoresForDemand

- GetRemoteSlaveCoreReplicationPolicy
- GetRemoteSlaveRecoveryPoint
- GetReplicatedAgentsRecoveryPointsInfo
- GetReplicationConfiguration
- IgnorePairingRequest
- RequestForceReplication
- RequestPairing
- RespondToAddAgentsByRequest
- RespondToPairingRequest
- SelectRangeRemoteAgentsRecoveryPoints
- SetAgentReplicationPauseConfiguration
- SetAgentReplicationPauseConfigurationForMasterCores
- SetAgentReplicationPauseConfigurationForSlaveCores
- SetAgentReplicationSettings
- SetRemoteSlaveCoreReplicationPolicy
- SetReplicationConfiguration
- SwitchFailoverAgentToReplicated
- SwitchReplicatedAgentToFailover
- UpdateSlaveCoreSettings
- VerifyAddAgentsByDemand
- VerifyAddAgentsByDemandForExistingCore
- VerifyAddAgentsByRequest
- VerifyAddAgentsByRequestForExistingCore
- VerifyCorePairingAbilityByDemand
- VerifyCorePairingAbilityByRequest

AddAgentsByDemand

Adiciona agentes ao emparelhamento existente sob demanda.

URI: replication/cores/{coreId}/agents/demand

Método HTTP: POST

AddAgentsByRequest

Adiciona agentes ao emparelhamento existente por solicitação.

URI: replication/cores/{coreId}/agents/request

Método HTTP: POST

DeleteAgentFromMaster

Exclui um agente do relacionamento de replicação apenas no lado do servo. O agente real replicado e protegido nos Cores mestre e servo permanece disponível.

URI: replication/masters/{coreId}/replicatedagents/{agentId}/?deleteRecoveryPoints={deleteRecoveryPoints}

Método HTTP: DELETE

DeleteAgentFromSlave

Exclui um agente do relacionamento de replicação apenas no lado do mestre. O agente real replicado e protegido nos Cores mestre e servo permanece disponível.

URI: replication/slaves/{coreId}/replicatedagents/{agentId}

Método HTTP: DELETE

DeleteMasterCore

Exclui o Core mestre remoto da replicação.

URI: replication/masters/{coreId}?deleteRecoveryPoints={deleteRecoveryPoints}

Método HTTP: DELETE

DeletePairing

Exclui o emparelhamento entre os Cores mestre e servo.

URI: replication/cores/{coreId}/pairing?deleteRecoveryPoints={deleteRecoveryPoints}

Método HTTP: DELETE

DeleteSlaveCore

Exclui o Core servo remoto da replicação.

URI: replication/slaves/{coreId}

Método HTTP: DELETE

DemandPairing

Instrui esse Core a enviar uma demanda de replicação a um Core remoto. Esta operação exige credenciais de administrador no Core remoto, mas, se bem-sucedida, tem efeito imediato. Retorna o ID do Core servo.

URI: replication/cores/pairing/demand

Método HTTP: POST

ForceReplication

Força a replicação de agentes.

URI: replication/force

Método HTTP: PUT

GetAgentReplicationSettings

Obtém definições de replicação do agente com o ID especificado.

URI: replication/agents/{agentId}

Método HTTP: GET

GetAgentRepositoryRelationships

Obtém os repositórios em um Core remoto para agentes.

URI: replication/cores/slaves/{slaveCoreId}/agentRepositoryRelationships

Método HTTP: GET

GetCoreIdByDescriptor

Testa um descritor de Core para validar a capacidade de conexão a ele. Retorna CoreId. Usa autenticação NTLM.

URI: replication/cores/descriptor

Método HTTP: PUT

GetCoreIdByUrl

Testa a conexão a um Core remoto. Retorna CoreId. Usa autenticação anônima.

URI: replication/cores/{hostUri}

Método HTTP: PUT

GetCountRemoteAgentsRecoveryPoints

Obtém a contagem de pontos de recuperação replicados em um Core servo remoto para o agente especificado. Não funciona com um Core mestre.

URI: replication/cores/{coreId}/agents/{agentid}/recoveryPointsCount

Método HTTP: GET

GetPendingPairingRequest

Obtém uma solicitação pendente para um ID de solicitação específico.

URI: replication/requests/pairing/pending/{requestId}

Método HTTP: GET

GetPendingPairingRequests

Obtém uma lista de todas as solicitações de emparelhamento de replicação pendentes recebidas por esse Core de Cores mestres remotos.

URI: replication/requests/pending

Método HTTP: GET

GetRemoteAgentsRecoveryPoints

Obtém os pontos de recuperação replicados em um Core servo remoto para o agente especificado. Não funciona com um Core mestre.

URI: replication/cores/{coreId}/agents/{agentid}/recoveryPoints

Método HTTP: GET

GetRemoteCoreRepositories

Obtém os repositórios em um Core remoto. São necessárias credenciais de administrador no Core remoto.

URI: replication/cores/slave/repositories

Método HTTP: PUT

GetRemoteCoreRepositoriesForDemand

Obtém os repositórios em um Core remoto para. Usa autenticação de certificado e funciona apenas no Core demandado.

URI: replication/cores/slaves/{slaveCoreId}/pairingdemand/repositories

Método HTTP: PUT

GetRemoteCores

Obtém uma lista de todos os Cores remotos que esse Core conhece, tanto mestres como servos

URI: replication/cores/?forceRefresh={forceRefresh}

Método HTTP: GET

GetRemoteMasterCoresForDemand

Obtém informações sobre Cores mestres remotos para o Core servo atual.

URI: replication/cores/slave/masters

Método HTTP: PUT

GetRemoteSlaveCoreReplicationPolicy

Obtém a política de replicação do Core servo remoto. Funciona apenas no lado do Core mestre.

URI: replication/cores/slaves/{slaveCoreId}/settings/policy

Método HTTP: GET

GetRemoteSlaveRecoveryPoint

Obtém os detalhes de um ponto de recuperação replicado em um Core servo remoto. Não funciona com um Core mestre.

URI: replication/cores/{coreId}/agents/{agentId}/rps/{recoveryPointId}

Método HTTP: GET

GetReplicatedAgentsRecoveryPointsInfo

Obtém a lista de agentes que possuem pontos de recuperação em um Core servo remoto.

URI: replication/cores/{coreId}/agents/rpsinfo

Método HTTP: GET

GetReplicationConfiguration

Obtém a configuração de replicação.

URI: replication/config

Método HTTP: GET

IgnorePairingRequest

Exclui uma solicitação de replicação pendente sem responder a ela.

URI: replication/requests/{requestId}

Método HTTP: DELETE

RequestForceReplication

Solicita uma replicação forçada.

URI: replication/requestForceReplication

Método HTTP: PUT

RequestPairing

Instrui esse Core a enviar uma solicitação de replicação para um Core remoto. A replicação será iniciada quando o Core remoto aprovar a solicitação. Retorna o ID do Core servo.

URI: replication/cores/pairing/request

Método HTTP: POST

RespondToAddAgentsByRequest

Responde a agentes pendentes de solicitações de replicação.

URI: replication/requests/pairing/{requestId}/agents

POST

RespondToPairingRequest

Responde a solicitações de replicação pendentes.

URI: replication/requests/pairing/{requestId}

Método HTTP: POST

SelectRangeRemoteAgentsRecoveryPoints

Obtém o intervalo de pontos de recuperação replicados em um Core servo remoto para o agente especificado. Não funciona com um Core mestre.

URI:
replication/cores/{coreId}/agents/{agentid}/skipCount/{skipCount}/maxCount/{maxCount}/recoveryPoints

Método HTTP: GET

SetAgentReplicationPauseConfiguration

Pausa a replicação do agente.

URI: replication/slaves/{slaveCoreId}/agents/{agentId}/pauseConfiguration

Método HTTP: POST

SetAgentReplicationPauseConfigurationForMasterCores

Pausa a replicação do agente.

URI: replication/masters/{masterCoreId}/agents/{agentId}/pauseConfiguration

Método HTTP: POST

SetAgentReplicationPauseConfigurationForSlaveCores

Pausa a replicação do agente.

URI: replication/slaves/agents/{agentId}/pauseConfiguration

Método HTTP: POST

SetAgentReplicationSettings

Ajusta as definições de replicação em um agente com o ID especificado.

URI: replication/agents/{agentId}

Método HTTP: PUT

SetRemoteSlaveCoreReplicationPolicy

Define a política de replicação do Core servo remoto. Funciona apenas no lado do Core mestre.
URI: replication/cores/slaves/{slaveCoreId}/settings/policy
Método HTTP: PUT

SetReplicationConfiguration

Define a configuração de replicação.
URI: replication/config
Método HTTP: PUT

SwitchFailoverAgentToReplicated

Converte o agente replicado para ativação pós-falha.
URI: replication/cores/{coreId}/agents/{agentId}/failover
Método HTTP: POST

SwitchReplicatedAgentToFailover

Converte o agente de ativação pós-falha para agente replicado.
URI: replication/cores/{coreId}/agents/{agentId}/failback?ignoreRunningReplicationJobs={ignoreReplication}
Método HTTP: POST

UpdateSlaveCoreSettings

Define a configuração do Core servo remoto. Funciona apenas no lado do Core mestre.
URI: replication/cores/slaves/{slaveCoreId}/settings
Método HTTP: PUT

VerifyAddAgentsByDemand

Confirma se agentes podem ser replicados sob demanda com segurança.
URI: replication/cores/slave/agents/demand/verify
Método HTTP: POST

VerifyAddAgentsByDemandForExistingCore

Confirma se agentes podem ser replicados sob demanda com segurança.
URI: replication/cores/slave/{coreId}/agents/demand/verify
Método HTTP: POST

VerifyAddAgentsByRequest

Confirma se agentes podem ser replicados por solicitação com segurança.
URI: replication/cores/slave/agents/request/verify
Método HTTP: POST

VerifyAddAgentsByRequestForExistingCore

Confirma se agentes podem ser replicados por solicitação com segurança.

URI: replication/cores/slave/{coreId}/agents/request/verify

Método HTTP: POST

VerifyCorePairingAbilityByDemand

Testa um descritor de Core para validar a capacidade de criar emparelhamento ao Core remoto. Retorna CoreId. Usa autenticação NTLM.

URI: replication/cores/verify/demand

Método HTTP: PUT

VerifyCorePairingAbilityByRequest

Testa um descritor de Core para validar a capacidade de criar emparelhamento ao Core remoto. Retorna CoreId. Usa autenticação anônima.

URI: replication/cores/verify/request/{hostUri}

Método HTTP: PUT

IReportingManagement

Esta seção descreve as operações de serviço disponíveis para IReportingManagement em report/.

O contrato de serviço IReportingManagement é a interface implementada pelo serviço de gerenciamento de relatórios do Core, que fornece funcionalidade de relatórios.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetAgentFailureReport
- GetAgentReport
- GetCoreFailureReport
- GetCoreReport
- GetDatabaseCoreIdentities
- GetSelfFailureReport
- GetSelfFailureReport
- GetSelfReport
- GetSummaryReport

GetAgentFailureReport

Obtém um relatório de falha para um agente específico

URI: report/agentFailureReport

Método HTTP: PUT

GetAgentReport

Obtém um relatório para um agente específico

URI: report/agentReport

Método HTTP: PUT

GetCoreFailureReport

Obtém um relatório de falha para um conjunto de Cores específico

URI: report/coreFailureReport

Método HTTP: PUT

GetCoreReport

Obtém um relatório para um conjunto de Cores específico.

URI: report/coreReport

Método HTTP: PUT

GetDatabaseCoreIdentities

Obtém a identidade (pares ID-nome) de Cores que possuem dados de relatórios no banco de dados usado atualmente pelo Core.

URI: report/databaseCoreIdentities

Método HTTP: GET

GetSelfFailureReport

Obtém um relatório de falha para esse Core.

URI: report/selfFailureReport

Método HTTP: PUT

GetSelfReport

Obtém um relatório para esse Core.

URI: report/selfReport

Método HTTP: PUT

GetSummaryReport

Obtém um relatório resumido para esse Core.

URI: report/summaryReport

Método HTTP: PUT

IRepositoryManagement

Esta seção descreve as operações de serviço disponíveis para IRepositoryManagement em reposManagement/.

O contrato de serviço IRepositoryManagement é a interface implementada pelo serviço de gerenciamento de repositório, que lida com as operações do Core relacionadas aos repositórios.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddExistentByConfigurations
- AddExistentWithIds
- AppendRepositoryFiles
- ApplyDefaultDeduplicationCacheConfiguration
- CheckRepository
- CheckRepositoryIntegrity
- CheckRepositoryIntegrityEstimate
- Create
- DeleteRepository
- GetConfiguration
- GetExistent
- GetFailedDirectories
- GetFreeDiskSpace
- GetRepositories
- GetRepositoriesCacheInfo
- GetRepositoryById
- GetRepositoryCacheInfo
- GetRepositoryFile
- GetRepositorySummaries
- GetRepositoryUsage
- IsRepoErrors
- IsRepositoryMounted
- MoveRepositoryFile
- ReformatRepository
- RenameRepository
- SetConfiguration
- SetRepositoryCacheParameters
- SetRepositoryFileSpecification
- UpdateRepositoriesDirectories
- UpdateRepositorySpecification
- UpdateWriteCachePolicy
- ValidateDirectoryPath
- VerifyFileSpecifications
- VerifyNetworkCredentials
- VerifyPaths

AddExistentByConfigurations

Carrega um ou vários repositórios existentes.
URI: reposManagement/repositories/addexistentbyconfigurations
Método HTTP: POST

AddExistentWithIds

Carrega repositórios existentes por lista de GUID.
URI: reposManagement/repositories/addexistentwithids
Método HTTP: POST

AppendRepositoryFiles

Anexa e monta arquivos adicionais em um repositório ativo.
URI: reposManagement/repositories/{repositoryId}/append
Método HTTP: POST

ApplyDefaultDeduplicationCacheConfiguration

Cria a configuração padrão de cache de deduplicação.
URI: reposManagement/defaults
Método HTTP: PUT

CheckRepository

Verifica um repositório.
URI: reposManagement/repositories/check
Método HTTP: POST

CheckRepositoryIntegrity

Verifica a integridade do repositório.
URI: reposManagement/repositories/checkRepositoryIntegrity
Método HTTP: POST

CheckRepositoryIntegrityEstimate

Estima a duração do trabalho de verificação de repositório.
URI: reposManagement/repositories/{repositoryId}/checkRepositoryIntegrityEstimate
Método HTTP: GET

Create

Cria um novo repositório.
URI: reposManagement/repositories
Método HTTP: PUT

DeleteRepository

Exclui o repositório especificado e todos os dados que ele contém.
URI: reposManagement/repositories/{repositoryId}
Método HTTP: DELETE

GetConfiguration

Define a configuração do serviço de repositório.
URI: reposManagement/config
Método HTTP: GET

GetExistent

Mostra a lista de repositórios existentes descritos pelo arquivo de configuração no diretório especificado.
URI: reposManagement/repositories/getexistent
Método HTTP: POST

GetFailedDirectories

Obtém os caminhos de diretórios de repositórios que não passam pela validação.
URI: reposManagement/repositories/failedDirectories
Método HTTP: GET

GetFreeDiskSpace

Obtém o espaço livre no diretório ou compartilhamento UNC.
URI: reposManagement/getFreeDiskSpace
Método HTTP: POST

GetRepositories

Obtém uma lista de todos os repositórios, incluindo configuração e status.
URI: reposManagement/repositories
Método HTTP: GET

GetRepositoriesCacheInfo

Obtém informações de cache de todos os repositórios.
URI: reposManagement/repositories/getRepositoriesCacheInfo
Método HTTP: POST

GetRepositoryById

Obtém informações sobre configuração e status de um repositório.
URI: reposManagement/repositories/{id}/id
Método HTTP: GET

GetRepositoryCacheInfo

Obtém as informações de cache do repositório.
URI: reposManagement/repositories/{repositoryId}/getRepositoryCacheInfo
Método HTTP: POST

GetRepositoryFile

Obtém as informações de configuração e status de um arquivo de repositório.
URI: reposManagement/repositories/{repositoryId}/files/{fileId}
Método HTTP: GET

GetRepositorySummaries

Obtém uma lista de todos os repositórios, incluindo configuração e status.
URI: reposManagement/repositorySummaries
Método HTTP: GET

GetRepositoryUsage

Obtém os usos atuais de um repositório especificado.
URI: reposManagement/repositories/{id}/usage
Método HTTP: GET

IsRepoErrors

Verifica se há algum repositório com erros. Retorna verdadeiro se ao menos um repositório contém erros.
URI: reposManagement/repositories/isRepoErrors
Método HTTP: GET

IsRepositoryMounted

Confirma se os caminhos de um determinado repositório estão acessíveis.
URI: reposManagement/repositories/{repositoryId}/isRepositoryMounted
Método HTTP: POST

MoveRepositoryFile

Move um arquivo de repositório.
URI: reposManagement/repositories/move
Método HTTP: POST

ReformatRepository

Reformata o repositório, excluindo os pontos de recuperação existentes.
URI: reposManagement/repositories/{repositoryId}/format
Método HTTP: POST

RenameRepository

Altera o nome de um repositório.
URI: reposManagement/repositories/{repositoryId}/{newReposName}/rename
Método HTTP: POST

SetConfiguration

URI: Define a configuração do serviço de repositório.
reposManagement/config
Método HTTP: POST

SetRepositoryCacheParameters

Atualiza os parâmetros de cache de um repositório.
URI: reposManagement/repositories/{repositoryId}/setRepositoryCacheParameters
PUT

SetRepositoryFileSpecification

Atualiza uma especificação de arquivo de repositório.
URI: reposManagement/repositories/{repositoryId}/file/{repositoryFileId}
PUT

UpdateRepositoriesDirectories

Atualiza os diretórios de repositórios.
URI: reposManagement/repositories/updateDirectories
PUT

UpdateRepositorySpecification

Aplica uma nova especificação a um repositório.
URI: reposManagement/repositories/updateRepositorySpecification
PUT

UpdateWriteCachePolicy

Atualiza as políticas de cache de gravação de arquivos.
URI: reposManagement/repositories/{repositoryId}/writePolicy
PUT

ValidateDirectoryPath

Realiza a validação do caminho do diretório de repositório especificado.
URI: reposManagement/repositories/validateDirectoryPath
POST

VerifyFileSpecifications

Confirma os caminhos e o espaço livre nos dispositivos especificados.

URI: reposManagement/repositories/verifyFileSpecifications

POST

VerifyNetworkCredentials

Confirma as credenciais de rede para os caminhos especificados.

URI: reposManagement/repositories/verifyNetworkCredentials

POST

VerifyPaths

Confirma se os caminhos de um determinado repositório estão acessíveis.

URI: reposManagement/repositories/{repositoryId}/verifyPaths

POST

IRollbackManagement

Esta seção descreve as operações de serviço disponíveis para IRollbackManagement em rollback/.

O contrato de serviço IRollbackManagement é a interface implementada pelo serviço de reversão do Core, que fornece funcionalidade do mecanismo Replay para restaurar dados a partir de pontos de recuperação.

NOTA: O recurso de restauração era designado anteriormente como *reversão*. Esse termo não é mais usado.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- CheckJobByAgentId
- CheckJobByRrcIp
- GeneratePartitionPlan
- GetDatabasesForRemount
- GetSummaryMetadata
- GetTargetDisks
- GetTargetInfo
- GetTargetVolumes
- StartRollback
- ValidateStoragePoolSettings
- ValidateSystemVolumeExistence
- VerifyRollbackRequest

CheckJobByAgentId

Verifica o estado do trabalho de reversão usando o ID de agente.

URI: rollback/checkJobByAgentId/{agentId}

Método HTTP: POST

CheckJobByRrcIp

Verifica o estado do trabalho de reversão usando o endereço IP do agente RRC.
URI: rollback/checkJobByRrcIp/{agentIp}
Método HTTP: POST

GeneratePartitionPlan

Gera um plano de partição para um determinado ponto de recuperação, lista de volumes e discos de destino.
URI: rollback/autoPartition
Método HTTP: POST

GetDatabasesForRemount

Obtém uma lista de bancos de dados para remontagem e avisos.
URI: rollback/databasesForRemount
Método HTTP: POST

GetSummaryMetadata

Obtém os discos que estão disponíveis em um determinado destino de reversão (restauração).
URI: rollback/summarymetadata
Método HTTP: PUT

GetTargetDisks

Obtém os discos que estão disponíveis em um determinado destino de reversão (restauração).
URI: rollback/targetDisks
Método HTTP: POST

GetTargetInfo

Obtém os discos e volumes que estão disponíveis em um determinado destino de reversão (restauração).
URI: rollback/targetInfo
Método HTTP: POST

GetTargetVolumes

Obtém os volumes que estão disponíveis em um determinado destino de reversão (restauração).
URI: rollback/targetVolumes
Método HTTP: POST

StartRollback

Inicia um trabalho de reversão (restauração).
URI: rollback/target
Método HTTP: POST

ValidateStoragePoolSettings

Valida se o recurso de pool de armazenamento foi ativado na máquina protegida.

URI: rollback/storagepool

Método HTTP: POST

ValidateSystemVolumeExistence

Valida a existência do volume do sistema.

URI: rollback/validateSystemVolumeExistence

Método HTTP: POST

VerifyRollbackRequest

Confirma a solicitação de reversão (restauração) de volumes e discos.

URI: rollback/verifyRollbackRequest

Método HTTP: POST

IRollupManagement

Esta seção descreve as operações de serviço disponíveis para IRollupManagement em rollup/.

O contrato de serviço IRollupManagement é a interface implementada pelo serviço de gerenciamento de rollup do Core, que fornece funcionalidade de rollup do mecanismo Replay.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ClearAgentRetentionPolicy
- ForceRollup
- GetAgentRetentionPolicy
- GetCoreRollupConfiguration
- GetGranularityIntervals
- SetAgentRetentionPolicy
- SetCoreRollupConfiguration

ClearAgentRetentionPolicy

Limpa a política de retenção de um agente e usa em seu lugar a política padrão do Core.

URI: rollup/agents/{agentId}

Método HTTP: DELETE

ForceRollup

Força um trabalho de rollup para o agente com o ID especificado.

URI: rollup/agents/{agentId}/force

Método HTTP: POST

GetAgentRetentionPolicy

Obtém a política de retenção para um ID de agente especificado.
URI: rollup/agents/{agentId}
Método HTTP: GET

GetCoreRollupConfiguration

Obtém a configuração de rollup do Core.
URI: rollup/config
Método HTTP: GET

GetGranularityIntervals

Obtém intervalos de granularidade para a linha do tempo de retenção.
URI: rollup/granularityIntervals
Método HTTP: PUT

SetAgentRetentionPolicy

Define a política de retenção no agente com o ID especificado.
URI: rollup/agents/{agentId}
Método HTTP: PUT

SetCoreRollupConfiguration

Define a configuração de rollup do Core.
URI: rollup/config
Método HTTP: PUT

ISeedDriveManagement

Esta seção descreve as operações de serviço disponíveis para ISeedDriveManagement em seedDrive/.

O contrato de serviço ISeedDriveManagement é a interface implementada pelo serviço de gerenciamento da unidade de propagação, que fornece funcionalidade de cópia e consumo do mecanismo Replay.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AbandonOutstandingSeedDrive
- GetConsumedSeedDrives
- GetOutstandingSeedDrives
- GetSeedDriveManifest
- StartConsumeSeedDrive
- StartCopySeedDrive

AbandonOutstandingSeedDrive

Exclui uma unidade de propagação da lista de unidades de propagação que estão aguardando consumo.

URI: seedDrive/outstandingSeedDrives/{seedDriveId}

Método HTTP: DELETE

GetConsumedSeedDrives

Obtém informações sobre unidades de propagação consumidas pelo agente replicado especificado no Core servo.

URI: seedDrive/consumedSeedDrives/{agentId}

Método HTTP: GET

GetOutstandingSeedDrives

Obtém unidades de propagação pendentes no Core mestre que estão aguardando consumo em Cores servos.

URI: seedDrive/outstandingSeedDrives

Método HTTP: GET

GetSeedDriveManifest

Obtém os metadados de uma unidade de propagação existente pelo ID do Core.

URI: seedDrive/metadataByCore/{coreId}

Método HTTP: POST

StartConsumeSeedDrive

Inicia o consumo de dados de pontos de recuperação a partir da unidade de propagação especificada pelo usuário.

URI: seedDrive/consume

Método HTTP: POST

StartCopySeedDrive

Inicia a cópia de dados de pontos de recuperação para a unidade de propagação especificada pelo usuário.

URI: seedDrive/copy

Método HTTP: POST

IServiceHostManagement

Esta seção descreve as operações de serviço disponíveis para IServiceHostManagement em servicehost/.

O contrato de serviço IServiceHostManagement é a interface implementada por uma classe que fornece uma interface de gerenciamento para o IServiceHost.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetApiVersionInfo
- GetConfiguration
- Restart
- SetConfiguration

- VerifyConnection

GetApiVersionInfo

Obtém informações sobre a versão da API.
URI: servicehost/apiVersion
Método HTTP: GET

GetConfiguration

Obtém a configuração atual de um servidor que aguarda chamadas REST.
URI: servicehost/config
Método HTTP: GET

Restart

Reinicia imediatamente um servidor que aguarda chamadas REST.
URI: servicehost/restart
Método HTTP: GET

SetConfiguration

Define a configuração atual de um servidor que aguarda chamadas REST.
URI: servicehost/config
Método HTTP: POST

VerifyConnection

Permite confirmar se o servidor de escuta está configurado corretamente e é capaz de receber chamadas REST.
URI: servicehost/verify
Método HTTP: GET

ISqlManagement

Esta seção descreve as operações de serviço disponíveis para ISqlManagement em sql/.

O contrato de serviço ISqlManagement é a interface implementada pelo serviço de gerenciamento de SQL do Core, que fornece verificações de capacidade de anexação e outras funcionalidades de gerenciamento de SQL específicas do Core.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- ForceAttachability
- GetAttachabilitySettings
- GetCoreSqlInstances
- SetAttachabilitySettings
- TestSqlConnection

ForceAttachability

Força um trabalho de capacidade de anexação para o agente com o ID especificado.
URI: sql/recoveryPoints/{recoveryPointId}/force
Método HTTP: POST

GetAttachabilitySettings

Obtém as definições de capacidade de anexação no nível de Core.
URI: sql/attachabilitySettings
Método HTTP: GET

GetCoreSqlInstances

Obtém as definições de capacidade de anexação no nível de Core.
URI: sql/coreSqlInstances
Método HTTP: GET

SetAttachabilitySettings

Obtém as definições de capacidade de anexação no nível de Core.
URI: sql/attachabilitySettings
Método HTTP: PUT

TestSqlConnection

Ajusta as definições de capacidade de anexação no nível de Core.
URI: sql/connection
Método HTTP: PUT

IStatusSummaryManagement

Esta seção descreve as operações de serviço disponíveis para IStatusSummaryManagement em status/.

O contrato de serviço IStatusSummaryManagement expõe informações de status resumidas sobre vários serviços no Core que são usados para exibir ícones de status nas guias da GUI.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- Crash
- GetAgentDashboardInfo
- GetCoreEventsInfo
- GetCoreHomeInfo
- GetCoreSystemInfo
- GetDashboardInfo
- GetFailedServicesInfo
- GetLatestEvents
- GetStatusSummary
- RetryStartFailedServices

Crash

Interrompe o processo.

URI: status/crash

Método HTTP: GET

GetAgentDashboardInfo

Obtém informações de status de um Agent específico.

URI: status/dashboard/{agentId}

Método HTTP: GET

GetCoreEventsInfo

Obtém informações sobre os eventos mais recentes do Core, como os eventos acumulados desde a última chamada para si próprio ou do início do Core se a chamada veio primeiro.

URI: status/coreEventsInfo

Método HTTP: POST

GetCoreHomeInfo

Obtém metadados do Core e 10 alertas recentes.

URI: status/coreHomeInfo

Método HTTP: GET

GetCoreSystemInfo

Obtém informações do sistema do Core, como montagens, metadados, definições, configuração de repositório e assim por diante.

URI: status/coreSystemInfo

Método HTTP: GET

GetDashboardInfo

Obtém as informações de status necessárias para exibir o painel na tela principal.

URI: status/dashboard

Método HTTP: GET

GetFailedServicesInfo

Obtém os nomes dos serviços com falha de inicialização.

URI: status/failedServicesInfo

Método HTTP: GET

GetLatestEvents

Obtém informações sobre os eventos mais recentes do Core, como os eventos acumulados desde a última chamada para si próprio ou do início do Core se a chamada veio primeiro.

URI: status/latestEventsInfo

Método HTTP: GET

GetStatusSummary

Obtém um resumo do status de todos os serviços, incluindo a API de resumo de status.
URI: status/statusSummary
Método HTTP: GET

RetryStartFailedServices

Tenta reiniciar os serviços com falha.
URI: status/restart/
Método HTTP: POST

ITransferQueueManagement

Esta seção descreve as operações de serviço disponíveis para ITransferQueueManagement em xfer/queue/.

O contrato de serviço ITransferQueueManagement é a API RESTful da fila de transferência.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AdjustTransferPriority
- CancelAllTransfers
- CancelTransfer
- GetActiveQueueEntries
- GetEntryInfo
- GetPendingQueueEntries
- GetQueueConfiguration
- GetQueueContents
- SetQueueConfiguration

AdjustTransferPriority

Ajusta a prioridade da transferência na fila.
URI: xfer/queue/entries/{transferid}
Método HTTP: POST

CancelAllTransfers

Cancela todas as transferências na fila.
URI: xfer/queue/entries
Método HTTP: DELETE

CancelTransfer

Cancela a entrada da fila de transferência identificada pelo ID de transferência.
URI: xfer/queue/entries/{transferid}
Método HTTP: DELETE

GetActiveQueueEntries

Obtém as entradas ativas na fila de transferência.

URI: xfer/queue/activeEntries

Método HTTP: GET

GetEntryInfo

Obtém as informações de uma entrada específica na fila de transferência.

URI: xfer/queue/entries/{transferid}

Método HTTP: GET

GetPendingQueueEntries

Obtém as entradas pendentes na fila de transferência.

URI: xfer/queue/pendingEntries

Método HTTP: GET

GetQueueConfiguration

Obtém a configuração da fila de transferência.

URI: xfer/queue/config

Método HTTP: GET

GetQueueContents

Obtém o conteúdo da fila de transferência.

URI: xfer/queue/entries

Método HTTP: GET

SetQueueConfiguration

Define a configuração da fila de transferência.

URI: xfer/queue/config

Método HTTP: POST

ITransferSchedulerManagement

Esta seção descreve as operações de serviço disponíveis para ITransferSchedulerManagement em xfer/schedule/. O contrato de serviço ITransferSchedulerManagement é a API RESTful do programador de transferência.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- AddScheduleTemplate
- ApplyRepositoryToUnprotectedAgents
- BatchAgentsProtectionPaused
- BatchAgentsProtectionResumed
- DeleteScheduleTemplate

- ForceAllTransfer
- ForceTransfer
- GetActualAgentProtectionConfiguration
- GetAgentConfiguration
- GetCachedAgentProtectionConfiguration
- GetScheduleTemplate
- GetScheduleTemplates
- RemoveRepositoryFromProtection
- SetAgentConfiguration
- SetAgentProtectionConfiguration
- UpdateScheduleTemplate

AddScheduleTemplate

Obtém a coleção de modelos de programa de transferência.
URI: xfer/schedule/transferScheduleTemplates
Método HTTP: POST

ApplyRepositoryToUnprotectedAgents

Aplica um novo repositório a agentes que não têm um repositório.
URI: xfer/schedule/applyrepository/{repositoryName}
Método HTTP: PUT

BatchAgentsProtectionPaused

Pausa a proteção de vários agentes.
URI: xfer/schedule/agentsPaused
Método HTTP: POST

BatchAgentsProtectionResumed

Retoma a proteção de vários agentes.
URI: xfer/schedule/agentsResumed
Método HTTP: POST

DeleteScheduleTemplate

Remove um modelo de programa de transferência.
URI: xfer/schedule/transferScheduleTemplates/{templateId}
Método HTTP: DELETE

ForceAllTransfer

Força uma transferência imediata de todos os agentes disponíveis.
URI: xfer/schedule/forcealltransfer
Método HTTP: POST

ForceTransfer

Força uma transferência imediata do grupo de proteção especificado.
URI: xfer/schedule/{agentId}/transfer
Método HTTP: POST

GetActualAgentProtectionConfiguration

Obtém os grupos de proteção reais configurados para o agente.
URI: xfer/schedule/{agentId}/actualProtectionConfiguration
Método HTTP: GET

GetAgentConfiguration

Obtém as definições de configuração de transferência do agente.
URI: xfer/schedule/{agentId}/config
Método HTTP: GET

GetCachedAgentProtectionConfiguration

Define os grupos de proteção configurados para o agente.
URI: xfer/schedule/{agentId}/pgs
Método HTTP: GET

GetScheduleTemplate

Obtém o modelo de programa de transferência por ID.
URI: xfer/schedule/transferScheduleTemplates/{templateId}
Método HTTP: GET

GetScheduleTemplates

Obtém a coleção de modelos de programa de transferência.
URI: xfer/schedule/transferScheduleTemplates
Método HTTP: GET

RemoveRepositoryFromProtection

Desassocia agentes de um repositório nomeado (por exemplo, um que tenha sido excluído).
URI: xfer/schedule/removerepository/{repositoryName}
Método HTTP: DELETE

SetAgentConfiguration

Ajusta as definições de configuração de transferência do agente.
URI: xfer/schedule/{agentId}/config
Método HTTP: PUT

SetAgentProtectionConfiguration

Define os grupos de proteção configurados para o agente.

URI: xfer/schedule/{agentId}/pgs
Método HTTP: PUT

UpdateScheduleTemplate

Atualiza um modelo de programa de transferência existente.
URI: xfer/schedule/transferScheduleTemplates/{templateId}
Método HTTP: PUT

IUtilitiesManagement

Esta seção descreve as operações de serviço disponíveis para IUtilitiesManagement em utilities/. O contrato de serviço IUtilitiesManagement é a API para diversos auxiliares.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetDomainInfo
- GetMachinesFromActiveDirectory
- GetMachinesFromActiveDirectoryByPage

GetDomainInfo

Obtém informações sobre domínio.
URI: utilities/domainInformation
Método HTTP: POST

GetMachinesFromActiveDirectory

Obtém todas as máquinas do Active Directory.
URI: utilities/activeDirectoryMachines
Método HTTP: POST

GetMachinesFromActiveDirectoryByPage

Obtém máquinas por página específica do Active Directory.
URI: utilities/activeDirectoryMachinesByPage
Método HTTP: POST

IVirtualDiskManagement

Esta seção descreve as operações de serviço disponíveis para IVirtualDiskManagement em vhd/. São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- BaseFileName
- BeginBatch
- Close
- Create
- Delete

- EndBatch
- HasSnapshot
- Open
- Read
- ReadCustomMetadata
- SectorSize
- SnapshotFileName
- TakeSnapshot
- TotalSectorCapacity
- TranslateSectorOffsetToChsTuple
- Write
- WriteCustomMetadata

BaseFileName

Obtém o nome do arquivo base do VHD.

URI: vhd/{id}/baseFileName

Método HTTP: GET

BeginBatch

Inicia o lote.

URI: vhd/{id}/beginBatch/{target}

Método HTTP: POST

Close

Fecha o VHD.

URI: vhd/{id}/close

Método HTTP: GET

Create

Cria um VHD.

URI:
vhd/createVhd?path={path}&bytesCapacity={bytesCapacity}&bytesPerSector={bytesPerSector}&containsBootSystemVolume={containsBootSystemVolume}&preallocate={preallocate}

Método HTTP: PUT

Delete

Exclui um snapshot ou arquivo base de VHD.

URI: vhd/{id}/delete/{target}

Método HTTP: POST

EndBatch

Encerra o lote.

URI: vhd/{id}/endBatch
Método HTTP: POST

HasSnapshot

Confirma se o VHD possui snapshot.
URI: vhd/{id}/hasSnapshot
Método HTTP: GET

Open

Abre o VHD.
URI: vhd/openVhd?path={path}
Método HTTP: PUT

Read

Grava dados brutos em VHD.
URI: vhd/{id}/read/{target}/{sectorOffset}/{sectorLength}
Método HTTP: POST

ReadCustomMetadata

Lê uma cadeia de caracteres de metadados personalizada definida pelo usuário.
URI: vhd/{id}/readCustomMetadata/{target}/{key}
Método HTTP: POST

SectorSize

Obtém o tamanho de setor do VHD.
URI: vhd/{id}/sectorSize
Método HTTP: GET

SnapshotFileName

Obtém o nome do arquivo de snapshot do VHD.
URI: vhd/{id}/snapshotFileName
Método HTTP: GET

TakeSnapshot

Gera um snapshot do VHD.
URI: vhd/{id}/takeSnapshot
Método HTTP: GET

TotalSectorCapacity

Obtém a capacidade do VHD.
URI: vhd/{id}/totalSectorCapacity
Método HTTP: GET

TranslateSectorOffsetToChsTuple

Traduz o deslocamento de setor para tupla CHS.

URI: vhd/{id}/translateSectorOffsetToChsTuple?sectorOffset={sectorOffset}

Método HTTP: GET

Write

Grava dados brutos em VHD.

URI: vhd/{id}/write/{target}/{sectorOffset}/{sectorLength}

Método HTTP: POST

WriteCustomMetadata

Lê uma cadeia de caracteres de metadados personalizada definida pelo usuário.

URI: vhd/{id}/writeCustomMetadata/{target}/{key}?value={value}

Método HTTP: POST

IWhiteLabelingManagement

Esta seção descreve as operações de serviço disponíveis para IWhiteLabelingManagement em whitelabeling/. O contrato de serviço IWhiteLabelingManagement expõe as cadeias de caracteres personalizáveis.

São fornecidos o URI e o método HTTP da operação de serviço, como se segue:

- GetWhiteLabelingInfo

GetWhiteLabelingInfo

Obtém cadeias de caracteres personalizáveis.

URI: whitelabeling/whiteLabelingInfo

Método HTTP: GET

Uso da API AppAssure Agent

A API AppAssure Agent é agrupada de acordo com as seguintes interfaces de categorias/serviços. Clique em uma categoria abaixo para exibir mais informações sobre as operações de serviço disponíveis para uma interface específica.

Os contratos de serviço contidos no conjunto de cliente do Agent são descritos na tabela a seguir:

Tabela 2. Contratos de serviço do Agent

Contrato de serviço	Uri	Descrição
IAgentMetadataManagement	metadata/	Interface implementada pelo serviço de metadados do agente, que mantém, armazena em cache e retorna metadados do agente.
IAgentPairManagement	pair/	Interface implementada pelo serviço de emparelhamento de agente, que fornece funcionalidade de emparelhamento nos agentes.
IAgentServiceHostManagement	agentServiceHost/	Interface implementada pelo serviço Agent, que realiza ações relacionadas ao ServiceHost do Agent.

Tabela 2. Contratos de serviço do Agent

Contrato de serviço	Uri	Descrição
IAgentSettingsManagement	settings/	Permite consultar e ajustar diversas definições do agente.
IAgentUpdateManagement	update/	Interface implementada pelo serviço de atualização do agente, que baixa e instala atualizações.
IApplicationIdManagement	id/	Expõe o ID exclusivo do aplicativo.
IDiagnosticsManagement	diag/	Replay.Common.Contracts.Diagnostics.IDiagnosticsManagement
IDriverChangeLogsManagement	driverchangelogs/	Fornece a capacidade de gerenciar logs de alterações AAFsFlt: enumerar, excluir, controlar a ativação de volumes.
IExchangeManagement	exchangedll/	Permite carregar DLLs do MS Exchange para o Core.
IExchangeServerManagement	exchangeServer/	Permite executar o comando no servidor do Exchange instalado na máquina física.
IHyperVAgentManagement	hypervagent/	Replay.Common.Contracts.Virtualization.IHyperVAgentManagement.
IPowerShellManagement	powerShell/	Interface que permite executar o script com parâmetros de um arquivo.
IRollbackManagement	rollback/	Serviço REST que expõe métodos para iniciar a restauração de dados de um ponto de recuperação em um agente.
IRrcRollbackManagement	rollback/	Serviço REST que expõe métodos para iniciar a restauração de dados de um ponto de recuperação em um agente.
IServiceHostManagement	servicehost/	Interface implementada por uma classe que fornece uma interface de gerenciamento ao IServiceHost.
IShadowCopyManagement	shadowcopy/	Expõe algumas informações de diagnóstico sobre o serviço Volume Shadow Copy (VSS).
ITransferManagement	transfer/	Interface de contrato WCF implementada por uma classe que implementa a interface de gerenciamento sobre o serviço de transferência.
IVirtualDiskManagement	vhd/	Replay.Common.Contracts.Virtualization.IVirtualDiskManagement
IWhiteLabelingManagement	whitelabeling/	Expõe as cadeias de caracteres personalizáveis.

IAgentMetadataManagement

Esta seção descreve as operações de serviço disponíveis para IAgentMetadataManagement em metadata/.

A interface IAgentMetadataManagement é implementada pelo serviço de metadados do agente, que mantém, armazena em cache e retorna metadados do agente.

São fornecidos o URI e o método HTTP de cada operação de serviço.

As operações de serviço incluem:

- GetCurrent
- GetCurrentCluster

- GetCurrentClusterSummary
- GetCurrentDeduplicationJobs
- GetCurrentSummary
- VerifyCredentials

GetCurrent

Obtém metadados completos armazenados em cache para o agente.

URI: metadata/fullMetadata

Método HTTP: PUT

GetCurrentCluster

Obtém metadados completos armazenados em cache para o agente.

URI: metadata/fullClusterMetadata

Método HTTP: PUT

GetCurrentClusterSummary

Obtém metadados completos armazenados em cache para o agente.

URI: metadata/fullClusterSummaryMetadata

Método HTTP: PUT

GetCurrentDeduplicationJobs

Obtém a lista dos trabalhos de deduplicação ativos atualmente.

URI: metadata/currentDeduplicationJobs

Método HTTP: GET

GetCurrentSummary

Obtém metadados resumidos armazenados em cache para o agente com metadados de servidores MS Exchange e SQL.

URI: metadata/summaryMetadata

Método HTTP: PUT

VerifyCredentials

Confirma as credenciais especificadas para servidores MS Exchange e SQL.

URI: metadata/credentials

Método HTTP: PUT

IAgentPairManagement

Esta seção descreve as operações de serviço disponíveis para IAgentPairManagement em pair/.

A interface IAgentPairManagement é implementada pelo serviço de emparelhamento de agente, que fornece funcionalidade de emparelhamento aos agentes.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- GetPairingSettings

- Pair
- RemovePairing
- VerifyConnect
- VerifyConnectWithOptionalAuthentication

GetPairingSettings

Obtém as definições de emparelhamento do Agent, incluindo ID do agente, nome do Core emparelhado e impressões digitais de certificado de segurança.

URI: pair/

Método HTTP: GET

Pair

Define um relacionamento entre um Core e o Agent, incluindo a troca de certificados de segurança.

URI: pair/

Método HTTP: PUT

RemovePairing

Remove o relacionamento entre o Agent e um Core.

URI: pair/

Método HTTP: DELETE

VerifyConnect

Permite confirmar a conexão com o agente especificado e retorna o ID real do agente.

URI: pair/connect

Método HTTP: GET

VerifyConnectWithOptionalAuthentication

Permite confirmar a conexão com o agente especificado, com esquema de autenticação opcional, e retorna o ID real do agente.

URI: pair/connect/?useNtlmOnly={useNtlmOnly}

Método HTTP: GET

IAgentServiceHostManagement

Esta seção descreve as operações de serviço disponíveis para IAgentServiceHostManagement em agentServiceHost/.

A interface IAgentServiceHostManagement é implementada pelo serviço Agent, que realiza ações relacionadas ao ServiceHost do Agent.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- ChangePort

ChangePort

Altera o número da porta usada pelo servidor que aguarda chamadas REST.

URI: agentServiceHost/port

Método HTTP: POST

IAgentSettingsManagement

Esta seção descreve as operações de serviço disponíveis para IAgentSettingsManagement em settings/.

O contrato de serviço IAgentSettingsManagement permite consultar e ajustar diversas definições para todos os agentes.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- GetAgentSettings
- SetAgentSettings

GetAgentSettings

Obtém definições globais gerais do Agent, como definições de tempo limite e nome de exibição.

URI: settings/agent

Método HTTP: GET

SetAgentSettings

Aplica definições globais gerais do Core, como, por exemplo, definições de tempo limite e nome de exibição.

URI: settings/agent

Método HTTP: PUT

IAgentUpdateManagement

Esta seção descreve as operações de serviço disponíveis para IAgentUpdateManagement em update/.

A interface IAgentUpdateManagement é implementada pelo serviço de atualização de agente, que baixa e instala atualizações.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- ApplyUpdate

ApplyUpdate

Realiza a atualização automática dos binários de serviço do Agent. Esse método é apenas para uso interno e não deve ser chamado pelos usuários.

URI: update/

Método HTTP: POST

IApplicationIdManagement

Esta seção descreve as operações de serviço disponíveis para IApplicationIdManagement em id/.

IApplicationIdManagement expõe o ID exclusivo do aplicativo.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- GetId

GetId

Obtém o ID do Core.

URI: id/

Método HTTP: GET

IDiagnosticsManagement

Esta seção descreve as operações de serviço disponíveis para IDiagnosticsManagement em diag/.

O contrato de serviço IDiagnosticsManagement é representado como Replay.Common.Contracts.Diagnostics.IDiagnosticsManagement.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- ExecuteRemoteCommand
- GetLog
- GetLogSession
- ReadFile
- RestartService
- UploadLogSessions

ExecuteRemoteCommand

Executa um comando remoto arbitrário.

URI: diag/command/

Método HTTP: POST

GetLog

Obtém todo o conteúdo do arquivo replay.log.

URI: diag/log/

Método HTTP: GET

GetLogSession

Empacota a sessão de log atual e a retorna como um fluxo de bytes. O conteúdo do fluxo é um Gibraltar (arquivo .glp).

URI: diag/logSession/

Método HTTP: GET

ReadFile

Lê um arquivo no sistema de arquivos local e o envia por fluxo de dados de volta ao cliente.

URI: diag/files/?q={path}

Método HTTP: GET

RestartService

Interrompe, força o encerramento (se necessário) e reinicia o serviço.

URI: diag/service/

Método HTTP: DELETE

UploadLogSessions

Carrega a sessão de log atual na estrutura de logs do Gibraltar (http://www.gibraltarsoftware.com/).

URI: diag/logSession/

Método HTTP: POST

IDriverChangeLogsManagement

Esta seção descreve as operações de serviço disponíveis para IDriverChangeLogsManagement em driverchangelogs/.

IDriverChangeLogsManagement permite gerenciar logs de alterações AAFsFlt: enumerar, excluir, controlar a ativação de volumes.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- DeleteDriverChangeLogFile
- DisableVolumeLogging
- EnableVolumeLogging
- EnumerateDriverChangeLogs

DeleteDriverChangeLogFile

Exclui um arquivo de log de alterações especificado para um volume.

URI: driverchangelogs/{volumeName}/{changeLogFile}

Método HTTP: DELETE

DisableVolumeLogging

Desativa o log de alterações de FS para um volume.

URI: driverchangelogs/{volumeName}/disablelogging

Método HTTP: POST

EnableVolumeLogging

Ativa o log de alterações de FS para um volume.

URI: driverchangelogs/{volumeName}/enablelogging

Método HTTP: POST

EnumerateDriverChangeLogs

Obtém uma coleção de arquivos de log de alterações para um volume.

URI: driverchangelogs/{volumeName}/

Método HTTP: GET

IExchangeManagement

Esta seção descreve as operações de serviço disponíveis para IExchangeManagement em exchangedll/.

IExchangeManagement permite carregar DLLs do MS Exchange para o Core.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- CancelTransmitFile
- ContinueTransmitFile
- EndTransmitFile
- GetExchangeDllInfo
- StartNewFileTransmitSession

CancelTransmitFile

Cancela a sessão de transmissão atual.
URI: exchangedll/sessions/{fileTransmitSessionId}/
Método HTTP: DELETE

ContinueTransmitFile

Lê dados do agente na sessão de transmissão atual.
URI: exchangedll/sessions/{fileTransmitSessionId}/data/{bytesToRead}
Método HTTP: POST

EndTransmitFile

Encerra a sessão de transmissão atual.
URI: exchangedll/sessions/{fileTransmitSessionId}/
Método HTTP: POST

GetExchangeDllInfo

Obtém informações sobre a biblioteca do MS Exchange.
URI: exchangedll/{fileName}/
Método HTTP: GET

StartNewFileTransmitSession

Inicia uma nova sessão de transmissão de arquivo.
URI: exchangedll/newsession/
Método HTTP: POST

IExchangeServerManagement

Esta seção descreve as operações de serviço disponíveis para IExchangeServerManagement em exchangeServer/.

IExchangeServerManagement permite executar comandos no Servidor do Exchange instalado na máquina física.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- CancelExchangeServerCommand
- ExecuteExchangeServerCommand
- GetExchangeServerCommandStatus

CancelExchangeServerCommand

Cancela o comando em execução.
URI: exchangeServer/cancelCommand
Método HTTP: DELETE

ExecuteExchangeServerCommand

Inicia/interrompe suavemente o Servidor do Exchange.
URI: exchangeServer/executeCommand
Método HTTP: PUT

GetExchangeServerCommandStatus

Consulta o status da operação atual de início/interrupção do Servidor do Exchange.
URI: exchangeServer/getCommandStatus
Método HTTP: GET

IHyperVAgentManagement

Esta seção descreve as operações de serviço disponíveis para IHyperVAgentManagement em hypervagent/.

O contrato de serviço IHyperVAgentManagement é representado por Replay.Common.Contracts.Virtualization.IHyperVAgentManagement.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- AddDvdDrive
- AddIsoImage
- AddNetworkAdapter
- AttachVirtualDisk
- DeleteVirtualMachine
- DetachVirtualDisk
- EndSession
- GetAvailableVirtualNetworks
- GetMaximumProcessorCount
- GetOrCreateVirtualMachineAndAttach
- GetSnapshotsCount
- GetVirtualDisks
- GetVirtualMachineName
- InsertIntegrationServices
- PingSession

- RenameVirtualMachine
- SetProcessorCount
- SetRamMegabytes
- VerifyConnection

AddDvdDrive

Adiciona uma unidade de DVD à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/dvd
Método HTTP: PUT

AddIsoImage

Adiciona uma imagem ISO a uma unidade de DVD. Cria a unidade de DVD, caso ela não exista.
URI: hypervagent/{virtualMachineId}/iso/{isoPath}
Método HTTP: PUT

AddNetworkAdapter

Adiciona um novo adaptador de rede à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/nic/{networkAdapterName}
Método HTTP: PUT

AttachVirtualDisk

Conecta um disco virtual à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/disks/{diskPath}/{storageController}
Método HTTP: PUT

DeleteVirtualMachine

Exclui a máquina virtual atual e desconecta-se dela.
URI: hypervagent/existent/{virtualMachineId}
Método HTTP: DELETE

DetachVirtualDisk

Desconecta um disco virtual da máquina virtual atual.
URI: hypervagent/{virtualMachineId}/disks/{diskPath}
Método HTTP: DELETE

EndSession

Determina ao Hyper-V Agent que conclua a sessão com a máquina virtual.
URI: hypervagent/{virtualMachineId}/endsession
Método HTTP: DELETE

GetAvailableVirtualNetworks

Obtém uma lista de adaptadores de rede virtuais disponíveis para uma máquina virtual no servidor Hyper-V.
URI: hypervagent/{virtualMachineId}/availablevirtualnetworks
Método HTTP: GET

GetMaximumProcessorCount

Obtém o número máximo de CPUs virtuais que podem ser conectadas a uma máquina virtual.
URI: hypervagent/cpu/{operatingSystemFamily}
Método HTTP: GET

GetOrCreateVirtualMachineAndAttach

Obtém ou cria a máquina virtual especificada no parâmetro de solicitação.
URI: hypervagent/getOrCreate
Método HTTP: POST

GetSnapshotsCount

Obtém a contagem de snapshots da máquina virtual.
URI: hypervagent/{virtualMachineId}/getSnapshotsCount
Método HTTP: GET

GetVirtualDisks

Obtém uma lista de discos virtuais conectados à máquina virtual atual.
URI: hypervagent/{virtualMachineId}/disks
Método HTTP: GET

GetVirtualMachineName

Obtém o nome da máquina virtual atual.
URI: hypervagent/{virtualMachineId}/name
Método HTTP: GET

InsertIntegrationServices

Monta o disco de instalação dos serviços de integração.
URI: hypervagent/{virtualMachineId}/integrationservices
Método HTTP: PUT

PingSession

Indica que a sessão ainda está em uso.
URI: hypervagent/{virtualMachineId}/pingSession
Método HTTP: PUT

RenameVirtualMachine

Altera o nome da máquina virtual atual.
URI: hypervagent/{virtualMachineId}/newname/{newVirtualMachineName}
Método HTTP: PUT

SetProcessorCount

Altera o número de CPUs virtuais na máquina virtual atual.
URI: hypervagent/{virtualMachineId}/cpu/{processorCount}
Método HTTP: PUT

SetRamMegabytes

Altera a quantidade de RAM na máquina virtual atual.
URI: hypervagent/{virtualMachineId}/ram/{ramValue}
Método HTTP: PUT

VerifyConnection

Confirma a conexão ao Hyper-V Agent em execução.
URI: hypervagent/connect
Método HTTP: GET

IPowerShellManagement

Esta seção descreve as operações de serviço disponíveis para IPowerShellManagement em powerShell/.

A interface IPowerShellManagement permite executar scripts com parâmetros de um arquivo.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- RunPowerShellScriptFromFile

RunPowerShellScriptFromFile

Executa um script PowerShell no agente.
URI: powerShell/
Método HTTP: POST

IRollbackManagement

Esta seção descreve as operações de serviço disponíveis para IRollbackManagement em rollback/.

O serviço REST IRollbackManagement expõe métodos para iniciar a restauração de dados a partir de um ponto de recuperação em um agente.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- CancelRollback
- DeterminateAutomaticallyAcquiringReplayEngineAddress
- GetRollbackMountDismountStatus
- PartitionDisks

- StartDismounting
- StartMounting
- StartRollback

CancelRollback

Cancela a operação de reversão (restauração) em andamento.

URI: rollback/

Método HTTP: DELETE

DeterminateAutomaticallyAcquiringReplayEngineAddress

Determina se o agente pode determinar automaticamente a aquisição do endereço de ReplayEngine.

URI: rollback/determinateAutomaticallyAcquiringReplayEngineAddress

Método HTTP: GET

GetRollbackMountDismountStatus

Consulta o status da operação atual de reversão (restauração).

URI: rollback/

Método HTTP: GET

PartitionDisks

Realiza particionamento automático de discos com base em informações de partição em um objeto de solicitação. Todas as partições existentes são removidas.

URI: rollback/partition

Método HTTP: POST

StartDismounting

Desmonta a lista de bancos de dados.

URI: rollback/dismount

Método HTTP: PUT

StartMounting

Monta uma lista de bancos de dados.

URI: rollback/mount

Método HTTP: PUT

StartRollback

Inicia uma operação de reversão (restauração) no agente.

URI: rollback/

Método HTTP: POST

IRrcRollbackManagement

Esta seção descreve as operações de serviço disponíveis para IRrcRollbackManagement em rollback/.

O serviço REST IRrcRollbackManagement expõe métodos para iniciar reversões (restauração de dados de um ponto de recuperação) em um agente.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- FixBootable

FixBootable

Realiza pós-processamento do volume de inicialização para corrigir o gerenciador de inicialização e tornar o volume inicializável após uma restauração partindo apenas do hardware. Esse método é apenas para uso interno e não deve ser chamado pelos usuários.

URI: rollback/fixBoot

Método HTTP: PUT

IServiceHostManagement

Esta seção descreve as operações de serviço disponíveis para IServiceHostManagement em servicehost/.

A interface IServiceHostManagement é implementada por uma classe que fornece uma interface de gerenciamento para o IServiceHost.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- GetApiVersionInfo
- GetConfiguration
- Restart
- SetConfiguration
- VerifyConnection

GetApiVersionInfo

Obtém informações sobre a versão da API.

URI: servicehost/apiVersion

Método HTTP: GET

GetConfiguration

Obtém a configuração atual de um servidor que aguarda chamadas REST.

URI: servicehost/config

Método HTTP: GET

Restart

Reinicia imediatamente um servidor que aguarda chamadas REST.

URI: servicehost/restart

Método HTTP: GET

SetConfiguration

Define a configuração atual de um servidor que aguarda chamadas REST.

URI: servicehost/config

Método HTTP: POST

VerifyConnection

Permite confirmar se o servidor de escuta está configurado corretamente e é capaz de receber chamadas REST.

URI: servicehost/verify

Método HTTP: GET

IShadowCopyManagement

Esta seção descreve as operações de serviço disponíveis para IShadowCopyManagement em shadowcopy/.

O contrato de serviço IShadowCopyManagement expõe algumas informações de diagnóstico sobre o serviço Volume Shadow Copy (VSS).

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- GetWriters

GetWriters

Obtém informações detalhadas sobre gravadores do serviço Volume Shadow Copy (VSS) instalados no Agent.

URI: shadowcopy/writers/

Método HTTP: GET

ITransferManagement

Esta seção descreve as operações de serviço disponíveis para ITransferManagement em transfer/.

ITransferManagement é uma interface de contrato WCF implementada por uma classe que, por sua vez, implementa a interface de gerenciamento sobre o serviço de transferência.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- DeleteChangeLogsAndMarkClean
- DeleteSnapshot
- FindIncompatibleProducts
- GetDriverMetadata
- GetShadowCopyFile
- GetVolumeAllocatedBlocks
- GetVolumeChangedBlocks
- GetVolumePhysicalDisks
- KeepSessionAlive
- SetDriverMetadata
- SetGlobalVolumeEnablement
- SetVolumeEnablement
- TakeSnapshot

DeleteChangeLogsAndMarkClean

Exclui os logs de alterações de Replay do volume.
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/logs
Método HTTP: DELETE

DeleteSnapshot

Exclui o snapshot.
URI: transfer/snapshots/{snapshotSetId}
Método HTTP: POST

FindIncompatibleProducts

Localiza e retorna os produtos incompatíveis instalados.
URI: transfer/incompatibleProducts
Método HTTP: POST

GetDriverMetadata

Obtém os metadados de driver de um volume no snapshot.
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/driver
Método HTTP: GET

GetShadowCopyFile

Obtém informações sobre arquivos de cópia de sombra que foram criados ao gerar o snapshot de VSS.
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/shadowCopyFile
Método HTTP: GET

GetVolumeAllocatedBlocks

Obtém uma representação binária da lista de blocos alocados no volume.
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/blocks/allocated
Método HTTP: GET

GetVolumeChangedBlocks

Obtém uma representação binária da lista de blocos alterados no volume.
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/blocks/changed
Método HTTP: GET

GetVolumePhysicalDisks

Obtém informações sobre o layout físico do volume no(s) disco(s) físico(s).
URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/disks
Método HTTP: GET

KeepSessionAlive

Mantém a sessão ativa.

URI: transfer/session/retention

Método HTTP: POST

SetDriverMetadata

Define os metadados de driver para um volume no snapshot. São definidos apenas os valores de metadados que não estão definidos com seus valores padrão.

URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/driver

Método HTTP: POST

SetGlobalVolumeEnablement

Ativa ou desabilita um volume. Como não requer IDs de snapshot, este método funciona globalmente.

URI: transfer/volumes/{volumeName}/enablement

Método HTTP: POST

SetVolumeEnablement

Ativa ou desabilita um volume.

URI: transfer/snapshots/{snapshotSetId}/volumes/{volumeName}/enablement

Método HTTP: POST

TakeSnapshot

Gera um snapshot de um ou mais volumes no agente.

URI: transfer/snapshots

Método HTTP: POST

IVirtualDiskManagement

Esta seção descreve as operações de serviço disponíveis para IVirtualDiskManagement em vhd/.

IVirtualDiskManagement é representado como
Replay.Common.Contracts.Virtualization.IVirtualDiskManagement.

São fornecidos o URI e o método HTTP de cada operação de serviço. As operações de serviço incluem:

- BaseFileName
- BeginBatch
- Close
- Create
- Delete
- EndBatch
- HasSnapshot
- Open
- Read
- ReadCustomMetadata

- SectorSize
- SnapshotFileName
- TakeSnapshot
- TotalSectorCapacity
- TranslateSectorOffsetToChsTuple
- Write
- WriteCustomMetadata

BaseFileName

Obtém o nome do arquivo base do VHD.

URI: vhd/{id}/baseFileName

Método HTTP: GET

BeginBatch

Inicia o lote.

URI: vhd/{id}/beginBatch/{target}

Método HTTP: POST

Close

Fecha o VHD.

URI: vhd/{id}/close

Método HTTP: GET

Create

Cria um VHD.

URI:
vhd/createVhd?path={path}&bytesCapacity={bytesCapacity}&bytesPerSector={bytesPerSector}&containsBootSystemVolume={containsBootSystemVolume}&preallocate={preallocate}

Método HTTP: PUT

Delete

Exclui um snapshot ou arquivo base de VHD.

URI: vhd/{id}/delete/{target}

Método HTTP: POST

EndBatch

Encerra o lote.

URI: vhd/{id}/endBatch

Método HTTP: POST

HasSnapshot

Confirma se o VHD possui snapshot.
URI: vhd/{id}/hasSnapshot
Método HTTP: GET

Open

Abre o VHD.
URI: vhd/openVhd?path={path}
Método HTTP: PUT

Read

Lê dados brutos do VHD.
URI: vhd/{id}/read/{target}/{sectorOffset}/{sectorLength}
Método HTTP: POST

ReadCustomMetadata

Lê uma cadeia de caracteres de metadados personalizada definida pelo usuário.
URI: vhd/{id}/readCustomMetadata/{target}/{key}
Método HTTP: POST

SectorSize

Obtém o tamanho de setor do VHD.
URI: vhd/{id}/sectorSize
Método HTTP: GET

SnapshotFileName

Obtém o nome do arquivo de snapshot do VHD.
URI: vhd/{id}/snapshotFileName
Método HTTP: GET

TakeSnapshot

Gera um snapshot do VHD.
URI: vhd/{id}/takeSnapshot
Método HTTP: GET

TotalSectorCapacity

Obtém a capacidade do VHD.
URI: vhd/{id}/totalSectorCapacity
Método HTTP: GET

TranslateSectorOffsetToChsTuple

Traduz o deslocamento de setor para tupla CHS.
URI: vhd/{id}/translateSectorOffsetToChsTuple?sectorOffset={sectorOffset}
Método HTTP: GET

Write

Grava dados brutos em VHD.
URI: vhd/{id}/write/{target}/{sectorOffset}/{sectorLength}
Método HTTP: POST

WriteCustomMetadata

Lê uma cadeia de caracteres de metadados personalizada definida pelo usuário.
vhd/{id}/writeCustomMetadata/{target}/{key}?value={value}
Método HTTP: POST

IWhiteLabelingManagement

Esta seção descreve as operações de serviço disponíveis para IWhiteLabelingManagement em whitelabeling/.

O contrato de serviço IWhiteLabelingManagement expõe as cadeias de caracteres personalizáveis.

São fornecidos o URI e o método HTTP de cada operação de serviço a seguir:

- GetWhiteLabelingInfo

GetWhiteLabelingInfo

Obtém cadeias de caracteres personalizáveis.
URI: whitelabeling/whiteLabelingInfo
Método HTTP: GET

Glossário

A

Agente

O AppAssure Agent é um software instalado em uma máquina física ou virtual que permite adicionar essa máquina à proteção no AppAssure Core.

AppAssure

O AppAssure estabelece um novo padrão de proteção de dados unificada, combinando cópia de segurança, replicação e recuperação em uma única solução, projetada para ser a cópia de segurança mais rápida e confiável para a proteção de máquinas virtuais (VM) e de ambientes físicos e de nuvem.

atribuição de marca branca

O AppAssure fornece a capacidade de os provedores de serviços de cópia de segurança e de recuperação após desastres colocarem um rótulo branco ou uma nova marca no AppAssure com sua própria identidade e, depois, vendê-lo ou distribuí-lo como seu próprio produto ou serviço.

C

capacidade de anexação do SQL

A capacidade de anexação do SQL é uma execução de teste dentro do AppAssure Core para garantir que todos os pontos de recuperação do SQL estejam sem erro e disponíveis para cópia de segurança no caso de falha.

capacidade de montagem

A montabilidade do Exchange é um recurso de detecção de corrupção que alerta os administradores sobre possíveis falhas e garante que todos os dados nos servidores do Exchange sejam recuperados com êxito em caso de falha.

caracteres proibidos

Caracteres proibidos são aqueles que não devem ser usados ao definir o nome de um objeto no AppAssure Core Console. Por exemplo, ao definir um nome de exibição para uma máquina protegida, não use os caracteres especiais a seguir:

Tabela 3. Caracteres proibidos

Caractere	Nome do caractere	Proibido em
?	ponto de interrogação	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
|	barra vertical	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
:	dois pontos	nome de exibição de máquina, chave de criptografia, repositório O uso desse símbolo é permitido ao especificar um caminho, como c:\data.

Tabela 3. Caracteres proibidos

Caractere	Nome do caractere	Proibido em
/	barra	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
\	barra invertida	nome de exibição de máquina, chave de criptografia, repositório O uso desse símbolo é permitido ao especificar um caminho local ou de rede, como c:\data ou \\ComputerName\SharedFolder\
*	asterisco	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
"	aspas	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
<	menor que	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
>	maior que	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho

Central Management Console

O AppAssure Central Management Console é um portal de gerenciamento de vários cores. Ele simplifica o processo de gerenciamento de diversas implementações do AppAssure Core. Usando o Central Management Console, é possível agrupar e gerenciar as implementações usando uma única interface baseada na Web.

chave de licença

Uma chave de licença é um método usado para registrar seu software ou appliance AppAssure. (Também é possível usar um arquivo de licença.) Você pode obter chaves ou arquivos de licença ao registrar uma conta no Portal de licenças do Dell AppAssure. Para obter mais informações, consulte Portal de licenças.

cluster

Consulte cluster de ativação pós-falha do Windows.

cluster Continuous Replication (CCR)

Uma solução não compartilhada de cluster de ativação pós-falha de armazenamento que usa a tecnologia integrada de envio de log assíncrono para criar e manter uma cópia de cada grupo de armazenamento em um segundo server de um cluster de ativação pós-falha. A CCR foi projetada para ser uma solução de um ou dois data centers, para fornecer alta disponibilidade e resiliência local. É um dos dois tipos de implementação de server de caixa de correio em cluster (CMS) disponíveis no Exchange 2007.

cluster de ativação pós-falha do Windows

Um grupo de computadores independentes que funcionam juntos para aumentar a disponibilidade de aplicativos e serviços. Os servers em cluster (chamados de nós) são conectados por cabos físicos e por software. Se um dos nós do cluster falhar, outro nó começará a prestar o serviço (um processo conhecido como ativação pós-falha). Os usuários têm interrupções mínimas no serviço. O AppAssure oferece suporte à proteção de vários tipos de cluster de SQL Server e Exchange Server.

cluster do servidor

Consulte cluster de ativação pós-falha do Windows.

compressão

A Storage Networking Industry Association (SNIA) define a compressão como o processo de codificação de dados que visa reduzir seu tamanho.

cópia de segurança de SQL

Uma cópia de segurança de SQL é uma cópia de dados que é usada para restaurar e recuperar esses dados em um SQL Server após uma falha do sistema. Com a cópia de segurança de SQL, você pode realizar a recuperação de todo o banco de dados SQL ou de um ou mais componentes do banco de dados.

cópia de segurança diferencial de SQL

Uma cópia de segurança diferencial do banco de dados é uma cópia cumulativa de todas as alterações nos dados desde a última cópia de segurança completa do banco de dados SQL. A criação de cópias de segurança diferenciais geralmente é mais rápida do que a de cópias completas do banco de dados, reduzindo também o número de logs de transações necessários para recuperar o banco de dados.

cópia de segurança do SharePoint

Uma cópia de segurança do SharePoint é uma cópia de dados que é usada para restaurar e recuperar esses dados em um servidor SharePoint após uma falha do sistema. Com a cópia de segurança do SharePoint, você pode realizar a recuperação de todo o farm do SharePoint ou de um ou mais componentes do farm.

Core

O AppAssure Core é o componente central da arquitetura do AppAssure. O Core fornece os serviços essenciais para cópia de segurança, recuperação, retenção, replicação, arquivamento e gerenciamento. Em um contexto de replicação, o Core também é chamado de *Core de origem*. O Core de origem é o núcleo originador, enquanto o Core de destino é o alvo da replicação (outro AppAssure Core em seu próprio servidor dedicado, onde as máquinas ou clusters protegidos são replicados).

Core de destino

Também chamado de *core de réplica*, é o AppAssure Core que recebe os dados replicados do core de origem.

Core remoto

Um Core remoto representa um AppAssure Core acessado por uma máquina que não é Core por meio do Local Mount Utility.

criptografia

Os dados são criptografados com a intenção de que estejam acessíveis apenas aos usuários autorizados que têm a chave de descriptografia apropriada. Os dados são criptografados usando AES de 256 bits no modo Cipher Block Chaining (CBC). No CBC, XOR é aplicado a cada bloco de dados com o bloco de texto cifrado anterior, antes de ser criptografado. Dessa forma, cada novo bloco de texto cifrado depende de todos os blocos anteriores de texto simples. Uma frase de acesso é usada como vetor de inicialização.

D

deduplicação global

A Storage Networking Industry Association (SNIA) define a deduplicação de dados como a substituição de várias cópias dos dados, com níveis variados de granularidade, por referências a uma cópia compartilhada, para economizar espaço de armazenamento ou largura de banda. O AppAssure Volume Manager realiza a deduplicação global de dados dentro de um volume lógico. O nível de granularidade da deduplicação é 8 KB. O escopo da deduplicação no AppAssure é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia.

F

frase de acesso

A frase de acesso é uma chave usada na criptografia de dados. Se a frase de acesso for perdida, os dados não poderão ser recuperados.

frases proibidas

Frases proibidas são frases (ou conjuntos de caracteres) que não devem ser usadas como nome de algum objeto no AppAssure Core Console, pois estão reservadas para uso pelos sistemas operacionais. É uma boa prática evitar o uso dessas frases sempre que possível. Por exemplo, ao definir um nome de exibição para uma máquina protegida, não use as frases a seguir:

Tabela 4. Frases proibidas

Frase	Uso geral	Proibida em
con	console	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
prn	porta da impressora	nome de exibição de máquina, chave de criptografia
aux	porta auxiliar	nome de exibição de máquina, chave de criptografia
nul	valor nulo	nome de exibição de máquina, chave de criptografia
com1 a com9	porta de comunicação	nome de exibição de máquina, chave de criptografia
lpt1 a lpt9	porta do terminal de impressão em linha	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho

funções de gerenciamento

O AppAssure Central Management Console introduz um novo conceito de funções de gerenciamento que permite dividir a responsabilidade administrativa entre administradores confiáveis de dados e serviços, além de acessar o controle de forma a oferecer suporte à delegação segura e eficiente da administração.

G

grupo de disponibilidade de banco de dados (DAG)

Um conjunto de até 16 servers de caixa de correio do Microsoft Exchange Server 2010 que fornece recuperação automática em nível de banco de dados após uma falha de banco de dados, server ou rede. Os DAGs usam a replicação contínua e um subconjunto de tecnologias de cluster de ativação pós-falha do Windows para fornecer alta disponibilidade e resiliência local. Os servers de caixa de correio em um DAG monitoram uns aos outros em busca de falhas. Quando um server de caixa de correio é adicionado a um DAG, ele funciona com os outros servers no DAG para fornecer recuperação automática ao nível de banco de dados após falhas de banco de dados.

I

imagem de base

A primeira transferência de cópia de segurança salva no Core é chamada de snapshot de imagem de base. Todos os dados em todos os volumes especificados (incluindo o sistema operacional, aplicativos e definições) são salvos no Core. Para obter mais informações, consulte snapshot.

L

Live Recovery

O AppAssure Live Recovery é uma tecnologia de recuperação instantânea para VMs e servers. Fornece um acesso quase contínuo a volumes de dados em um servidor virtual ou físico, que permite recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

Local Console

O Local Console é uma interface baseada na Web que permite gerenciar totalmente o AppAssure Core.

Local Mount Utility

O Local Mount Utility (LMU) é um aplicativo que pode ser obtido por download e permite montar um ponto de recuperação em um AppAssure Core remoto a partir de qualquer máquina.

M

máquina de réplica de destino

A instância de uma máquina protegida em um core de destino é conhecida como agente de destino ou agente de réplica.

máquina protegida

Uma máquina protegida, também conhecida como agente, é um computador físico ou máquina virtual protegido pelo AppAssure Core. A máquina deve ter o software de agente do AppAssure instalado para ser protegida.

máquina replicada

Uma máquina replicada (também conhecida como Core de destino) é uma cópia de um computador físico ou máquina virtual protegida (conhecido como Core de origem).

N

nó de cluster

Máquina individual que faz parte de um cluster de ativação pós-falha do Windows.

P

pontos de recuperação

Os pontos de recuperação são uma coleção de snapshots de vários volumes de disco. Por exemplo, C:, D: e E.

Portal de licenças

O Portal de licenças do Dell AppAssure é uma interface da Web na qual os usuários e parceiros podem baixar software, registrar appliances do AppAssure e gerenciar assinaturas de licença. Os usuários do Portal de licenças podem registrar uma conta, baixar software AppAssure Core e Agent, gerenciar grupos, monitorar a atividade de grupos, registrar máquinas, registrar appliances, convidar usuários e gerar relatórios. Para obter mais informações, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.

PowerShell scripting

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O AppAssure inclui SDKs de cliente abrangentes para PowerShell scripting que permitem aos administradores automatizar a administração e o gerenciamento dos recursos do AppAssure pela execução de comandos diretos ou por meio de scripts.

propagação

Na replicação, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas, o que é útil para grandes conjuntos de dados ou locais com links lentos.

Q

quórum

Para um cluster de ativação pós-falha, o número de elementos que devem estar on-line para determinado cluster continuar em execução. Os elementos relevantes nesse contexto são os nós do cluster. Esse termo também pode se referir ao recurso com capacidade de quórum selecionado para manter os dados de configuração necessários para a recuperação do cluster. Esses dados contém detalhes de todas as alterações aplicadas ao banco de dados de cluster. O recurso de quórum geralmente é acessível a outros recursos de cluster de modo que qualquer nó de cluster tem acesso às mais recentes alterações do banco de dados. Por padrão há apenas um recurso de quórum por cluster de server. A configuração de quórum especial (definições de cluster de ativação pós-falha) determina o ponto em que muitas falhas interrompem a execução do cluster.

R

replicação

A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Ela representa o relacionamento entre os cores de origem e de destino no mesmo local ou em dois locais com link lento, em que o core de origem transmite de forma assíncrona os dados ao core de destino ou de origem em base por agente.

repository

O repositório, gerenciado pelo AppAssure Core, é uma pasta usada para armazenar os snapshots capturados dos servers e máquinas protegidos. O repositório pode residir em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

restore

O processo de restaurar um ou mais volumes de armazenamento em uma máquina a partir de pontos de recuperação salvos no AppAssure Core é chamado de restauração. Anteriormente era chamado de reversão.

retenção

A retenção define o período pelo qual os snapshots de cópia de segurança de máquinas protegidas são armazenados no AppAssure Core. A política de retenção é aplicada aos pontos de recuperação por meio do processo de rollup.

rollup

Trata-se de um procedimento de manutenção noturna interna que reforça a política de retenção por meio de colapso e eliminação de pontos de recuperação datados. O AppAssure reduz o rollup apenas a operações de metadados.

S

single copy cluster

Uma solução compartilhada de cluster de ativação pós-falha de armazenamento, que usa uma única cópia de um grupo de armazenamento no armazenamento que é compartilhado entre os nós do cluster. É um dos dois tipos de implementação de server de caixa de correio em cluster disponíveis no Exchange 2007.

Sistema de arquivos de objeto

O armazenamento de objeto escalável do AppAssure é um componente de sistema de arquivos de objeto. Ele trata todos os blocos de dados, dos quais os snapshots são derivados, como objetos. Ele armazena, recupera, mantém e replica esses objetos. Foi projetado para oferecer desempenho de entrada e saída (I/O) escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção. O sistema de arquivos de objeto faz interface direta com tecnologias de armazenamento padrão do setor.

Smart Agent

O AppAssure Smart Agent é instalado nas máquinas protegidas pelo AppAssure Core. O Smart Agent rastreia os blocos alterados no volume de disco e cria um snapshot dos blocos alterados em um intervalo de proteção predefinido.

snapshot

Snapshot é um termo comum do setor que define a capacidade de capturar e armazenar o estado de um volume de disco em um determinado ponto, enquanto os aplicativos estão executando. O snapshot é crítico em caso de necessidade de recuperação do sistema devido a uma interrupção ou falha do sistema. Os snapshots do AppAssure reconhecem o aplicativo, ou seja, todas as transações abertas e os logs de transação contínua são concluídos e os caches são limpos antes da criação do snapshot. O AppAssure usa o Microsoft Volume Shadow Services (VSS) para facilitar snapshots consistentes de falhas de aplicativos.

snapshot incremental

Snapshots incrementais são cópias de segurança compostas apenas de dados alterados na máquina protegida desde a última cópia de segurança. São salvos regularmente no Core, com base no intervalo definido (por exemplo, a cada 60 minutos). Para obter mais informações, consulte snapshot.

soma de verificação

A soma de verificação é uma função que cria blocos de dados que são usados para detectar erros acidentais ocorridos durante a transmissão ou o armazenamento.

standby virtual

O Standby virtual é um processo físico para virtual (P2V) que cria uma máquina virtual clone de uma máquina protegida ou agente. Um standby virtual pode ser criado usando um processo de exportação *ad hoc* ou de *atualização contínua*. Um standby virtual criado usando uma *atualização contínua* é atualizado de forma incremental após cada snapshot capturado no agente de origem.

T

Transport Layer Security

Transport Layer Security (TLS) é um protocolo moderno de rede de criptografia projetado para garantir a segurança da comunicação pela Internet. Esse protocolo, definido pela Força-Tarefa de Engenharia de Internet, é o sucessor do Secure Sockets Layer (SSL). O termo SSL ainda é geralmente usado, e os protocolos são interoperáveis (um cliente TLS pode fazer o downgrade para se comunicar com um server SSL).

True Scale

True Scale é a arquitetura escalável do AppAssure.

truncamento de log

O truncamento de log é uma função que remove registros de log do log de transações. Para uma máquina do SQL Server, quando você forçar o truncamento dos registros do SQL Server, esse processo identifica espaço livre no server do SQL. Para uma máquina do Exchange Server, você força o truncamento dos logs do Exchange Server. Essa ação libera espaço no server do Exchange.

U

Universal Recovery

A tecnologia AppAssure Universal Recovery oferece flexibilidade ilimitada de restauração de máquinas. Permite realizar uma recuperação monolítica de/para qualquer plataforma física ou virtual de sua escolha, bem como atualizações de recuperação incremental para máquinas virtuais a partir de qualquer origem física ou virtual. Também permite realizar a recuperação de arquivos individuais, pastas, e-mail, itens de calendário, bancos de dados e aplicativos no nível de aplicativo, de item e de objeto.

V

Verified Recovery

A tecnologia Verified Recovery é usada para realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Suporta vários sistemas de arquivo e servidores.

Volume Manager

O AppAssure Volume Manager gerencia objetos e, depois, os armazena e apresenta como um volume lógico. Ele aproveita a arquitetura de pipeline dinâmico para fornecer escalabilidade TruScale, paralelismo e modelo assíncrono de entrada e saída (I/O) para alta taxa de transferência com latência mínima de I/O.

Retornar ao início

Sobre o Dell

A Dell escuta os clientes e fornece tecnologia inovadora, soluções empresariais e serviços globais de confiança e valor. Para obter mais informações, visite www.software.dell.com/br-pt.

Contatos da Dell

Suporte técnico:
Suporte online

Vendas e dúvidas sobre produtos:
(800) 306-9329

E-mail:
info@software.dell.com

Recursos do suporte técnico

O suporte técnico está disponível para clientes que compraram produtos de software da Dell com um contrato de manutenção válido e clientes que estão usando versões de teste. Para acessar o Portal de suporte, visite http://support.software.dell.com/pt-br/.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. Além disso, o Portal fornece acesso direto a engenheiros de suporte de produtos por meio de um sistema online de Solicitação de serviço.

O site permite que você:

- Crie, atualize e gerencie as Solicitações (casos) de serviço.
- Visualize artigos da Base de conhecimento.
- Obtenha notificações de produtos.
- Baixe o software. No caso de software de teste, acesse Downloads de teste.
- Assista a vídeos instrucionais.
- Participe de discussões da comunidade.
- Converse com um engenheiro do suporte.