

Guia de Administração do Symantec™ IT Management Suite 7.5 com tecnologia Altiris™

Guia de Administração do Symantec™ IT Management Suite 7.5 com tecnologia Altiris™

O software descrito neste documento é fornecido sob um contrato de licença e pode ser usado somente de acordo com os termos desse contrato.

Avisos legais

Copyright © 2013 Symantec Corporation. Todos os direitos reservados.

Symantec, o logotipo da Symantec, o logotipo da marca de verificação e quaisquer marcas comerciais da Altiris ou da Symantec usadas no produto são as marcas comerciais ou as marcas registradas da Symantec Corporation ou de seus afiliados nos E.U.A. e em outros países. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Este produto da Symantec pode conter software de terceiros para o qual são necessárias atribuições fornecidas pela Symantec a esses terceiros ("Programas de terceiros"). Alguns Programas de terceiros estão disponíveis sob licenças de software de código aberto ou livre. O Contrato de licença que acompanha o Software licenciado não altera seus direitos ou suas obrigações em relação a licenças de software livre ou de código-fonte aberto. Para obter mais informações sobre os programas de terceiros, consulte o documento Avisos de terceiros para este produto da Symantec, que pode estar disponível em <http://www.symantec.com/about/profile/policies/eulas/>, o apêndice Avisos legais de terceiros que pode ser incluído nesta documentação e/ou o Arquivo Leia-me dos Avisos legais de terceiros que pode acompanhar este produto da Symantec.

O produto descrito neste documento é distribuído sob licenças que restringem seu uso, cópia, distribuição e descompilação ou engenharia reversa. Nenhuma parte deste documento pode ser reproduzida por forma ou meio algum sem a autorização prévia por escrito da Symantec Corporation e seus licenciadores, se houver.

A DOCUMENTAÇÃO É FORNECIDA "NO ESTADO EM QUE SE ENCONTRA" E TODAS AS CONDIÇÕES, REPRESENTAÇÕES E GARANTIAS EXPLÍCITAS OU IMPLÍCITAS, INCLUINDO QUALQUER GARANTIA IMPLÍCITA DE COMERCIALIZABILIDADE, ADEQUAÇÃO A UM FIM ESPECÍFICO OU NÃO INFRINGIMENTO, SÃO RENUNCIADAS, EXCETO NA EXTENSÃO EM QUE TAIS RENÚNCIAS SEJAM CONSIDERADAS INVÁLIDAS NOS TERMOS DA LEI. A SYMANTEC CORPORATION NÃO É RESPONSÁVEL POR DANOS INCIDENTAIS OU CONSEQUENCIAIS RELACIONADOS AO FORNECIMENTO, DESEMPENHO OU USO DESTA DOCUMENTAÇÃO. AS INFORMAÇÕES CONTIDAS NESTA DOCUMENTAÇÃO ESTÃO SUJEITAS A ALTERAÇÕES SEM AVISO PRÉVIO.

O Software licenciado e a Documentação são considerados software comercial para computadores, conforme definido na FAR 12.212 e sujeito a direitos restritos, conforme definido no artigo 52.227-19 da FAR "Software comercial para computadores - Direitos restritos" e DFARS 227.7202, "Direitos em Software comercial para computadores ou documentação de software comercial para computadores", conforme aplicável, e todas regulamentações sucessoras. Qualquer uso, modificação, reprodução, apresentação, exibição ou divulgação do Software licenciado e da documentação pelo governo dos EUA deve ser feita exclusivamente de acordo com os termos deste Contrato.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com.br>

Suporte técnico

O suporte técnico da Symantec mantém centros de suporte global. A principal função do suporte técnico é responder às consultas específicas sobre recursos e funcionalidades de produtos. A equipe de suporte técnico cria também o conteúdo para nossa Base de conhecimento online. A equipe de suporte técnico trabalha em colaboração com as outras áreas funcionais dentro da Symantec para responder a suas perguntas de forma oportuna. Por exemplo, a equipe de suporte técnico trabalha com a engenharia de produtos e com o Symantec Security Response para fornecer serviços de alerta e atualizações das definições de vírus.

As ofertas de suporte da Symantec incluem o seguinte:

- Várias opções de suporte que oferecem a você a flexibilidade de selecionar a quantidade adequada de serviço para organizações de qualquer porte
- Suporte por telefone e/ou com base na Web, fornecendo respostas rápidas e informações atualizadas
- Segurança em upgrade que fornece upgrades de software
- Suporte global comprado em um horário de expediente regional ou 24 horas por dia, 7 dias por semana
- Ofertas de serviço Premium que incluem Serviços de gerenciamento de conta

Para obter informações sobre as ofertas de suporte da Symantec, acesse nosso site no seguinte URL:

www.symantec.com/pt/br/business/support/

Os serviços de suporte serão fornecidos de acordo com seu contrato de suporte e a política de suporte técnico corporativo do momento.

Contato com o Suporte técnico

Os clientes com um contrato de suporte atual podem acessar as informações de Suporte técnico no URL:

www.symantec.com/pt/br/business/support/

Antes de entrar em contato com o Suporte técnico, certifique-se de satisfazer os requisitos do sistema que estão relacionados na documentação de seu produto. Além disso, você deverá estar em frente ao computador no qual ocorreu o problema, caso seja necessário reproduzir o problema.

Quando entrar em contato com o Suporte técnico, tenha as seguintes informações disponíveis:

- Nível de versão do produto

- Informações sobre o hardware
- Memória disponível, espaço em disco e informações sobre a NIC
- Sistema operacional
- Nível de versão e de patch
- Topologia da rede
- Informações sobre roteador, gateway e endereço IP
- Descrição do problema:
 - Mensagens de erro e arquivos de log
 - Soluções de problemas que foram executadas antes de entrar em contato com a Symantec
 - Alterações recentes feitas do software e na rede

Licenciamento e registro

Se seu produto da Symantec exigir registro ou uma chave de licença, acesse nossa página da Web do suporte técnico no seguinte URL:

www.symantec.com/pt/br/business/support/

Atendimento ao cliente

Informações do atendimento ao cliente estão disponíveis no URL:

www.symantec.com/pt/br/business/support/

O atendimento ao cliente está disponível para ajudá-lo em perguntas não técnicas, como os seguintes tipos de problemas:

- Questões relacionadas ao licenciamento e à serialização do produto
- Atualizações de registro do produto, como alterações de endereço e de nome
- Informações gerais sobre o produto (recursos, disponibilidade de idiomas, fornecedores locais)
- Informações mais recentes sobre atualizações e upgrades de produtos
- Informações sobre garantia de upgrade e contratos de suporte
- Informações sobre a compra de produtos da Symantec
- Aconselhamento sobre opções de suporte técnico da Symantec
- Questões não técnicas de pré-vendas
- Questões relacionadas a CD-ROMs, DVDs ou manuais

Recursos de contrato de suporte

Se desejar entrar em contato com a Symantec sobre um contrato de suporte atual, contate a equipe de administração de contratos de suporte de sua região:

Ásia Pacífico e Japão	customercare_apac@symantec.com

Europa, Oriente Médio e África	semea@symantec.com

América do Norte e América Latina	supportsolutions@symantec.com

Sumário

Suporte técnico	4
Seção 1 Introdução aos principais componentes do IT Management Suite	23
Capítulo 1 Introdução ao Symantec Management Platform	24
Sobre o Symantec Management Platform	24
O que há de novo no IT Management Suite 7.5	25
Componentes do Symantec Management Platform	28
Como funciona o pcAnywhere Solution	29
Sobre como adicionar produtos à plataforma	30
Onde obter mais informações	31
Capítulo 2 Introdução ao Console de gerenciamento Symantec	33
Sobre o Console de gerenciamento Symantec	33
Sobre as exibições do console	35
Sobre a exibição Computadores	35
Para pesquisar um computador e salvar a pesquisa como um filtro	38
Sobre a exibição Software	40
Para pesquisar o software e salvar a pesquisa	40
Sobre a janela Catálogo de software	42
Sobre a exibição Trabalhos/Tarefas	43
Sobre a exibição Políticas	43
Sobre operadores da pesquisa	44
Para configurar as exibições aprimoradas	45
Acesso ao Console de gerenciamento Symantec	47
Para acessar a documentação do Console de gerenciamento Symantec	49
Para acessar a página Meu portal	49

	Para acessar a página Início do Gerenciamento do Notification Server	50
	Para personalizar o Console de gerenciamento Symantec	51
	Para personalizar o menu do console	52
	Para adicionar ações definidas pelo usuário ao menu contextual	53
	Para criar e modificar exibições	55
	Para adicionar novos itens diretamente a uma exibição	57
	Para criar e modificar páginas do portal	57
	Para criar e modificar Web parts	60
	Para salvar elementos do console como arquivos XML	61
Seção 2	Para configurar os servidores do Symantec Management Platform	63
Capítulo 3	Para configurar o Notification Server	64
	Sobre o Notification Server	64
	Sobre como configurar o Notification Server	65
	Para definir configurações do Notification Server	66
	Configurações de processamento do Notification Server	67
	Configurações do servidor de e-mail e do endereço	71
	Configurações de registro em log da mensagem de status	72
	Para abrir o Visualizador de logs	72
	Configurações do servidor proxy	73
	Configurações da credencial de ponto de distribuição	74
	Como definir as configurações do Notification Server com o configurador do NS	75
	Para configurar o banco de dados de gerenciamento de configuração	76
	Para limpar o banco de dados de gerenciamento de configuração	79
	Como salvar o histórico de dados de recursos no CMDb	81
Capítulo 4	Para configurar a segurança	83
	Sobre a segurança do Symantec Management Platform	83
	Para configurar a segurança do Symantec Management Platform	84
	Para criar e configurar funções de segurança	88
	Para atribuir privilégios a uma função de segurança	93
	Para criar e configurar contas de usuário do Symantec Management Platform	225

Para especificar detalhes gerais da conta de usuário do Symantec Management Platform	98
Configuração das credenciais para uma conta do usuário do Symantec Management Platform	99
Para adicionar membros a uma função de segurança	101
Para atribuir uma conta de usuário do Symantec Management Platform a uma função de segurança	102
Para adicionar funções de segurança como membros de outras funções de segurança	102
Para atribuir permissões de segurança a pastas e itens	103
Para personalizar a herança de permissões	104
Funções predefinidas de segurança	106
Tarefas de gerenciamento de segurança do Symantec Management Platform	108
Para definir as configurações de bloqueio e complexidade da senha	109
Para desbloquear credenciais bloqueadas	113
Para acessar o Gerenciador de função de segurança	113
Para obter a propriedade de uma pasta ou item	115
Para gerenciar credenciais	115

Capítulo 5	Para configurar agendas	117
	Como o Symantec Management Platform usa agendamentos	117
	Componentes de um agendamento do Symantec Management Platform	119
	Para gerenciar agendamentos compartilhados	122
	Para configurar um agendamento	123
	Para exibir do calendário de agendamento interno do Notification Server	124

Capítulo 6	Para configurar sites e servidores de sites	127
	Sobre os serviços de site	127
	Sobre a manutenção de sites	128
	Para gerenciar sites	129
	Para gerenciar servidores de sites	131
	Para atribuir um servidor de sites a um site manualmente	133
	Para gerenciar agentes atribuídos manualmente	134
	Para gerenciar sub-redes	135
	Sobre como definir as configurações do serviço de site	138
	Para configurar definições do serviço de pacotes	139
	Para definir configurações do serviço de tarefas	139

Capítulo 7	Para configurar o servidor de pacotes para Linux	141
	Sobre o servidor de pacotes para Linux	141
	Sobre a integração do Apache Web Server com o servidor de pacotes para Linux	142
	Sobre a detecção do Apache Web Server	143
	Requisitos para configurar o servidor de pacotes e o Apache Web Server	145
	Requisitos para configurar o HTTPS e o HTTP	146
	O exemplo da configuração de servidor de pacotes que usa o diretório da Web principal para os links de servidor de pacotes	147
	Exemplo de configuração do servidor de pacotes que usa um alias para os links do servidor de pacotes	150
Capítulo 8	Para configurar a hierarquia	153
	Sobre a hierarquia do Notification Server	153
	Requisitos da hierarquia	155
	Para implementar a hierarquia do Notification Server	156
	Para criar e gerenciar relacionamentos hierárquicos	157
	Para configurar um relacionamento hierárquico entre dois computadores do Notification Server	161
	Para configurar a replicação de hierarquia e as regras da replicação de hierarquia	163
	Para configurar a replicação de hierarquia personalizada	165
	Para sobrepor o agendamento da replicação diferencial da hierarquia	167
	Para replicar manualmente dados selecionados	168
	Para configurar uma política de automação da hierarquia	168
	Para executar relatórios de hierarquia	169
	Atualização de dados de resumo	170
Capítulo 9	Para configurar a replicação	172
	Sobre replicação e regras de replicação	172
	Requisitos de replicação	174
	Para configurar regras de replicação	175
Capítulo 10	Para executar uma configuração de primeira instalação	177
	Para executar as tarefas de configuração inicial	177
	Descoberta de computadores	179

	Para instalar o Symantec Management Agent e os plug-ins da solução	181
	Opções de configuração de agente e tarefa	184
	Coleta de informações do inventário	185
	Para agendar gerenciamento de patches	187
Seção 3	Para descobrir os recursos na rede	189
Capítulo 11	Para descobrir computadores Windows	190
	Métodos de descoberta de recursos	190
	Métodos de descoberta para computadores Windows	191
	Para descobrir computadores com descoberta de recursos de domínio	192
Capítulo 12	Para importar recursos do Active Directory	197
	Sobre a importação do Microsoft Active Directory	197
	Sobre a importação das associações de recursos	198
	Para importar recursos usando a importação do Microsoft Active Directory	199
	Para criar e modificar regras de importação de recursos	201
	Para agendar regras de importação de recursos	204
	Para configurar o agendamento de sincronização de diretório	205
	Para executar manualmente regras de importação de recursos	206
Capítulo 13	Para descobrir dispositivos de rede	208
	Sobre a Descoberta de rede	208
	Para descobrir dispositivos de rede	209
	Para definir as configurações de descoberta	210
	Para criar tarefas de descoberta de rede usando o assistente	212
	Para criar e modificar manualmente as tarefas de Descoberta de rede	213
	Para criar perfis de conexão com Descoberta de rede	214
	Para criar ou duplicar um perfil de conexão	215
	Métodos de descoberta de dispositivos de rede	216
	Sobre a seleção de intervalos de rede para descobrir	217
	Para exibir dispositivos descobertos em exibições organizacionais	219
	Para exibir relatórios de descoberta	219

Para classificar dispositivos SNMP	220
Para delegar tarefas de Descobertas de rede aos usuários não administradores	221
Para adicionar usuários não administradores às funções de segurança para executar tarefas de Descoberta de rede	224
Para ativar funções de usuário que não seja o administrador para criar ou executar tarefas de Descoberta de rede	226
Para conceder privilégios de funções de usuário que não seja o administrador para criar credenciais e perfis de conexão	229
Para fornecer acesso de função de usuário que não seja o administrador ao perfil de conexão padrão	230
Para ativar funções diferentes das funções de segurança predefinidas para criar e executar tarefas usando o Assistente de Descoberta de rede.	231
Para tornar um perfil de conexão somente leitura	232
Importação de arquivos Management Information Bases (MIB)	233

Seção 4 Para instalar e configurar o Symantec Management Agent 235

Capítulo 14 Introdução ao Symantec Management Agent	236
Sobre o Symantec Management Agent	236
Sobre o registro do agente	237

Capítulo 15 Para instalar o Symantec Management Agent em computadores-cliente	238
Métodos de instalação do Symantec Management Agent	238
Para instalar o Symantec Management Agent em computadores Windows	240
Pré-requisitos de instalação do Symantec Management Agent para Windows	242
Para criar uma política de registro do agente	243
Para especificar as configurações de instalação do Symantec Management Agent para Windows	246
Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual	246
Para instalar o Symantec Management Agent para Windows com uma instalação pull manual	248

	Para executar uma instalação agendada do Symantec Management Agent para Windows	249
	Para exibir relatórios de status da instalação	250
	Para exibir e gerenciar o status do registro do agente	251
	Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac	255
	Para criar um arquivo CSV para importar computadores UNIX, Linux e Mac	256
	Pré-requisitos de instalação do Symantec Management Agent para UNIX, Linux e Mac	258
	Para especificar as configurações de instalação do Symantec Management Agent para UNIX, Linux e Mac	259
	Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual	260
	Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação pull manual	264
Capítulo 16	Para fazer o upgrade e desinstalar o Symantec Management Agent	266
	Métodos para fazer upgrade do Symantec Management Agent	266
	Métodos de desinstalação do Symantec Management Agent	268
	Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent	268
	Sobre a comunicação do agente legado	272
	Para configurar o pacote do Symantec Management Agent	273
	Para remover manualmente o Symantec Management Agent para Windows	274
Capítulo 17	Para configurar o Symantec Management Agent	276
	Para configurar o Symantec Management Agent	276
	Para definir as configurações globais de agentes	277
	Para definir as configurações do agente de destino	278
	Para configurar políticas de janela de manutenção	280

Seção 5	Para implementar o gerenciamento habilitado para nuvem	283
Capítulo 18	Introdução ao gerenciamento habilitado para nuvem	284
	Sobre o gerenciamento habilitado para nuvem	284
Capítulo 19	Para preparar o ambiente para o gerenciamento habilitado para nuvem	287
	Para preparar o ambiente para o gerenciamento habilitado para nuvem	287
	Para configurar o Notification Server para usar o HTTPS	290
	Para aplicar uma autoridade de certificação raiz a um computador gerenciado	292
	Para redirecionar o Symantec Management Agent para usar HTTPS	295
	Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem	296
	Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS	302
	Para configurar sites e servidores de sites para atender agentes habilitados para nuvem	304
Capítulo 20	Para configurar o gerenciamento habilitado para nuvem	307
	Para configurar o gerenciamento habilitado para nuvem	307
	Para configurar o DefaultAppPool para suar o Modo integrado de canal gerenciado	310
	Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.	311
	Sobre a preparação do computador gateway da Internet	313
	Download e execução do pacote de instalação de gateway da Internet	315
	Para configurar o gateway da Internet	317
	Para configurar a política de Configurações do gerenciamento habilitado para nuvem	320
	Para instalar o Symantec Management Agent em um computador desconectado	324

Capítulo 21	Para executar tarefas de gerenciamento habilitado para nuvem	328
	Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem	328
	Para gerar um certificado temporário do cliente	330
	Para instalar um certificado temporário em um computador gerenciado	332
	Para revogar um certificado do gerenciamento habilitado para nuvem	333
	Para forçar o Symantec Management Agent a usar um gateway da Internet especificado	336
	Para fazer backup e restaurar um gateway da Internet	337
	Para exibir relatórios do gerenciamento habilitado para nuvem	339
Seção 6	Para gerenciar recursos do Symantec Management Platform	340
Capítulo 22	Para configurar a segurança dos recursos	341
	Para configurar a segurança dos recursos	341
	Para criar e configurar uma exibição organizacional	344
	Para criar e preencher um grupo ou exibição organizacional	345
	Para criar e configurar um grupo organizacional	346
	Para exibir recursos em um grupo organizacional	347
	Para definir a segurança da configuração em um grupo organizacional	348
	Considerações sobre o escopo do recurso	349
Capítulo 23	Para configurar filtros e destinos de recursos	354
	Sobre filtros de recursos	354
	Criação ou modificação de um filtro	355
	Para criar um novo filtro	357
	Para modificar um filtro existente	357
	Para selecionar o tipo de consulta de filtros	358
	Para definir uma consulta de recursos para um filtro	359
	Para definir uma consulta SQL para um filtro	361
	Para especificar inclusões e exclusões de filtros	362
	Para atualização a associação de um filtro	364
	Execução de ações em recursos do filtro	365
	Exibição das dependências do filtro	366

	Sobre destinos de recursos	367
	Agendamento de atualizações da participação em recursos	368
Capítulo 24	Para configurar pacotes	371
	Alteração das configurações de um pacote	371
	Atualização dos pontos de distribuição para um pacote	372
	Como ativar o acesso a um pacote em um local de origem do UNC	373
	Gerenciamento de programas do pacote	374
Capítulo 25	Para usar políticas	376
	Sobre políticas do Symantec Management Platform	377
	Sobre políticas baseadas em usuário	377
	Gerenciamento de políticas do Symantec Management Platform	379
	Para aplicar uma política usando o recursos de arrastar e soltar	379
	Especificação dos destinos de uma política ou tarefa	380
	Modificação de um destino de recurso	382
	Como criar um alvo do recurso	383
	Seleção de um destino de recurso existente	384
	Como salvar um destino de recurso nomeado	384
	Especificação de regras de filtragem para destinos de recurso	385
	Seleção de destinos de recurso nomeados	386
	Especificação de um agendamento de política	388
	Para configurar as políticas de instalação, de upgrade e de desinstalação do agente/plug-in	390
	Sobre as políticas de automação	392
	Componentes-chave das políticas de automação	393
	Gerenciamento de políticas de automação	394
	Criação ou modificação de políticas de automação agendadas	396
	Criação ou modificação de políticas de automação baseadas em mensagens	399
	Especificação da fonte de dados da política de automação	401
	Como especificar a ação da política de automação	402
	Para selecionar um trabalho ou tarefa à política de automação	404
	Para criar e modificar tarefas de política de automação	405
Capítulo 26	Para usar tarefas e trabalhos	407
	Sobre o Gerenciamento de tarefas	407
	Componentes do gerenciamento de tarefas	409
	Como o servidor de tarefas usa o mecanismo de ativação	410

Sobre quando usar tarefas, trabalhos e políticas	413
Sobre tarefas em execução na hierarquia	414
Sequenciamento de tarefas	417
Para implementar um servidor de tarefas	418
Para criar uma tarefa	419
Criação de trabalhos	420
Para executar um trabalho ou uma tarefa usando o recurso de arrastar e soltar	421
Execução de um trabalho ou uma tarefa	422
Para reexecutar uma tarefa com falha	423
Para adicionar um agendamento a uma política, tarefa ou trabalho	425
Exibição do status da tarefa no Symantec Management Agent	426
Exibição e edição das permissões em um tipo de tarefa	426
Para criar tarefas para propriedades de entrada ou saída de tarefas	427
Para limpar dados de tarefas	429
Para limpar dados da versão da tarefa	430
Alteração das configurações do Client Task Agent	431
Acesso ao Portal de trabalhos e tarefas	432
 Capítulo 27	
Para usar o Gerenciador de recursos	434
Sobre gerenciamento de recursos	434
Acesso ao Gerenciador de recursos	435
Exibição dos dados de inventário para uma classe de dados	436
Exibição dos dados de evento para uma classe de dados	437
Adição de recursos a um grupo organizacional	437
Tarefas do Gerenciador de recursos	438
 Capítulo 28	
Para usar relatórios do Notification Server	440
Sobre relatórios do Notification Server	440
Para exibir e gerenciar dados de recursos com relatórios do Notification Server	441
Para extrair resultados do relatório do Notification Server	442
Para exibir resultados do relatório do Notification Server	444
Para usar resultados do relatório do Notification Server	445
Para salvar os resultados do relatório do Notification Server como um arquivo	446
Para criar um filtro estático dos resultados do relatório do Notification Server	447

	Para salvar os resultados do relatório do Notification Server como uma captura de imagem	448
	Para salvar os resultados do relatório do Notification Server como uma Web part	449
Capítulo 29	Para criar relatórios personalizados do Notification Server	450
	Componentes de um relatório personalizado do Notification Server	450
	Para criar e modificar relatórios personalizados do Notification Server	452
	Para criar um relatório personalizado do Notification Server	455
	Para modificar um relatório personalizado existente do Notification Server	456
	Para definir uma consulta de recursos para um relatório personalizado	457
	Para definir uma consulta SQL para um relatório personalizado	459
	Para definir provedores de valores e parâmetros para um relatório personalizado	460
	Para criar ou modificar uma exibição em gráfico para um relatório personalizado	462
	Para criar ou modificar uma exibição em grade para um relatório personalizado	464
	Para configurar ações de busca detalhada para um relatório personalizado	465
	Para especificar as propriedades de um relatório personalizado	468
Capítulo 30	Para exibir informações dos recursos	470
	Sobre recursos	470
	Exibição das informações da classe de dados dos recursos	471
	Exibição das informações do tipo de associação dos recursos	471
	Exibição das informações do tipo de recurso	471

Seção 7	Para gerenciar dados do CMDDB com o Data Connector	473
Capítulo 31	Introdução ao Data Connector	474
	Sobre o Data Connector	474
	Como o Data Connector funciona	474
	O que pode ser feito com o Data Connector	476
Capítulo 32	Para executar tarefas de gerenciamento de dados	477
	Para importar e exportar dados	477
	Sobre o pré-processamento de dados antes das importações de dados	479
	Criação de uma definição de fonte de dados	479
	Para criar uma regra de transferência de dados	480
	Para criar uma chave de pesquisa de recursos	481
	Execução de uma regra de transferência de dados como uma tarefa	482
	Exibir resumos da transferência de dados	483
	Verificação de integridade das regras de transferência de dados	483
	Para criar uma regra para editar dados do CMDDB	484
	Execução de uma regra de CMDDB como uma tarefa	485
	Para criar uma classe de dados virtual	486
	Configuração das opções de limpeza de logs detalhados do Data Connector	487
Apêndice A	Privilégios e permissões de segurança	488
	Categorias de privilégio de segurança	489
	Categorias de permissão de segurança	491
	Privilégios do perfil de conexão	492
	Privilégios de gerenciamento	493
	Privilégios do sistema	494
	Privilégios da credencial	497
	Privilégios do diretório de fluxo de trabalho	497
	Privilégios do Symantec Management Console	498
	Privilégios do Gerenciamento de software	499
	Privilégios do menu contextual	501
	Menu contextual - privilégios de exemplos de conector	502

	Menu de clique com o botão direito do mouse - Privilégios de hierarquia	503
	Menu de clique com o botão direito do mouse - Privilégios de ações	504
	Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos	505
	Permissões de gerenciamento de recursos	506
	Permissões do sistema	506
	Permissões do servidor de tarefas	507
	Permissões de relatório	507
	Permissões de políticas	508
	Permissões de pasta	508
	Permissões de filtros	508
	Permissões do perfil de conexão	509
	Permissões do Gerenciador de credenciais	509
Apêndice B	Symantec Management Agent	511
	Intervalos recomendados de atualização de dados do Symantec Management Agent	511
	Symantec Management Agent para comandos de solução de problemas de UNIX, Linux e Mac	512
Apêndice C	Tópicos de referência do gerenciamento habilitado para nuvem	516
	Ferramentas de linha de comando do Notification Server	516
	Configurações suportadas para servidores de pacotes em um ambiente misto	517
	Efeitos do gerenciamento habilitado para nuvem na funcionalidade do servidor de sites	518
	Scripts de gerenciamento de gateway da Internet	520
	Sobre o balanceamento de carga do gateway da Internet	521
	Parâmetros do pacote de instalação do agente habilitado para nuvem	522
	Parâmetros da linha de comando para a configuração de agente habilitado para nuvem	523
Apêndice D	Configurações do relatório personalizado	526
	Página de edição de relatório personalizado	527
	Página de edição do relatório personalizado: guia Fonte de dados	528

Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta	530
Página de edição do relatório personalizado: guia Fonte de dados : guia Campos	533
Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta parametrizada	534
Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta	535
Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro	536
Página de edição do relatório personalizado: guia Fonte de dados : guia Capturas de imagem de dados	536
Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida	538
Página de edição do relatório personalizado: guia Fonte de dados : guia Resultados	539
Página de edição do relatório personalizado: guia Exibições para uma exibição de gráfico	540
Página de edição do relatório personalizado: guia Exibições para uma exibição em grade	543
Caixa de diálogo Editar os campos fonte	544
Caixa de diálogo Editar parâmetro	546

Apêndice E	Campos passíveis de script para modificar regras de CMDb e de importação e exportação de recursos	548
	Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDb	548
	Sintaxe de expressão	549
	Operadores de expressão	550
	Valores definidos pelo usuário	550
	Operadores de sequências de caracteres	550
	Caracteres curinga	551
	Tipos agregados	551
	Funções de expressão	551

Apêndice F	Avisos legais de terceiros no Symantec™ Management Platform 7.5	555
	Third-Party Legal Notices	556
	7-Zip	556
	Apache HTTP Server	557

Apache Xerces C++	560
Boost	564
Bouncy Castle	565
Curl	565
glibc	566
Libatomics_Ops	575
LibXML2	577
Makeself	577
Microsoft Anti-Cross Site Scripting Library	584
OpenPegasus	585
OpenSSL 0.9.8u	586
OpenSSL 0.9.8y	589
OpenSSL 1.0.1e	592
plists-cs	595
SQLite	595
Windows Template Library 'WTL' v8.0	595
Zlib	597
Índice	598

Introdução aos principais componentes do IT Management Suite

- [Capítulo 1. Introdução ao Symantec Management Platform](#)
- [Capítulo 2. Introdução ao Console de gerenciamento Symantec](#)

Introdução ao Symantec Management Platform

Este capítulo contém os tópicos a seguir:

- [Sobre o Symantec Management Platform](#)
- [O que há de novo no IT Management Suite 7.5](#)
- [Componentes do Symantec Management Platform](#)
- [Como funciona o pcAnywhere Solution](#)
- [Sobre como adicionar produtos à plataforma](#)
- [Onde obter mais informações](#)

Sobre o Symantec Management Platform

O Symantec Management Platform proporciona um conjunto de serviços que podem ser utilizados pelas soluções de TI. As soluções conectam-se à plataforma e usam seus serviços, tais como segurança, geração de relatórios, comunicações, implementação de pacotes e dados do Configuration Management Database (CMDB). Como as soluções compartilham a mesma plataforma, podem compartilhar serviços e dados da plataforma. Os dados compartilhados são mais úteis que os dados disponíveis a uma única solução. Por exemplo, uma solução faz a coleta de dados sobre o software que é instalado em computadores da empresa e outra usa os dados para gerenciar licenças de software. Uma terceira solução também pode usar esses dados para ajudá-lo a atualizar o software. Essa integração de soluções e a plataforma facilita o uso das diferentes soluções, pois funcionam em um ambiente comum e são administradas através de uma interface comum.

A plataforma proporciona os seguintes serviços:

- Segurança com base em funções
- Comunicações e gerenciamento de clientes
- Execução de políticas e tarefas agendadas ou acionadas por eventos
- Instalação e implementação de pacote
- Geração de relatórios
- Gerenciamento centralizado através de uma única interface comum
- Banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database)
- Software Management Framework

Quando você instalar uma solução ou um conjunto, a plataforma será instalada também, caso ainda não esteja.

Consulte [“Componentes do Symantec Management Platform”](#) na página 28.

Consulte [“Como funciona o pcAnywhere Solution”](#) na página 29.

Consulte [“Sobre como adicionar produtos à plataforma”](#) na página 30.

Consulte [“O que há de novo no IT Management Suite 7.5”](#) na página 25.

O que há de novo no IT Management Suite 7.5

No IT Management Suite 7.5, os seguintes novos recursos foram introduzidos:

Tabela 1-1 Lista de novos recursos

Recurso	Descrição
Aprimoramentos gerais	■ Os administradores observarão o desempenho até 15 vezes mais rápido do console em relação a releases anteriores. ■ A nova funcionalidade Nova execução de tarefa permite executar novamente tarefas nos computadores nos quais a tarefa falhou. ■ A nova página flipbook Entrega de software permite exibir e tomar ações relacionadas a informações de resumo sobre tarefas de Entrega rápida e políticas de Entrega gerenciada em seu ambiente.

Recurso	Descrição
Gerenciamento habilitado para nuvem (CEM)	O gerenciamento habilitado para nuvem (CEM) permite gerenciar endpoints em trânsito mesmo quando eles não estiverem conectados à rede da empresa pelo VPN. Esta funcionalidade ajuda a melhorar a cobertura de implementação de software e patches para seus funcionários móveis e remotos. O CEM permite uma comunicação totalmente segura entre endpoints em roaming e Notification Server(s) na rede interna. As seguintes soluções e funcionalidade são suportadas no CEM: ■ Gerenciamento de tarefas O Gerenciamento de tarefas permite executar todos os tipos de tarefas no modo CEM. Contudo, a conexão de ativação ao Task Server não é estabelecida no modo CEM e a execução imediata da tarefa não está disponível. As tarefas podem ser executadas com até 60 minutos de atraso de acordo com as configurações padrão. A execução do Task Server em um computador-cliente habilitado para nuvem e gerenciado na Internet não é suportada e pode conduzir a comportamento indesejável. ■ Inventory Solution O inventário de hardware, o inventário de software, o inventário personalizado, o inventário do servidor e os recursos de medição de aplicativos são suportados. O CEM é suportado em computadores Windows somente. ■ Software Management Solution ■ Patch Management Solution
Registro do agente	Junto com o recurso do gerenciamento habilitado para nuvem, que permite gerenciar os dispositivos que estão fora do firewall, o recurso de registro do agente foi adicionado ao IT Management Suite 7.5 para garantir que apenas endpoints confiáveis possam se comunicar com o Notification Server. O recurso de registro do agente exige que um endpoint tenha permissão para comunicar-se com o Notification Server para que possa ser gerenciado por esse Notification Server.
Modo de Comunicação de agente legado (LAC, Legacy Agent Communication)	O modo de Comunicação do agente legado (LAC) permite controlar se os computadores que usam versões mais antigas do Symantec Management Agent podem se comunicar com Notification Server 7.5 com upgrade. Esta opção permite fazer o upgrade dos agentes em seu ambiente em etapas, em vez de atualizar todos eles imediatamente após o upgrade do Notification Server.

Recurso	Descrição
A lista de sistemas operacionais suportados foi expandida.	O seguinte sistema operacional é suportado agora para a instalação do Symantec Management Platform e de seus componentes: ■ Windows Server 2008 R2 SP1 (64 bits) As seguintes versões dos SQL Servers são suportadas agora para o banco de dados de gerenciamento de configuração (CMDB): ■ Microsoft SQL Server 2008 R2 SP1 ■ Microsoft SQL Server 2008 SP3 ■ Microsoft SQL Server 2012 Os seguintes sistemas operacionais são suportados agora para a instalação do Symantec Management Agent: ■ Windows 7 SP1 ■ Windows 8 ■ Windows Server 2008 R1 SP2 ■ Windows Server 2012 ■ Red Hat Enterprise Linux 5.7, 5.8, 6.2 e 6.3 Nota: Os sistemas operacionais Windows 8 e Windows Server 2012 não são suportados para o uso como servidores de sites.
Suporte para Internet Explorer 10 (modo de compatibilidade) no Portal de software	O Portal de software do Software Management Solution suporta agora o Internet Explorer 10 no modo de compatibilidade.
O novo Visualizador de logs foi implementado.	Os seguintes novos recursos foram introduzidos no novo Visualizador de logs: ■ É possível carregar uma grande quantidade de arquivos de log sem consumir muitos recursos do servidor. ■ O mecanismo de filtro foi simplificado e as definições do filtro podem ser salvas para uso posterior. ■ O mecanismo de marcador foi introduzido. ■ É possível pesquisar nos arquivos de log sem carregá-los no Visualizador de logs.
A funcionalidade SuppressReportAutorun foi implementada.	Quando SuppressReportAutorun estiver ativado e você abrir algum relatório, esse não será executado imediatamente. Para ver os resultados do relatório, clique em Atualizar. Por padrão, a funcionalidade SuppressReportAutorun está desativada. Você pode ativá-la no Configurador do NS, em Configurações principais > Interface do usuário > Relatório > SuppressReportAutorun.

Recurso	Descrição
A verificação da licença do CMDB Solution foi removida.	A verificação de licença do CMDB Solution foi removida, disponibilizando o CMDB Solution a todas as soluções Altiris como um recurso. Você pode agora instalar o CMDB Solution como um recurso do inventário, do Client Management Suite e do Server Management Suite. Já vem instalado no Asset Management Suite, no ServiceDesk e no IT Management Suite. Nota: Em uma hierarquia, o CMDB Solution deve ser instalado no Notification Server pai. Não instale o CMDB Solution em um Notification Server filho.
O Out of Band Management Component foi removido.	No IT Management Suite 7.5, o Out of Band Management Component não está mais disponível. Se você fizer o upgrade das versões anteriores do IT Management Suite, o utilitário OOBRemover removerá os itens do Out of Band Management do Notification Server, dos servidores de sites e dos computadores-cliente.
Mudanças nas notas de release do IT Management Suite 7.5 e na documentação do Symantec Management Platform 7.5.	No IT Management Suite 7.5, a maioria das notas de release específicas da solução foram depreciadas para as soluções que são componentes das seguintes séries: ■ Asset Management Suite ■ Client Management Suite ■ Server Management Suite Você pode encontrar as informações das notas de release depreciadas específicas da solução nas notas de release específicas das respectivas séries. Para obter mais informações, consulte o seguinte artigo: http://www.symantec.com/docs/DOC5702

Componentes do Symantec Management Platform

Tabela 1-2 Componentes do Symantec Management Platform

Componente	Descrição
Notification Server e Symantec Management Console	O serviço do Symantec Management Platform que processa os eventos, além de facilitar a comunicação com os computadores gerenciados, também coordena o trabalho dos outros serviços do Symantec Management Platform. O console é a interface do usuário com base na Web do computador do Notification Server que permite gerenciar a plataforma e suas soluções. Consulte “Sobre o Notification Server” na página 64. Consulte “Sobre o Console de gerenciamento Symantec” na página 33.

Componente	Descrição
Banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database)	O banco de dados que armazena todas as informações dos computadores gerenciados. Consulte “Para configurar o banco de dados de gerenciamento de configuração” na página 76.
Servidores de sites	O Symantec Management Platform pode hospedar diversos tipos de componentes middleware, como serviços de pacotes, serviços de tarefas e serviços de implementação de site. O nome oficial de um componente de middleware é "serviço de site." Todo componente que hospeda um serviço de site é conhecido como um servidor de sites. Servidores de sites podem hospedar um ou mais destes serviços. Consulte “Sobre os serviços de site” na página 127.
Symantec Management Agent	O software que é instalado em um computador para permitir a monitoração e gerenciamento pelo Notification Server. Após o Symantec Management Agent ter sido instalado, esse computador torna-se um computador gerenciado. Consulte “Sobre o Symantec Management Agent” na página 236.
Software Management Framework	Uma interface que permite criar e gerenciar os recursos de software que estão no Catálogo de software. Permite também gerenciar os pacotes que estão na Biblioteca de software. A exibição Software fornece um local central para iniciar as tarefas relacionadas ao software que são executadas em sua organização.
Relatórios	Uma maneira de coletar as informações automatizadas. Você pode exibir relatórios de qualquer computador gerenciado no Symantec Management Console. Consulte “Para exibir e gerenciar dados de recursos com relatórios do Notification Server” na página 441.

Consulte [“Sobre o Symantec Management Platform”](#) na página 24.

Consulte [“Como funciona o pcAnywhere Solution”](#) na página 29.

Como funciona o pcAnywhere Solution

O Symantec pcAnywhere Solution usa a tecnologia de controle remoto. Você pode então conectar-se a outro computador ou servidor e trabalhar como se estivesse em frente a ele. O pcAnywhere Solution oferece suporte a conexões de rede em uma rede local (LAN), rede de longa distância (WAN) ou na Internet.

Pode ser útil compreender um pouco da terminologia do pcAnywhere. Por exemplo, o computador-cliente é chamado de computador-host porque hospeda a conexão. O computador do administrador é chamado de computador remoto ou de console. Essa terminologia é originada da computação de mainframe, na qual um usuário

remoto é normalmente conectado a um servidor ou a um computador mainframe. No pcAnywhere, o quadro em sessão é chamado de visualizador.

Na maioria dos casos, um usuário remoto inicia a conexão. Ele fornece as informações necessárias para conectar-se ao computador-host. O usuário remoto também pode selecionar opções para aumentar a segurança ou otimizar o desempenho. Para estabelecer uma conexão, o computador-host deve estar configurado para esperar conexões de entrada do pcAnywhere Solution.

O pcAnywhere Solution inclui as Web parts do pcAnywhere para configuração, relatórios do Notification Server, a interface do Gerenciador do pcAnywhere e o software pcAnywhere Solution.

O pcAnywhere Solution fornece a você os seguintes recursos:

- Segurança com base em funções através de páginas do console
- Configurações de controle do host gerenciado
- Log de auditoria e geração de relatórios
- Suporte a mecanismos de segurança e escopo
- Integração VNC e RDP

O pcAnywhere Solution também incorpora os seguintes recursos do Notification Server:

- Servidor de tarefas
- Hierarquia
- Políticas com base no usuário

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.

Consulte [“Sobre o Gerenciamento de tarefas ”](#) na página 407.

Consulte [“Sobre políticas baseadas em usuário”](#) na página 377.

Sobre como adicionar produtos à plataforma

Um ampla variedade de produtos pode ser executada no Symantec Management Platform. A Symantec e outras empresas fornecem produtos adicionais que são executados na plataforma. Por exemplo, o Symantec Client Management Suite ajuda você a gerenciar computadores endpoint, enquanto que o Symantec Server Management Suite ajuda a gerenciar servidores.

Você usa o Symantec Installation Manager para gerenciar a instalação de produtos adicionais na plataforma. Na página Instale novos produtos, do Symantec Installation Manager, é possível exibir uma lista de produtos disponíveis. Você pode, em seguida, facilmente instalar e avaliar um produto. Produtos têm geralmente uma

licença de avaliação de 30 dias. Você pode exibir uma lista de todos os produtos instalados na página Produtos instalados do Symantec Installation Manager.

Quando você comprar produtos, o Symantec Installation Manager gerenciará também as licenças. Na página Licenciamento do produto, é possível aplicar licenças aos produtos instalados e exibir o status de licenças aplicadas.

Para obter mais informações, consulte o *Guia de Planejamento de Implementação do IT Management Suite*.

Onde obter mais informações

Use os seguintes recursos de documentação para conhecer e usar este produto.

Tabela 1-3 Recursos de documentação

Documento	Descrição	Local
Notas de versão	Informações sobre novos recursos e problemas importantes.	A página Produtos suportados de A a Z , que está disponível no seguinte URL: http://www.symantec.com/business/support/index?page=products Abra a página de suporte de seu produto e, em seguida, em Tópicos comuns , clique em Notas de versão .
Guia do Usuário	Informações sobre como usar este produto, inclusive informações técnicas e instruções detalhadas para a realização de tarefas comuns.	■ A Biblioteca de documentação, disponível no Symantec Management Console, no menu Ajuda. ■ A página Produtos suportados de A a Z, que está disponível no seguinte URL: http://www.symantec.com/business/support/index?page=products Abra a página de suporte de seu produto e, em seguida, em Tópicos comuns, clique em Documentation.
Ajuda	Informações sobre como usar este produto, inclusive informações técnicas e instruções detalhadas para a realização de tarefas comuns. A ajuda está disponível em nível de solução e de conjunto. Essas informações estão disponíveis no formato de ajuda em HTML.	A Biblioteca de documentação, disponível no Symantec Management Console, no menu Ajuda . A ajuda contextual está disponível para a maioria das telas no Symantec Management Console. É possível abrir a ajuda contextual das seguintes maneiras: ■ Clique na página e pressione a tecla F1. ■ Use o comando Context, disponível no Console de gerenciamento Symantec, no menu Ajuda.

Além da documentação do produto, você pode usar os recursos a seguir para conhecer os produtos da Symantec.

Tabela 1-4 Recursos para obter informações sobre os produtos da Symantec

Recurso	Descrição	Local
Base de conhecimento de suporte do SymWISE	Artigos, incidentes e problemas relacionados a produtos da Symantec.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase (em inglês)
Symantec Connect	Um recurso online que contém fóruns, artigos, blogs, downloads, eventos, vídeos, grupos e ideias para usuários dos produtos da Symantec.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation Aqui está a lista de links para vários grupos no Connect: ■ Implementação e criação de imagens http://www.symantec.com/connect/groups/deployment-and-imaging (em inglês) ■ Descoberta e inventário http://www.symantec.com/connect/groups/discovery-and-inventory (em inglês) ■ Administrador do ITMS http://www.symantec.com/connect/groups/itms-administrator ■ Gerenciamento do Mac http://www.symantec.com/connect/groups/mac-management (em inglês) ■ Monitor Solution e integridade do servidor http://www.symantec.com/connect/groups/monitor-solution-and-server-health (em inglês) ■ Gerenciamento de patches http://www.symantec.com/connect/groups/patch-management (em inglês) ■ Geração de relatórios http://www.symantec.com/connect/groups/reporting (em inglês) ■ ServiceDesk e fluxo de trabalho http://www.symantec.com/connect/workflow-servicedesk ■ Gerenciamento de software http://www.symantec.com/connect/groups/software-management (em inglês) ■ Gerenciamento de servidores http://www.symantec.com/connect/groups/server-management ■ Workspace Virtualization e fluxo contínuo http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming (em inglês)

Introdução ao Console de gerenciamento Symantec

Este capítulo contém os tópicos a seguir:

- [Sobre o Console de gerenciamento Symantec](#)
- [Sobre as exibições do console](#)
- [Acesso ao Console de gerenciamento Symantec](#)
- [Para acessar a documentação do Console de gerenciamento Symantec](#)
- [Para acessar a página Meu portal](#)
- [Para acessar a página Início do Gerenciamento do Notification Server](#)
- [Para personalizar o Console de gerenciamento Symantec](#)

Sobre o Console de gerenciamento Symantec

O Console de gerenciamento Symantec (normalmente chamado "o console") é uma interface do usuário com base na Web que é a ferramenta principal para interagir com o Notification Server e seus componentes e para gerenciar recursos.

O Console de gerenciamento Symantec é dividido nas seguintes áreas:

Cabeçalho

A parte superior do console que inclui o seguinte:

- Menus, que permitem acessar as páginas e as caixas de diálogos do console que fornecem a funcionalidade de gerenciamento do Notification Server. As soluções da Symantec instaladas no sistema podem adicionar novos itens ao menu.
- Caixa de pesquisa, que permite pesquisar os dados dos recursos que você deseja. Quando você executar uma pesquisa, um painel de pesquisa aparecerá abaixo, no qual você digitará o termo da pesquisa.
- Uma barra da trilha de navegação que mostra o caminho do menu da página atualmente exibida.

Área do conteúdo

A parte do console que está abaixo do cabeçalho pode mostrar um dos seguintes itens:

- **Exibição**
Uma exibição é composta de uma exibição em árvore e de um painel de conteúdo. A exibição em árvore, no painel esquerdo, mostra uma disposição hierárquica dos itens que você pode selecionar e com os quais pode trabalhar. O painel de conteúdo, à direita, exibe as páginas baseadas em seleções de exibição em árvore.
- **Página do portal**
Uma página do portal exibe uma coleção de diferentes informações contidas nas Web parts. O Notification Server inclui páginas do portal predefinidas e outras páginas do portal podem ser incluídas com soluções. Você também pode criar suas próprias páginas do portal.
- **Página completa**
Uma página completa tem um único painel de conteúdo sem exibição em árvore.

Algumas páginas do console suportam a personalização, que é a capacidade de uma página do console de preservar o estado de seus controles por usuário. Por exemplo, um dia o usuário A pode abrir uma página de filtro e, para atender a sua preferência pessoal, reordenar as colunas na grade. Nesse meio tempo, o usuário B abre a mesma página, mas deixa a grade com sua configuração padrão. No seguinte dia, quando os usuários abrirem essa página de filtro, o usuário A verá a página como ele a configurou no dia anterior. O usuário B ainda verá a exibição padrão como ele a deixou no dia anterior.

A personalização é aplicada atualmente às páginas de geração de relatórios e de filtro e ao estado da árvore de navegação nas páginas de exibição. Além disso, a página Meu portal é personalizada para cada usuário.

Sobre as exibições do console

Uma exibição é um layout em painel duplo com uma árvore de navegação no lado esquerdo e o conteúdo no lado direito. A árvore de navegação contém os links para os itens do Console de gerenciamento Symantec e permite agrupar os itens de diferentes partes do console em uma estrutura apropriada. Um item pode aparecer várias vezes em uma exibição e em qualquer número de exibições diferentes. Uma exibição pode incluir pastas, links de itens e links da Web. O Symantec Management Platform e as soluções incluem as exibições predefinidas que você pode modificar e ampliar conforme a necessidade. Você também pode criar as suas próprias exibições.

Consulte [“Para criar e modificar exibições”](#) na página 55.

Consulte [“Para adicionar novos itens diretamente a uma exibição”](#) na página 57.

As exibições permitem organizar e acessar o Symantec Management Platform e a funcionalidade da solução. Você pode configurar exibições para refletir a funcionalidade fornecida por uma solução ou por um recurso, ou para fornecer aos usuários uma função específica com acesso às tarefas apropriadas.

A estrutura padrão da árvore de navegação que você pode ver no painel esquerdo é a estrutura real da pasta. Cada item aparece somente uma vez na estrutura real. As pastas em uma exibição podem ser as pastas virtuais, que não existem na estrutura real ou podem ser links para as pastas reais. Um link para uma pasta real inclui tudo que estiver nessa pasta. Se algum item novo for adicionado à estrutura real nessa pasta, ele será automaticamente incluído na exibição. Você não pode excluir itens de uma pasta de uma exibição, mas você pode excluí-los da exibição. Assim, o link entre a exibição e o item é quebrado: o item real não é excluído.

A segurança é aplicada às exibições; assim, o que você vê em uma exibição depende de seus privilégios da segurança e permissões. Para ter um privilégio ou uma permissão sobre uma pasta em uma exibição, deve-se definir diretamente na exibição e também na pasta real. Você pode ver somente alguns dos itens em uma exibição, mas outros usuários podem ver mais ou menos.

Sobre a exibição Computadores

Nota: Você deve ter um dos seguintes produtos instalados para ver esta página: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para acessar a exibição aprimorada **Computadores**, no Console de gerenciamento Symantec, clique em **Gerenciar > Computadores**.

A exibição **Computadores** oferece duas maneiras de verificar computadores em seu ambiente, as exibições individual e resumida.

Nota: Você pode alternar entre estas exibições clicando nas setas duplas (>> ou <<) à direita do cabeçalho **Computadores**.

Exibição individual

A exibição individual fornece detalhes sobre um computador específico. Você pode especificar este computador no painel de navegação à esquerda ou na caixa de diálogo da pesquisa, no painel **Lista**.

Tabela 2-1 Exibição individual

Painel de navegação (Contém pesquisas salvas e grupos e exibições organizacionais)	Painel de listas (Exibe os computadores da pesquisa salva ou de grupos e exibições organizacionais selecionados)	Painel de detalhes (Exibe detalhes de inventário sobre os computadores selecionados)
Computadores Pesquisas salvas ■ Novos computadores ■ Agente instalado ■ <Definido pelo usuário> Todas as exibições de computador ■ Todos os computadores ■ Máquina virtual Blades: ■ Computadores ■ Trabalhos/Tarefas ■ Políticas ■ Software	Campo de pesquisa Resultados da pesquisa	Páginas do flipbook: ■ Geral ■ Identificação ■ Detalhes do Symantec Management Agent (precisa do agente instalado) ■ Hardware ■ Rede ■ Unidades ■ Módulos de memória ■ Hotfixes da Microsoft ■ Programas licenciados Blades ■ Trabalhos/Tarefas ■ Políticas ■ Software

Exibição resumida

A exibição resumida adiciona um flipbook com três páginas que fornecem informações acionáveis sobre entregas de software, fabricantes e sistemas

operacionais em seu ambiente. A seleção no painel de navegação muda os resultados no painel de resumo e no painel de listas. Clicar em um gráfico ou em um item da legenda nas páginas do flipbook refinará mais o resultado. Você poderá então adicionar mais critérios à pesquisa avançada.

Você pode alternar entre as páginas do flipbook clicando nos links nas páginas do flipbook.

Tabela 2-2 Exibição resumida

Painel de navegação (Contém pesquisas salvas e grupos e exibições organizacionais)	Painel de resumo (Contém um flipbook com 3 páginas)	Painel de listas (Exibe os computadores da pesquisa salva ou de grupos e exibições organizacionais selecionados)
Computadores	■ Entregas de software ■ Fabricantes ■ Sistemas operacionais	Campo de pesquisa
Pesquisas salvas ■ Novos computadores ■ Agente instalado ■ <Definido pelo usuário>		Resultados da pesquisa
Exibição Todos os computadores ■ Todos os computadores ■ Máquina virtual		
Blades ■ Computadores ■ Trabalhos/Tarefas ■ Políticas ■ Software		

A exibição **Computadores** permite executar as tarefas a seguir:

- Pesquisar computadores e salvar os resultados da pesquisa para reutilização como um filtro personalizado em computadores de destino com trabalhos, tarefas, políticas ou entrega de software.
Consulte [“Para pesquisar um computador e salvar a pesquisa como um filtro”](#) na página 38.

- Crie e gerencie grupos e exibições organizacionais.
Consulte [“Para criar e preencher um grupo ou exibição organizacional”](#) na página 345.
- Arraste e solte computadores em grupos e exibições organizacionais.
Consulte [“Para criar e preencher um grupo ou exibição organizacional”](#) na página 345.
- Exiba e execute ações sobre informações de resumo para tarefas de Entrega rápida e políticas de Entrega gerenciada
Consulte [“Para reexecutar uma tarefa com falha”](#) na página 423.
- Exiba informações de resumo de fabricantes de hardware e sistemas operacionais

Para pesquisar um computador e salvar a pesquisa como um filtro

Na exibição **Computadores**, você pode pesquisar um computador ou um grupo específico de computadores aplicando ou modificando uma pesquisa predefinida salva. Uma pesquisa salva é um filtro especial que exibe uma lista dinâmica de computadores que cumprem os critérios de filtragem. Você pode também criar uma pesquisa salva completamente nova.

Consulte [“Sobre a exibição Computadores ”](#) na página 35.

A lista **Todos os computadores** é o ponto de partida que exibe todos os computadores e todas as pesquisas salvas.

Para pesquisar um computador e salvar a pesquisa como um filtro

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Computadores**.
- 2 No painel de listas, no campo de pesquisa, digite o nome completo ou parte do nome de um computador.

Nome completo	Digite o nome completo de um computador ou de um grupo de computadores específicos que você deseja encontrar.

Nome parcial	Digite um nome parcial se desejar que a pesquisa retorne todos os computadores que contenham uma string de texto específica em qualquer lugar no nome. Para exibir todos os computadores com um prefixo do local, como Índia, é possível digitar Ind . Os resultados da pesquisa exibem todos os computadores que contêm a string.

- 3 (Opcional) Para usar recursos de pesquisa avançada, clique na seta para baixo, ao lado do campo de pesquisa, e selecione o critério de pesquisa que você quer aplicar.

Consulte [“Sobre operadores da pesquisa”](#) na página 44.

- 4 (Opcional) Para selecionar vários critérios de pesquisa, clique na seta para baixo, ao lado da lista suspensa **Adicionar critérios de pesquisa**, selecione um critério, e repita a etapa para adicionar outros critérios.

Para remover um critério de pesquisa, deixe o campo vazio.

- 5 (Opcional) Se os critérios que você quiser usar não estiverem relacionados na lista suspensa da pesquisa avançada, crie critérios de pesquisa personalizados. Para criar um critério de pesquisa personalizado:

- No painel da lista, clique na seta para baixo ao lado do campo de pesquisa.
- Na lista suspensa **Adicionar critérios de pesquisa**, clique em **Adicionar critérios personalizados**.
- Na caixa de diálogo **Adicionar critérios de pesquisa**, marque as classes de dados e as colunas que você quer usar para critérios de pesquisa. Observe que a seleção de colunas preenche os critérios de pesquisa na lista suspensa e disponibiliza critérios adicionais como parte de sua pesquisa.
- Clique em **OK**.

- 6 Para salvar a pesquisa, clique no ícone de salvar, na área da pesquisa avançada.

Note que qualquer campo que não contiver um valor será ignorado na consulta e não será salvo quando você salvar a pesquisa.

- 7 Na caixa de diálogo **Salvar pesquisa**, no campo **Nome**, digite um nome e clique em **OK**.

A pesquisa salva é exibida em **Pesquisas salvas**, no painel de navegação, e torna-se disponível para que você o utilize novamente.

- 8 (Opcional) Se você usar uma pesquisa salva somente como um filtro direcionado a trabalhos, tarefas ou políticas, e não quiser que ela apareça no painel de navegação, será possível ocultá-la. Para ocultar a pesquisa salva, faça o seguinte:

- Clique com o botão direito do mouse em **Pesquisas salvas** e clique em **Gerenciar pesquisas salvas**.
- Na caixa de diálogo **Gerenciar pesquisas salvas**, desmarque a caixa ao lado da pesquisa que você não quer exibir.

- Clique em **Fechar**.

Vídeo: Para obter mais informações sobre a criação de pesquisas avançadas salvas nas exibições aprimoradas, veja [Creating Advanced Saved Searches in Enhanced Console Views Video \(em inglês\)](#) no Symantec Connect.

Sobre a exibição Software

Nota: Você deve ter uma das seguintes soluções ou séries instaladas para ver esta página: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para acessar a exibição aprimorada **Software**, no Console de gerenciamento Symantec, clique em **Gerenciar > Software**.

A exibição **Software** oferece três painéis: painel de navegação à esquerda, uma lista de software e um painel de campo de pesquisa no centro, e um painel de conteúdo à direita. O painel de navegação contém pesquisas salvas. O painel de listas exibe os itens de software da pesquisa salva selecionada. O painel de conteúdo exibe os detalhes sobre o software que você selecionou.

A exibição **Software** permite executar as tarefas a seguir:

- Pesquisar software por nome, fabricante ou outros critérios.
Consulte [“Para pesquisar o software e salvar a pesquisa”](#) na página 40.
- Gerenciar produtos de software.
- Instalar software usando o recursos de arrastar e soltar.
- Gerenciar licenças de software.
- Controlar o uso e as licenças do software.

Vídeo: para obter mais informações sobre como gerenciar software nas exibições aprimoradas, veja [Importing Software Using Enhanced Console Views Video \(em inglês\)](#), [Managing Imported Software Using Enhanced Console Views Video \(em inglês\)](#) e [Deploying Software Using Enhanced Console Views Video \(em inglês\)](#) no Symantec Connect.

Para pesquisar o software e salvar a pesquisa

Na exibição aprimorada **Software**, os resultados da pesquisa que aparecem no painel de listas não são filtrados automaticamente. Você pode usar a pesquisa e os recursos de pesquisa avançada para reduzir e refinar sua lista, até que o painel de listas contenha o software específico.

Consulte [“Sobre a exibição Software”](#) na página 40.

Você pode salvar as pesquisas de software personalizadas e reutilizá-las mais tarde. As pesquisas salvas aparecem no painel de navegação, no subpainel **Software instalado**. Você pode usar pesquisas salvas como filtros para direcionar tarefas, trabalhos e políticas para o software. Você também pode usar pesquisas salvas para entregar o software em computadores ou grupos de computadores específicos.

Para pesquisar um software específico e salvar a pesquisa

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Software**.
- 2 No painel de navegação, clique em uma pesquisa salva que você queira usar como ponto de partida de sua pesquisa.
- 3 No painel de listas, no campo de pesquisa, digite os critérios de pesquisa.
- 4 (Opcional) Para usar recursos de pesquisa avançada, clique na seta para baixo, ao lado do campo de pesquisa, e selecione o critério de pesquisa que você quer aplicar.

Consulte [“Sobre operadores da pesquisa”](#) na página 44.

- 5 (Opcional) Para selecionar vários critérios de pesquisa, clique na seta para baixo, ao lado da lista suspensa de critérios de pesquisa, selecione um critério, e repita a etapa para adicionar outros critérios.
- 6 (Opcional) Se os critérios que você quiser usar não estiverem relacionados na lista suspensa da pesquisa avançada, crie critérios de pesquisa personalizados. Para criar um critério de pesquisa personalizado:
 - Na lista suspensa **Adicionar critérios de pesquisa**, clique em **Adicionar critérios personalizados**.
 - Na caixa de diálogo **Adicionar critérios de pesquisa**, marque as classes de dados e as colunas que você quer usar para critérios de pesquisa. Observe que a seleção de colunas preenche os critérios de pesquisa na lista suspensa e disponibiliza critérios adicionais como parte de sua pesquisa.
 - Clique em **OK**.
- 7 Para salvar a pesquisa, clique no ícone de salvar, na área da pesquisa avançada.

Note que qualquer campo que não contiver um valor será ignorado na consulta e não será salvo quando você salvar a pesquisa.

- 8 Na caixa de diálogo **Salvar pesquisa**, no campo **Nome**, digite um nome e clique em **OK**.
- A pesquisa salva parece em **Software instalado**, no painel de navegação, e torna-se disponível para reutilização.
- 9 (Opcional) Se você usar uma pesquisa salva somente como um filtro direcionado a trabalhos, tarefas ou políticas, e não quiser que ela apareça no painel de navegação, será possível ocultá-la. Para ocultar a pesquisa salva, faça o seguinte:
- Clique com o botão direito do mouse em **Software instalado** e clique em **Gerenciar pesquisas salvas**.
 - Na caixa de diálogo **Gerenciar pesquisas salvas**, desmarque a caixa ao lado da pesquisa que você não quer exibir.
 - Clique em **Fechar**.

Sobre a janela Catálogo de software

Nota: Você deve ter uma das seguintes soluções ou séries instaladas para ver esta página: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

A janela **Catálogo de software** aparece na exibição **Software**.

Para acessar a exibição aprimorada **Catálogo de software**, no Console de gerenciamento Symantec, clique em **Gerenciar > Catálogo de software**. Você pode também navegar até **Gerenciar > Software**, clicar com o botão direito do mouse em **Software instalado** e clicar em **Gerenciar catálogo de software**.

Consulte "[Sobre a exibição Software](#)" na página 40.

Na janela **Catálogo de software**, você pode executar as seguintes tarefas de gerenciamento de software:

- Importar ou adicionar novos componentes e produtos de software.
Você pode importar o software mesmo se ele não estiver no inventário.
- Adicionar o software recém-descoberto ou indefinido que você pretende gerenciar em sua lista de software gerenciado.
- Mover o software recém-descoberto ou indefinido que você não pretende gerenciar em sua lista de software não gerenciado.
- Mover produtos de software de uma lista para outra conforme mudarem suas necessidades.

- Excluir um produto de software. Esta ação cancela a associação entre os componentes de software e os pacotes através dos quais eles são fornecidos. Quando você excluir um produto de software, seus componentes serão relacionados novamente no painel **Software recém-descoberto/indefinido**.

Sobre a exibição Trabalhos/Tarefas

Nota: Você deve ter uma das seguintes soluções ou séries instaladas em para ver essa exibição: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para acessar a exibição **Trabalhos / Tarefas**, no Console de gerenciamento Symantec, clique em **Gerenciar > Trabalhos e tarefas**.

A exibição **Trabalhos/Tarefas** permite exibir e trabalhar com todos os trabalhos e tarefas disponíveis. Por exemplo, para executar trabalhos e tarefas, você pode arrastá-los e soltá-los em um ou mais computadores. Você pode também usar a opção **Execução rápida** para visar a um trabalho ou uma tarefa sem precisar exibir os detalhes manualmente.

Consulte [“Para executar um trabalho ou uma tarefa usando o recurso de arrastar e soltar”](#) na página 421.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Sobre a exibição Políticas

Nota: Você deve ter uma das seguintes soluções ou séries instaladas para ver esta página: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para acessar a exibição aprimorada **Políticas**, no Console de gerenciamento Symantec, clique em **Gerenciar > Políticas**.

A exibição aprimorada **Políticas** permite exibir e trabalhar com todas as políticas disponíveis. É possível executar todas as funções comuns de aplicar regras e correções a computadores. Você pode definir os agendamentos da verificação de conformidade e ativar políticas. Você pode iniciar políticas arrastando-as e soltando-as em um ou mais computadores. Você pode também usar a opção **Aplicar rapidamente** para visar uma política sem exibir os detalhes manualmente.

Consulte [“Para aplicar uma política usando o recursos de arrastar e soltar”](#) na página 379.

Consulte “[Especificação dos destinos de uma política ou tarefa](#)” na página 380.

Sobre operadores da pesquisa

Você poderá usar os operadores da pesquisa para reduzir os resultados quando pesquisar um item ou um grupo específico de itens.

Consulte “[Para pesquisar um computador e salvar a pesquisa como um filtro](#)” na página 38.

Consulte “[Para pesquisar o software e salvar a pesquisa](#)” na página 40.

As seguintes condições gerais de pesquisa se aplicam:

- As aspas limitam a pesquisa para uma correspondência exata.
“**Windows XP**” = computadores que executam **EXACT MATCH** de Windows XP.
“**Adobe Acrobat**” = computadores que executam **EXACT MATCH** Adobe Acrobat.
- A omissão de aspas permite a correspondência com texto de pesquisa em qualquer lugar de uma string.
Windows XP = computadores em que o **LIKE** Windows XP é executado em qualquer lugar no nome.
Adobe Acrobat = computadores que executam **LIKE** Adobe Acrobat em qualquer lugar do nome.

Tabela 2-3 Procure os operadores que você pode usar para expressar vários argumentos

Argumento	Símbolo	Descrição
Ou	Símbolo da barra vertical ().	Este operador não exige espaços à esquerda. Quando você pesquisar um computador, os exemplos do uso são: ■ Windows XP = computadores que executam LIKE Windows OR LIKE XP ■ XP 2000 2003 = computadores que executam LIKE XP OR LIKE 2000 OR LIKE 2003 Quando você pesquisar um software, o exemplo do uso será da seguinte forma: ■ Adobe Microsoft = fabricante do software LIKE Adobe OR LIKE Microsoft

Argumento	Símbolo	Descrição
E, adicionar ou incluir	Sinal positivo (+).	Este operador não exige espaço à esquerda. Quando você pesquisar um computador, os exemplos do uso são: ■ Windows+XP = computadores que executam LIKE Windows AND XP ■ Windows+2008 = computadores que executam LIKE Windows AND 2008 Quando você pesquisar um software, o exemplo do uso será da seguinte forma: ■ Adobe+Microsoft = fabricante do software LIKE Adobe AND Microsoft
Não, menos ou não inclui	Sinal negativo (-).	Este operador exige um espaço à esquerda. Se você inserir um sinal negativo sem um espaço à direita, ele não será interpretado como um operador. Como melhor prática, inicie com o grupo geral no qual você deseja fazer a pesquisa e insira o texto de exclusão. Quando você pesquisar um computador, os exemplos do uso são: ■ Windows [espaço] -XP = computadores que executam Windows NOT LIKE XP ■ Windows Server [espaço] -2003 = computadores que executam Windows Server NOT LIKE 2003 Os seguintes exemplos presumem que os computadores são nomeados com numerais, como pc-1, pc-12, pc-27, pc-125, pc-218, pc-243 e pc-321: ■ pc- [espaço] -1 = computadores nomeados pc- NOT LIKE 1, 12, 125, 218, 321 ■ pc- [espaço] --1 = computadores nomeados pc- NOT LIKE 27, 218, 321 Quando você pesquisar um software, o exemplo do uso será da seguinte forma: ■ -Adobe -Microsoft = fabricante do software NOT LIKE Adobe e NOT LIKE Microsoft

Para configurar as exibições aprimoradas

As exibições aprimoradas no Console de gerenciamento Symantec permitem definir configurações específicas. É possível configurar campos de pesquisa específicos para que você possa ver seus resultados quando digitar o parâmetro. Você pode configurar estes mesmos campos de pesquisa para que seja possível ver seus resultados somente depois de pressionar **Enter**. Você pode configurar as exibições aprimoradas para usar o IME (Input Method Editor) para que seja possível inserir caracteres de dois bytes nestas exibições. Você pode configurar também o número de computadores e de softwares que aparecerão na lista de resultados. Se você

gerenciar um número muito grande de computadores, esta configuração pode melhorar o tempo de carregamento.

Para definir as configurações das exibições aprimoradas

- 1 No **Symantec Management Console**, no menu **Settings**, clique em **Console > Exibições aprimoradas**.
- 2 Na caixa de diálogo **Configurações de exibições aprimoradas**, defina as seguintes configurações:

Pesquisar

Ao digitar - esta opção permite visualizar os resultados enquanto você digita os requisitos no campo de pesquisa. A configuração padrão é **Ao digitar**.

Após pressionar Enter - esta opção permite visualizar seus resultados somente depois que você digitar os requisitos no campo de pesquisa e pressionar **Enter**.

Estas opções de pesquisa afetam os seguintes campos de pesquisa:

- A exibição **Computers**, campo de pesquisa do painel central, que inclui todas as pesquisas salvas e filtradas
- A exibição **Software**, campo de pesquisa do painel central, que inclui todas as pesquisas salvas e filtradas

Permitir IME (Input Method Editor) para digitar caracteres de linguagem de dois bytes

Ativa o suporte a IME para exibições aprimoradas e para o portal Primeira instalação. Quando esta opção estiver selecionada, você poderá usar o IME para digitar caracteres de dois bytes nestas páginas.

Limitar as listas de resultados de computador e software a

Limita o número de computadores ou software que pode aparecer em uma lista de resultados. Se seu ambiente tiver uma hierarquia com milhares de computadores, as listas poderão levar muito tempo para serem carregadas e poderão até mesmo atingir o tempo limite. Este limite define quantas linhas a consulta deve retornar. A configuração padrão é de 20.000, mas você pode reduzir esta configuração para melhorar o tempo de carregamento. Se houver linhas adicionais, a última linha indicará que há mais registros e permitirá que você os carregue.

3 Clique em **OK**.

Acesso ao Console de gerenciamento Symantec

O Console de gerenciamento Symantec (normalmente mencionado como “o console”) pode ser acessado do computador que está executando o Notification Server ou remotamente. Uma conexão remota requer que o computador remoto tenha acesso ao computador do Notification Server e esteja executando uma versão suportada do Microsoft Windows e do Microsoft Internet Explorer. Como o console é baseado em navegador da Web, você não precisa instalar nenhum software especial para usar o console.

Consulte [“Sobre o Console de gerenciamento Symantec”](#) na página 33.

Você deve ser um membro de uma ou mais funções de segurança do Notification Server para acessar o console.

Consulte [“Sobre a segurança do Symantec Management Platform”](#) na página 83.

Nota: O Symantec Management Platform oferece suporte à autenticação NTLM para conexões remotas. Isso permite acessar o Console de gerenciamento Symantec através de um computador remoto sem que um nome de usuário e uma senha sejam solicitados (chamado também de “login único” no console). Você deve estar conectado ao computador remoto com uma conta do Symantec Management Platform e usar o FQDN para obter o nome do Notification Server

Se você for alertado para obter um nome de usuário e uma senha ao se conectar ao Console de gerenciamento Symantec, poderá precisar adicionar o nome do Notification Server (FQDN) à zona de sites confiáveis do computador remoto. Isso pode ser feito através do Painel de controle, na caixa de diálogo Propriedades da Internet na guia Segurança.

O console suporta Microsoft Internet Explorer 7.0 de 32 bits. Todos os controles Active-X usados são de 32 bits; portanto, navegadores de 64 bits não são suportados. Se você abrir o console com um navegador não suportado, uma mensagem será exibida na linha superior. A mensagem avisa que o navegador não é suportado e que alguns recursos podem não estar disponíveis. Use navegadores não suportados por sua conta e risco.

Alguns controles Active-X devem estar instalados para permitir que o console funcione corretamente. Você precisa ter uma conta de administrador no computador do console ou ter os controles Active-X apropriados instalados pelo seu suporte de TI.

Nota: Se você enfrentar problemas, como páginas do console que mostram mensagens de erro, perda de dados ou controles da interface do usuário se comportando de maneira inesperada, verifique se o nome do Notification Server está especificado corretamente. O nome do Notification Server deve conter somente caracteres alfanuméricos. Caracteres especiais, incluindo o caractere de sublinhado, não são permitidos.

Para acessar localmente o Console de gerenciamento Symantec

- ◆ No computador local, no menu **Iniciar**, clique em **Todos os programas > Symantec > Console de gerenciamento Symantec**.

Para acessar remotamente o Console de gerenciamento Symantec

- 1 Em um computador remoto, abra o Internet Explorer e consulte o seguinte URL:

http://Nome do Notification Server/altiris/console

O nome do Notification Server deve ser o nome de domínio totalmente qualificado. Você pode usar https, se necessário. Se o Notification Server não estiver na porta 80, você precisará incluir o número da porta apropriado depois do nome do Notification Server.

- 2 Se estiver conectado no computador remoto com uma conta que não é do Symantec Management Platform, você será solicitado a inserir seu nome de usuário e senha.

Se você estiver conectado ao computador remoto com uma conta do Symantec Management Platform, o recurso de login único controlará o acesso automaticamente. Se o prompt for exibido, você poderá precisar adicionar o nome do Notification Server (FQDN) à zona de sites confiáveis no computador remoto.

Para acessar a documentação do Console de gerenciamento Symantec

Há duas maneiras de acessar a documentação no Console de gerenciamento Symantec: ajuda contextual e biblioteca de documentação. A ajuda contextual permite acessar informações específicas ao local (página, caixa de diálogo ou guia) em que você está no console. Quando você acessar a ajuda contextual, o Guia do Usuário do produto associado ao local será aberto em uma nova janela que exibe o tópico apropriado.

A biblioteca de documentação é uma página no Console de gerenciamento Symantec que permite acessar a documentação que é fornecida com cada produto instalado, como Guias do Usuário, Guias de Administração, Guias de Implementação e notas de release. A documentação pode ser localizada no computador do Notification Server, como Guias do Usuário, ou em um site, como as notas de versão. Algumas documentações estão no formato Adobe Acrobat e exigem o Adobe Acrobat Reader para serem exibidas ou impressas.

Consulte [“Sobre o Console de gerenciamento Symantec”](#) na página 33.

Para acessar a ajuda contextual da documentação

- 1 No Console de gerenciamento Symantec, certifique-se que o local em que você deseja acessar a ajuda está ativo.

Para ativar um local, clique em algum lugar no local. Por exemplo, clique na página ou na caixa de diálogo.
- 2 Execute um destes procedimentos:
 - No menu **Ajuda**, clique em **Contexto**.
 - Pressione a tecla **F1**.

Para acessar a biblioteca de documentação

- 1 No Console de gerenciamento Symantec, no menu **Ajuda**, clique em **Biblioteca de documentação**.
- 2 Na página **Biblioteca de documentação**, clique no link associado à documentação que você deseja acessar.

Para acessar a página Meu portal

Meu portal é a página padrão exibida quando um novo usuário abre o Console de gerenciamento Symantec.

Todas as mudanças que um usuário fizer na página Meu portal, tal como adição, edição ou remoção de Web Parts, serão personalizadas a esse usuário. As

mudanças são salvas de acordo com o ID do usuário. Quando o próximo usuário fizer logon e selecionar a página Meu portal do menu Console, a página personalizada será recarregada automaticamente.

Consulte [“Para criar e modificar páginas do portal”](#) na página 57.

Para acessar a página Meu portal

- ◆ No Console de gerenciamento Symantec, no menu **Início**, clique em **Meu portal**.

Para acessar a página Início do Gerenciamento do Notification Server

A página Início do Gerenciamento do Notification fornece acesso a informações importantes sobre o Notification Server e as soluções instaladas.

A página Início do Gerenciamento do Notification Server inclui as seguintes informações:

Gerenciador de recursos	Um link que permite selecionar um recurso para exibição no console do Gerenciador de recursos.
Produtos instalados	Lista das soluções que estão instaladas no Notification Server.
Servidores de sites	Lista de serviços e servidores de sites incluídos no site do Notification Server.
Hierarquia	Detalhes da hierarquia a que o Notification Server pertence. Estas informações serão exibidas somente se o Notification Server for membro de uma hierarquia.
Status da instalação do agente	Status da instalação do Symantec Management Agent nos computadores que você deseja gerenciar.
Licenças	Relaciona o seguinte para cada solução: ■ Número total de licenças disponíveis ■ Número de licenças em uso ■ Datas de expiração da licença (se aplicável)

A página Início do Gerenciamento do Notification Server, assim como todas as páginas do portal, é personalizável. Você pode configurar a página com as informações que achar mais úteis.

Consulte [“Para criar e modificar páginas do portal”](#) na página 57.

Para acessar a página Início do Gerenciamento do Notification Server

- ◆ No Console de gerenciamento Symantec, no menu **Início**, clique em **Gerenciamento do Notification Server > Portal**.

Para personalizar o Console de gerenciamento Symantec

Você pode personalizar o Console de gerenciamento Symantec para atender aos requisitos de sua organização. Por exemplo, talvez você queira adicionar itens extras de submenu ao menu do console para atender aos usuários em sua organização. Você não pode mudar as opções de nível superior do menu e você não pode editar ou remover quaisquer dos itens do submenu fornecidos com o Console de gerenciamento Symantec.

A maioria das personalizações aplica-se a todo o sistema. Para conseguir uma personalização em nível de função, você pode usar a segurança em itens. Por exemplo, você pode criar uma página do portal que seja acessível somente a uma determinada função. Nesse caso, a personalização é implementada com permissões em itens, não privilégios. Exibições, árvores e menus também podem ser personalizados usando a segurança. Por exemplo, um administrador da Symantec pode definir a permissão de um item da árvore ou de uma opção de menu, de modo que os usuários em uma função possam visualizar, mas os usuários em outra função não possam. Porém, a página Meu portal e a personalização por página aplicam-se por usuário.

Tabela 2-4 Tarefas de personalização

Tarefa	Descrição
Personalizar menus	Adicione submenus e itens de submenu e configure a estrutura do menu que melhor atende a sua organização. Consulte “Para personalizar o menu do console” na página 52.
Personalizar menus de contexto	Adicione ações definidas pelo usuário ao menu contextual. Consulte “Para adicionar ações definidas pelo usuário ao menu contextual” na página 53.

Tarefa	Descrição
Personalizar exibições	Crie e modifique exibições para configurar a estrutura da árvore de navegação que melhor atende a sua organização. Consulte “Para criar e modificar exibições” na página 55. Consulte “Para adicionar novos itens diretamente a uma exibição” na página 57.
Personalizar páginas do portal	Crie e modifique as páginas do portal. Uma página do portal é uma página do Console de gerenciamento Symantec que pode ser personalizada para se adaptar às suas necessidades. Você pode usar uma página do portal para consolidar as informações-chave em uma única página de fácil exibição. Uma página do portal pode exibir o status do Symantec Management Platform e dos computadores gerenciados ou quaisquer outras informações que você queira disponibilizar. Por exemplo, você pode incluir páginas externas da Web, páginas da intranet, RSS feeds ou seus próprios aplicativos. Consulte “Para criar e modificar páginas do portal” na página 57.
Personalizar Web parts	Crie e modifique as Web parts que você usa para criar páginas do portal. Consulte “Para criar e modificar Web parts” na página 60.

Você pode salvar seus elementos personalizados do console como arquivos XML e restaurá-los quando necessário, importando os arquivos apropriados.

Consulte [“Para salvar elementos do console como arquivos XML”](#) na página 61.

Para personalizar o menu do console

Você pode personalizar o menu do console para atender a seus requisitos. As opções de menu fornecidas com o Symantec Management Platform são somente leitura e não podem ser modificadas. É possível adicionar novos submenus e modificá-los conforme a necessidade. Você pode mover ou excluir qualquer item de menu, exceto aqueles que foram designados como somente leitura.

Consulte [“Para personalizar o Console de gerenciamento Symantec”](#) na página 51.

Para personalizar o menu do console

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Console > Menus**.
- 2 Na página **Editar menu**, execute as tarefas apropriadas de personalização:

Para adicionar itens de menu	1	No painel esquerdo, clique com o botão direito do mouse no item de menu ao qual você quer adicionar o novo item de menu e clique em Novo item .
	2	Na página Detalhes do menu , especifique os detalhes do item de menu e clique em Aplicar .
Para adicionar submenus	1	No painel esquerdo, clique com o botão direito do mouse no item de menu ao qual você quer adicionar o submenu e clique em Novo submenu .
	2	Clique em Aplicar .
Para importar itens do submenu de um arquivo XML	1	No painel esquerdo, clique com o botão direito do mouse no submenu no qual você quer importar itens de menu e clique em Importar submenu .
	2	Na caixa de diálogo Escolha o arquivo XML para importar , selecione o arquivo XML apropriado e clique em Abrir .
	3	Clique em Aplicar .
Para exportar um submenu para um arquivo XML	1	No painel esquerdo, clique com o botão direito do mouse no submenu que você quer exportar e clique em Exportar...
	2	Na caixa de diálogo Arquivo de destino para o XML exportado , especifique o nome e o local do arquivo XML e clique em Salvar .
Para importar o menu inteiro do console de um arquivo XML	1	No painel esquerdo, na barra de ferramentas, clique no ícone de Importar todo o menu .
	2	Na caixa de diálogo Escolha o arquivo XML para importar , selecione o arquivo XML apropriado e clique em Abrir .

Para adicionar ações definidas pelo usuário ao menu contextual

O menu contextual do console (“clique com o botão direito do mouse”) contém as opções do menu relevantes para a pasta ou item em que você clicou. Um conjunto padrão de opções de menu de clique com o botão direito do mouse é fornecido com o Notification Server e as soluções instaladas podem adicionar mais opções.

A maioria das opções do conjunto padrão é função comum que está disponível para a maior parte das pastas e itens.

Você pode criar ações definidas pelo usuário e disponibilizá-las no menu contextual. A ação pode ser um dos seguintes itens:

- Abra um URL e substitua detalhes dos recursos selecionados no URL. Por exemplo, o nome dos recursos.
- Execute uma linha de comando no computador do Notification Server ou no computador no qual o navegador está em execução.

Nota: Cada usuário que desejar executar ações do clique com o botão direito da linha de comando em um computador precisa ter o certificado SSL apropriado instalado no computador. Você pode fazer o download do certificado SSL que você precisa na página **Certificado de ação do clique com o botão direito da linha de comando**.

Você pode especificar os recursos a que a ação se aplica selecionando o tipo de recursos e (opcionalmente) filtrando os recursos em uma pesquisa. Quando você clica com o botão direito do mouse em um recurso do tipo apropriado que atenda à consulta de filtro (se um filtro foi especificado), o menu contextual que aparece incluirá a ação definida pelo usuário.

Você precisa que o privilégio da nova ação do clique com o botão direito possa adicionar uma ação definida pelo usuário ao menu contextual.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Para adicionar uma ação definida pelo usuário ao menu contextual

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Console > Ações de clique com o botão direito**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta em que você deseja adicionar a ação e , em seguida, clique em **Novo(a) > Ação do clique com o botão direito**.
- 3 Na página **Nova ação de clique com o botão direito do mouse**, especifique o nome e a descrição apropriados.
- 4 Configure a ação que você deseja fazendo as configurações apropriadas:

Ativar

A ação deve ser ativada para ser incluída no menu contextual. A nova ação está desativada por padrão, o que permite configurar e testar a ação antes de disponibilizá-la aos usuários do console.

Tipo de recurso	O tipo do recurso ao qual a ação se aplica. Por padrão, todos os recursos do tipo especificado estão incluídos. Se deseja aplicar a ação a um subconjunto específico de recursos, você pode filtrar os recursos com uma expressão de consulta apropriada.
Tipo da ação	Na lista suspensa, selecione o tipo de ação apropriada: ■ URL Na caixa URL base, especifique o URL apropriado. O URL pode ser a outra página no Console de gerenciamento Symantec, uma intranet externa ou um site da Internet. ■ Linha de comando Na caixa Linha de comando, especifique a linha de comando apropriada. Marque a caixa de seleção Executar no servidor para executar a linha de comando do servidor. Se você deixar esta caixa de seleção desmarcada, a linha de comando será executada no computador em que a ação é chamada.
Parâmetros de substituição	Os parâmetros da substituição permitem usar uma variável na linha de comando ou URL e tem o valor substituído pelo o valor apropriado no tempo de execução. Por exemplo, o nome do recurso, o endereço IP ou o GUID. Para cada parâmetro de substituição que você deseja incluir: 1 Clique em Adicionar. 2 Na janela Selecionar atributos, selecione o atributo que você deseja usar como um parâmetro e clique em OK. 3 Em Nome do parâmetro, digite o nome apropriado para o parâmetro.

5 Clique em **Aplicar**.

Consulte [“Para personalizar o Console de gerenciamento Symantec”](#) na página 51.

Para criar e modificar exibições

O Notification Server e as soluções incluem exibições predefinidas que você pode modificar e ampliar conforme a necessidade. Você também pode criar e modificar suas próprias exibições.

Consulte [“Sobre as exibições do console”](#) na página 35.

Para criar ou modificar uma exibição

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Console > Exibições**.
- 2 No painel esquerdo, na pasta **Exibições**, execute um destes procedimentos:

Para criar uma nova exibição Clique com o botão direito do mouse na pasta a que você deseja adicionar a exibição e selecione **Novo(a) > Exibição**.

Para modificar uma exibição existente Clique com o botão direito do mouse na exibição que você deseja modificar e selecione **Editar exibição**.

- 3 Na página **Editar exibição**, especifique os detalhes apropriados nos seguintes campos:

Nome	O nome de exibição.
Descrição	Uma descrição da exibição.
Exibir página do portal	Permite selecionar uma página do portal para associar-se à pasta-raiz da exibição. Quando a pasta-raiz é selecionada no painel esquerdo, a página do portal especificada é exibida no painel de conteúdo.
Conteúdo desta exibição	Exibe a estrutura da exibição que você está criando e permite criar novas pastas e excluir os itens que você não deseja.. O conteúdo é classificado alfabeticamente, com as pastas na parte superior, seguidas pelos itens. Não é possível modificar a estrutura.
Itens disponíveis	Exibe a estrutura de árvore do Console de gerenciamento Symantec e permite selecionar as pastas e os itens que você deseja incluir na exibição.

Para adicionar um item à exibição:

- 1 Na lista suspensa **Árvore**, selecione a árvore da qual você deseja selecionar itens.
- 2 Expanda a árvore e selecione a pasta ou o item que você deseja adicionar à exibição.
- 3 Clique em **Adicionar**.

- 4 Clique em **OK**.

Para adicionar novos itens diretamente a uma exibição

Você pode adicionar novas pastas, links de item e da Web diretamente a uma exibição. Você também pode adicionar novas exibições para criar uma hierarquia de exibições.

Consulte [“Sobre as exibições do console”](#) na página 35.

Para adicionar um novo componente diretamente a uma exibição

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Console > Exibições**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta para a qual você deseja adicionar a nova pasta ou item e selecione a opção apropriada:

Nova > Pasta Na caixa de diálogo **Nova pasta**, digite o novo nome da pasta e clique em **Aplicar**.

Novo(a) > Link do item Na janela **Editar link do item**, selecione o item para o qual você deseja criar um link do item e clique em **OK**.

Novo(a) > Link da Web Na caixa de diálogo **Configuração do link da Web** especifique o URL da página da Web ao qual você deseja vincular.

Opcionalmente, você pode especificar o seguinte:

- URL da imagem do ícone
Se desejar usar um ícone na exibição em árvore, especifique o URL para o arquivo de imagem apropriado.
- Frame de destino
O padrão é rightPane, que é a principal área de conteúdo, normalmente conhecida como o painel direito.

Clique em **Aplicar**.

Nova > Exibição Na janela **Editar exibição**, crie a exibição apropriada.

Consulte [“Para criar e modificar exibições”](#) na página 55.

Para criar e modificar páginas do portal

Uma página do portal é uma página do Console de gerenciamento Symantec que pode ser personalizada para se adaptar às suas necessidades. Você pode usar uma página do portal para consolidar as informações-chave em uma única página de fácil exibição. Uma página do portal pode exibir o status do Symantec Management Platform e dos computadores gerenciados ou quaisquer outras informações que você queira disponibilizar. Por exemplo, você pode incluir páginas

externas da Web, páginas da intranet, RSS feeds ou seus próprios aplicativos. Isto é mais conveniente do que exibir várias páginas diferentes do console para coletar as informações que você deseja.

Consulte [“Para personalizar o Console de gerenciamento Symantec”](#) na página 51.

A maioria das páginas do portal está disponível a todos os usuários do console. A exceção é a página Meu portal, que é uma página do portal especial e exclusiva para cada usuário.

Consulte [“ Para acessar a página Meu portal”](#) na página 49.

Nota: Para exibir uma página do portal, você precisa ter permissão de leitura na página do portal.

As páginas do portal são construídas com base nas Web parts. Você pode criar e personalizar Web parts de acordo com seus requisitos e adicioná-las às suas páginas do portal.

Os tipos de Web parts são os seguintes:

Relatório	Exibe as informações recuperadas de um relatório.
URL	Um link para outra página da Web (como uma página em sua intranet corporativa ou um site externo).

As páginas do portal podem ter até três colunas. As Web parts podem ser exibidas em uma página do portal em três tamanhos diferentes, dependendo de qual coluna forem colocadas ou se forem divididas em todas as colunas. As colunas da esquerda e do meio tem a mesma largura (as Web parts nelas são "pequenas") e a coluna direita é mais larga (as Web parts aqui são "grandes"). Como alternativa, uma Web part pode usar a largura da página inteira (a Web part tem "várias colunas"). Estas Web parts com várias colunas são mostradas na parte superior ou na parte inferior da página do portal. Quando você projetar uma Web part nova, você precisará garantir que ela seja exibida apropriadamente em qualquer tamanho. Você não pode definir um tamanho específico como uma propriedade da Web part.

Você pode recolher uma Web part clicando na seta no topo à direita e expandi-la clicando na seta novamente. Isto permite incluir Web parts lentas durante o carregamento ou que são raramente usadas em uma página do portal.

As páginas do portal têm os dois modos de operação seguintes:

Exibição	A página do portal é somente leitura. Você pode exibir todas as Web parts, mas não pode fazer nenhuma alteração. Algumas páginas do portal que são fornecidas por soluções da Symantec podem ser restritas ao modo de exibição para impedir que qualquer um modifique o conteúdo.
Editar	Se você tiver permissão de gravação na página do portal, poderá editá-la. Você pode adicionar, remover, redimensionar e solicitar novamente as Web parts em uma página do portal. A árvore de Web parts é exibida à esquerda da página, permitindo que você arraste e solte as Web parts nos locais apropriados. Para remover uma Web part de uma página do portal, clique no símbolo X no canto superior direito da Web part.

Consulte [“Para criar e modificar Web parts”](#) na página 60.

Para criar ou modificar uma página do portal

- No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Console > Páginas do portal**.
- Execute um destes procedimentos:

Para criar uma página do portal nova	No painel esquerdo, clique com o botão direito do mouse na pasta Páginas do portal e selecione Novo(a) > Página do portal .
Para modificar uma página do portal existente	No painel esquerdo, na pasta Páginas do portal , selecione a página que você deseja editar. No canto superior direito da página do portal, clique em Editar .
- Na página **Configuração da página do portal** especifique o nome e a descrição da página e selecione as Web parts que você deseja usar na página do portal.

Nome	O nome da página do portal.
Descrição	Uma descrição da página do portal.
Painel Web parts	Este painel contém a lista de Web parts disponíveis que você pode adicionar à página do portal. Para adicionar uma Web part: - Selecione a Web part e clique em Adicionar. - Na página do portal, clique na Web part e a arraste até o local apropriado na página.

- 4 Se desejar remover uma Web part da página, no frame apropriado da Web part, clique no símbolo de **Excluir** no canto superior direito.
- 5 Clique em **Aplicar**.

Para criar e modificar Web parts

As Web parts são minipáginas da Web que você pode usar como blocos de construção para páginas do portal. Uma Web part pode exibir um relatório ou o conteúdo de uma página da Web. O console é fornecido com um conjunto de Web parts predefinidas que você pode usar para criar suas páginas do portal. Você pode modificar estas Web parts e criar novas.

Consulte [“Para criar e modificar páginas do portal”](#) na página 57.

Você também pode criar uma Web part de relatórios diretamente de um relatório.

Consulte [“Para salvar os resultados do relatório do Notification Server como uma Web part”](#) na página 449.

Para criar ou modificar uma Web part

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Console > Web parts**.
- 2 Execute um destes procedimentos:

Para criar uma nova Web part No painel esquerdo, expanda a pasta **Web parts** e clique com o botão direito do mouse na pasta para a qual você deseja adicionar a nova Web part.

Clique em **Nova > Web part**.

Para modificar uma Web part existente No painel esquerdo, expanda a pasta Web parts e selecione a Web part que você deseja modificar.

- 3 Na página **Configuração da Web part**, especifique os parâmetros da Web part:

Nome O nome da Web part.

Descrição Uma descrição da Web part.

Conteúdo da Web part	O conteúdo da Web part. Você pode escolher um dos seguintes itens: ■ Resultados do relatório Se você escolher essa opção, precisará selecionar o relatório apropriado. O relatório é executado quando você abre uma página do portal que contém a Web part; assim, os resultados são sempre atualizados. ■ Mostrar URL Se você escolher essa opção, especifique o URL apropriado.
Altura fixa	Selecione essa opção para especificar uma altura fixa para a Web part e digite a altura (em pixels) na caixa de diálogo adjacente. Se essa opção não for selecionada, a Web part será redimensionada de acordo com o conteúdo que exibir.
Tamanho padrão	O tamanho padrão da Web part: ■ Pequeno ■ Grande ■ Com várias colunas Quando a Web part for adicionada a uma página do portal, seu local padrão será determinado por seu tamanho padrão. Se você mover a Web part para outro local, ela será redimensionada automaticamente.
- 4 Se deseja cancelar as alterações sem salvar qualquer coisa, clique em **Cancelar**.
 - 5 Clique em **Salvar alterações**.
 - 6 Se deseja visualizar a Web part que você especificou, clique em **Mostrar visualização**.

Para salvar elementos do console como arquivos XML

Você pode salvar elementos do console (itens de menu, exibições, páginas do portal ou Web parts) como arquivos XML. Talvez você queira fazer isso para criar arquivos de backup antes de personalizar o console. Você também poderia fazer isso para criar arquivos XML que pode personalizar e importar como elementos personalizados do console para outros Notification Servers.

Consulte [“Para personalizar o Console de gerenciamento Symantec”](#) na página 51.

Para restaurar elementos do console, importe-os dos arquivos XML apropriados. Os elementos do console são identificados por suas GUIDs. Os elementos no arquivo XML importado sobrescrevem os elementos existentes que têm GUIDs correspondentes. Todos os elementos no XML que não têm GUIDs correspondentes no console são adicionados como itens novos.

Nota: Você precisa ter privilégios Importar XML para poder importar arquivos XML. Por padrão, somente a função Administrador Symantec tem este privilégio.

Para salvar um elemento do console como um arquivo XML

- 1 No Symantec Management Console, no painel esquerdo, clique no nó da árvore que você quer salvar.
- 2 Clique com o botão direito do mouse e clique em **Exportar**.
- 3 Na caixa de diálogo **Arquivo de destino para o XML exportado**, especifique o nome e o local do arquivo XML e clique em **Salvar**.

Para restaurar um elemento do console de um arquivo XML

- 1 No Symantec Management Console, no painel esquerdo, selecione a pasta na qual você quer restaurar o elemento.
- 2 Clique com o botão direito do mouse e clique em **Importar**.
- 3 Na caixa de diálogo **Escolha o arquivo XML para importar**, selecione o arquivo XML apropriado.
- 4 Se deseja impedir quaisquer alterações ao elemento importado, selecione **Abrir como somente leitura**.
- 5 Clique em **Abrir**.

Para configurar os servidores do Symantec Management Platform

- [Capítulo 3. Para configurar o Notification Server](#)
- [Capítulo 4. Para configurar a segurança](#)
- [Capítulo 5. Para configurar agendas](#)
- [Capítulo 6. Para configurar sites e servidores de sites](#)
- [Capítulo 7. Para configurar o servidor de pacotes para Linux](#)
- [Capítulo 8. Para configurar a hierarquia](#)
- [Capítulo 9. Para configurar a replicação](#)
- [Capítulo 10. Para executar uma configuração de primeira instalação](#)

Para configurar o Notification Server

Este capítulo contém os tópicos a seguir:

- [Sobre o Notification Server](#)
- [Sobre como configurar o Notification Server](#)
- [Para definir configurações do Notification Server](#)
- [Como definir as configurações do Notification Server com o configurador do NS](#)
- [Para configurar o banco de dados de gerenciamento de configuração](#)
- [Para limpar o banco de dados de gerenciamento de configuração](#)
- [Como salvar o histórico de dados de recursos no CMDB](#)

Sobre o Notification Server

O Notification Server é o componente do servidor primário no Symantec Management Platform. O Notification Server coordena várias soluções e fornece a principal interface do usuário, administração com base em políticas, geração de relatórios e notificações. O Notification Server hospeda o console de gerenciamento com base na Web que permite gerenciar os componentes do Symantec Management Platform.

Consulte [“Componentes do Symantec Management Platform”](#) na página 28.

Consulte [“Sobre como configurar o Notification Server”](#) na página 65.

O Notification Server é responsável pelo gerenciamento de tarefas e políticas predefinidas que estão disponíveis em cada solução instalada. Estas políticas e

tarefas ativam os componentes do Notification Server que processam diversas funções.

As funções do Notification Server incluem o seguinte:

- Descoberta de recursos na rede
- Instalação e configuração do agente de gerenciamento nos endpoints
- Coleta de informações relatadas pelo cliente e armazenamento no CMDB
- Geração de relatórios da Web detalhados
- Envio de informações da política para os endpoints
- Distribuição de pacotes de software

Sobre como configurar o Notification Server

As configurações padrão do Notification Server são apropriadas para a maioria das finalidades e você não precisa normalmente alterá-las. Estas configurações padrão serão especificadas quando você instalar o Symantec Management Platform. Porém, conforme as necessidades de sua organização mudam, você pode fazer as alterações de configuração apropriadas.

Consulte [“Sobre o Notification Server”](#) na página 64.

Tabela 3-1 Tipos de configurações

Configuração	Descrição
Defina as configurações do Configuration Management Database (CMDB).	Consulte “Para configurar o banco de dados de gerenciamento de configuração” na página 76.
Defina a limpeza do banco de dados.	Consulte “Para limpar o banco de dados de gerenciamento de configuração” na página 79.
Configure a retenção do histórico de dados dos recursos.	Consulte “Como salvar o histórico de dados de recursos no CMDB” na página 81.
Definir as configurações do Notification Server Estas configurações incluem o processamento de evento, o registro em log da mensagem de status, os endereços do servidor da mensagem de e-mail e padrão e um servidor proxy.	Consulte “Para definir configurações do Notification Server” na página 66.

Configuração	Descrição
Defina as configurações do Notification Server que não aparecem no Symantec Management Console.	Consulte “Como definir as configurações do Notification Server com o configurador do NS” na página 75.
Especifique as credenciais do ponto de distribuição de pacotes de entrega de software.	Consulte “Configurações da credencial de ponto de distribuição” na página 74.

Para definir configurações do Notification Server

As configurações do Notification Server que você pode definir incluem processamento de eventos, registro em log da mensagem de status, servidor de mensagens de e-mail e endereços padrão.

Consulte [“Sobre como configurar o Notification Server”](#) na página 65.

Você também pode definir outras configurações do Notification Server com o configurador do NS

Consulte [“Como definir as configurações do Notification Server com o configurador do NS”](#) na página 75.

Para definir as configurações do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, na pasta **Configurações**, expanda **Notification Server** e clique em **Configurações do Notification Server**.

- 3 Na página **Configurações do Notification Server**, faça as mudanças apropriadas nas seguintes guias:

Processamento	Você pode ativar ou desativar o processamento de eventos do Notification Server (NSE, Notification Server Event), especificar a identidade do aplicativo do Notification Server e reiniciar serviços do Notification Server manualmente. Consulte “Configurações de processamento do Notification Server” na página 67.
E-mail	Você pode especificar o servidor de e-mail usado pelo Notification Server e definir os endereços de e-mail padrão Para e De. Consulte “Configurações do servidor de e-mail e do endereço” na página 71.
Log	Você pode especificar os tipos de mensagens de status, como erros do Notification Server, avisos e mensagens de informações, que você deseja que sejam registrados em log pelo Notification Server. Consulte “Configurações de registro em log da mensagem de status” na página 72.
Proxy	Se não desejar permitir que os usuários do Notification Server tenham acesso direto à rede, você poderá configurar um servidor proxy. Consulte “Configurações do servidor proxy” na página 73.
Credencial de ponto de distribuição	Você pode especificar as credenciais que o Notification Server usará para acessar os pontos de distribuição de pacotes. Consulte “Configurações da credencial de ponto de distribuição” na página 74.

- 4 Clique em **OK**.

Configurações de processamento do Notification Server

Na guia **Processamento**, você pode ativar ou desativar o processamento do evento do Notification Server (NSE) e especificar a identidade do aplicativo do Notification Server. Um NSE é um arquivo XML transferido entre o Notification Server e o Symantec Management Agent (incluindo os plug-ins da solução).

Nesta guia, você pode também configurar a comunicação do agente legado.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Tabela 3-2 Opções na guia **Processamento**

Opção	Descrição
Processamento do servidor	O processamento do servidor será ativado por padrão quando você instalar o Notification Server, mas poderá haver ocasiões em que será necessário desativá-lo ou reativá-lo. Por exemplo, quando você instala uma solução, todo o processamento de eventos é pausado automaticamente. Depois que a instalação for concluída, o processamento de eventos deve ser reiniciado automaticamente. Se isso não acontecer, uma mensagem de aviso aparecerá no Console de gerenciamento Symantec e você será alertado a reativar o processamento do NSE (Notification Server Event) manualmente. Para reativar o processamento do NSE, clique na mensagem de aviso e, na caixa de diálogo que aparecer, clique em Reiniciar. OS NSEs recebidos enquanto o processamento do NSE estiver desativado serão armazenados no computador do Notification Server e gerenciados depois que o processamento do NSE estiver ativado novamente. Os NSEs contêm informações como: ■ Comunicação com o Symantec Management Agent ■ Processamento de eventos ■ Inventário básico ou completo ■ Sucesso ou falha do download do pacote

Opção	Descrição
Identidade do aplicativo	

Opção	Descrição
	A identidade do aplicativo do Notification Server é a conta na qual o Notification Server é executado. Especifique o nome do usuário e a senha apropriados quando instalar o Notification Server e você precisará somente atualizá-los quando necessário. Por exemplo, se sua organização tem uma política de alteração de senha, as credenciais de acesso do CMDB podem ser forçadas a mudar. A identidade do aplicativo não tem mais permissão para acessar o servidor SQL. Aviso: Não é possível usar caracteres especiais no nome do usuário ou na senha da identidade do aplicativo. Use apenas caracteres alfanuméricos. O ID do usuário que você define requer as seguintes permissões: ■ As permissões locais de administrador no Notification Server e em alguns computadores remotos Windows 2000 /XP/2003/Vista que você quiser instalar o Symantec Management Agent. ■ Permissão para atuar como parte do sistema operacional e fazer logon como um trabalho de lotes e um serviço. ■ Permissão para fazer logon no servidor SQL. Se o ID do usuário não tiver essa permissão, você poderá especificar um nome do usuário e uma senha diferentes para fazer logon no CMDB. ■ Permissão para conectar a algum servidor SQL no qual o Notification Server pode se ligar. Por exemplo, um banco de dados de SMS do Administrador da Web para SMS ou banco de dados de concessão para o Contract Management Solution. Os serviços do Notification Server serão reiniciados automaticamente quando a identidade do aplicativo for alterada. Porém, a opção Reiniciar serviços permite reiniciar manualmente os serviços quando necessário. Por exemplo, se você faz uma mudança no banco de dados, você precisa reiniciar os serviços para que as alterações sejam aplicadas. Se a senha da identidade do aplicativo falhar, o Notification Server não poderá acessar o CMDB. Você não pode redefinir a identidade do aplicativo pelo Console de gerenciamento Symantec, porque o console usa a mesma senha para acessar o Notification Server. Você precisa usar o utilitário ASConfig para acessar diretamente os serviços da Web e

Opção	Descrição
	redefinir a senha de identidade do aplicativo usando a linha de comando apropriada.
Comunicação do agente legado	Permite controlar se os endpoints que usam versões mais antigas do Symantec Management Agent podem se comunicar com o Notification Server com upgrade. Se o modo Comunicação do agente legado (LAC, Legacy Agent Communication) estiver desativado, você poderá gerenciar ativamente somente os agentes com upgrade. Se o modo LAC estiver ativado, você poderá executar um conjunto limitado de funções de gerenciamento nos agentes legados. Consulte “Sobre a comunicação do agente legado” na página 272.

Configurações do servidor de e-mail e do endereço

Você pode definir um servidor de e-mail e os endereços de e-mail Para e De das mensagens de e-mail do Notification Server. O Notification Server usa SMTP para enviar mensagens de e-mail. O endereço de e-mail pode ser qualquer endereço válido do SMTP que seu servidor SMTP reconhecer.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Você pode ativar as soluções da Symantec para que lhe enviem mensagens de e-mail com base nos dados recebidos pelo Notification Server. O endereço de e-mail que você especificar pode receber avisos sobre relatórios executados com êxito, ações de automação executadas e sobre verificações da escalabilidade do sistema. Estes e-mails ajudam a monitorar e gerenciar suas atividades do Notification Server.

As configurações de e-mail são definidas quando você instala o Notification Server e, normalmente, não é preciso modificá-las. Porém, se o servidor SMTP for modificado, ou se você desejar que outra pessoa receba as mensagens de e-mail, será necessário fazer as mudanças apropriadas.

A opção **Enviar e-mail de teste** permite testar o servidor de e-mail e as configurações de endereço enviando uma mensagem com as configurações atuais. É necessário confirmar as mudanças clicando em OK antes de enviar o e-mail de teste.

Configurações de registro em log da mensagem de status

É possível especificar os tipos de mensagens de status, tais como erros, avisos e mensagens de informações do Notification Server, que você deseja que o Notification Server registre em log. Por padrão, as mensagens de log geradas pelo Notification Server são gravadas nos arquivos de log no diretório `...\Arquivos de programas\Altiris\Notification Server\Logs`.

Nota: Quando você fizer o upgrade do Notification Server 6.x para o 7.x, o Assistente de Migração gravará todas as mensagens no local do arquivo de log do 6.x em vez de gravá-las no local do arquivo de log do 7.0. O local do arquivo de log do 6.x é `...\Arquivos de programas\Altiris\Notification Server\Logs`. Você precisa verificar este arquivo de log para ver todos os erros de migração. O Visualizador de logs exibe apenas os logs que são arquivados no local padrão do 7.0. As entradas do log de migração não são incluídas.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Você pode registrar alguns dos seguintes tipos de mensagem:

- Erros
- Avisos
- Informações
- Rastreo
- Detalhado

Você também pode armazenar arquivos de log anteriores a um período específico. Se você definir esta opção, os arquivos de log relevantes serão arquivados diariamente às 5:00.

Consulte [“Para abrir o Visualizador de logs”](#) na página 72.

Para abrir o Visualizador de logs

O Visualizador de logs permite monitorar diversos locais de logs para diferentes componentes, como o IT Management Suite, o Symantec Management Agent e o Symantec Installation Manager. O Visualizador de logs detectará automaticamente se o componente estiver instalado em um local personalizado e monitorará o caminho personalizado. O Visualizador de logs relaciona os eventos, erros e avisos em tempo real que ocorrem ao executar qualquer ação. Estas mensagens ajudam a monitorar e solucionar problemas no Notification Server.

Você pode usar o Visualizador de logs para determinar os problemas e suas causas. Depois de identificar erros ou avisos no Visualizador de logs, você poderá usar as

mensagens de erro para pesquisar na Base de conhecimento da Symantec artigos que possam ajudá-lo a corrigir o erro. Também é possível levar o problema à equipe de suporte técnico.

O Visualizador de logs permite executar as seguintes tarefas:

- Exibir mensagens informativas, de erro, de aviso, de rastreamento e de detalhamento.
- Pesquise os logs e exiba os resultados.
- Marque os itens do log.
- Filtrar os logs para exibir um subconjunto de mensagens.
- Salvar as definições do filtro para uso posterior.
- Execute a pesquisa nos arquivos de log sem carregá-los no Visualizador de logs.

Consulte [“Configurações de registro em log da mensagem de status”](#) na página 72.

A release 7.5 do IT Management Suite introduz um novo Visualizador de logs com usabilidade e funcionalidades aprimoradas. Note que você pode também usar o antigo Visualizador de logs Altiris que foi mantido no produto para fins de compatibilidade, chamado agora de Visualizador de logs legado.

Para abrir o novo Visualizador de logs

- ◆ No computador do Notification Server, clique em **Iniciar** e depois em **Todos os programas > Symantec > Diagnóstico > Visualizador de logs Altiris**.

Para abrir o Visualizador de logs legado

- ◆ No computador do Notification Server, clique em **Iniciar** e depois em **Todos os programas > Symantec > Diagnóstico > Ferramentas legadas > Visualizador de logs Altiris legado**.

Configurações do servidor proxy

Se não deseja que os usuários do Notification Server tenham acesso direto à rede, você pode configurar um servidor proxy. Por exemplo, se você tiver o Notification Server e seus computadores gerenciados dentro do firewall de sua organização, um servidor proxy fornecerá a segurança. Você pode configurar um servidor proxy para fornecer uma maneira segura por meio do firewall sem expor o Notification Server. Essa configuração ajuda o Notification Server a obter patches ou fazer o download de soluções de sites externos com segurança.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Usar um servidor proxy pode aprimorar o desempenho do Notification Server usando menos largura de banda e filtrando solicitações ao requerer arquivos da Internet. Um exemplo são os dados de PMImport.

A opção **Testar configurações** valida as configurações do servidor proxy tentando conectar-se a um site externo.

Se forem exibidas mensagens de erro quando você testar as configurações, assegure-se de que suas credenciais de autenticação estejam corretas. Assegure-se de que seu servidor proxy esteja em execução e de que não haja nenhum erro geral de rede.

Configurações da credencial de ponto de distribuição

Você pode especificar as credenciais de ponto de distribuição (DPC) usadas pelo Notification Server para acessar pacotes de entrega de software. Esses pacotes estão localizados em um compartilhamento de rede que é acessado através de um caminho UNC. O Notification Server publica esses pacotes em um diretório HTTP virtual que usa o DPC para se conectar ao compartilhamento UNC.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Especifique as credenciais de ponto de distribuição antes de criar um pacote de software que será acessado de um caminho UNC existente. As credenciais devem ter permissão para validar contas do usuário e ter permissão de leitura em todos os arquivos nos pontos de distribuição remotos.

O Notification Server pode usar qualquer uma das seguintes credenciais:

Credencial de conectividade do agente	Todos os Symantec Management Agents usam a Credencial de conectividade do agente (CCA) para se conectar a recursos protegidos. A CCA é definida na política de configurações globais de agentes.
Credenciais especificadas pelo usuário	Se os pacotes estiverem armazenados em um local que não é acessível com a Credencial de conectividade do agente, será possível torná-los acessíveis. Para tornar os pacotes acessíveis especifique o nome de usuário e a senha de uma conta que tem o acesso apropriado. Não é possível usar caracteres especiais no nome do usuário ou na senha. Use apenas caracteres alfanuméricos.

Como definir as configurações do Notification Server com o configurador do NS

O configurador do NS é uma ferramenta de configuração que permite alterar a maioria das principais configurações do Notification Server. Estas configurações incluem muitas que não são acessíveis do Console de gerenciamento Symantec. Você apenas deverá usar o configurador do NS para alterar estas configurações se souber qual efeito cada configuração terá no sistema.

Consulte [“Sobre como configurar o Notification Server”](#) na página 65.

Quando um usuário iniciar o configurador do NS, uma verificação de segurança será executada para determinar se ele tem permissão para exibir ou modificar as configurações do Notification Server. Se um usuário não tiver permissão, uma mensagem de aviso será exibida e a ferramenta será fechada.

Para definir as configurações do Notification Server com o configurador do NS

- 1 Para iniciar o configurador do NS, execute o arquivo NSConfigurator.exe.
Este arquivo está em Arquivos de programas\Altiris\Notification Server\Bin\Tools. Quando você executar esta ferramenta, será aberto o arquivo CoreSettings.config que está em Arquivos de programas\Altiris\Notification Server\Config.
- 2 Execute um destes procedimentos para encontrar a configuração que deseja alterar:
 - Na árvore de navegação no painel esquerdo, localize a configuração.
 - No campo de pesquisa, no canto direito superior, digite seu texto e clique em **Pesquisar**. Na lista de resultados da pesquisa, clique no link **Mostrar** para essa configuração.
- 3 No painel direito, altere a configuração e clique em **Salvar**.
Se você digitar um valor inválido para uma configuração, uma mensagem de erro aparecerá. Você apenas poderá salvar suas alterações se digitar um valor válido.
- 4 Para restaurar o valor padrão, clique em **Restaurar padrão**.
A opção **Restaurar padrão** aparecerá apenas se a configuração tiver um valor padrão.

Para configurar o banco de dados de gerenciamento de configuração

O Notification Server tem um banco de dados, denominado Configuration Management Database (CMDB). Tanto o Notification Server como as soluções usam o CMDB para armazenar itens de configuração e dados de recursos.

O processamento de banco de dados é um dos maiores consumidores de recursos no Symantec Management Platform. O número de soluções instaladas em seu ambiente e o modo como são usadas têm influência sobre os requisitos do banco de dados. O número de computadores gerenciados que relatam a cada computador do Notification Server também influencia os requisitos do banco de dados.

Cada computador do Notification Server pode ser configurado para usar um banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database) local ou remoto. Um computador do Notification Server com um banco de dados local exige mais recursos do que um computador do Notification Server com uma configuração de banco de dados remoto.

Você pode usar as seguintes configurações para o CMDB:

Configuração de CMDB local	Em uma configuração de servidor de CMDB local, você instala o CMDB no mesmo computador que o Notification Server. Esta configuração é aceitável para os ambientes que têm de 1.000 a 5.000 endpoints. Nestes ambientes, há disputa mínima de recursos entre serviços do Notification Server e os serviços do CMDB.

Configuração de CMDB remoto	Em uma configuração de CMDB remoto, você instala o CMDB em um computador diferente do computador do Notification Server. Esta configuração é recomendada para a maioria dos ambientes. Nesta configuração, a carga de trabalho do CMDB é descarregada do computador do Notification Server. O servidor do CMDB e o computador do Notification Server devem ter uma conexão de rede de alta velocidade entre eles. A Symantec recomenda Ethernet de 1 GB.

Você pode fazer todas as alterações necessárias às configurações do CMDB. Quando o Notification Server é instalado, o CMDB é configurado como parte do processo de instalação. Você não precisa normalmente fazer mais alterações.

Porém, poderá haver ocasiões quando será necessário alterar as configurações do CMDB. Por exemplo, se você fizer um upgrade do hardware no qual o Microsoft SQL Server é executado ou se você for instruído a fazer isso pelo suporte da Symantec.

Para configurar o Configuration Management Database

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Notification Server > Configurações do banco de dados**.

- 2 Na página **Configurações do banco de dados**, na guia **Geral** e na guia **Relatórios**, faça as mudanças de configuração apropriadas.

Nome do servidor de banco de dados	O nome do servidor SQL que contém o CMDB. Use o formato <i>nome_do_servidor\nome_da_instância</i>. Por exemplo, SydNS\sql_cp1_cs_as.
Credenciais do banco de dados	O nome do usuário e a senha que são necessários para acessar o CMDB. Você pode usar as credenciais do aplicativo do Notification Server para a autenticação do Windows. Convém usar este método para evitar ser afetado por qualquer política de alteração da senha que for aplicada em sua organização. As credenciais do aplicativo são especificadas na guia Processamento, da página Configurações do servidor Consulte “Configurações de processamento do Notification Server” na página 67. Você também tem a opção de usar a autenticação do SQL. Você pode especificar o nome de usuário e a senha apropriados de login do SQL para usar a autenticação do SQL. Nota: Se desejar alternar a autenticação do banco de dados com o SQL, será necessário fazer esta alteração em ambas as guias (Geral e Relatórios). A guia Geral é a guia padrão que aparecerá quando você abrir a página Configurações do banco de dados. Se você fizer a mudança apenas na guia Geral, o Notification Server não estará funcionando completamente e poderá haver erros com algumas operações.
Nome do banco de dados	Você pode selecionar um banco de dados existente na lista dos bancos de dados disponíveis ou criar um novo banco de dados. Se você selecionar um banco de dados existente, certifique-se de que seja a mesma versão que o Notification Server.
Reparar banco de dados	Permite reparar o CMDB. Talvez seja necessário fazer este procedimento ao restaurar o Notification Server de um backup para um computador novo.

Tempo limite de comando

Especifique o período de tempo no qual o Notification Server tentará processar uma consulta, como executar um relatório ou atualizar um filtro.

Convém alterar este valor por razões de desempenho, como uma carga elevada no servidor SQL que faz com que as consultas atinjam o tempo limite.

A Symantec recomenda definir o valor do tempo limite do ASP Script no Microsoft IIS como um valor igual ou superior ao valor de **Tempo limite de comando**. Consulte o administrador do banco de dados antes de fazer qualquer alteração.

Credenciais do relatório público

O contexto de segurança a ser usado para executar consultas do relatório no CMDB.

Essas credenciais fornecem menos segurança do que as credenciais do banco de dados (que são para o administrador do banco de dados). Essas credenciais são usadas para acessar o banco de dados e para executar a consulta SQL apropriada quando um usuário executa um relatório.

3 Clique em **Salvar alterações**.

Consulte [“Sobre como configurar o Notification Server”](#) na página 65.

Para limpar o banco de dados de gerenciamento de configuração

Para gerenciar o tamanho do banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database), é possível especificar por quanto tempo determinados tipos de dados são armazenados. Você pode especificar o comprimento do armazenamento para dados como relatórios, computadores gerenciados e dados de evento. Por exemplo, se houver baixo desempenho ao executar relatórios, tente limpar os eventos ou configurar as opções de limpeza de eventos para que menos dados sejam salvos.

Consulte [“Para configurar o banco de dados de gerenciamento de configuração”](#) na página 76.

Os dados que podem ser apagados do CMDB são:

- Capturas de imagem de relatório
Capturas de imagem anteriores a um período de tempo especificado podem ser excluídas.

- Os computadores gerenciados que não se comunicaram com o Notification Server por um período de tempo maior que o especificado Estes podem ser excluídos ou definidos como desativados. O CMDDB é atualizado quando sua agenda de limpeza é executada.
- Dados do evento de recurso
Dados de eventos anteriores a um período de tempo especificado podem ser excluídos. Opcionalmente, é possível especificar um número máximo de linhas para manter. Se a tabela de dados do evento atingir esse tamanho, novas linhas continuarão a ser adicionadas até a próxima atualização agendada. Quando o agendamento da limpeza do CMDDB for executado, a tabela voltará a seu tamanho máximo. A tabela será ajustada removendo as linhas mais antigas, mesmo se os dados mais antigos não tiverem sido retidos pelo tempo especificado.
Você pode ter as mesmas configurações para todas as classes de dados ou definir configurações personalizadas para algumas ou todas as classes de dados. Uma configuração personalizada para uma classe de dados substitui a configuração global. Se nenhuma configuração personalizada é feita para uma classe de dados, a configuração global é usada para aquela classe de dados. A mesma agenda de limpeza do CMDDB é usada em todos os casos.

A agenda de limpeza do CMDDB é uma agenda do Windows que você define ao instalar o Notification Server. Não é possível modificá-lo no Symantec Management Console. Se desejar fazer quaisquer mudanças, você pode fazê-las no Painel de controle do Windows.

Para limpar o Configuration Management Database

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Notification Server > Manutenção da purga**.
- 2 No painel esquerdo, na pasta **Manutenção da purga**, clique em **Manutenção da purga**.

- 3 Na página **Manutenção da purga**, defina as configurações nas seguintes guias:

Manutenção da purga

Permite especificar as configurações de apagamento de relatórios, os dados de registro do agente e as configurações de apagamento de dados do computador.

Note que a opção **Apagar entradas desatualizadas de registro do agente** excluirá somente os itens com status **Bloqueado**.

Para sobrepor o agendamento de apagamento e apagar imediatamente o CMDB, clique em **Purgar agora**.

Configurações da purga de dados do evento de recurso

Permite especificar as configurações de apagamento de dados de eventos de recursos desejadas.

Configurações de limpeza de captura de imagem de dados de relatório

Permite especificar as configurações de apagamento de captura de imagem dos dados.

Para sobrepor o agendamento de apagamento e apagar imediatamente o CMDB, clique em **Purgar agora**.

- 4 Clique em **Salvar alterações**.

Como salvar o histórico de dados de recursos no CMDB

O Notification Server captura os dados de recursos em tempo real enquanto coleta os dados de inventário. Você pode optar por criar um histórico de dados de recursos para cada tipo de recurso e associação de recursos. Para cada histórico, você pode especificar quanto tempo reter os dados de histórico no CMDB.

Consulte [“Para configurar o banco de dados de gerenciamento de configuração”](#) na página 76.

Um histórico de dados de recursos pode incluir dados de algumas das classes de dados. Um histórico da associação de recursos pode incluir dados de quaisquer tipos da associação de recursos.

Para salvar o histórico de dados de recursos no CMDB

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Notification Server > Manutenção da purga**.
- 2 No painel esquerdo, na pasta **Manutenção da purga**, clique em **Histórico de recursos**.

3 Na página **Histórico de recursos**, para cada tipo de classe de dados de recursos e tipo de associação de recursos que você deseja configurar, tome as seguintes medidas nas guias apropriadas:

- Expanda a classe de dados ou o tipo de associação.
- Selecione as classes ou as associações de dados para as quais você deseja criar o histórico de dados de recursos.
- Para cada classe ou associação de dados, especifique o período para o qual você deseja manter o histórico de dados de recursos.
Na lista suspensa correspondente, selecione o período de tempo (Dias, Semanas ou Meses). Digite em seguida o número apropriado de dias, semanas ou meses.

Todos os dados de recursos mais antigos que o período especificado para seu tipo serão excluídos do CMDB na agenda de limpeza.

4 Clique em **Salvar alterações**.

Para configurar a segurança

Este capítulo contém os tópicos a seguir:

- [Sobre a segurança do Symantec Management Platform](#)
- [Para configurar a segurança do Symantec Management Platform](#)
- [Tarefas de gerenciamento de segurança do Symantec Management Platform](#)

Sobre a segurança do Symantec Management Platform

O Symantec Management Platform usa segurança baseada em função; isso significa que o acesso do usuário é baseado na função de segurança do usuário. Uma função de segurança é um conjunto de privilégios e permissões que é concedido a todos os membros da função. A segurança baseada na função permite criar e manter um pequeno número de funções de segurança. Você pode atribuir cada conta do usuário do Symantec Management Platform à função apropriada, em vez de atribuir privilégios e permissões específicos a cada usuário individual. Porém, você também pode atribuir permissões específicas a contas individuais do usuário.

As contas do usuário, que são chamadas, às vezes, de usuários, não são as mesmas que os recursos do usuário no Symantec Management Platform. Um recurso do usuário é uma entidade usada para associar dispositivos gerenciados ao proprietário do dispositivo. Os recursos existentes do usuário e as contas do usuário que podem fazer logon no Console de gerenciamento Symantec ou executar um fluxo de trabalho são entidades separadas.

Uma função de segurança controla o acesso do usuário ao Symantec Management Platform usando o seguinte:

- **Privilégios**
Um privilégio aplica-se a todo o sistema. Os privilégios são atribuídos apenas às funções e não podem ser atribuídos diretamente a contas individuais do usuário. Um privilégio atribuído a uma função permite que uma conta do usuário que seja membro dessa função execute uma ação específica no Symantec Management Platform ou no Console de gerenciamento Symantec. Em alguns casos, a função de usuário exige permissões correspondentes. Consulte [“Categorias de privilégio de segurança”](#) na página 489.
- **Permissões em pastas e itens**
As permissões especificam o acesso que uma função de segurança ou uma conta do usuário têm a uma pasta ou item do Console de gerenciamento Symantec. Uma permissão em uma função de segurança aplica-se a todos os membros dessa função. Uma permissão em uma pasta aplica-se a todos os itens contidos diretamente nessa pasta. Consulte [“Categorias de permissão de segurança”](#) na página 491.
- **Permissões em exibições e grupos organizacionais**
Uma exibição organizacional é um agrupamento hierárquico de recursos (como grupos organizacionais) que reflete uma exibição ou estrutura real de sua organização. Você pode configurar a segurança dos recursos atribuindo as permissões apropriadas para cada função de segurança em cada exibição organizacional. Você também pode atribuir as permissões apropriadas nos grupos organizacionais dentro de cada exibição. Uma permissão atribuída a um grupo organizacional aplica-se a todos os recursos nesse grupo. Por padrão, a permissão aplica-se a todos os seus grupos filho. Você não pode atribuir permissões diretamente a recursos específicos.

Os privilégios, as permissões em pastas e em itens e as permissões em exibições e grupos organizacionais funcionam em conjunto. Você precisa atribuir a combinação apropriada a cada função de segurança para garantir às contas do usuário o acesso necessário para executar suas atividades.

Consulte [“Para configurar a segurança do Symantec Management Platform”](#) na página 84.

Consulte [“Tarefas de gerenciamento de segurança do Symantec Management Platform”](#) na página 108.

Para configurar a segurança do Symantec Management Platform

Para dar acesso às contas do usuário ao Symantec Management Platform, às soluções instaladas e aos dados contidos no CMDB, você precisa configurar as

funções de segurança. Você deverá atribuir os privilégios e as permissões apropriados a cada função. É necessário criar suas contas de usuário do Symantec Management Platform e adicionar cada conta à função apropriada.

Consulte [“Sobre a segurança do Symantec Management Platform”](#) na página 83.

Tabela 4-1

Processo de configuração da segurança do Symantec Management Platform

Etapa	Ação	Descrição
Etapa 1	Crie e configure as funções de segurança de que você precisa.	As funções de segurança controlam o acesso ao Symantec Management Platform, à funcionalidade instalada da solução e a todos os dados contidos no CMDB. Você pode criar novas funções de segurança das seguintes maneiras: ■ Crie novas funções de segurança. ■ Duplicar funções de segurança existentes. ■ Importar usuários e grupos de domínio do Active Directory. Consulte “Para criar e configurar funções de segurança” na página 88.
Etapa 2	Atribua os privilégios apropriados às funções de segurança.	Um privilégio permite que um membro da função execute uma ação específica no Symantec Management Platform ou em itens no Console de gerenciamento Symantec. Para executar uma ação em um item, a função deve ter a permissão necessária no item. Consulte “Para atribuir privilégios a uma função de segurança” na página 93.

Etapa	Ação	Descrição
Etapa 3	Crie e configure as contas do usuário de que você precisa.	Cada conta do usuário do Symantec Management Platform contém as credenciais que o usuário precisa para acessar o Console de gerenciamento Symantec ou para executar um fluxo de trabalho. As credenciais podem ser nomes de usuário e senhas do Symantec Management Platform internos ou contas do Windows. As credenciais internas são usadas atualmente somente para a integração do fluxo de trabalho. As credenciais do Windows são necessárias para acessar o Console de gerenciamento Symantec. Você pode criar contas de usuário das seguintes maneiras: ■ Criar contas de usuário completamente novas. ■ Duplicar contas de usuário existentes. ■ Importar usuários e grupos de domínio do Active Directory. Consulte “Para criar e configurar contas de usuário do Symantec Management Platform” na página 225. Consulte “Para especificar detalhes gerais da conta de usuário do Symantec Management Platform” na página 98. Consulte “Configuração das credenciais para uma conta do usuário do Symantec Management Platform” na página 99.
Etapa 4	Adicione membros às funções de segurança apropriadas.	Um usuário obtém acesso ao Symantec Management Platform, às soluções instaladas e aos dados contidos no CMDB através da participação da função de segurança. Você pode atribuir um usuário a qualquer número de funções de segurança. Um usuário que seja membro de várias funções de segurança tem a união de todos os privilégios e as permissões que as funções concedem. Consulte “Para adicionar membros a uma função de segurança” na página 101. Consulte “Para atribuir uma conta de usuário do Symantec Management Platform a uma função de segurança” na página 102. Consulte “Para adicionar funções de segurança como membros de outras funções de segurança” na página 102.

Etapa	Ação	Descrição
Etapa 5	Para cada função de segurança, atribua permissões nas pastas e nos itens contidos no Console de gerenciamento Symantec.	As permissões especificam o acesso que cada função de segurança tem a uma pasta do Console de gerenciamento Symantec ou a um item específico. Uma permissão em um item aplica-se apenas ao item. Uma permissão em uma pasta aplica-se a todos os itens contidos diretamente nessa pasta. Por padrão, o conteúdo de uma pasta herda todas suas permissões. Consulte “Para atribuir permissões de segurança a pastas e itens” na página 103.
Etapa 6	(Opcional) Para cada função de segurança, modifique a herança de permissão na estrutura de pastas do Console de gerenciamento Symantec.	Modificar a herança de permissão permite personalizar as permissões na estrutura de pastas do Console de gerenciamento Symantec. Isto significa que você pode conceder uma permissão específica em uma pasta pai, mas remover essa permissão de algum ou de todo o conteúdo da pasta. Lembre-se de que você configura permissões em pastas e os itens nessas pastas. Se você configurar uma pasta e conceder permissões de gravação para uma função específica, essa função terá a permissão de gravação na pasta e em todo o seu conteúdo. Se a pasta contiver 100 itens e você não quiser que esses itens herdem a permissão de gravação da pasta pai, será possível cancelar a herança de permissão. Nesse caso, os usuários que forem membros da função à qual você concedeu a permissão de gravação terão permissão de gravação apenas na pasta. Porém, não terão a permissão de gravação nos itens que a pasta contém. A herança de permissão em uma pasta ou em um item aplica-se a todas as funções de segurança. Você não pode personalizar a herança de permissão por função. Consulte “Para personalizar a herança de permissões” na página 104.

Etapa	Ação	Descrição
Etapa 7	(Opcional) Configure a segurança dos recursos.	Por padrão, todas as funções de segurança predefinidas têm a permissão de leitura em recursos. Os recursos relativos à segurança são controlados especialmente no Symantec Management Platform: apenas os usuários que forem membros da função Administradores da Symantec terão o acesso completo aos recursos por padrão. Os usuários que forem membros da função Supervisores da Symantec terão permissões de leitura em recursos por padrão. Nenhuma outra função de segurança predefinida tem permissões em todos os recursos. Consulte "Funções predefinidas de segurança" na página 106. Se desejar restringir ou controlar o acesso aos recursos, você poderá configurar a segurança dos recursos. Você configura a segurança dos recursos criando uma ou mais exibições organizacionais que modelam sua estrutura de recursos. Você controla o acesso aos recursos atribuindo permissões a cada função de segurança nas exibições organizacionais e nos grupos apropriados.

Para criar e configurar funções de segurança

Uma função de segurança é um conjunto de privilégios e permissões que é concedido a todos os membros da função. O uso de segurança com base em função permite criar e manter um pequeno número de funções de segurança e atribuir a cada usuário a função apropriada. Você não precisa atribuir privilégios e permissões a cada conta de usuário individual. Você pode atribuir uma conta de usuário a várias funções de segurança: um membro de várias funções de segurança tem a combinação de todos os privilégios e de todas as permissões que essas funções concedem.

Consulte ["Sobre a segurança do Symantec Management Platform"](#) na página 83.

As funções de segurança podem ser aninhadas: uma função pode ser um membro de uma ou mais funções e sua participação pode incluir funções e contas do usuário. A única restrição é que você não pode criar uma participação da função circular onde uma função é um membro de si mesma.

Os privilégios, as permissões em pastas e em itens e as permissões em exibições e grupos organizacionais funcionam em conjunto. Você precisa atribuir a combinação apropriada a cada função de segurança para garantir às contas do usuário o acesso necessário para executar suas atividades. Os privilégios somente podem ser atribuídos às funções de segurança, mas as permissões podem ser atribuídas às funções de segurança e às contas do usuário.

Você deve decidir quais funções de segurança serão configuradas com base nos grupos lógicos de funcionários de TI ou usuários em sua organização. Por exemplo, convém ter uma função de funcionário de TI de nível 1, uma função de gerenciamento de nível superior e uma função de recursos humanos. Todas as contas do usuário em uma função de segurança recebem os mesmos privilégios e permissões; assim, elas têm o mesmo nível de acesso ao Symantec Management Platform.

É possível criar e configurar uma função de segurança de uma das seguintes maneiras:

Crie uma nova função de segurança completamente ou duplique uma função de segurança existente.	O Symantec Management Platform e algumas soluções incluem funções de segurança predefinidas. Consulte “Funções predefinidas de segurança” na página 106. Se as funções de segurança predefinidas não atenderem às necessidades de sua organização, você poderá criar novas funções ou duplicar as funções existentes para criar novas funções. Você pode então modificar os privilégios e as permissões conforme for apropriado. Consulte “Para criar uma nova função de segurança ou duplicar uma função de segurança existente” na página 90.
Importe grupos de domínio e usuários com o Active Directory.	Quando importar grupos de domínio do Active Directory, uma função de segurança será criada no servidor do Symantec Management Platform para o grupo de domínio que você quer importar. Membros deste grupo de domínio, incluindo usuários e subgrupos, também são importados. Os usuários são criados como contas e os subgrupos são criados como funções. O relacionamento da participação é retido durante a importação. Consulte “Para importar grupos e usuários de domínio do Active Directory” na página 91.

Durante a instalação do Symantec Management Platform, o administrador que instala o Platform é atribuído automaticamente à função de Administrador Symantec. O administrador pode, então, criar novas funções de segurança necessárias e atribuir a cada função os privilégios e as permissões apropriados. O administrador pode, então, atribuir a cada usuário uma ou mais funções.

A Symantec recomenda configurar as funções de segurança antes que o Notification Server esteja implementado em sua rede de produção.

Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para configurar a segurança do Symantec Management Platform”](#) na página 84.

Para criar uma nova função de segurança ou duplicar uma função de segurança existente

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, em **Gerenciamento de conta**, clique em **Funções**.
- 3 Na página **Funções**, no painel esquerdo, tome uma das seguintes ações:

Para criar uma função nova Clique em **Adicionar**.

Na caixa de diálogo **Nova função**, digite o nome da nova função de segurança e clique em **OK**.

A função nova aparece na lista de funções e as configurações padrão são mostradas no painel direito.

Para duplicar uma função existente

Selecione a função de segurança que você quer duplicar.

Clique com o botão direito do mouse na função e clique em **Clone**.

- 4 No painel direito, defina as configurações apropriadas nas seguintes guias:

Membros	As funções e as contas do usuário atribuídas à função. Uma participação da função pode incluir qualquer número de contas do usuário e funções. Os membros de uma função têm todos os privilégios e permissões que a função concede. Consulte “Para adicionar membros a uma função de segurança” na página 101.
Membro de	As funções de segurança às quais a função pertence. A função tem a união das permissões e dos privilégios destas funções, combinados com todas as permissões e privilégios adicionais que forem atribuídos diretamente à função. Consulte “Para adicionar funções de segurança como membros de outras funções de segurança” na página 102.
Privilégios	Os privilégios que a função concede a seus membros. Um privilégio permite que uma conta do usuário execute uma ação específica no Symantec Management Platform ou em itens no Console de gerenciamento Symantec. Em alguns casos, a conta do usuário também deve ter uma permissão correspondente no item. Consulte “Para atribuir privilégios a uma função de segurança” na página 93.

- 5 (Opcional) Se desejar acessar o Gerenciador de função de segurança para visualizar ou configurar permissões para a função de segurança, clique em **Mostrar o console do Gerenciador de função de segurança**.

- 6 Clique em **Salvar alterações**.

Para importar grupos e usuários de domínio do Active Directory

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, na descrição rotulada **Importar o papel e os recursos da conta de <origem de dados>, de (nenhum). Executar essa importação no agendamento especificado**, clique no grupo de usuários **(nenhum)**.
- 3 (Opcional) Crie suas próprias regras de função e de importação de conta.
- 4 Na caixa de diálogo **Selecionar grupos de segurança**, pesquise os grupos de domínio que você quer adicionar; por exemplo, Administradores e Usuários.
- 5 Clique em **Adicionar** para adicionar os grupos selecionados, e clique em **OK**.

- 6 Execute a regra como uma importação completa para importar o grupo de domínio selecionado.
- 7 (Opcional) você pode também agendar uma importação completa para executar em intervalos apropriados.

Você pode usar este agendamento para sincronizar sua participação na função de segurança com a participação do grupo do domínio. Isto significa que se você remover um usuário de domínio do grupo do domínio, a conta de segurança correspondente será removida da função de segurança correspondente. Igualmente se você adicionar um usuário de domínio ao grupo do domínio, a conta de segurança correspondente será criada e adicionada à função de segurança correspondente. Observe que se um usuário de domínio for removido de um grupo do domínio, a conta de segurança correspondente não será excluída. Apenas a participação na função de segurança é removida.

- 8 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 9 No painel esquerdo, na pasta **Gerenciamento de conta**, clique em **Funções** e depois clique na função que você quer editar.

- 10 (Opcional) No painel direito, defina as configurações apropriadas nas seguintes guias:

Membros	As funções e as contas do usuário atribuídas à função. Uma participação da função pode incluir qualquer número de contas do usuário e funções. Os membros de uma função têm todos os privilégios e permissões que a função concede. Consulte “Para adicionar membros a uma função de segurança” na página 101. Observe que você não deve modificar manualmente membros de funções importados do Active Directory. Esta restrição existe porque todas as execuções subsequentes da regra sobrescreverão a configuração da participação. As funções que você importar do Active Directory são projetadas para manter a mesma participação dos grupos de domínio correspondentes.
Membro de	As funções de segurança às quais a função pertence. A função tem a união das permissões e dos privilégios destas funções, combinados com todas as permissões e privilégios adicionais que forem atribuídos diretamente à função. Consulte “Para adicionar funções de segurança como membros de outras funções de segurança” na página 102.
Privilégios	Os privilégios que a função concede a seus membros. Um privilégio permite que uma conta de usuário execute uma ação específica no Symantec Management Platform ou em itens do Console de gerenciamento Symantec. Em alguns casos, a conta do usuário também deve ter uma permissão correspondente no item. Consulte “Para atribuir privilégios a uma função de segurança” na página 93.

- 11 (Opcional) Se desejar acessar o Gerenciador de função de segurança para visualizar ou configurar permissões para a função de segurança, clique em **Mostrar o console do Gerenciador de função de segurança**.
- 12 Clique em **Salvar alterações**.

Para atribuir privilégios a uma função de segurança

Você precisa especificar os privilégios que cada função de segurança concederá a seus membros. Um privilégio permite que o usuário execute uma ação específica no Symantec Management Platform ou em itens no Console de gerenciamento

Symantec. Para executar uma ação em um item, a função do usuário deve ter a permissão necessária no item. Por exemplo, se você fornecer a uma função os privilégios de iniciar e interromper tarefas, será preciso atribuir a permissão de executar tarefas à função para as tarefas apropriadas. A função não pode acessar nenhuma tarefa que não tenha a permissão de executar tarefa para essa função.

Consulte [“Para atribuir permissões de segurança a pastas e itens”](#) na página 103.

A atribuição de privilégios a uma função de segurança faz parte da configuração das funções de segurança. Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para criar e configurar funções de segurança”](#) na página 88.

Para atribuir privilégios a uma função de segurança

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Funções**.
- 3 Na página **Funções**, no painel esquerdo, clique na função de segurança que deseja configurar.
- 4 No painel direito, na guia **Privilégios**, selecione os privilégios que deseja atribuir à função.

Para selecionar um privilégio, verifique caixa de seleção correspondente.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

- 5 Clique em **Salvar alterações**.

Para criar e configurar contas de usuário do Symantec Management Platform

O Symantec Management Platform tem suas próprias contas de usuário. As versões anteriores ao Symantec Management Platform 7.1 usavam usuários e grupos do Windows para a segurança do usuário. Os usuários do Windows ainda são utilizados, mas não são mais o único mecanismo de segurança.

As contas do usuário, que são chamadas, às vezes, de usuários, não são as mesmas que os recursos do usuário no Symantec Management Platform. Um recurso do usuário é uma entidade usada para associar dispositivos gerenciados ao proprietário do dispositivo. Os recursos existentes do usuário e as contas do usuário que podem fazer logon no Console de gerenciamento Symantec ou executar um fluxo de trabalho são entidades separadas.

Uma conta do usuário do Symantec Management Platform é vinculada às credenciais do Windows necessárias para que o usuário acesse o Console de

gerenciamento Symantec. A conta do usuário também pode ser vinculada às credenciais internas que podem ser usadas para acessar outros serviços do Symantec Management Platform, como fluxos de trabalho. A conta do usuário pode ser adicionada às funções de segurança apropriadas: uma conta tem a união de todos os privilégios e permissões concedidos pelas funções às quais pertence.

Uma credencial é algo que uma conta do usuário fornece para provar sua identidade. No Symantec Management Platform, uma credencial pode ser um nome de usuário e uma senha ou uma conta do Windows. A conta do usuário associa uma ou mais credenciais a um usuário específico e permite que o usuário acesse os serviços do Console de gerenciamento Symantec ou do Symantec Management Platform.

O Symantec Management Platform utiliza dois tipos de credenciais:

Credencial interna	Permite que um usuário acesse os serviços adequados do Symantec Management Platform usando um nome de usuário e uma senha armazenados no CMDB. Por razões de segurança, apenas o valor de hash da senha é armazenado. Uma conta do usuário não pode usar credenciais internas para acessar o Console de gerenciamento Symantec. As credenciais internas são atualmente usadas apenas para a integração do fluxo de trabalho.
Credencial do Windows	Permite que um usuário acesse os serviços do Console de gerenciamento Symantec e do Symantec Management Platform usando um nome de usuário e senha do Windows. Para usar credenciais do Windows, o Notification Server deve estar no domínio do usuário, ou o domínio do usuário deve ser confiável para o domínio do Notification Server. Você deverá configurar credenciais do Windows se sua organização usar contas do Windows internamente. Usar credenciais do Windows permite aplicar requisitos da complexidade da senha, alterar senhas periodicamente, manter o histórico da senha e executar outras tarefas de gerenciamento da senha no Windows.

Você pode configurar suas contas do usuário do Symantec Management Platform para cumprir os requisitos de sua organização. Você precisa criar todas as contas que desejar e atribuí-las às funções de segurança apropriadas. Cada conta tem a união de todos os privilégios e permissões concedidos pelas funções às quais pertencem.

Crie e configure uma conta de usuário de uma das seguintes maneiras:

- Crie uma nova conta de usuário ou duplique uma conta de usuário existente.

- Importe usuários e grupos de domínio do Active Directory.

Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte “[Para configurar a segurança do Symantec Management Platform](#)” na página 84.

Para criar uma nova conta de usuário ou duplicar uma conta de usuário existente

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Contas**.
- 3 Na página **Contas**, no painel esquerdo, tome uma das seguintes ações:

Para criar uma nova conta	Clique em Adicionar. Na caixa de diálogo Nova conta, digite o novo nome da conta do Symantec Management Platform e clique em OK. A nova conta aparece na lista de contas. Por padrão, o status da nova conta é Inativo.
Para duplicar uma conta existente	Clique com o botão direito do mouse na conta do Symantec Management Platform que você quer duplicar e configurar. Digite o nome da cópia nova desta conta e clique em OK.

- 4 No painel direito, defina as configurações apropriadas nas seguintes guias:

Geral

Os detalhes gerais da conta. Incluem o nome completo e o endereço de e-mail do usuário para quem a conta é criada, o status e as credenciais da conta.

Consulte [“Para especificar detalhes gerais da conta de usuário do Symantec Management Platform”](#) na página 98.

Consulte [“Configuração das credenciais para uma conta do usuário do Symantec Management Platform”](#) na página 99.

Membro de

As funções de segurança às quais a conta pertence. A conta tem a união de todos os privilégios e permissões concedidos pelas funções às quais pertencem.

Consulte [“Para atribuir uma conta de usuário do Symantec Management Platform a uma função de segurança”](#) na página 102.

- 5 Clique em **Salvar alterações**.

Para importar grupos e usuários de domínio do Active Directory

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, na descrição rotulada **Importar o papel e os recursos da conta de <origem de dados>, de (nenhum). Executar essa importação no agendamento especificado**, clique no grupo de usuários **(nenhum)**.
- 3 (Opcional) Crie suas próprias regras de função e de importação de conta.
- 4 Na caixa de diálogo **Selecionar grupos de segurança**, pesquise os grupos do domínio de que você quer importar contas de usuário; por exemplo, Administradores e Usuários.
- 5 Clique em **Add** e em **OK** para adicionar os grupos selecionados.

- 6 Execute a regra como uma importação completa para importar os grupos selecionados do domínio.
- 7 (Opcional) você pode também agendar uma importação completa para executar em intervalos apropriados.

Você pode usar este agendamento para sincronizar sua participação na função de segurança com a participação do grupo do domínio. Isto significa que se você remover um usuário de domínio do grupo do domínio, a conta de segurança correspondente será removida da função de segurança correspondente. Igualmente se você adicionar um usuário de domínio ao grupo do domínio, a conta de segurança correspondente será criada e adicionada à função de segurança correspondente. Observe que se um usuário de domínio for removido de um grupo do domínio, a conta de segurança correspondente não será excluída. Apenas a participação na função de segurança é removida.

Vídeo para obter mais informações sobre como criar contas de usuário do Symantec Management Platform, veja [Creating a Limited ITMS Administrator Role Video \(em inglês\)](#) no Symantec Connect.

Para especificar detalhes gerais da conta de usuário do Symantec Management Platform

Você precisa especificar o nome completo e o endereço de e-mail do usuário para quem a conta é criada. Você também poderá alterar o status da conta de Inativo para Ativo, quando apropriado.

Consulte [“Para criar e configurar contas de usuário do Symantec Management Platform”](#) na página 225.

Para especificar detalhes gerais da conta do usuário do Symantec Management Platform

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Contas**.
- 3 Na página **Contas**, no painel esquerdo, clique na conta que deseja configurar.
- 4 No painel direito, na guia **Geral** especifique os detalhes da conta editando as caixas apropriadas:

Nome completo	O nome completo do usuário a quem a conta pertence.
E-mail	O endereço de e-mail do usuário da conta.

- 5 (Opcional) Se desejar ativar ou desativar a conta, clique no ícone de status na barra de título e selecione **Ativo** ou **Inativo**.
- 6 Clique em **Salvar alterações**.

Configuração das credenciais para uma conta do usuário do Symantec Management Platform

Você precisa configurar as credenciais apropriadas a cada conta do usuário do Symantec Management Platform. Você pode adicionar uma credencial interna do Symantec Management Platform e uma credencial do Windows a uma conta do usuário. A credencial do Windows emula o comportamento das versões anteriores do Symantec Management Platform.

Uma credencial interna permite que um usuário acesse os serviços adequados do Symantec Management Platform usando um nome de usuário e uma senha armazenados no CMDB. Atualmente, as credenciais internas são usadas apenas para a integração do fluxo de trabalho.

Uma credencial do Windows permite que uma conta do usuário acesse os serviços do Console de gerenciamento Symantec e do Symantec Management Platform usando um nome de usuário e uma senha do Windows. Para usar credenciais do Windows, o Notification Server deve estar no domínio do usuário ou o domínio do usuário deve ser confiável para o domínio do Notification Server.

Você deverá configurar credenciais do Windows se sua organização usar contas do Windows internamente. Usar credenciais do Windows permite aplicar requisitos da complexidade da senha, alterar senhas periodicamente, manter o histórico da senha e executar outras tarefas de gerenciamento da senha no Windows.

Consulte [“Para criar e configurar contas de usuário do Symantec Management Platform”](#) na página 225.

Para configurar as credenciais para uma conta do usuário do Symantec Management Platform

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Contas**.
- 3 Na página **Contas**, no painel esquerdo, clique na conta que deseja configurar.

- 4 No painel direito, na guia **Geral**, em **Credenciais**, clique em **Adicionar credencial** e, em seguida, execute um destes procedimentos:

Para adicionar uma credencial do Windows à conta

Clique em **Windows** e, em seguida, especifique o nome de usuário apropriado do Windows, no formato Domínio/Nome de usuário, na caixa de diálogo **Credencial do Windows**.

Se a conta do Windows estiver no mesmo domínio que o Notification Server, será possível omitir o domínio e especificar apenas o nome de usuário.

Se você especificar uma conta do Windows que já estiver atribuída a uma conta do usuário, a credencial do Windows será removida da conta existente. A credencial do Windows é então adicionada à nova conta do usuário.

Para adicionar uma credencial interna à conta

Clique em **Interno** e, em seguida, na caixa de diálogo **Criar credencial interna** especifique a senha apropriada.

A senha deve atender às configurações de complexidade da senha.

Consulte [“Para definir as configurações de bloqueio e complexidade da senha”](#) na página 109.

O nome de usuário da credencial é o nome da conta do Symantec Management Platform e você não pode mudá-lo.

- 5 Clique em **OK**.

A credencial nova é adicionada à lista **Credenciais**.

- 6 (Opcional) Se desejar modificar uma credencial, selecione-a na lista **Credenciais** e clique em **Editar**. Na caixa de diálogo **Editar credencial do Windows** ou na caixa de diálogo **Editar credencial interna**, faça as alterações apropriadas e clique em **OK**.

Por razões de segurança, a caixa de diálogo **Editar credencial interna** não exibe a senha atual. Se você especificar uma nova senha, a credencial será atualizada de maneira apropriada. Se você deixar a caixa **Senha** vazia, a senha original será preservada.

- 7 (Opcional) Se desejar excluir uma credencial, selecione-a na lista **Credenciais** e clique em **Excluir**.

- 8 Clique em **Salvar alterações**.

Para adicionar membros a uma função de segurança

Você precisa atribuir os membros apropriados, contas do usuário e outras funções de segurança, a cada uma de suas funções de segurança. Você precisa ser um membro da função de Administradores da Symantec ou de uma função que tenha o privilégio Alterar segurança para adicionar membros. Você pode atribuir uma conta do usuário a qualquer número de funções de segurança. Os membros de uma função têm todos os privilégios e as permissões concedidos à função.

Você pode adicionar uma função a várias funções de segurança, mas não pode criar uma participação circular onde uma função específica torna-se membro de si mesma. Um membro de várias funções de segurança tem a união de todos os privilégios e as permissões que essas funções concedem.

A adição de membros a uma função de segurança faz parte da configuração das funções de segurança. Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para criar e configurar funções de segurança”](#) na página 88.

Para adicionar membros a uma função de segurança

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Funções**.
- 3 Na página **Funções**, no painel esquerdo, clique na função de segurança que deseja configurar.
- 4 No painel direito, na guia **Membros**, clique em **Adicionar membro** e, então, execute uma das seguintes ações:

Para adicionar uma conta do usuário à função Clique em **Adicionar conta**.

Para adicionar outra função de segurança à função Clique em **Adicionar função**.

- 5 Na caixa de diálogo **Selecionar contas** ou **Selecione funções**, selecione as contas do usuário ou as funções de segurança que deseja adicionar e clique em **OK**.
- 6 Na guia **Membros**, verifique se a lista de membros está correta. Você pode remover todas as que não quiser.
- 7 Clique em **Salvar alterações**.

Para atribuir uma conta de usuário do Symantec Management Platform a uma função de segurança

Você precisa atribuir cada conta do usuário do Symantec Management Platform às funções de segurança apropriadas. Você precisa ser um membro da função de Administradores da Symantec ou de uma função que tenha o privilégio Alterar segurança para atribuir uma participação da função. A conta tem a união de todos os privilégios e permissões concedidos pelas funções às quais pertencem.

Consulte [“Para criar e configurar contas de usuário do Symantec Management Platform”](#) na página 225.

Para atribuir uma conta do Symantec Management Platform a uma função de segurança

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Contas**.
- 3 Na página **Contas**, no painel esquerdo, clique na conta que deseja configurar.
- 4 No painel direito, na guia **Membro de**, defina as configurações apropriadas.
- 5 Clique em **Adicionar função**.
- 6 Na caixa de diálogo **Selecionar função(ões)**, selecione as funções de segurança às quais deseja adicionar a conta e clique em **OK**.
- 7 Na guia **Membro de**, verifique se a lista de funções de segurança está correta. Você pode remover todas as que não quiser.
- 8 Clique em **Salvar alterações**.

Para adicionar funções de segurança como membros de outras funções de segurança

Você pode adicionar uma função como um membro de outras funções de segurança. Você precisa ser um membro da função de Administradores da Symantec ou de uma função que tenha o privilégio Alterar segurança para atribuir uma participação da função. Você pode adicionar uma função a várias funções de segurança, mas não pode criar uma participação circular onde uma função específica torna-se membro de si mesma. Uma função recebe a união de todos os privilégios e permissões concedidos pelas funções às quais ela pertence.

Adicionar uma função como um membro de outra função é o mesmo que a adição de outra função à sua participação. Este método permite adicionar uma função específica a diversas funções em um único procedimento. A alternativa seria

configurar todas as outras funções e adicionar especificamente a função à participação de cada uma.

Adicionar funções de segurança como membros de outras funções de segurança faz parte da configuração de funções de segurança. Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para criar e configurar funções de segurança”](#) na página 88.

Para adicionar uma função de segurança como um membro de outras funções de segurança

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Funções**.
- 3 Na página **Funções**, no painel esquerdo, clique na função de segurança que deseja configurar.
- 4 No painel direito, na guia **Membro de**, defina as configurações apropriadas.
- 5 Clique em **Adicionar função**.
- 6 Na caixa de diálogo **Selecionar função(ões)**, selecione as funções de segurança às quais deseja adicionar a função e clique em **OK**.
- 7 Na guia **Membro de**, verifique se a lista de funções de segurança está correta. Você pode remover todas as que não quiser.
- 8 Clique em **Salvar alterações**.

Para atribuir permissões de segurança a pastas e itens

Você pode especificar as permissões não herdadas que se aplicam a cada pasta ou item para cada função de segurança. Estas são combinadas com as permissões que são herdadas da pasta pai. As permissões combinadas determinam o acesso que a função de segurança tem a essa pasta ou item específicos. Por padrão, todas as pastas ou itens filho herdam o conjunto de permissões.

Consulte [“Para acessar o Gerenciador de função de segurança”](#) na página 113.

Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para configurar a segurança do Symantec Management Platform”](#) na página 84.

Para atribuir permissões de segurança a pastas e itens

- 1 No Gerenciador de função de segurança, na lista suspensa **Função**, selecione a função de segurança para a qual você deseja definir permissões.
- 2 (Opcional) Na lista suspensa **Exibição**, selecione uma categoria do item para exibir a estrutura da pasta que contém os itens relevantes.
Se desejar exibir a estrutura completa da pasta, selecione **Todos os itens**.
- 3 No painel esquerdo, selecione a pasta ou o item para o qual você deseja definir permissões.
Note que alguns itens podem estar ocultos por padrão. Para ver todos os itens, clique no ícone **Mostrar itens ocultos**, na barra de ferramentas. Esta funcionalidade somente está disponível para as funções com o privilégio **Alterar segurança** atribuído a elas.

Aviso: Tenha cuidado ao editar as permissões de segurança de um item oculto, porque não são projetadas para ser modificadas.

- 4 No painel direito, no painel **Não herdado**, faça as alterações apropriadas às configurações da permissão.
- 5 (Opcional) Se desejar configurar a herança de permissão para esta pasta ou item, clique em **Avançado**.
Consulte [“Para personalizar a herança de permissões”](#) na página 104.
- 6 Clique em **Salvar alterações**.

Para personalizar a herança de permissões

Por padrão, a herança de permissão é ativada para todas as pastas e itens. As pastas e os itens filho herdam as permissões de segurança para cada função atribuída a uma pasta. As permissões herdadas não podem ser modificadas nas pastas e nos itens filho, mas as permissões não herdadas adicionais podem ser especificadas. As permissões não herdadas são aplicadas diretamente à pasta ou ao item e podem ser modificadas a qualquer momento. As configurações da permissão em cada pasta ou item são a combinação das configurações herdadas e não herdadas. O conjunto de permissões combinado é aplicado a todas as pastas ou itens filho. Todas as mudanças feitas nas configurações de permissões de uma pasta são aplicadas imediatamente a todas as pastas ou itens filho.

Você pode desativar a herança de permissão para qualquer pasta ou item. Permite remover algumas das permissões herdadas da pasta ou do item, mas preserva-os em sua pasta pai. As configurações da herança de permissão que você aplica a

uma pasta ou a um item aplicam-se a cada função de segurança. Você não pode personalizar configurações da herança para funções específicas.

Aviso: Desativar a herança de permissões em uma pasta ou em um item pode causar negações de acesso inesperadas para as contas do usuário. Se você desativar a herança de permissões, assegure-se de que haja permissões explicitamente especificadas na pasta ou no item para que as contas do usuário tenham o acesso adequado.

Você também pode remover todas as permissões não herdadas das pastas ou dos itens, deixando somente as permissões herdadas. Convém remover todas as permissões não herdadas para retirar as permissões personalizadas que foram adicionadas às pastas ou aos itens filho. Também convém usar este recurso para restaurar um conjunto de permissões padrão em todas as pastas e itens filho.

Consulte [“Para atribuir permissões de segurança a pastas e itens”](#) na página 103.

Esta tarefa é uma etapa do processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para configurar a segurança do Symantec Management Platform”](#) na página 84.

Para personalizar a herança de permissão de uma pasta ou item

- 1 No Gerenciador de função de segurança, no painel esquerdo, selecione a pasta ou o item para o qual você deseja configurar a herança de permissão.
- 2 No painel direito, clique em **Avançado**.
- 3 Na janela Permissões para: Na janela *Nome do item*, na lista **Conta/Grupo/Função**, selecione a função de segurança ou a conta do usuário para o qual você deseja configurar permissões.

Se desejar adicionar outra função de segurança ou conta do usuário à lista, clique em **Adicionar**. Na janela **Adicionar Trustees**, escolha a função de segurança ou a conta de usuário apropriada.
- 4 (Opcional) No painel **Permissões para**, mude as permissões atribuídas à função de segurança selecionada para esta pasta ou item.

Você pode usar estes recursos somente para as permissões não herdadas. Não é possível editar as permissões herdadas.

5 Execute uma das seguintes ações:

Para herdar permissões da pasta pai	Selecione Herdar as entradas de permissão do objeto pai que se aplica aos objetos filho. As configurações da permissão herdada na pasta ou no item são atualizadas para refletir as configurações atuais da permissão na pasta pai.
Para desativar a herança de permissões	Desmarque Herdar as entradas de permissão do objeto pai que se aplica aos objetos filho. Você tem a escolha de copiar as permissões herdadas atuais da pasta pai ou de remover todas as permissões herdadas. Nenhuma alteração subsequente às configurações da permissão na pasta pai afetam as configurações de permissão na pasta ou no item.
Para remover todas as permissões não herdadas das pastas e dos itens filho	Selecione Substituir permissões em todos os objetos filho. As configurações não herdadas das permissões são limpas em todas as pastas e itens filho, mantendo somente as permissões herdadas.

6 Clique em **Salvar alterações**.

7 (Opcional) Se você desativou a herança de permissão, na caixa de diálogo **Comportamento de permissões herdadas**, clique na opção apropriada:

Copiar	As permissões herdadas atuais são mescladas com as configurações de permissões não herdadas nesta pasta ou item.
Remover	As permissões herdadas atuais são removidas, mantendo somente as permissões não herdadas. Certifique-se de que você tenha as permissões não herdadas apropriadas na pasta ou no item antes de selecionar esta opção.

8 Clique em **Cancelar** para fechar a janela Permissões para: Janela *Nome do item*.

Funções predefinidas de segurança

O Symantec Management Platform inclui um conjunto de funções de segurança predefinidas que você pode usar. Se as funções de segurança predefinidas não

atenderem às necessidades de sua organização, você poderá criar novas. Você também pode editar as funções de segurança predefinidas especificando privilégios e permissões diferentes.

Consulte [“Para criar e configurar funções de segurança”](#) na página 88.

Tabela 4-2 Funções de segurança predefinidas do Symantec Management Platform

Função de segurança	Descrição
Todos	Uma função de primeiro nível que contém todas as funções e contas do usuário. A participação desta função é calculada automaticamente e não pode ser modificada manualmente. Por padrão, esta função não tem privilégios atribuídos. Quando você mudar permissões e privilégios desta função, as mudanças serão aplicadas automaticamente a todas funções e contas do usuário restantes.
Administradores Symantec	Têm todos os privilégios e permissões de segurança atribuídos; assim, têm acesso completo a todos os aspectos do Symantec Management Platform e a todas as soluções instaladas. Você pode modificar a participação desta função de segurança, mas não pode mudar seus privilégios e suas permissões.
Supervisores da Symantec	Tem gerenciamento completo e a maioria dos privilégios do menu contextual. Tem privilégios limitados de sistema atribuídos. Tem a permissão de leitura nos recursos, inclusive em recursos de segurança. Tem o acesso completo às configurações do gerenciamento habilitado para nuvem, inclusive à configuração de novo um gateway da Internet e à geração do pacote de instalação do Symantec Management Agent.
Trabalhadores do nível 2 da Symantec	Tem os privilégios de gerenciamento completo e a maioria dos privilégios do menu de clique com o botão direito do mouse atribuídos. Tem a permissão de leitura em recursos, exceto em recursos de segurança. Tem acesso limitado às configurações do gerenciamento habilitado para nuvem. Por exemplo, os funcionários de nível 2 da Symantec podem criar uma política de Configurações do gerenciamento habilitado para nuvem.

Função de segurança	Descrição
Trabalhadores do nível 1 da Symantec	Não têm privilégios atribuídos. Tem a permissão de leitura em recursos, exceto em recursos de segurança.
Symantec Software Librarian	Tem os privilégios do Software Management Framework e os privilégios das ações do menu de clique com o botão direito do mouse atribuídos. Os privilégios são limitados àqueles necessários para criar e gerenciar pacotes de software.
Convidados Symantec	Não têm privilégios atribuídos. Tem permissão de leitura em relatórios.
Usuários autenticados\Autoridade NT	Qualquer usuário que fizer logon no Console de gerenciamento Symantec será automaticamente um membro desta função. A participação desta função é calculada automaticamente e não pode ser modificada manualmente. Por padrão, esta função não tem privilégios ou permissões atribuídos.

Tarefas de gerenciamento de segurança do Symantec Management Platform

Tabela 4-3 Tarefas de gerenciamento de segurança do Symantec Management Platform

Tarefa	Descrição
Definir configurações de bloqueio e complexidade da senha.	Você pode especificar os requisitos apropriados de complexidade da senha para impedir que as contas do usuário do Symantec Management Platform criem senhas fracas. Qualquer alteração que você fizer às configurações de complexidade da senha não afetará as senhas existentes. As regras de complexidade da senha serão aplicadas apenas quando as senhas forem criadas ou alteradas. Consulte “Para definir as configurações de bloqueio e complexidade da senha” na página 109.

Tarefa	Descrição
Desbloquear credenciais bloqueadas.	Você pode desbloquear as credenciais internas que foram bloqueadas depois de excedido o número máximo de tentativas malsucedidas de logon. Consulte “Para desbloquear credenciais bloqueadas” na página 113.
Exibir e gerenciar permissões das funções de segurança.	O Gerenciador de função de segurança permite exibir e definir permissões para funções de segurança. Você também pode usar o Gerenciador de função de segurança para obter propriedade de um item. Consulte “Para acessar o Gerenciador de função de segurança” na página 113.
Obter propriedade de uma pasta ou de um item.	Você poderá tomar a posse de um item se suas permissões forem removidas acidentalmente e o proprietário não puder mais acessá-lo. Depois que você toma a posse, pode redefinir as permissões apropriadas e restaurar o acesso para o proprietário original. Consulte “Para obter a propriedade de uma pasta ou item” na página 115.
Gerenciar credenciais.	As soluções de gerenciamento normalmente criam credenciais quando elas são necessárias para executar uma tarefa. Consulte “Para gerenciar credenciais” na página 115.

Para definir as configurações de bloqueio e complexidade da senha

A página **Configurações da senha** permite definir as configurações de bloqueio e complexidade da senha para credenciais internas. Estas configurações aplicam-se às credenciais internas apenas: não se aplicam às senhas gerenciadas externamente, como uma conta do Windows. Estas configurações de complexidade e bloqueio são frequentemente necessárias para que seja cumprida a política de controle de acesso de uma organização.

Você precisa especificar os requisitos apropriados de complexidade da senha para impedir que as contas de usuário do Symantec Management Platform criem senhas fracas.

Nota: Qualquer alteração que você fizer às configurações de complexidade da senha não afetará as senhas existentes. As regras de complexidade da senha serão aplicadas apenas quando as senhas forem criadas ou alteradas.

Você não pode especificar restrições temporais como permitir que contas do usuário façam logon apenas durante determinados períodos de tempo ou em dias específicos da semana. Para configurar este tipo de restrição, é possível usar uma tarefa agendada, um fluxo de trabalho ou uma política de automação que desative e ative contas nos horários apropriados.

Você não pode configurar a idade máxima da senha para credenciais internas. A idade máxima da senha para credenciais do Windows deve ser gerenciada usando uma política do Windows.

Consulte [“Para desbloquear credenciais bloqueadas”](#) na página 113.

Você precisa especificar condições apropriadas de bloqueio da senha para impedir o acesso não autorizado ao Symantec Management Platform. Todas as alterações que você fizer às configurações de bloqueio da senha serão aplicadas a todas as tentativas subsequentes de logon com falhas. A configuração do máximo de tentativas malsucedidas permitidas não se aplica ao número de tentativas anteriores de logon com falhas.

Para definir configurações de complexidade e bloqueio da senha

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Configurações de senha**.

3 Na página **Configurações de senha**, na guia **Complexidade da senha**, defina as configurações de complexidade da senha:

Permitir senhas em branco	Permite especificar se uma credencial pode ter uma senha vazia. Se você ativar esta configuração, o comprimento mínimo da senha será desativado. Por padrão, esta configuração está desativada.
Comprimento mínimo da senha	Permite especificar o número mínimo de caracteres que a senha deve conter. Se desejar definir o comprimento como zero (0), será necessário também ativar a configuração Permitir senhas em branco. O valor padrão é seis (6).
Número mínimo de caracteres não alfabéticos	Permite especificar o número mínimo de caracteres não alfabéticos que a senha deve conter. Os caracteres não alfabéticos são números (como 1, 2, 3 etc.) e caracteres especiais (como!, ?, & etc.) O valor padrão é um (1).
Conter nome da conta	Permite especificar se a senha pode conter o nome de conta do usuário. Observe que esse parâmetro não diferencia maiúsculas e minúsculas. Por padrão, esta configuração está desativada.

- Na página **Configurações de senha**, na guia **Bloqueio de senha**, especifique as condições apropriadas de bloqueio da senha:

Ative o bloqueio de credenciais	Especifica se deverão ser bloqueadas as credenciais quando o número máximo especificado de tentativas malsucedidas de logon for atingido. Por padrão, esta configuração está ativada.
Limite interno de bloqueio da credencial	Especifica o número máximo de tentativas de logon que um usuário pode fazer com qualquer credencial específica. Se um usuário tentar a autenticação com uma senha incorreta mais do que o número de vezes especificado, a credencial será bloqueada durante o período definido de bloqueio. As tentativas malsucedidas de logon são contadas desde quando as credenciais são criadas. As tentativas com falha não precisam acontecer em um período mínimo de tempo. Não há um tempo máximo depois do qual uma tentativa com falha não é mais contada. Se você alterar esta configuração para reduzir o número máximo de tentativas malsucedidas permitidas, o valor novo não será aplicado a nenhuma conta até a próxima tentativa de logon. Se a próxima tentativa obtiver êxito, a contagem será redefinida a zero (todas as falhas anteriores serão apagadas). Porém, se a próxima tentativa falhar, a contagem de tentativas com falhas será avaliada. Se o número máximo for atingido (ou, possivelmente, já tiver sido excedido), a conta será bloqueada.
Duração do bloqueio	Especifica o período de tempo durante o qual as credenciais bloqueadas não podem ser usadas. O período padrão é 1.800 minutos (30 horas). Todas as tentativas de logon que o usuário fizer durante este período falharão, mesmo se as credenciais corretas forem fornecidas. Quando o período de bloqueio expirar, as mesmas credenciais serão válidas novamente. Não é necessária uma redefinição automática da senha. Você pode especificar um período infinito de bloqueio digitando um valor de -1. Neste cenário, uma credencial bloqueada permanece bloqueada até que um administrador a desbloqueie manualmente. Consulte “Para desbloquear credenciais bloqueadas” na página 113.

- Clique em **Salvar alterações**.

Consulte [“Tarefas de gerenciamento de segurança do Symantec Management Platform”](#) na página 108.

Para desbloquear credenciais bloqueadas

A página **Desbloquear credenciais** permite desbloquear as credenciais internas que foram bloqueadas depois de excedido o número máximo de tentativas malsucedidas de logon.

Consulte [“Para definir as configurações de bloqueio e complexidade da senha”](#) na página 109.

Para desbloquear credenciais bloqueadas

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Desbloquear credenciais**.
- 3 Na página **Desbloquear credenciais**, na lista de credenciais bloqueadas, selecione as credenciais que deseja desbloquear.
- 4 Clique em **Desbloquear credenciais**.

Para acessar o Gerenciador de função de segurança

O Gerenciador de função de segurança é um console especial que permite visualizar e configurar permissões para funções de segurança. O console permite selecionar uma função específica de segurança e visualizar as permissões que são associadas a cada item para a função de segurança. Você pode visualizar os itens por tipo ou visualizar todos os itens disponíveis e selecionar a pasta ou o item em que configurar as permissões. Por padrão, os itens e as pastas filho herdam todas as permissões de uma pasta. Você pode modificar a herança de permissão para atender seus requisitos.

Você também pode usar o Gerenciador de função de segurança para obter propriedade de um item. Talvez seja necessário obter propriedade se as permissões em um item forem removidas acidentalmente de modo que o proprietário não tenha mais acesso a elas. Ao obter a propriedade de um item, você pode redefinir as permissões adequadas e restaurar o acesso para o proprietário original.

Tabela 4-4 Maneiras de acessar o Gerenciador de função de segurança

Opção	Descrição
Diretamente do menu Configurações do Console de gerenciamento Symantec.	O Gerenciador de função de segurança é aberto com sua função de segurança selecionada e com a exibição Todas as classes de dados mostrada.
Do painel direito da página Funções .	O Gerenciador de função de segurança é aberto com a função de segurança apropriada selecionada e com a exibição Todas as classes de dados mostrada.
Do menu Ações para uma função de segurança.	O Gerenciador de função de segurança é aberto com a função de segurança apropriada selecionada e com a exibição Todas as classes de dados mostrada.
Do menu de clique com o botão direito do mouse para um item ou pasta no painel esquerdo.	Você usaria normalmente este método para definir permissões em um item ou pasta específico. O Gerenciador de função de segurança abre com sua função de segurança selecionada e a pasta apropriada selecionada.

Para acessar o Gerenciador de função de segurança através do menu do Console de gerenciamento Symantec

- ◆ No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Permissões**.

Para acessar o Gerenciador de função de segurança para uma função de segurança específica

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 2 No painel esquerdo, clique em **Gerenciamento de conta > Funções**.
- 3 Na página **Funções**, no painel esquerdo, clique na função de segurança que deseja configurar.
- 4 Execute um destes procedimentos:
 - No painel direito, clique em **Mostrar o console do Gerenciador de Função de Segurança**.
 - Clique em **Ações > Gerenciador de função de segurança**.
 - Clique com o botão direito do mouse na função de segurança que você quer configurar e clique em **Gerenciador de função de segurança**.

Para acessar o Gerenciador de função de segurança para uma pasta específica

- 1 No Console de gerenciamento Symantec, abra uma exibição que contenha a pasta em que você quer definir permissões de segurança.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta e clique em **Segurança**.

Para obter a propriedade de uma pasta ou item

Você também pode usar o Gerenciador de função de segurança para obter propriedade de um item. Isso pode ser necessário se as permissões de um item forem removidas acidentalmente de modo que o proprietário não tenha mais acesso a ele. Obtendo propriedade, você pode redefinir as permissões adequadas e restaurar o acesso para o proprietário original.

Para tomar a posse de uma pasta ou de um item, é necessário o privilégio Obter propriedade e a permissão Controle total na pasta ou no item. A função Administrador Symantec tem esse privilégio e essa permissão em todos os itens e pastas.

Consulte [“Para personalizar a herança de permissões”](#) na página 104.

Para obter propriedade de uma pasta ou de um item

- 1 No Gerenciador de função de segurança, no painel esquerdo, selecione a pasta ou o item para o qual você deseja obter propriedade.
- 2 No painel direito, clique em **Avançado**.
- 3 Na janela Permissões para: *Nome do item*, clique em **Obter propriedade**.
- 4 Clique em **Salvar alterações**.
- 5 Clique em **Cancelar** para fechar a janela Permissões para: janela *Nome do item*.

Para gerenciar credenciais

O gerenciador de credenciais fornece um local de armazenamento seguro para nomes de usuário e senhas. As soluções de gerenciamento instaladas definem os tipos de credenciais que o gerenciador de credenciais armazena.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Consulte [“Permissões do Gerenciador de credenciais”](#) na página 509.

O acesso às credenciais é controlado usando a segurança integrada baseada em funções do Symantec Management Platform.

As soluções de gerenciamento normalmente criam credenciais quando elas são necessárias para executar uma tarefa. Para definir uma credencial manualmente, você precisa saber o tipo de credencial usado e as informações necessárias para esse tipo de credencial.

Quando uma credencial for criada, o acesso será concedido apenas ao criador. Editar credenciais permite atualizar a senha e conceder acesso a usuários e grupos adicionais.

Você pode também excluir as credenciais. Antes de excluir uma credencial, certifique-se de que ela não seja necessária como parte de uma tarefa de gerenciamento ativa.

Para criar uma credencial

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Monitoração e alertas > Configurações de credenciais > Gerenciamento de credenciais**.
- 3 No painel direito, clique em **Adicionar credenciais**.
- 4 Na caixa de diálogo **Adicionar credenciais**, selecione um tipo de credencial e forneça os valores necessários.
- 5 Clique em **OK**.

Para editar credenciais

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Monitoração e alertas > Configurações de credenciais > Gerenciamento de credenciais**.
- 3 No painel direito, selecione uma credencial e clique em **Edit**.
- 4 Na caixa de diálogo **Editar credencial**, atualize as credenciais e clique em **OK**.

Para configurar agendas

Este capítulo contém os tópicos a seguir:

- [Como o Symantec Management Platform usa agendamentos](#)
- [Componentes de um agendamento do Symantec Management Platform](#)
- [Para gerenciar agendamentos compartilhados](#)
- [Para configurar um agendamento](#)
- [Para exibir do calendário de agendamento interno do Notification Server](#)

Como o Symantec Management Platform usa agendamentos

O Symantec Management Platform usa agendamentos para tarefas e políticas.

Consulte [“Componentes de um agendamento do Symantec Management Platform”](#) na página 119.

Tabela 5-1 Usos do agendamento

Uso	Descrição
Agenda de tarefas e políticas do servidor	Muitas operações do Symantec Management Platform são agendadas para ocorrer em intervalos regulares. Algumas dessas operações precisam ser executadas frequentemente, como atualizar a associação de grupos e filtros de recursos, outras são menos frequentes, como apagar registros antigos do CMDB. Essas agendas são configuradas geralmente para repetir em intervalos regulares e permanecem ativas por um período indefinido.

Uso	Descrição
Agendamento de tarefas do agente	As agendas podem ser usadas quando você quer executar operações em computadores gerenciados. Por exemplo, instalar um patch para corrigir uma vulnerabilidade em um aplicativo ou coletar o inventário para fins de conformidade. Normalmente, você deseja executar a operação o mais breve possível e deseja executá-la apenas uma vez. Você pode agendar tarefas do agente para serem executadas: ■ Imediatamente ■ Imediatamente, se uma janela de manutenção estiver aberta ■ Na próxima vez em que um usuário fizer logon no computador ■ Na próxima vez em que o computador for ligado. Em algumas ocasiões convém agendar a operação para ocorrer em data e hora específicas. Por exemplo, às 21:00 do próximo domingo, para garantir que a operação não interfira na capacidade do usuário em trabalhar. Em raras ocasiões você pode precisar agendar uma tarefa para que ela seja repetida. Porém, uma operação de repetição seria considerada geralmente uma política baseada em tarefas.
Agendamento de políticas de agente	Uma política de agente é uma indicação sobre como um computador deve ser gerenciado. Por exemplo, uma política de agente pode fazer o seguinte: ■ Não permitir que o software seja executado ■ Exigir que um software seja instalado ■ Exigir que as informações do inventário sobre um computador não sejam mais antigas que N dias Para funcionar corretamente, algumas políticas de agente precisam ser agendadas para serem executadas em intervalos apropriados. Por exemplo, uma política de conformidade do software precisa verificar periodicamente se o computador está em conformidade e executar a correção apropriada caso não esteja. Do mesmo modo, uma política de inventário precisa garantir que os dados de inventário sejam atuais. Estas agendas são geralmente agendamentos recorrentes com uma repetição possível durante o dia de trabalho. As políticas de agente são frequentemente agendadas para serem executadas quando o computador é iniciado ou quando um usuário faz logon. Quando você configura essas agendas, é preciso também considerar como elas interagem com as janelas de manutenção que estão configuradas nos computadores gerenciados. Consulte “Para definir as configurações globais de agentes” na página 277. Consulte “Para definir as configurações do agente de destino” na página 278.

Uso	Descrição
Agenda de janelas de manutenção do agente	Uma agenda da janela de manutenção é essencialmente um agendamento recorrente com uma duração. Você não precisa agendar janelas de manutenção usando a inicialização do computador, o logon do usuário ou os outros eventos. As janelas de manutenção não têm nenhuma necessidade de repetição durante o dia de trabalho. Consulte “Para configurar políticas de janela de manutenção” na página 280.

Componentes de um agendamento do Symantec Management Platform

Os agendamentos do Symantec Management Platform permitem executar operações únicas e repetidas no computador do Notification Server e nos computadores gerenciados em horários apropriados, sem exigir a intervenção manual. Por exemplo, os filtros de recursos precisam ser atualizados frequentemente, o CMDB precisa ser limpo regularmente e os pacotes devem ser atualizados em intervalos apropriados. Todas estas tarefas devem ser agendadas para serem executadas em horários e frequências que melhor atendam às necessidades de sua organização.

Consulte [“Como o Symantec Management Platform usa agendamentos”](#) na página 117.

O Symantec Management Platform utiliza dois tipos de agendamento:

Compartilhada	São definidas no Notification Server como itens compartilhados que estão disponíveis para qualquer operação agendada. Consulte “Para gerenciar agendamentos compartilhados” na página 122.
Personalizar	São configuradas independentemente em cada tarefa, política ou regra agendada. Não podem ser compartilhadas com nenhuma outra tarefa, política ou regra.

Tabela 5-2 Componentes de um agendamento

Componente	Descrição
Período e fuso horário ativos	O período e o fuso horário ativos definem o período de tempo em que uma agenda pode ocorrer. Todas as agendas, acionadores e modificadores têm as seguintes propriedades: Fuso horário O fuso horário em que a tarefa é agendada para executar. O fuso horário pode ser local, Servidor ou UTC. Data de início A data e hora quando o período ativo da agenda inicia. Uma agenda não pode ser acionada antes de sua data de início. Data final A data e hora quando o período ativo da agenda termina. Se a data final não estiver especificada, a agenda permanecerá ativa indefinidamente. Uma agenda não pode ser acionada após sua data final. Um agendamento não pode ser executado fora de seu período ativo. Isto aplica-se mesmo se o agendamento tiver sido acionado dentro de seu período ativo, mas não pôde ser executado naquela hora por um modificador.

Componente	Descrição
Acionadores	Um acionador é um evento que faz com que a agenda se torne ativa. Um acionador pode ser um horário e uma data específicos ou um evento, como um usuário que faça logon em um computador. Os acionadores controlam quando a agenda ocorre e se repete. Se uma agenda contiver vários acionadores, ela será executada cada vez que um de seus acionadores ocorrer. Os acionadores de agendamento podem ter as seguintes propriedades: Exato Determina o comportamento quando uma tarefa agendada não puder ser executada no horário exato em que foi agendada. Se a propriedade estiver definida como verdadeira, a tarefa agendada será executada no horário exato, ou não será executada. Se as condições forem de que a tarefa não pode ser executada no horário agendado exato, a tarefa agendada não será executada. Se a propriedade for definida como falsa, a tarefa agendada será executada no horário exato ou assim que for possível após o horário agendado. Por exemplo, uma tarefa é agendada para ser executada todas as noites às 2:00, mas o computador está sempre desligado nesse horário. A configuração Exata permite executar a tarefa sempre que o computador é ligado após aquele horário. Esta propriedade aplica-se para o logon, a inicialização e outros eventos, bem como aos horários especificados. Duração O período de tempo em que a agenda está ativa. A duração pode ser de até 24 horas. Repetição O intervalo em que a tarefa deve ser repetida durante o período ativo da agenda. O intervalo da repetição pode ser de até 24 horas.

Componente	Descrição
Modificadores	Os modificadores são condições adicionais necessárias para que o agendamento seja acionado. Todos os modificadores aplicam-se a todos os acionadores. - Somente quando um usuário estiver conectado Quando o acionador ocorrer em um computador de destino, o Symantec Management Agent desse computador fará uma verificação para assegurar-se de que um usuário está conectado antes de executar o agendamento. Se nenhum usuário estiver conectado, a agenda não será executada nesse computador. - Apenas quando nenhum usuário estiver conectado Quando o acionador ocorre, o computador de destino é verificado para assegurar-se de que nenhum usuário esteja conectado. Se um usuário estiver conectado, a agenda não será executada nesse computador.

Para gerenciar agendamentos compartilhados

Qualquer número de itens agendados (como políticas, tarefas ou regras de replicação) podem usar um agendamento compartilhado. A alternativa para usar um agendamento compartilhado é de definir um agendamento personalizado na política ou na tarefa.

Consulte [“Componentes de um agendamento do Symantec Management Platform”](#) na página 119.

Os agendamentos compartilhados não podem substituir as janelas de manutenção. Se deseja que um item agendado seja executado fora de uma janela de manutenção, você precisa configurar o agendamento personalizado apropriado.

Um conjunto de agendamentos compartilhados padrão é fornecido no Symantec Management Platform. É possível modificá-los para satisfazer seus requisitos, mas você não pode excluí-los. Por exemplo, é possível configurar o agendamento do horário comercial para ser executado em intervalos regulares durante suas horas normais de funcionamento. Você pode configurar o agendamento de atualização de pacotes para ser executado em um momento apropriado que seja fora das horas de funcionamento. Você também pode criar novos agendamentos compartilhados que sejam necessários e excluí-los quando eles não forem mais necessários.

Você pode ativar ou desativar cada agendamento compartilhado conforme apropriado. Todos os agendamentos compartilhados ativados estão disponíveis a qualquer item agendado. Se você desativar um agendamento compartilhado, os itens agendados que usam o agendamento serão desativados.

Consulte [“Para exibir do calendário de agendamento interno do Notification Server”](#) na página 124.

Para gerenciar agendamentos compartilhados

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Notification Server > Agendamentos compartilhados**.
- 2 Na página **Agendamentos compartilhados**, execute um dos seguintes procedimentos:

Para adicionar um novo agendamento

Clique em **Adicionar agendamento** e, em seguida, no Editor de agendamento, especifique os detalhes apropriados.

Consulte [“Para configurar um agendamento”](#) na página 123.

Para editar um agendamento

Clique no nome do agendamento e, no Editor de agendamento, especifique os detalhes apropriados.

Consulte [“Para configurar um agendamento”](#) na página 123.

Para ativar um agendamento

Marque a caixa de seleção apropriada. Se deseja desativar o agendamento, limpe a caixa de seleção.

Para excluir um agendamento

No final da linha apropriada, à direita, clique em **Excluir**.

Para ver quais itens usam atualmente um agendamento

Na lista suspensa **Itens usando no momento**, selecione o agendamento apropriado.

Os nomes de todos os itens (como tarefas, políticas e regras de replicação) que usam o agendamento selecionado serão mostrados no painel inferior.

Para configurar um agendamento

O **Editor de agendamento** permite configurar um agendamento para atender a seus requisitos.

Consulte [“Componentes de um agendamento do Symantec Management Platform”](#) na página 119.

Consulte [“Para gerenciar agendamentos compartilhados”](#) na página 122.

Para configurar um agendamento

- 1 Na janela **Editor de agenda**, na caixa de diálogo **Nome**, digite o nome da agenda.
- 2 Em **Agendar tarefa**, selecione o acionador ou a frequência do agendamento.

- 3 Na guia **Detalhes**, especifique o horário de início da agenda e os dias, as semanas ou os meses nos quais executá-lo.
- 4 Se deseja que a agenda esteja ativa em uma faixa específica de datas, na guia **Avançado** especifique as datas apropriadas de início e de término.
Por padrão, uma nova agenda é ativada assim que for criada (a partir da data atual). A agenda permanece ativa indefinidamente (nenhuma data final é especificada).
- 5 Se deseja que a agenda repita uma tarefa em intervalos regulares sempre que a agenda for executada, na guia **Avançado**, marque **Repetir tarefa**.
Especifique a frequência e a duração apropriadas.
- 6 Se deseja que esta agenda contenha várias agendas, marque **Usar agendas múltiplas**.
- 7 Para cada agenda adicional que você deseja adicionar a esta agenda, clique em **Nova** e conclua as etapas de [2](#) a [5](#).
- 8 Clique em **OK**.

Para exibir do calendário de agendamento interno do Notification Server

Você pode exibir as informações da agenda do Notification Server no calendário de agenda interna. Os itens agendados que você pode exibir no calendário incluem as tarefas que são executadas no Notification Server, políticas e em políticas de automação. Incluem também agendamentos compartilhados, períodos de bloqueio, janelas de manutenção e agendamentos internos do Notification Server. As soluções da Symantec podem acrescentar itens agendados adicionais ao calendário.

Consulte [“Componentes de um agendamento do Symantec Management Platform”](#) na página 119.

Os seguintes tipos de itens agendados são exibidos:

Itens de período	Definem somente um horário de início e são executados por um período indefinido. Os exemplos incluem janelas de manutenção, períodos de bloqueio e agendas compartilhadas.

Itens de evento	Têm um horário de término definido. Os exemplos incluem tarefas, trabalhos, agendas personalizadas e políticas. Observe que as políticas não estão sempre em execução nos horários mostrados no calendário. As políticas não são tão determinadas quanto as tarefas; assim, podem estar sujeitas a atraso. Tarefas e trabalhos são sempre executados nos horários exibidos no calendário.

A exibição Calendário permite verificar que agendas estão configuradas por períodos de tempo determinados, como dias, semanas ou meses específicos. Nas exibições Semana e Mês, você pode clicar em um dia específico para abrir a exibição Dia para o dia determinado.

Alguns itens agendados usam agendas compartilhadas, em vez de definirem suas próprias agendas. As relações compartilhadas de agendamento são representadas no painel esquerdo da exibição Dia. Os itens agendados são agrupados no agendamento compartilhado a que se referem.

Cada agenda tem um símbolo associado que a liga à página de configuração apropriada, caso uma esteja disponível. Você pode clicar no símbolo para fazer uma busca detalhada na página de configuração, que abre em uma janela nova. Se nenhuma página de configuração estiver disponível para uma agenda, o símbolo padrão do calendário é usado e nenhuma funcionalidade de busca detalhada existirá.

Consulte [“Para gerenciar agendamentos compartilhados”](#) na página 122.

Consulte [“Para configurar um agendamento”](#) na página 123.

Para exibir o calendário da agenda do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server** e clique em **Calendário de agendamentos internos**.
- 3 Na exibição **Exibição de calendário para agendamentos internos do NS**, na lista suspensa **Exibir**, selecione a exibição que você deseja usar.

- 4 Selecione o período de tempo que você deseja exibir clicando no símbolo apropriado:

Dia	Mostra os detalhes de cada agendamento que é executado uma ou mais vezes por dia. As agendas são listadas em ordem de seus horários de início. O painel esquerdo lista as agendas e o painel direito mostra suas ocorrências no calendário. A exibição Dia é a padrão. Cada ocorrência de um item de período é exibida em forma de diamante. Cada ocorrência de um item de evento é exibida normalmente como uma barra, mas aquelas que ocorrem em intervalos muito curtos são exibidas como diamantes pequenos. Para maior clareza na tela, os eventos com um intervalo inferior a 15 minutos (por padrão) são omitidos. A cor em segundo plano identifica o horário comercial definido para a organização.
Semana	Mostra os detalhes de cada agendamento que é executado menos de uma vez por dia, mas ao menos uma vez por semana.
Mês	Mostra os detalhes de cada agendamento que é executado menos de uma vez por semana. Os itens de período são omitidos e os itens de evento são resumidos a seus horários de início, horários de final e títulos.

- 5 Para exibir períodos de tempo anteriores ou posteriores, clique em **Voltar** ou **Avançar**, aquele que for apropriado.

Para configurar sites e servidores de sites

Este capítulo contém os tópicos a seguir:

- [Sobre os serviços de site](#)
- [Sobre a manutenção de sites](#)
- [Para gerenciar sites](#)
- [Para gerenciar servidores de sites](#)
- [Para atribuir um servidor de sites a um site manualmente](#)
- [Para gerenciar agentes atribuídos manualmente](#)
- [Para gerenciar sub-redes](#)
- [Sobre como definir as configurações do serviço de site](#)
- [Para configurar definições do serviço de pacotes](#)
- [Para definir configurações do serviço de tarefas](#)

Sobre os serviços de site

O Symantec Management Platform pode hospedar diversos tipos de componentes de middleware, tais como servidores de pacotes, servidores de tarefas e servidores de inicialização. Os componentes do Middleware podem ser instalados em computadores diferentes do computador do Notification Server. Estes serviços atuam como o primeiro ponto de contato para os Symantec Management Agents, assim reduzindo a carga no Notification Server.

O nome oficial para um componente de middleware é “serviço de site.” Todo o computador que hospeda um serviço de site é conhecido como um servidor de sites. Um servidor de sites pode ter um ou mais serviços de site instalados nele. Por exemplo, se você instalar o serviço de site do serviço do pacote (o “serviço de pacotes”) em um computador, esse computador se tornará um servidor de sites.

Servidores de sites podem ajudar o Notification Server. Servidores de sites podem estender a arquitetura, melhorar a eficiência da distribuição e reduzir requisitos da largura de banda da rede.

O Notification Server controla a implementação, a configuração e a manutenção contínua dos serviços de site. Os serviços de pacotes, de tarefas e de inicialização fornecem aos Symantec Management Agents os pacotes, as tarefas e os broadcasts de PXE.

O Notification Server executa as seguintes funções para o gerenciamento do site:

- Controla a implementação e a remoção de serviços de site e dos servidores de sites
- Garante que o serviço de site seja instalado somente nos computadores que atendem aos requisitos mínimos do sistema

Você usa a manutenção do site para criar grupos lógicos de endpoints para equilibrar a carga em servidores de sites. Por exemplo, é possível distribuir pacotes eficientemente a seus Symantec Management Agents com vários servidores de pacotes. Os servidores de pacotes controlam a maioria das funções de distribuição de pacotes, o que libera o Notification Server para executar outras atividades.

Consulte [“Sobre a manutenção de sites”](#) na página 128.

Sobre a manutenção de sites

A manutenção de sites é o gerenciamento dos sites, sub-redes e serviços de site em sua organização. Você pode gerenciar seus computadores de acordo com o site e a sub-rede, o que permite controlar grupos de computadores ao mesmo tempo que minimiza o consumo da largura de banda. Um site é tipicamente um local físico em sua organização (tal como um edifício específico ou um andar de um edifício). Uma sub-rede é uma faixa de endereços lógicos em sua rede.

Sob condições normais de funcionamento cada servidor de pacotes ou servidor de tarefas presta serviços de manutenção apenas aos Symantec Management Agents que existem nos sites atribuídos. Se nenhum site foi definido, todos os servidores de sites estarão disponíveis para hospedar todos os Symantec Management Agents (embora este método não seja recomendado).

Se nenhum site for definido para um servidor de pacotes ou um servidor de tarefas, o Notification Server usa as seguintes regras:

- O Notification Server tenta primeiro encontrar todos os servidores de sites na mesma sub-rede que o computador da solicitação. Se algum for encontrado, este servidor de sites será retornado ao Symantec Management Agent.
- Se nenhum servidor de sites for encontrado na mesma sub-rede que o computador da solicitação, todos os servidores de sites serão retornados ao Symantec Management Agent.
- Se nenhum servidor de sites estiver disponível, o agente será dirigido para o computador do Notification Server.

Você pode atribuir servidores aos sites usando os seguintes métodos:

- Atribuir a sub-rede que contém o servidor de sites a um site.
Consulte [“Para gerenciar sub-redes”](#) na página 135.
- Atribuir o servidor de sites a um site.
Consulte [“Para atribuir um servidor de sites a um site manualmente”](#) na página 133.
- Usar o Conector do Active Directory para executar a tarefa.
O Conector do Active Directory substitui todas as sub-redes e sites que entram em conflito com ele. Por exemplo, se você atribuir manualmente sub-redes a um site que esteja em conflito com o que está no Conector do Active Directory, as informações do Active Directory serão usadas.

Depois que a lista de servidores de sites disponíveis é retornada ao Symantec Management Agent, o agente escolhe o servidor de sites mais apropriado.

Servidores de sites e computadores gerenciados podem ter vários NIC e endereços IP; portanto, podem pertencer a mais de um site com a atribuição da sub-rede.

Consulte [“Sobre os serviços de site”](#) na página 127.

Consulte [“Para gerenciar sites”](#) na página 129.

Consulte [“Para gerenciar servidores de sites”](#) na página 131.

Consulte [“Para gerenciar sub-redes”](#) na página 135.

Para gerenciar sites

Você precisa configurar todos os sites necessários de sua organização. Você pode executar uma regra de importação de site para coletar automaticamente as informações do site para sua organização pelo Active Directory. Você também pode criar sites manualmente e atribuir sub-redes e servidores de sites apropriados a eles.

Para gerenciar sites

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 Execute uma das seguintes opções:

Criar um site novo	1 No painel esquerdo, clique em Novo(a) > Site. 2 Na janela Novo site, na caixa Nome, digite o nome do novo site. 3 Se você quiser atribuir imediatamente sub-redes ao site, especifique as sub-redes apropriadas. 4 Clique em OK.
Modificar um site	1 No painel esquerdo, selecione o site que você deseja modificar e clique em Configurar. 2 Se desejar mudar o nome do site, na janela Editar site, na caixa Nome, digite o novo nome. 3 Para mudar a sub-redes que estão atribuídas ao site, especifique as sub-redes apropriadas. 4 Clique em OK.
Excluir um site	No painel esquerdo, selecione o site que você deseja excluir e clique em Excluir. Nenhuma sub-rede atribuída ao site é excluída. Elas não estão designadas e podem ser designadas a um site diferente. Nenhum servidor de sites dentro das sub-redes afetadas é usado até que ele seja atribuído a um site diferente.
Remover um servidor de sites manualmente atribuído de um site	No painel esquerdo, no servidor de sites, selecione o site que você deseja remover e clique em Excluir. O servidor de sites não é afetado e continua a servir todos os outros sites aos quais foi atribuído. Essa opção se aplica somente aos servidores de sites que são atribuídos manualmente aos sites. Um servidor de sites que pertença a um site por meio de sua participação na sub-rede não pode ser removido desse site.

Remover uma sub-rede de um site No painel esquerdo, no site, selecione a sub-rede que você deseja excluir e clique em **Excluir**.

Excluir uma sub-rede faz com que ela não seja designada a site algum. Quaisquer sub-redes abrangidas que não forem designadas manualmente a um site também se tornarão não designadas. Quaisquer servidores de sites na sub-rede ou sub-redes abrangidas não servem mais o site. Porém, eles continuam servindo a todos os sites a que foram atribuídos manualmente.

Gerenciar agentes atribuídos manualmente Você pode atribuir agentes a um site e remover os que não forem mais necessários.

Consulte [“Para gerenciar agentes atribuídos manualmente”](#) na página 134.

Para gerenciar servidores de sites

Você precisa criar todos os servidores de sites necessários em sua organização e atribuí-los aos sites apropriados. Para criar servidores de sites, selecione os computadores que você quer usar e especifique os serviços de site que deseja instalar em cada um. Você também pode modificar servidores de sites existentes adicionando ou removendo serviços do site. O Notification Server distribui os pacotes de instalação apropriados aos computadores selecionados e remove os que não forem mais necessários. Observe que as alterações serão feitas quando os Symantec Management Agents nos computadores de destino fizerem suas próximas solicitações de configuração, o que pode não acontecer imediatamente.

Para assegurar-se de que os serviços de site estejam instalados e configurados corretamente, a Symantec recomenda que você instale os serviços de site com o Console de gerenciamento Symantec.

Nota: O computador do servidor de tarefas deve ter o IIS 6.0 ou o IIS 7.0 e recurso .NET Framework 3.5 ativado.

Quando um servidor de sites for selecionado, a página Serviços do site mostrará as estatísticas de cada serviço do site que estiver instalado nela. A exibição recolhida mostra detalhes de resumo enquanto a exibição expandida abre um painel para cada serviço de site que mostra detalhes completos e informações gráficas. Cada painel de serviço do site inclui também um link para a página correspondente de configurações globais.

A barra de título de cada serviço de site contém um símbolo que mostra seu status atual:

Verde	O serviço está instalado e executando no servidor de sites.
Amarelo	O serviço não está instalado atualmente no servidor de sites.
Laranja	O serviço está em um estado de aviso.
Vermelho	O serviço não pode ser usado. Um pacote é inválido.

Para gerenciar servidores de sites

1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.

2 Execute uma das seguintes opções:

Criar um servidor de sites

1 No painel esquerdo, clique em **Novo(a) > Site Server**.

2 Na janela **Selecionar computadores**, selecione os computadores aos quais você quer adicionar os serviços de site e clique em **OK**.

A lista no painel esquerdo contém todos os computadores que estão disponíveis para serem usados como servidores de sites. Quando instalar o Symantec Management Platform, você precisará aguardar alguns minutos para que o sistema preencha esta lista.

3 Na caixa de diálogo **Adicionar/remover serviços**, selecione as caixas de seleção apropriadas para selecionar os serviços de site que você quer instalar em cada servidor de sites e clique em **Avançar**.

Todos os serviços de site disponíveis são relacionados em cada computador, permitindo que você selecione qualquer combinação de serviços para cada computador. As caixas de seleção para quaisquer tipos de serviço cuja instalação não seja permitida em um computador específico estarão em cinza. Você pode agrupar a lista por servidores de sites ou por serviços. Ao selecionar um nó pai na lista, você seleciona todos os seus filhos.

Se qualquer caixa de seleção já estiver selecionada, isso indicará que o serviço de site correspondente já está instalado. Se deseja removê-lo, desmarque a caixa de seleção.

4 Clique em **OK**.

Modificar um servidor de sites	1	Na tabela Informações detalhadas , assegure-se de que a exibição de servidores de sites esteja selecionada e escolha o servidor de sites apropriado.
	2	Clique no símbolo de Editar .
Atribuir manualmente um servidor de sites a um site		Selecione o servidor de sites apropriado e clique em Atribuir ao site .
		Consulte “Para atribuir um servidor de sites a um site manualmente” na página 133.
Remover um servidor de sites manualmente atribuído de um site		No painel esquerdo, no servidor de sites, selecione o site que você deseja remover e clique em Excluir .
		O servidor de sites não é afetado e continua a servir todos os outros sites aos quais foi atribuído. Essa opção se aplica somente aos servidores de sites que são atribuídos manualmente aos sites. Um servidor de sites que pertença a um site por meio de sua participação na sub-rede não pode ser removido desse site.

Vídeo: para obter mais informações sobre a instalação de um servidor de tarefas, consulte [Rolling out a Task Server with ITMS Video - Part 1, Windows XP \(em inglês\)](#) e [Rolling out a Task Server with ITMS Video - Part 2, Windows 2008 R2 \(em inglês\)](#) no Symantec Connect.

Para atribuir um servidor de sites a um site manualmente

Servidores de sites servem automaticamente ao site para o qual sua sub-rede principal está atribuída. Servidores de sites podem ter vários NIC/IPs e estar em mais de uma sub-rede e, conseqüentemente, podem pertencer a mais de um site. Você também pode atribuir manualmente cada servidor de sites a um ou mais sites. A coluna Atribuído manualmente na tabela Informações detalhadas indica se o servidor de sites foi atribuído manualmente ao site.

Consulte [“Para gerenciar servidores de sites”](#) na página 131.

Quando você atribui manualmente um servidor de sites a um site, somente o servidor de sites é atribuído ao site selecionado. A sub-rede que inclui o servidor de sites não é afetada.

Para atribuir manualmente um servidor de sites a um site

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 Na tabela **Informações detalhadas**, assegure-se de que a exibição do servidor de sites esteja selecionada e escolha os servidores de sites apropriados.
- 3 Clique em **Atribuir ao site**.
- 4 Na janela **Selecione um site**, escolha o site ao qual você deseja atribuir o servidor de sites.
- 5 Clique em **OK**.

Para gerenciar agentes atribuídos manualmente

Um agente atribuído manualmente é um computador cuja atribuição a um site é feita de modo manual e não através de sua sub-rede. Convém atribuir manualmente computadores específicos a um site para não precisar realizar a atribuição de sub-rede. Você pode atribuir manualmente novos agentes a um site, atribuindo os destinos de recursos relevantes ao site. É possível remover todos os agentes que você não deseja no site, atribuindo os destinos de recursos apropriados a um site diferente.

Nota: Quando o agente atribuído manualmente for um servidor de tarefas, a mudança não será formalizada a menos que você redefina o Symantec Management Agent no computador. Uma maneira de redefinir o Symantec Management Agent é clicar em **Redefinir agente**, na guia **Status da tarefa** do Symantec Management Agent. Outra forma é executar a tarefa Redefinir Task Agent no computador.

Para gerenciar agentes atribuídos manualmente

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 No painel esquerdo, expanda o site ou o Servidor de sites que você deseja modificar e clique em **Agentes atribuídos manualmente**.
- 3 Na página **Agentes atribuídos manualmente**, faça qualquer uma das seguintes ações:

Adicionar agentes atribuídos manualmente a um site	Clique em Nova e, na janela Selecione um grupo, selecione ou crie os destinos de recursos apropriados. Consulte “Seleção de destinos de recurso nomeados” na página 386.
Atribuir novamente os agentes atribuídos manualmente a outro site	Esta opção está disponível somente no nó Site, não no nó Serviços de site. Selecione os destinos de recursos apropriados e clique em Atribuir ao site. Na janela Selecione um site, selecione o site apropriado e clique em OK.
Remover agentes atribuídos manualmente de um site	Selecione os destinos de recursos apropriados e clique em Excluir.

Para gerenciar sub-redes

Você precisa criar todas as sub-redes em sua organização e atribuí-las aos sites apropriados. Você pode ressincronizar as sub-redes quando necessário e excluir todas as sub-redes que não mais existirem.

As sub-redes podem ser determinadas nos dados do inventário básico que são importados do Active Directory ou adicionados manualmente. Você pode executar uma regra de importação da sub-rede para coletar automaticamente as informações da sub-rede do Active Directory.

As sub-redes sempre têm no sufixo o número de bits definido na máscara da rede; por exemplo, 192.168.0.0/24. As sub-redes são exibidas sempre em uma árvore hierárquica. O escopo do recurso é aplicado para que você possa ver somente as sub-redes que contêm os recursos aos quais você tem acesso.

Você precisa atribuir cada sub-rede ao site apropriado. Por padrão, todas as sub-redes abrangidas (uma sub-rede cujo intervalo de IP está contido completamente dentro de outra sub-rede) são atribuídas automaticamente ao mesmo site. Porém, você pode manualmente substituir a abrangência da sub-rede, atribuindo explicitamente uma sub-rede abrangida a um site diferente. Por padrão, as sub-redes abrangidas são exibidas em suas sub-redes principais no painel esquerdo. Porém, quando uma sub-rede abrangida for atribuída manualmente a um site diferente de seu pai, ela será exibida no site ao qual está atribuída.

Todos os servidores de sites em uma sub-rede são atribuídos automaticamente ao mesmo site que a sub-rede. Esta atribuição não será desfeita se você atribuir manualmente um servidor de sites a um site diferente. Um servidor de sites pode ser atribuído manualmente a qualquer número de sites, além do site que servir por meio de sua atribuição da sub-rede.

Para gerenciar sub-redes

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 Execute uma das seguintes opções:

Criar uma nova sub-rede

- 1 No painel esquerdo, clique em **Novo(a) > Sub-rede**.
- 2 Na caixa de diálogo **Nova sub-rede**, especifique o endereço de rede da sub-rede, a máscara da sub-rede, o site ao qual você quer atribuir esta sub-rede, e clique em **OK**.

Quando você pressionar **Tab** ou clicar nesta caixa de diálogo após ter digitado o endereço de rede da sub-rede, uma máscara será selecionada automaticamente de acordo com as seguintes regras:

- O sistema examina o primeiro octeto de um endereço IPv4 para determinar se ele é uma sub-rede de classe A, B ou C. Assim, ele seleciona a máscara padrão apropriada.
- Se o endereço de rede for mais específico (isto é, octeto diferente de zero) do que o permitido para essa classe, os bytes adicionais serão definidos na máscara padrão.
- Se o endereço não estiver em um formato reconhecido, ou o último octeto for diferente de zero, nenhuma máscara padrão será sugerida.

Você pode editar a máscara padrão manualmente, caso necessário. Observe que depois de editar manualmente a máscara da sub-rede, atualizar o endereço da rede na caixa **Sub-rede** não atualizará mais a máscara.

Excluir uma sub-rede

No painel esquerdo, o expandir **Gerenciamento de site > Sub-redes**, selecione a sub-rede que você quer excluir e clique em **Excluir**.

Se excluir uma sub-rede que você criou manualmente, ela será excluída permanentemente. Porém, todas as sub-redes importadas do inventário básico ou do Active Directory são restauradas quando os dados são atualizados.

Atribuir uma sub-rede a um site

- 1 No painel esquerdo, expanda **Gerenciamento de site** e clique em **Sub-redes**.
- 2 No painel direito, selecione a sub-rede apropriada e clique em **Atribuir ao site**.
- 3 Na caixa de diálogo **Selecione um site**, selecione o site ao qual você quer atribuir a sub-rede e clique em **OK**.

Ressincronizar
sub-redes

1 No painel esquerdo, expanda **Gerenciamento de site** e clique em **Sub-redes**.

2 No painel direito, clique em **Ressincronizar sub-redes**.

O Notification Server consulta o CMDB para obter as informações atuais da sub-rede. Ele lê a atribuição da sub-rede incluída nos resultados da verificação mais recente do inventário do agente. Assim, o Notification Server atualiza a lista de sub-redes de maneira apropriada.

Sobre como definir as configurações do serviço de site

As configurações do serviço de site são geralmente as configurações globais padrão. Todas as mudanças que você fizer nas configurações para um tipo específico de serviço de site serão aplicadas a todos os serviços de site daquele tipo. Porém, é possível que alguns tipos de serviço de site tenham configurações que possam ser definidas em serviços individuais, substituindo os padrões globais. Por exemplo, cada servidor de pacotes pode ser configurado como Com restrição ou Sem restrição, substituindo a configuração padrão.

Você pode exibir e modificar as configurações globais para cada serviço de site. Cada serviço de site, como servidores de pacotes, tem uma página que permite editar suas configurações globais.

No painel esquerdo, os serviços instalados são mostrados abaixo de cada servidor de sites. A página correspondente mostra o resumo de serviço do servidor de sites. O painel é expandido por padrão em vez de estar recolhido para estatísticas como na página do servidor de sites. O link Alterar configurações permite editar as configurações globais para esse tipo de serviço.

Para muitos serviços, as informações resumidas mostradas aqui podem ser as mesmas informações resumidas e expansíveis na página do servidor de sites. Porém, o Symantec Management Platform permite que um serviço forneça um controle diferente neste contexto, se apropriado. Por exemplo, se houver uma página completa de dados disponíveis, ela será exibida na página do serviço de site. Um conjunto de dados resumidos é exibido na página do servidor de sites.

Consulte [“Para configurar definições do serviço de pacotes”](#) na página 139.

Consulte [“Para definir configurações do serviço de tarefas”](#) na página 139.

Consulte os tópicos sobre o serviço de monitoração no *Guia do Usuário do Monitor Solution*.

Para configurar definições do serviço de pacotes

É necessário definir as configurações globais do serviço de pacotes. Estas configurações são aplicadas a todos os serviços de pacotes que são instalados em servidores de sites em seu Symantec Management Platform.

Para definir as configurações do serviço de pacotes

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 No painel esquerdo, expanda **Configurações > Serviço de pacote** e clique em **Configurações do serviço de pacotes**.
- 3 Na página **Configurações do serviço de pacotes**, defina as configurações apropriadas:

Para definir as configurações globais do serviço de pacotes No painel **Configurações globais do serviço de pacotes**, faça as mudanças necessárias.

Para obter mais informações, clique na página e pressione **F1**.

Para configurar servidores de pacotes sem restrição No painel **Seleção de servidor do Servidor de pacote com limites**, configure cada servidor de pacotes marcando ou desmarcando a caixa de seleção Limitados, conforme for apropriado.

Você pode usar a lista suspensa Site para exibir as informações resumidas sobre todos os servidores de pacotes em um site específico ou em todos os sites.

- 4 Clique em **Salvar alterações**.

Para definir configurações do serviço de tarefas

Você pode aplicar as configurações do serviço de tarefas aos servidores de tarefas usados por computadores, usuários ou recursos. O Notification Server aplica essas configurações aos serviços de tarefas escolhidos que estão instalados nos Site Servers em seu ambiente.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para definir configurações do serviço de tarefas

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 No painel esquerdo, expanda **Configurações > Task Service > Configurações** e clique em **Configurações do Task Service**.
- 3 Na página **Configurações do Task Service**, defina as configurações apropriadas.

Para obter mais informações, clique na página e pressione **F1**.

- 4 No painel **Aplicado a**, clique em **Aplicar a** para selecionar os computadores, usuários ou recursos aos quais essas configurações do serviço de tarefas se aplicam.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Estas configurações se aplicam aos serviços de tarefas usados por esses computadores, usuários ou recursos.

- 5 Clique em **Salvar alterações**.

Para configurar o servidor de pacotes para Linux

Este capítulo contém os tópicos a seguir:

- [Sobre o servidor de pacotes para Linux](#)
- [Sobre a integração do Apache Web Server com o servidor de pacotes para Linux](#)
- [Sobre a detecção do Apache Web Server](#)
- [Requisitos para configurar o servidor de pacotes e o Apache Web Server](#)
- [Requisitos para configurar o HTTPS e o HTTP](#)
- [O exemplo da configuração de servidor de pacotes que usa o diretório da Web principal para os links de servidor de pacotes](#)
- [Exemplo de configuração do servidor de pacotes que usa um alias para os links do servidor de pacotes](#)

Sobre o servidor de pacotes para Linux

Para designar um computador Linux como um servidor de pacotes, assegure-se de que o computador esteja executando o seguinte software:

- Symantec Management Agent para UNIX, Linux e Mac
Este agente era previamente conhecido como o agente Altiris para UNIX e Linux.

O Symantec Management Agent para UNIX, Linux e Mac é executado em um computador gerenciado. Esse agente deve corresponder à versão do agente que está instalada no computador do Notification Server no Symantec Management Platform. Se o agente no computador gerenciado for mais antigo

do que o agente no Notification Server, faça seu upgrade. Após fazer o upgrade do agente, o computador gerenciado pode tornar-se um servidor de pacotes.

- Apache Web Server versão 2.0 ou 2.2
 Consulte [“Sobre a integração do Apache Web Server com o servidor de pacotes para Linux”](#) na página 142.

As seguintes plataformas de servidor são suportadas:

- Red Hat Enterprise Linux Server 5
- Red Hat Enterprise Linux Server 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11 SP1, 11 SP2

O servidor de pacotes para Linux suporta locais alternativos de download. Os caminhos para locais alternativos são convertidos automaticamente do estilo Windows para UNIX se você incluir a barra à direita. Por exemplo, se você tiver o Patch Management Solution instalado, será possível mudar as configurações de política e pacote ao instalar patches. No Symantec Management Console, em **Configurações > Todas as configurações > Software > Gerenciamento de patches**, você clica em uma página de configurações do fornecedor; por exemplo, você clicaria em **Configurações do Red Hat > Configurações de correção do patch do Red Hat**. Quando você clicar na guia **Configurações de políticas e pacotes**, você verá a página **Configurações de correção** para o produto selecionado. Este é o lugar onde você pode marcar **Usar local de download alternativo no Servidor de pacotes**. Quando você digitar o local alternativo de download, será necessário usar o caminho completo do Windows. Nessas e em instâncias semelhantes, inclua uma barra à direita no caminho do estilo Windows para garantir que ele seja convertido corretamente em um caminho do estilo UNIX.

Correto:	A barra à direita significa que o caminho do Windows é convertido corretamente em /path/.
C:\path\	
Incorreto:	Se você omitir a barra à direita, o caminho do Windows será convertido incorretamente.
C:\path	

Sobre a integração do Apache Web Server com o servidor de pacotes para Linux

Você integra o servidor de pacotes para Linux ao Apache Web Server para expor pacotes e capturas de imagem de pacotes ao Symantec Management Agent. As capturas de imagem são obtidas por download do Notification Server para o

Symantec Management Agent em todas as plataformas suportadas através de URLs do HTTP.

Consulte [“Sobre o servidor de pacotes para Linux”](#) na página 141.

É sempre feito download dos pacotes e das capturas de imagem para diretórios do servidor de pacotes. Os únicos arquivos que são criados no Apache Web Server são diretórios, links simbólicos e arquivos .htaccess. Os links simbólicos são criados para os arquivos de pacote e da captura de imagem. Os arquivos .htaccess bloqueiam os arquivos de pacote com senhas.

Quando um computador Linux se tornar um servidor de pacotes, o agente desse computador tentará criar dois compartilhamentos principais de HTTP.

Esses compartilhamentos são criados no espaço virtual da Web do Apache Web Server da seguinte forma:

- /Altiris/PS/Snapshots
 - /Altiris/PS/Packages Note /Altiris/PS
- Este segundo diretório é criado se necessário.

O arquivo de manifesto do pacote não será usado quando um servidor de pacotes para Linux fizer o download de um pacote para a distribuição. A exceção é se o pacote está localizado no mesmo diretório do servidor de pacotes para Linux e entrega de software. Todas as permissões do arquivo de pacote são definidas para permitir o acesso de clientes ao Apache Web Server. Esse acesso é tipicamente com 0x744.

Dependendo da configuração específica do Apache Web Server, diretórios são criados na raiz do diretório da Web. Um exemplo é /var/www/html em um sistema típico do Linux Red Hat. O Package Server Agent lê o arquivo de configuração do Apache Web Server para determinar este local.

Consulte [“Sobre a detecção do Apache Web Server”](#) na página 143.

Se você escolher, é possível especificar que o servidor de pacotes crie os diretórios em um local alternativo. Use uma diretriz do alias do Apache Web Server para especificar um diretório separado.

Consulte [“Requisitos para configurar o servidor de pacotes e o Apache Web Server”](#) na página 145.

Consulte [“Requisitos para configurar o HTTPS e o HTTP”](#) na página 146.

Sobre a detecção do Apache Web Server

Você pode detectar o Apache Web Server automaticamente ou manualmente.

Consulte [“Sobre a integração do Apache Web Server com o servidor de pacotes para Linux”](#) na página 142.

Consulte [“Requisitos para configurar o servidor de pacotes e o Apache Web Server”](#) na página 145.

Se você escolher a Detecção automática, o Symantec Management Agent procurará o Apache HTTPD ou HTTPD2 executável nos seguintes locais de diretório:

- /bin:/usr/bin:/sbin:/usr/sbin:/usr/sbin:/usr/etc:/etc:/usr/bsd:/usr/local/bin:/usr/contrib/bin/
- Variável de CAMINHO do sistema
- /opt/apache/bin:/usr/apache/bin:/usr/apache2/bin:/usr/local/apache/bin:/usr/local/apache2/bin:/usr/local/bin:/opt/freeware/apache/bin:/opt/freeware/apache2/bin:/opt/freeware/apache/sbin:/opt/hpws/apache/bin:/opt/apache2:/usr/local/apache+php

Se ambos os executáveis HTTPD e HTTPD2 forem encontrados, tanto o Apache 2.0 e Apache 2.2 serão instalados.

Além disso, se ambos os arquivos executáveis forem encontrados, o arquivo que corresponde a um processo em execução será usado. O arquivo padrão é HTTPD2.

Se o Apache Web Server não puder ser detectado automaticamente, poderá ser necessário detectá-lo manualmente. O Apache Web Server poderá não ser detectado automaticamente se o arquivo executável for renomeado. Se várias instalações tiverem ocorrido, o Apache Web Server errado poderá ser detectado. Em qualquer uma dessas situações, é necessário especificar manualmente o local do Apache Web Server.

Para especificar o Apache Web Server manualmente, será necessário editar a seção **[httpd Integration]** do arquivo client.conf no agente. Nesta seção, é necessário especificar a configuração do “apache_exe_location”.

Quando o Apache Web Server executável for localizado, ele será usado para determinar o local padrão do arquivo de configuração do Apache Web Server. O arquivo de configuração é necessário para determinar se a configuração do Apache Web Server é apropriada para o uso do servidor de pacotes. O arquivo de configuração também permite que o programa de instalação determine as configurações que são aplicáveis ao servidor de pacotes. As configurações aplicáveis incluem as portas que são usadas ou se o servidor é ativado por SSL.

Se o Symantec Management Agent para UNIX, Linux e Mac não puder encontrar o arquivo de configuração do Apache Web Server, ele localizará nos seguintes locais:

- /etc/httpd/conf

- /etc/httpd/2.0/conf

Como uma alternativa para a detecção automática, você poderá editar a seção **[Httpd Integration]** do arquivo client.conf do Symantec Management Agent para UNIX, Linux e Mac. Quando você editar o arquivo, especifique o apache_config_location. Qualquer configuração que é alterada, torna-se o padrão.

Você pode usar a opção “-f” do Apache Web Server durante a instalação para realocar o arquivo de configuração de seu local padrão. Se você realocar o arquivo, será necessário especificar o local do apache_config_location. O servidor de pacotes para Linux não suporta arquivos gerados mod_perl de httpd.conf.

Requisitos para configurar o servidor de pacotes e o Apache Web Server

Para o servidor de pacotes para Linux trabalhar com o Apache Web Server, determinados requisitos devem ser cumpridos. Quando estes requisitos forem cumpridos, o Symantec Management Agent para UNIX, Linux e Mac enviará a função do Apache HTTP Server. Esta função permite que o computador seja usado como um servidor de pacotes para Linux.

Consulte [“Sobre a detecção do Apache Web Server”](#) na página 143.

Os requisitos de configuração são da seguinte forma

- Versão 2.0 ou 2.2 do Apache Web Server está instalada.
- O servidor de pacotes para Linux usa apenas o Apache Web Server principal ou o Apache Web Server padrão.
 Todas as outras seções de host virtual na configuração do Apache Web Server são ignoradas, com as seguintes exceções:
 - As configurações globais e o host virtual **_default_** são lidos para as configurações principais do servidor.
 - O primeiro host virtual que define um servidor SSL é considerado o servidor principal SSL. Suas configurações são usadas para integração e todos os outros hosts virtuais SSL são ignorados.
- O local do espaço da Web do Apache Web Server, onde os arquivos e os diretórios do servidor de pacotes serão criados, deve ter as seguintes opções ativadas:
 - **FollowSymLinks**
 - **AllowOverride**

O local do espaço da Web do Apache Web Server também deve ser acessível com o HTTP anônimo. O local é um diretório virtual **/Altiris/PS/**.

Consulte [“Requisitos para configurar o HTTPS e o HTTP”](#) na página 146.

- Se o HTTP e o HTTPS estiverem definidos para o Apache Web Server, o servidor do HTTPS será usado.
- As portas não padrão são detectadas e usadas, mas o Apache Web Server principal deve estar acessível através do nome do host do computador. A política **Listen** para o servidor principal deve vir antes de todas as outras instruções de **Porta** e política de Listen no arquivo de configuração.
- O Apache Web Server deve estar em execução.
- Nenhum módulo de compactação é usado com o Apache Web Server. Este requisito existe porque a entrega de pacotes não suporta esses módulos.
- Você pode precisar reiniciar o Symantec Management Agent para UNIX, Linux e Mac depois de fazer mudanças no arquivo httpd.conf. Os arquivos podem não ter efeito até depois que você reiniciar o agente.

Requisitos para configurar o HTTPS e o HTTP

O Symantec Management Agent para UNIX, Linux e Mac usa qualquer tipo de Apache Web Server que está disponível. Ele pode usar HTTP ou HTTPS.

Consulte [“Requisitos para configurar o servidor de pacotes e o Apache Web Server”](#) na página 145.

Se o Apache Web Server suportar ambos os tipos de servidor da Web, o servidor de pacotes para Linux usará o HTTPS. A integração com o SSL através do HTTPS é a opção padrão porque é a mais segura. Se desejar usar o servidor HTTP, será possível mudar a configuração **[httpd Integration] "integrate_with"**.

Tabela 7-1 Abordagens recomendadas para instalar o Apache Web Server para suporte a servidores de pacotes para UNIX e Linux

Opção	Descrição
Instale uma versão em pacote do Apache Web Server. No Linux, o Apache Web Server distribuído é o mais apropriado.	Esta instalação contém os arquivos executáveis e os arquivos exe de suporte técnico em /usr/sbin ou /usr/bin .

Opção	Descrição
Instale o pacote do Apache Web Server no local recomendado.	Um exemplo de um local padrão apropriado é /usr/local ou /opt .
Deixe o diretório Configuração em seu local padrão. Este requisito garante que o Symantec Management Agent para UNIX, Linux e Mac pode facilmente detectar o Apache Web Server e o arquivo de configuração. Se você não mover o diretório de configuração, não terá que especificar configurações manuais extras.	O diretório de configuração padrão é o local que foi compilado em seu .exe ou /etc/httpd/conf .

Se você mudar os arquivos de configuração do Apache Web Server enquanto o Symantec Management Agent estiver em execução, os dados serão enviados para o Notification Server após um curto período de tempo. Depois que os dados de função do Apache Web Server forem enviados para o Notification Server, o computador se tornará um servidor de pacotes candidato. Se você quiser acelerar este processo, deverá executar o arquivo executável **aex-sendbasicinventory** manualmente. Execute o arquivo executável do shell no computador-cliente que é visado para a instalação do servidor de pacotes. Atualize o Notification Server com as alterações.

Dois exemplos de configuração estão disponíveis.

Consulte “[O exemplo da configuração de servidor de pacotes que usa o diretório da Web principal para os links de servidor de pacotes](#)” na página 147.

Consulte “[Exemplo de configuração do servidor de pacotes que usa um alias para os links do servidor de pacotes](#)” na página 150.

O exemplo da configuração de servidor de pacotes que usa o diretório da Web principal para os links de servidor de pacotes

Esta configuração geralmente exige a modificação mínima em uma configuração padrão ou pronta para uso do Apache Web Server. Nesta configuração, um diretório virtual chamado **/Altiris/PS** é criado automaticamente no diretório HTML principal do Apache.

Consulte “[Requisitos para configurar o HTTPS e o HTTP](#)” na página 146.

A configuração de exemplo contém os seguintes diretórios:

- **Capturas de imagem**

■ Pacotes

Os links simbólicos são criados nestes diretórios para cada pacote compartilhado. Os pacotes em si são armazenados no diretório **VAR** do Package Server Agent.

Esta configuração inclui tanto um Apache HTTP Server quanto um HTTPS. O servidor de pacotes usa o servidor HTTPS se ele estiver disponível. O servidor HTTPS garante um ambiente operacional mais seguro e permite o uso de Credenciais de acesso do pacote.

Diversas verificações de arquivos de configuração são realizadas. Os arquivos de configuração que estão listados nesta seção são exemplos. Esses exemplos são da instalação padrão do Apache Web Server como parte de uma distribuição legada do Red Hat Linux.

Check number 1; Listen statement é da seguinte forma:

```
...## When we also provide SSL we have to listen to the ## standard
HTTP port (see above) and to the HTTPS port ## <IfDefine HAVE_SSL>
Listen 80 Listen 443 Listen 10.10.10.10:8080 </IfDefine>...
```

Assegure-se de que a instrução Listen para cada um dos servidores principais seja a primeira Instrução de escuta de seu tipo no arquivo de configuração. Os servidores principais HTTP e HTTPS devem ser as primeiras duas indicações de Listen.

Você deve remover o IP ou assegurar-se de que ele seja o mesmo IP em que o nome do host é resolvido, conforme relatado para o Notification Server.

Check number 2; Main directory options é da seguinte forma:

```
...

# DocumentRoot: The directory out of which you will serve your
Notification Server Reference 62

# documents. By default, all requests are taken from this directory,
but

# symbolic links and aliases may be used to point to other locations.
DocumentRoot "/var/www/html" ...

# This should be changed to whatever you set DocumentRoot to.

#<Directory "/var/www/html">

# This may also be "None", "All", or any combination of "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".

# Note that "MultiViews" must be named *explicitly* --- "Options All"
# does not give it to you.
```

O exemplo da configuração de servidor de pacotes que usa o diretório da Web principal para os links de servidor de pacotes

```
Options Indexes FollowSymLinks

# This controls which options the .htaccess files in directories can
# override. Can also be "All", or any combination of "Options",
"FileInfo",

# "AuthConfig", and "Limit" AllowOverride AuthConfig

# Controls who can get stuff from this server.

Order allow,deny

Allow from all

</Directory>

...
```

Encontre o nó **<Diretório>** do diretório **DocumentRoot** e assegure-se de que as seguintes opções estejam definidas:

- **FollowSymLinks**
- **AllowOverride AuthConfig** or **Allow override All**

Check number 3; Check SSL host é da seguinte forma:

```
## SSL Virtual Host Context

<VirtualHost _default_:443>

# General setup for the virtual host

DocumentRoot "/var/www/html"

ErrorLog logs/error_log

TransferLog logs/access_log Notification Server Reference 63

# SSL Engine Switch:

# Enable/Disable SSL for this virtual host.

SSLEngine on

...
```

Assegure-se de que o host virtual **SSH_default_** tenha a porta correta. A porta deve corresponder ao primeiro SSH Listen. Assegure-se de que o **DocumentRoot** do host virtual seja o mesmo que o **DocumentRoot** do servidor principal.

O **DocumentRoot** do host pode ser diferente do **DocumentRoot** do servidor principal. O **DocumentRoot** do host deve ter um nó de **<Diretório>** que seja configurado com as mesmas opções que estão especificadas em **Check number 2**.

Exemplo de configuração do servidor de pacotes que usa um alias para os links do servidor de pacotes

Convém manter o servidor de pacotes para o diretório virtual do Linux completamente separado do diretório do Apache Web Server. Para mantê-los separados, siga este exemplo de configuração. Este exemplo de configuração mantém todos os links simbólicos fora do diretório principal do Apache Web Server. Ele garante que as opções do FollowSymLinks não são necessárias no diretório principal.

Consulte [“Requisitos para configurar o HTTPS e o HTTP”](#) na página 146.

Um alias é usado no arquivo de configuração do Apache Web Server para separar o diretório virtual **/Altiris/ PS**. O servidor de pacotes para Linux detecta automaticamente este alias e cria os subdiretórios necessários no local correto.

Os subdiretórios são:

- **Pacotes**
- **Capturas de imagem**

É feito download dos pacotes reais no diretório **VAR** no agente.

Os arquivos de configuração que são usados nesta seção são exemplos. O exemplo é da instalação padrão do Apache Web Server como parte de uma distribuição legada do Red Hat Linux.

O **Check number 1; Listen statement** é da seguinte forma:

```
...## When we also provide SSL we have to listen to the
## porta padrão HTTP (consulte acima) e para a porta HTTPS
##
<IfDefine HAVE_SSL>
Listen 80
Listen 443
Listen 10.10.10.10:8080
</IfDefine>
...
```

Assegure-se de que a instrução Listen para cada um dos servidores principais seja a primeira Instrução de escuta de seu tipo no arquivo de configuração. Os servidores principais HTTP e HTTPS devem ser as primeiras duas indicações de Listen.

Você deve remover o IP ou assegurar-se de que ele seja o mesmo IP em que o nome do host é resolvido, conforme relatado para o Notification Server. Você pode usar números de porta, exceto 80 e 443. O servidor de pacotes para Linux detecta as portas. Porém, ele usa sempre a porta do primeiro Listen no arquivo de configuração do Apache Web Server.

Check number 2; Create Alias and aliases directory options é da seguinte forma:

```
...

# Aliases: Adicione aqui quantos aliases você precisa (não há limite).
O formato é

# Alias fakename realname

#

<IfModule mod_alias.c>

...

Alias /Altiris/PS /var/altiris/www/ps

<Directory /var/altiris/www/ps >

Options FollowSymLinks

AllowOverride All

</Directory> </IfModule>

# End of aliases.
```

Você deve executar estas etapas na seguinte ordem:

- Crie a indicação do Alias e o nó do **<Diretório>** para o diretório de destino do alias.
- Assegure-se de que as seguintes opções estejam definidas nesse diretório:
 - **FollowSymLinks**
 - **AllowOverride AuthConfig** or **Allow override All**
- Crie o diretório de destino.
- Defina as permissões corretas no diretório de destino para garantir que os clientes do Apache Web Server possam fazer o download dos arquivos desse diretório.
- Para garantir que o diretório funcione, coloque um arquivo de texto nele. Então, procure um URL, como `http://your.server.name/Altiris/PS/testfile.txt`. Neste

Exemplo de configuração do servidor de pacotes que usa um alias para os links do servidor de pacotes

exemplo, `your.server.name` e `testfile.txt` são: o próprio nome de seu servidor e o nome do arquivo de texto que você criou.

Check number 3; Check SSL host é da seguinte forma:

```
...  
## SSL Virtual Host Context  
<VirtualHost _default_:443>  
# General setup for the virtual host  
DocumentRoot "/var/www/html"  
ErrorLog logs/error_log  
TransferLog logs/access_log  
# SSL Engine Switch:  
# Enable/Disable SSL for this virtual host.  
SSLEngine on  
...
```

Assegure-se de que o host virtual `SSH _default_` tenha a porta correta. Ele deve corresponder ao primeiro `SSH Listen`. Assegure-se de que o `DocumentRoot` seja o mesmo que o `DocumentRoot` do servidor principal.

Para configurar a hierarquia

Este capítulo contém os tópicos a seguir:

- [Sobre a hierarquia do Notification Server](#)
- [Requisitos da hierarquia](#)
- [Para implementar a hierarquia do Notification Server](#)

Sobre a hierarquia do Notification Server

A tecnologia de hierarquia foi projetada para reduzir o custo total de propriedade (TCO, total cost of ownership) do gerenciamento de software e soluções da Symantec em vários Notification Servers. A hierarquia reduz o TCO suplementando o sistema do Notification Server com recursos de gerenciamento centralizado.

Consulte [“Requisitos da hierarquia”](#) na página 155.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

A Hierarquia define os fluxos de informações através de vários Notification Servers em uma empresa. Se você tem vários Notification Servers, você pode usar a hierarquia para definir as coleções de Notification Servers que compartilham configurações e de dados comuns. A hierarquia pode distribuir e sincronizar todas as alterações feitas a configurações e dados compartilhados. A hierarquia permite gerenciar as soluções da Symantec através de vários Notification Servers de um local central.

Algumas soluções, como Inventory Solution, Patch Management Solution e Software Management Solution, são configuradas para participar da hierarquia. Para obter mais informações sobre uma solução específica, consulte a documentação da solução apropriada.

A hierarquia usa replicação para copiar e sincronizar objetos e dados compartilhados entre Notification Servers dentro da mesma estrutura hierárquica. Em intervalos agendados, cada servidor dentro de uma hierarquia sincroniza objetos e dados com os pais e filhos imediatos.

Consulte [“Sobre replicação e regras de replicação”](#) na página 172.

Uma topologia de hierarquia define a relação entre os Notification Servers, que por sua vez controla como a sincronização ocorre entre os nós adjacentes.

Uma topologia de hierarquia cumpre às seguintes regras:

- Cada Notification Server pode ter zero ou um pai.
- Cada Notification Server pode ter zero ou mais filhos.

Na hierarquia, os objetos e dados são restritos para replicar nas direções conhecidas; assim, a sincronização é previsível e escalonável. Como a hierarquia replica cada objeto ou parte de dados em somente um sentido, o gerenciamento de conflitos é trivial e a fonte sempre tem a prioridade.

Tabela 8-1 Objetos que podem ser sincronizados entre Notification Servers

Objeto	Descrição
Itens de configuração e gerenciamento	As políticas, as tarefas, os filtros e os relatórios são replicados abaixo de uma hierarquia. Consulte “Sobre tarefas em execução na hierarquia” na página 414.
Configurações de segurança	Funções, privilégios e permissões de segurança são replicados de maneira decrescente em uma hierarquia.
Recursos	As informações de recursos, como computadores, usuários, sites e suas classes de dados associadas, são replicadas de maneira crescente ou decrescente em uma hierarquia.
Pacotes	Os pacotes associados aos recursos de software e as classes de dados associadas aos pacotes são replicadas de maneira decrescente em uma hierarquia.
Eventos	As classes de eventos, como execução de entrega de software, são replicadas de maneira crescente ou decrescente em uma hierarquia.

Nota: Algumas soluções da Symantec criam regras personalizadas para replicação a fim de garantir que determinados itens sejam sempre sincronizados.

Requisitos da hierarquia

Para compartilhar ou receber configurações comuns e dados com vários computadores do Notification Server, é necessário primeiro adicionar o computador do Notification Server a uma hierarquia. Como os computadores do Notification Server podem ser gerenciados localmente, cada computador do Notification Server deve ser adicionado ou removido individualmente de uma hierarquia com as credenciais de acesso apropriadas. Normalmente, o Administrador Symantec que gerencia o design de topologia acessa remotamente os computadores do Notification Server em outros sites para adicioná-los a uma hierarquia.

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Os requisitos para configurar a hierarquia são:

- O tráfego na rede deve ser roteável entre computadores do Notification Server adjacentes dentro da hierarquia.
- O tráfego HTTP/HTTPS rede deve ser permitido entre os computadores do Notification Server adjacentes na hierarquia.
- Se você usar certificados autoassinados para computadores do Notification Server, assegure-se de que a confiança entre esses computadores esteja estabelecida. Para fazer isso, no **Console de gerenciamento Microsoft**, na loja de **Certificados (computador local)**, instale manualmente certificados para **Autoridade de certificação raiz confiável**.
- Relacionamentos confiáveis devem existir entre os computadores do Notification Server adjacentes na hierarquia ou então as credenciais de contas com privilégios que facilitem a confiança devem ser conhecidas.
- Cada computador do Notification Server deverá ser capaz de resolver o nome e o endereço de rede de computadores do Notification Server adjacentes na hierarquia.
- Deve existir largura de banda suficiente entre os sites do Notification Server para suporte a pacotes e à replicação de dados.
A largura de banda e o hardware necessários dependem do tamanho da topologia de hierarquia e dos dados replicados.
- Um site deve existir para cada computador do Notification Server e uma sub-rede que contenha o Notification Server deve ser incluída. O site também deve conter um servidor de pacotes (um servidor de sites que esteja executando o serviço do pacote) que sirva ao computador do Notification Server.

Consulte [“Sobre os serviços de site”](#) na página 127.

Para implementar a hierarquia do Notification Server

Para compartilhar ou receber dados e definições de configurações comuns com vários Notification Servers, adicione o computador do Notification Server a uma hierarquia e configure as regras de replicação necessárias.

Tabela 8-2 Processo para implementar a hierarquia do Notification Server

Etapa	Ação	Descrição
Etapa 1	Criar os relacionamentos hierárquicos apropriados entre Notification Servers.	Você cria uma hierarquia ao criar uma série de relacionamentos pai para filho e filho para pai que vinculam os computadores do Notification Servers em seu sistema. Consulte “Para criar e gerenciar relacionamentos hierárquicos” na página 157. Consulte “Para configurar um relacionamento hierárquico entre dois computadores do Notification Server” na página 161.
Etapa 2	Criar e ativar as regras de replicação apropriadas para especificar os dados para replicar na hierarquia.	A replicação de hierarquia de recursos e eventos é configurada usando regras de replicação. Essas regras definem os dados que você deseja replicar em outros Notification Servers. Consulte “Para configurar a replicação de hierarquia e as regras da replicação de hierarquia” na página 163. Se desejar configurar a replicação de hierarquia personalizada para itens de configuração e gerenciamento, especifique as configurações apropriadas. Consulte “Para configurar a replicação de hierarquia personalizada” na página 165.

Etapa	Ação	Descrição
Etapa 3	(Opcional) Execute tarefas manuais de replicação.	Os computadores do Notification Server em uma hierarquia normalmente são sincronizados de acordo com o agendamento de replicação configurado nas regras de replicação. Caso necessário, você pode manualmente substituir o agendamento da replicação diferencial de seu Notification Server e acionar as regras de replicação de hierarquia imediatamente. Consulte “Para sobrepor o agendamento da replicação diferencial da hierarquia” na página 167. Você também pode replicar os dados selecionados diretamente de um Notification Server para todos os Notification Servers filho sem incluí-lo em uma regra de replicação. A replicação manual é uma replicação única que ocorre imediatamente. Você precisa ter a permissão de leitura na ação do item do menu do botão direito do mouse Replicar agora para executar a replicação manual. Consulte “Para replicar manualmente dados selecionados” na página 168.
Etapa 4	(Opcional) Defina políticas de automação de hierarquia.	As políticas de automação da hierarquia enviarão notificações por e-mail quando determinados eventos ocorrerem na hierarquia. Consulte “Para configurar uma política de automação da hierarquia” na página 168.
Etapa 5	Execute um relatório de hierarquia.	Você pode executar um relatório em qualquer Notification Server na hierarquia para extrair dados do CMDB. Atualize os dados de resumo antes de executar um relatório de hierarquia. Consulte “Para executar relatórios de hierarquia” na página 169. Consulte “Atualização de dados de resumo” na página 170.

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.

Consulte [“Requisitos da hierarquia”](#) na página 155.

Para criar e gerenciar relacionamentos hierárquicos

Você cria uma hierarquia ao criar uma série de relacionamentos pai para filho e filho para pai que vinculam os computadores do Notification Servers em seu sistema. Você pode adicionar seu Notification Server (aquele em que você está conectado, que pode ser um logon remoto) a uma hierarquia como o filho de um Notification Server remoto existente ou como seu pai.

Você pode adicionar seu Notification Server (aquele em que você está conectado, que pode ser um logon remoto) a uma hierarquia como o filho de um computador do Notification Server remoto existente ou como seu pai. Para criar um relacionamento hierárquico, você necessita de uma conta de administrador da Symantec (ou uma conta com privilégios equivalentes) em ambos os computadores. Para adicionar ou remover computadores do Notification Server de uma hierarquia, você precisará do privilégio **Gerenciar topologia de hierarquia** no Notification Server no qual a ação será realizada.

Você pode visualizar e configurar a hierarquia do computador do Notification Server usando o Symantec Management Console. Se for o administrador de Hierarquia, você poderá ver somente o pai e os filhos (em todos os níveis) de seu Notification Server.

Observe que todas as ações que você toma são baseadas em seu Notification Server. Clicar com o botão direito do mouse em um computador do Notification Server não executa um logon remoto em nenhum computador do Notification Server remoto. Abre um menu contextual que contém as ações que você pode executar nesse servidor, que é diferente para os computadores locais e remotos. Um conjunto completo de ações está disponível para o servidor local, mas somente um conjunto limitado está disponível para servidores remotos. Ações como a extração de relatórios são executadas no banco de dados apropriado.

As ações que você pode executar na hierarquia são relativas ao seu computador do Notification Server, que é o computador ao qual você está conectado. Se você tiver o privilégio **Gerenciar hierarquia** em um computador do Notification Server remoto, poderá executar um logon remoto nesse computador. Você pode então abrir o Console de gerenciamento Symantec e executar a configuração da hierarquia relativa a esse computador.

Você pode ativar ou desativar a replicação de hierarquia em computadores específicos do Notification Server a qualquer momento. Por exemplo, você pode usar este recurso para desativar temporariamente a replicação de hierarquia durante tarefas de manutenção como instalação, upgrades ou desinstalação da solução. Desativar a replicação em um computador do Notification Server não afetará o agendamento de replicação nos outros computadores do Notification Server na hierarquia. Porém, nenhum dado passará pelo computador desativado; assim, a replicação para a camada inferior será interrompida no pai e a replicação para a camada superior será interrompida nos filhos.

Um símbolo colorido na página **Gerenciamento da hierarquia** indica todos os alertas da hierarquia. As cores que você pode ver e o status do alerta correspondente são os seguintes:

Amarelo	Status de alerta baixo.

Laranja Status de alerta médio.

Vermelho Status do alerta crítico.

Por exemplo, se você tentar replicar os mesmos para camadas superiores e inferiores da hierarquia do mesmo computador do Notification Server, um alerta crítico será lançado. Os dados devem ser replicados somente para uma direção. Se o computador do Notification Server pai ou filho tiver as mesmas regras de replicação de hierarquia implementadas, isso poderá gerar um conflito de dados.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para criar e gerenciar relacionamentos hierárquicos

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- 2 Na página **Gerenciamento da hierarquia**, na guia **Topologia**, na lista suspensa **Exibição**, selecione **Diagrama** para exibir a hierarquia no formato gráfico.

Use a exibição **Grade** apenas para copiar dados para a área de transferência. Ela contém os dados que não são exibidos em **Diagrama**.

3 Execute uma das seguintes tarefas:

Adicione um Notification Server novo a uma hierarquia	Consulte “Para configurar um relacionamento hierárquico entre dois computadores do Notification Server” na página 161.
Modifique um relacionamento hierárquico entre dois Notification Servers	Consulte “Para configurar um relacionamento hierárquico entre dois computadores do Notification Server” na página 161.
Remova o Notification Server da hierarquia	Clique com o botão direito do mouse no computador do Notification Server que deseja remover e clique em Remover .
Ativar ou desativar a replicação de hierarquia	Convém desativar a participação da hierarquia quando você executar manutenção em um Notification Server. Clique com o botão direito do mouse no computador do Notification Server em que você quer ativar ou desativar a replicação de hierarquia e em Ativar replicação ou Desativar replicação, o que for apropriado. Desativar a replicação de hierarquia afeta somente a agenda de replicação de hierarquia. Essa ação não tem nenhum efeito sobre nenhuma replicação autônoma que for configurada de ou para outro Notification Server. Sincronizar manualmente a hierarquia não muda essa configuração, mas substitui a configuração para executar uma replicação única dos itens apropriados.
Substitua manualmente o agendamento de replicação de hierarquia para um Notification Server	Consulte “Para sobrepor o agendamento da replicação diferencial da hierarquia” na página 167.
Execute um relatório de hierarquia	Consulte “Para executar relatórios de hierarquia” na página 169.

4 Clique em **Salvar alterações**.

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.

Consulte [“Requisitos da hierarquia”](#) na página 155.

Vídeo: para obter mais informações sobre como configurar uma hierarquia, veja [Setting Up a Hierarchy in the IT Management Suite Video \(em inglês\)](#) no Symantec Connect.

Para configurar um relacionamento hierárquico entre dois computadores do Notification Server

Você pode configurar um relacionamento hierárquico (pai ou filho) entre seu computador do Notification Server e o computador do Notification Server remoto. Você precisa especificar o nome, o URL (que deve incluir todas as configurações HTTPS ou de porta não padrão) e os detalhes de acesso ao computador do Notification Server remoto. Você precisa também fornecer os detalhes de acesso de seu computador do Notification Server local. Por padrão, o agendamento de replicação de hierarquia alterna a replicação entre cada par de computadores do Notification Server. É possível mudar o agendamento de replicação para satisfazer a seus requisitos, mas você deverá certificar-se de que a alternância na replicação seja mantida.

Ambos os computadores do Notification Servers devem ter um servidor de pacotes disponível em seus respectivos sites. O servidor de pacotes é necessário por razões de desempenho. Você não poderá criar um relacionamento hierárquico entre dois computadores do Notification Server se um deles não tiver um servidor de pacotes disponível.

As credenciais de aplicativo do Notification Server devem ser estáveis e não ser alteradas regularmente como algumas senhas da conta do usuário. Se a senha da conta de aplicativo do computador do Notification Server tornar-se inválida, uma mensagem será exibida no console. A mensagem solicita que você use a ferramenta de linha de comando ASConfig para fazer as atualizações necessárias.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para configurar um relacionamento hierárquico entre dois computadores do Notification Server

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Gerenciamento do Notification Server > Hierarquia**.
- 2 Na página Gerenciamento da hierarquia, na guia **Topologia**, clique com o botão direito do mouse em seu Notification Server e clique na opção apropriada:
 - **Adicionar > Pai**
 - **Adicionar > Filho**

- 3 Em **Bem-vindo ao Assistente de Adição de nó de hierarquia**, na página **Notification Server**, digite o nome, o URL e as credenciais de acesso do computador do Notification Server remoto.

As credenciais de acesso devem ser uma conta de administrador da Symantec ou uma conta equivalente no Notification Server remoto.
- 4 Clique em **Avançadas**.
- 5 Na caixa de diálogo **Retornar configuração da credencial**, especifique a conta de administrador da Symantec (ou equivalente) usada pelo computador do Notification Server remoto para comunicar-se com o computador do Notification Server local e depois clique em **OK**.
- 6 Em **Bem-vindo ao Assistente de Adição de nó de hierarquia**, clique em **Avançar**.
- 7 Na página **Agendamentos de replicação**, configure os agendamentos de replicação diferencial e completa, ative aquelas que você deseja usar no computador do Notification Server e clique em **Avançar**.

Por padrão, somente o agendamento da replicação diferencial está ativada. A replicação completa é usada raramente, pois coloca uma carga pesada no computador do Notification Server. Porém, você pode ativá-la quando necessário. Você deve agendar a replicação em horários que não entrem em conflito com os agendamentos de replicação de outros computadores do Notification Servers na hierarquia.

Consulte [“Para gerenciar agendamentos compartilhados”](#) na página 122.
Consulte [“Para configurar um agendamento”](#) na página 123.
- 8 Na página **Confirmar configurações**, verifique se as configurações estão corretas e clique em **Concluir**.

O computador do Notification Server local usa as informações especificadas para localizar e verificar o computador do Notification Server remoto e configurar o relacionamento hierárquico apropriado com o mesmo.

Se o computador do Notification Server remoto não tiver um servidor de pacotes disponível em seu site, a verificação falhará e o relacionamento hierárquico não poderá ser estabelecido.

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.
Consulte [“Requisitos da hierarquia”](#) na página 155.

Para configurar a replicação de hierarquia e as regras da replicação de hierarquia

A replicação de hierarquia especifica o que é replicado na hierarquia. Ela não tem efeito algum sobre a replicação autônoma que você pode configurar entre dois Notification Servers.

Quando você adicionar o Notification Server a uma hierarquia, você poderá especificar o que replicar para o Notification Server pai e para todos os Notification Server filho. Por padrão, tudo é replicado (replicação completa), o que pode consumir largura de banda excessiva. A Symantec recomenda que você configure a replicação de hierarquia em cada Notification Server para melhor atender aos requisitos de sua organização.

Nota: A replicação não é suportada entre dois Notification Servers que tenham versões diferentes do IT Management Suite instaladas. Por exemplo, você não pode replicar dados de um servidor 7.0 em um servidor 7.1.

Todos os dados que forem replicados de um Notification Server pai terão prioridade e sobrescreverão os dados correspondentes em seus servidores filho. Os itens replicados de configuração e gerenciamento que são recebidos de um servidor-pai são geralmente somente leitura; portanto, não podem ser modificados. A configuração somente leitura garante a replicação para camadas inferiores em uma hierarquia. Se quiser permitir adições aos itens replicados em servidores filho, você precisará desbloquear os itens relevantes no computador do Notification Server no qual eles foram criados. Por exemplo, talvez você queira permitir que as políticas sejam ativadas e desativadas nos Notification Servers filho.

A replicação de hierarquia de recursos e eventos é configurada usando regras de replicação. Estas regras definem os dados que você quer replicar em outros Notification Servers. Cada regra replica os dados especificados em um sentido somente, até o Notification Server pai ou para baixo nos Notification Server filho. Se você configurar duas regras que tenham o mesmo tipo de recurso sendo replicado em ambas as direções, um alerta crítico será emitido e as regras de replicação não serão executadas.

Você pode incluir destinos de recursos em uma regra de replicação de recursos. O escopo do recurso aplica-se ao conteúdo (recursos) dos destinos que são replicados. Consequentemente, os recursos replicados dependerão do proprietário do destino do recurso. O administrador do Notification Server pode optar por replicar destinos de recursos em seu estado atual (de propriedade de outra pessoa, com o escopo correspondente). Como alternativa, eles podem obter propriedade dos destinos, salvá-los com o escopo do administrador (que contém mais recursos geralmente) e replicá-los nesse estado. Todos os membros atuais de um destino

de recurso são replicados. O item real do destino de recurso é replicado em segundo plano como um item dependente. Por exemplo, quando uma regra de replicação for criada no pai que se aplica a um destino de recurso. O destino de recurso será replicado como um item dependente quando a própria regra de replicação for replicada na hierarquia.

Hierarquia tem dois modos de replicação:

Diferencial	Replica os objetos e dados que foram alterados desde a última replicação. Este modo é ativado por padrão e reduz a carga e a largura de banda usadas pela hierarquia.
Completa	Replica todos os objetos e dados. Este modo está ativado por padrão.

Para minimizar a carga na rede e impedir colisões de dados, é necessário agendar a replicação de hierarquia em uma hora diferente para cada Notification Server na hierarquia.

Consulte [“Para configurar um agendamento”](#) na página 123.

A replicação de hierarquia sincroniza tipos diferentes de objetos das seguintes maneiras:

Objetos de segurança	Objetos de segurança, como funções e privilégios, sempre usam replicação completa. A replicação diferencial não é uma opção para objetos somente leitura como esses.
Itens	Os itens usam a replicação diferencial, que é controlada verificando cada item para procurar mudanças e replicando aqueles que foram alterados.
Recursos	Os recursos usam replicação diferencial. A replicação diferencial é baseada no carimbo de hora de "última modificação" nos dados de origem. Qualquer dado que tenha sido alterado desde a última replicação é copiado no servidor de destino. Os dados no destino são então verificados, caso a verificação de dados tenha sido ativada na regra de replicação apropriada. A verificação de dados impõe uma carga de processamento significativa ao Notification Server. Para reduzir esta carga, você pode verificar uma porcentagem específica dos dados no servidor de destino com cada replicação. Por exemplo, se você verificar 10% dos dados de cada replicação, isso garantirá que todos os dados foram verificados após 10 replicações.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para configurar a replicação de hierarquia e as regras da replicação de hierarquia

- No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- Na página **Gerenciamento da hierarquia**, selecione a guia **Replicação**.
- Configure a replicação de hierarquia selecionando as opções apropriadas.
Para obter mais informações, clique na página e pressione **F1**.
- Para configurar as regras da replicação de hierarquia, execute uma das seguintes ações:

Crie uma nova regra de replicação de hierarquia

- Clique em **Adicionar**.
- Na caixa de diálogo **Regra de replicação**, especifique as configurações apropriadas.

Para obter mais informações, clique na página e pressione **F1**.
- Clique em **Salvar alterações**.

Para modificar uma regra existente de replicação de hierarquia

- Selecione a regra apropriada e clique em **Editar**.
- Na caixa de diálogo **Regra de replicação**, especifique as configurações apropriadas.
- Clique em **Salvar alterações**.

Ative uma regra da replicação de hierarquia

Selecione **Ativado** ao lado do nome da regra de replicação.

Exclua uma regra da replicação de hierarquia

Selecione a regra apropriada e clique em **Excluir**.

As regras de replicação fornecidas com Notification Server ou com as soluções instaladas não podem ser excluídas. Porém, você pode ativar e desativar regras quando necessário e editar o nome e a descrição da regra.

- Clique em **Salvar alterações**.

Para configurar a replicação de hierarquia personalizada

Você pode configurar a replicação de hierarquia personalizada para itens de configuração e gerenciamento e também para privilégios e funções de segurança.

O relatório atual de Replicação de itens que você pode acessar no painel Itens de configuração e gerenciamento relaciona todos os itens que foram ativados para replicação usando a replicação de hierarquia personalizada. Quando os itens selecionados forem replicados, todos os itens dependentes que não tiverem sido ativados serão incluídos automaticamente. Estes itens não aparecem no relatório de Replicação de itens. Para ver uma lista de todos os itens que foram replicados, você precisa visualizar o relatório de Objetos replicados.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para configurar a replicação de hierarquia personalizada para itens de configuração e gerenciamento

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- 2 Na página **Gerenciamento da hierarquia**, na guia **Replicação**, no painel **Itens de configuração e gerenciamento**, clique em **Personalizado**.
- 3 Clique em **Salvar alterações**.
- 4 No Console de gerenciamento Symantec, no painel esquerdo, clique com o botão direito do mouse na pasta ou no item que você quer replicar e clique em **Hierarquia > Ativar replicação**.
- 5 Se você tiver selecionado uma pasta, na caixa de diálogo **Comportamento de replicação herdado**, especifique se incluir o conteúdo da pasta na replicação:

Para incluir todo o conteúdo da pasta Clique em **Sim**.

Para replicar somente a pasta sem o conteúdo Clique em **Não**.

Caso necessário, você pode manualmente ativar ou desativar subpastas específicas em outro momento.

Para configurar a replicação de hierarquia personalizada para funções e privilégios de segurança

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- 2 Na página de **Gerenciamento da hierarquia**, na guia **Replicação**, em **Segurança**, clique em **Personalizado**.

- 3 Clique em **Selecionar funções e privilégios de segurança**.
- 4 Na janela **Selecionar funções e privilégios de segurança**, selecione as funções e os privilégios que você quer replicar.
- 5 Clique em **OK**.
- 6 Clique em **Salvar alterações**.

Para sobrepor o agendamento da replicação diferencial da hierarquia

Os computadores do Notification Server em uma hierarquia normalmente são sincronizados de acordo com o agendamento de replicação configurado nas regras de replicação. Caso necessário, você pode manualmente substituir o agendamento da replicação diferencial de seu Notification Server e acionar as regras de replicação de hierarquia imediatamente. Aciona o agendamento diferencial da hierarquia ao nó filho selecionado. As regras de replicação de hierarquia ajustadas para serem executadas no agendamento diferencial são executadas imediatamente. As regras definidas para serem executadas em agendamentos personalizados não são acionadas para serem executadas naquele momento. Você pode replicar dados manualmente em seu Notification Server apenas através de um Notification Server remoto pai ou filho.

Você não pode manualmente substituir a replicação para um Notification Server remoto. Você somente pode executar uma operação que afete seu Notification Server. Você pode fazer logon no Notification Server remoto para torná-lo seu Notification Server e substituir manualmente as agendas da replicação diferenciais em seus Notification Servers pai ou filho.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para sobrepor o agendamento da replicação diferencial da hierarquia

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- 2 Na página **Gerenciamento da hierarquia**, na guia **Topologia**, clique com o botão direito do mouse no computador do Notification Server do qual você quer replicar dados.
- 3 Clique em **Hierarquia > Replicar para...**
 Essa opção aciona as regras de replicação de hierarquia que apontam para o Notification Server (atualmente conectado) local. Você não pode replicar dados do Notification Server remoto para nenhum outro servidor remoto.
- 4 Na caixa de diálogo de confirmação, clique em **OK**.

Para replicar manualmente dados selecionados

Você pode substituir as regras de replicação do Notification Server executando uma replicação manual de hierarquia de uma pasta ou item específico. A replicação manual replica os dados selecionados nos Notification Servers filho imediatamente. Os dados são replicados independentemente das agendas de replicação ou da inclusão de dados nas regras de replicação.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para replicar manualmente dados selecionados do Notification Server

- 1 No Console de gerenciamento Symantec, no painel esquerdo, clique com o botão direito do mouse na pasta ou no item que você deseja replicar.

Se você selecionar uma pasta, a replicação incluirá todo o conteúdo (todos os níveis de subpastas e de itens que ela contiver). Todas as pastas pai (mas não seu conteúdo) são replicadas também para manter os caminhos da pasta dentro da estrutura.
- 2 Clique em **Hierarquia > Replicar agora...**
- 3 Na caixa da caixa de diálogo de confirmação, clique em **OK**.

Para configurar uma política de automação da hierarquia

As políticas de automação da hierarquia enviarão notificações por e-mail quando determinados eventos ocorrerem na hierarquia. Você precisa ativar as políticas que deseja usar. Você não pode modificar as políticas padrão, mas pode duplicá-las para criar novas políticas. Assim, você pode configurar políticas para atender a seus requisitos.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para configurar uma política de automação da hierarquia

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 No painel esquerdo, clique em uma das seguintes políticas:

Alertas críticos da hierarquia

Envia um alerta de e-mail de alta prioridade ao administrador do sistema de notificação sempre que um alerta crítico é recebido no Notification Server local.

Os estados de alerta crítico também são indicados na guia **Topologia** na página Gerenciamento da hierarquia.

Ativar/desativar hierarquia

Envia um alerta por e-mail de alta prioridade ao administrador do sistema de notificações sempre que a replicação de hierarquia for ativada ou desativada no Notification Server local.

Alertas de alta importância da hierarquia

Envia um alerta por e-mail de alta prioridade ao administrador do sistema de notificações sempre que um alerta de alta importância for recebido no Notification Server local.

Alteração de estrutura hierárquica

Envia um alerta de e-mail de alta prioridade ao administrador do sistema de notificações sempre que o Notification Server for adicionado ou removido da hierarquia.

- 3 No painel direito, especifique as configurações da política e clique em **Salvar alterações**.
- 4 Na barra de ferramentas, clique em **Ativar**.

Para executar relatórios de hierarquia

Você pode executar um relatório em qualquer Notification Server na hierarquia para extrair dados do CMDB. Convém atualizar os dados de resumo antes de executar um relatório de hierarquia. Você pode atualizar os dados de resumo sob demanda ou agendar atualizações.

Consulte [“Atualização de dados de resumo”](#) na página 170.

Algumas soluções instaladas podem fornecer relatórios de hierarquia agrupados. Estes relatórios resumem os dados relevantes da hierarquia e os resultados contêm uma única linha para cada Notification Server. Você pode executar os relatórios completos em um Notification Server específico clicando duas vezes na linha apropriada.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para executar um relatório da hierarquia

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Hierarquia**.
- 2 Na página **Gerenciamento da hierarquia**, na guia **Topologia**, clique com o botão direito do mouse no computador do Notification Server no qual você deseja executar um relatório.
- 3 Clique em **Relatórios** e clique no relatório apropriado.
- 4 Na página do relatório, especifique todos os parâmetros que você deseja usar e atualize o relatório.

Consulte [“Para extrair resultados do relatório do Notification Server”](#) na página 442.

Atualização de dados de resumo

Se você precisar gerar dados para relatórios ativados por hierarquia, será possível atualizar dados de resumo no servidor de tarefas. Você pode atualizar dados de resumo sob demanda, agendar uma atualização única ou criar um agendamento personalizado para atualizações recorrentes.

Um agendamento padrão executa a tarefa automaticamente todos os dias. Se desejar atualizações diárias dos dados de inventário, você não precisará mudar o agendamento de atualização.

Esta tarefa é uma etapa no processo de implementação da hierarquia do Notification Server.

Consulte [“Para implementar a hierarquia do Notification Server”](#) na página 156.

Para atualizar dados de resumo sob demanda

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Notification Server > Configurações de tarefas > Atualizar dados do resumo**.
- 3 No painel **Atualizar dados do resumo**, clique com o botão direito do mouse na tarefa que você deseja executar e clique em **Iniciar agora**.

Você pode clicar em **Detalhes** para visualizar mais informações sobre a tarefa antes que você a execute.

- 4 Se o agendamento que deseja executar não estiver na lista, crie um agendamento personalizado.

Para criar um agendamento

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Notification Server > Configurações de tarefas > Atualizar dados do resumo**.
- 3 Na página **Atualizar dados do resumo**, clique em **Novo agendamento**.
- 4 Na caixa de diálogo **Novo agendamento**, especifique as configurações do agendamento e clique em **Agendar**.

Para obter mais informações, clique na página e pressione **F1**.

Consulte [“Para executar relatórios de hierarquia”](#) na página 169.

Para configurar a replicação

Este capítulo contém os tópicos a seguir:

- [Sobre replicação e regras de replicação](#)
- [Requisitos de replicação](#)
- [Para configurar regras de replicação](#)

Sobre replicação e regras de replicação

A replicação é a transferência em sentido único de dados entre dois Notification Servers.

Consulte [“Requisitos de replicação”](#) na página 174.

Nota: A replicação não é suportada entre dois Notification Servers que tenham versões diferentes do IT Management Suite instaladas. Por exemplo, você não pode replicar dados de um servidor 7.0 em um servidor 7.1.

A funcionalidade de replicação autônoma descrita aqui é diferente da replicação de hierarquia. A replicação autônoma define o fluxo das informações entre dois Notification Servers. A replicação de hierarquia fornece uma sincronização confiável e escalonável de dados entre vários Notification Servers.

A replicação pode ser configurada para replicar dados fora da estrutura de hierarquia. Por exemplo, ao enviar dados para um servidor externo que confira as informações específicas de relatórios.

Os seguintes tipos de replicação são aceitos:

Diferencial	Replica os objetos e dados que foram alterados desde a última replicação. Este método é o método recomendado, pois reduz o consumo da largura de banda e carga da rede quando os dados são replicados.
Completa	Replica todos os objetos e dados. Este método é geralmente usado para a replicação de hierarquia. Uma replicação completa é, em geral, executada mensalmente para garantir a replicação completa. A replicação autônoma não executa a replicação completa como a replicação de hierarquia faz. A replicação autônoma é sempre diferencial.

Outra diferença entre a replicação de hierarquia e a replicação é que dentro de uma hierarquia os dados replicados são protegidos e (por padrão) são somente leitura. A propriedade é aplicada de modo que os Notification Server filho não possam automaticamente sobrescrever os dados replicados dos Notification Servers pai. Alguns dados incluem as configurações que ativam sua edição no destino e eles podem ser configurados conforme for apropriado. A replicação não tem essa propriedade; assim, todos os dados replicados podem ser editados nos Notification Servers de destino.

Para configurar a replicação, você precisa configurar as regras de replicação apropriadas em cada computador do Notification Server. Cada regra especifica os dados que serão replicados desse servidor (servidor de origem) para um ou mais servidores de destino especificados e também o agendamento que será usado.

Consulte [“Para configurar regras de replicação”](#) na página 175.

Você pode criar uma regra de replicação para os seguintes itens:

Eventos	Replica eventos do Notification Server.
Itens	Replica itens de configuração e gerenciamento do Notification Server, como políticas, filtros e relatórios.

Recursos	Replica os tipos de recursos, destinos de recursos e classes de dados específicos do Notification Server. Se você incluir destinos de recursos em uma regra de replicação de recursos, lembre-se de que o escopo dos recursos se aplicará ao conteúdo (recursos) do destino replicado. Consequentemente, os recursos replicados dependerão do proprietário do destino do recurso. O administrador do Notification Server pode optar por replicar destinos de recursos em seu estado atual (de propriedade de outra pessoa, com o escopo correspondente). Como alternativa, eles podem obter propriedade dos destinos, salvá-los com o escopo do administrador (que contém mais recursos geralmente) e replicá-los nesse estado. Todos os membros atuais de um destino de recurso são replicados. O item real do destino de recurso é replicado em segundo plano como um item dependente. O destino aplicado a uma regra autônoma será replicado quando a própria regra autônoma for replicada. Quando a regra for executada, o destino não será enviado.
Segurança	Replica privilégios e funções de segurança do Notification Server. Estão disponíveis dois tipos de regras de replicação da segurança: privilégio e função. O procedimento de configuração é idêntico para ambos. Quando você incluir uma função de segurança em uma regra de replicação, será necessário também configurar uma regra de replicação para replicar todos os privilégios na função. A função de segurança replicada não reconhecerá nenhum privilégio que já exista no computador do Notification Server de destino.

Requisitos de replicação

Os requisitos para configurar a replicação em seu sistema de notificação devem ser satisfeitos antes de configurar qualquer replicação.

Os requisitos de replicação são:

- O tráfego de rede deverá poder ser roteado entre Notification Servers.
- O tráfego HTTP/HTTPS deverá ser permitido entre Notification Servers.
- Os relacionamentos de confiança devem existir entre os Notification Servers, ou as credenciais para as contas com privilégios que facilitam a confiança devem ser conhecidas.
- Cada Notification Server deverá ser capaz de resolver o nome e o endereço de rede de qualquer Notification Server para o qual replica dados.

- Deve existir largura de banda suficiente entre os Notification Servers para suporte a pacotes e à replicação de dados.
A largura de banda e o hardware necessários dependem do tamanho de sua topologia de infraestrutura e dos dados replicados.
- Cada Notification Server deve ter um servidor de sites que esteja executando o serviço do pacote disponível. O serviço do pacote deve servir ao computador do Notification Server.

Consulte [“Sobre replicação e regras de replicação”](#) na página 172.

Para configurar regras de replicação

Antes de você começar a replicar dados de um Notification Server a outro, você precisará planejar sua replicação. Isto é, garantir que os dados semelhantes não sejam aprovados em ambas as direções. Se algum de seus servidores fizer parte de uma hierarquia, você precisará certificar-se de que a replicação não entre em conflito com o processo de replicação de hierarquia. O Notification Server não realiza verificação para assegurar que sua configuração da replicação esteja consistente com a hierarquia. Uma implementação mal planejada pode criar conflitos de dados ou sobrescrever nos CMDDBs afetado.

Consulte [“Sobre replicação e regras de replicação”](#) na página 172.

Consulte [“Requisitos de replicação”](#) na página 174.

A regra deve ser ativada para que a replicação especificada ocorra. Você pode ativar e desativar regras de replicação a qualquer momento, de acordo com as necessidades de sua empresa. Para cada regra que é ativada, os dados especificados são replicados de acordo com a agenda definida.

Você pode replicar dados a qualquer momento executando as regras de replicação apropriadas. No console, clique com o botão direito do mouse na regra e clique em **Executar**. A execução de uma regra de replicação substitui sua agenda e replica os dados especificados para os servidores de destino imediatamente. A execução de uma regra de replicação é uma operação única e não altera a agenda de replicação. Todas as regras de replicação continuam a ser executadas conforme a agenda.

Nota: A replicação não é suportada entre dois Notification Servers que tenham versões diferentes do IT Management Suite instaladas. Por exemplo, você não pode replicar dados de um servidor 7.0 em um servidor 7.1.

Para configurar uma regra de replicação

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda a pasta **Configurações > Notification Server > Replicação**.
- 3 Na pasta **Replicação**, execute uma das seguintes ações:

Crie uma nova regra de replicação

Clique com o botão direito do mouse na pasta apropriada e clique em **Nova > Regra de replicação**.

A nova regra aparece na pasta e é selecionada automaticamente.

Modifique uma regra de replicação existente

Expanda a pasta apropriada e selecione a regra de replicação que você deseja modificar.

Ative ou desative uma regra de replicação

Expanda a pasta apropriada e clique com o botão direito do mouse na regra de replicação e clique em **Ativar** ou **Desativar**, o que for apropriado.

Você também pode ativar ou desativar uma regra na página **Regra de replicação**, clicando no ícone de status da regra (Ativar/Desativar) para alternar a configuração.

Execute uma regra de replicação

Expanda a pasta apropriada, clique com o botão direito do mouse na regra de replicação que você deseja executar e clique em **Executar**.

- 4 Na página **Regra de replicação**, especifique as configurações apropriadas. Para obter mais informações, clique na página e pressione **F1**.
- 5 Clique em **Salvar alterações**.

Para executar uma configuração de primeira instalação

Este capítulo contém os tópicos a seguir:

- [Para executar as tarefas de configuração inicial](#)

Para executar as tarefas de configuração inicial

Quando você instalar o Symantec Management Platform, você configurará o Notification Server como parte do processo de instalação. Nenhuma configuração adicional é necessária antes de começar a usar o Notification Server.

No caso improvável de você instalar o Symantec Management Platform sem acompanhar versões de determinados produtos, você verá vários links para páginas de configuração. Neste cenário, será necessário configurar a plataforma manualmente.

Consulte [“Sobre como configurar o Notification Server”](#) na página 65.

Contudo, quando instalar o Symantec Management Platform e as versões de acompanhamento de determinados produtos, você visualizará uma página do portal **Bem-vindo ao Console de gerenciamento Symantec**, que simplifica o processo de configuração inicial.

Você verá a página **Bem-vindo ao Symantec Management Console** se tiver instalado alguns dos seguintes produtos:

- IT Management Suite
- Server Management Suite

■ Client Management Suite

Algumas das soluções incluídas em seu conjunto podem exigir configuração antes que você possa usá-las. A página do portal **Bem-vindo ao Symantec Management Console** é o único ponto de entrada para executar as ações chave da configuração para soluções nos pacotes que você instalou. Estas ações representam as configurações essenciais que você precisa definir para começar a usar as soluções.

Depois que você executar a configuração de primeira instalação, poderá ser necessário executar tarefas adicionais de configuração. A necessidade de executar etapas adicionais depende das soluções e dos conjuntos que você tiver instalado inicialmente ou que você instalar depois da primeira instalação. Além disso, configurações avançadas estão disponíveis no menu **Configurações** e poderão estar disponíveis de outras áreas de soluções individuais.

Para obter mais informações sobre as opções de configuração para as soluções e os produtos individuais, consulte a documentação dos produtos.

Tabela 10-1 Processo para executar as tarefas de configuração inicial

Etapa	Tarefa	Descrição
Etapa 1	Descubra computadores.	Você deve importar ou descobrir os computadores que estão em seu ambiente. Consulte “Descoberta de computadores” na página 179.
Etapa 2	Instale o Symantec Management Agent e os plug-ins da solução.	Depois de descobrir os computadores em seu ambiente, instale o Symantec Management Agent e os plug-ins da solução nos computadores que você quer gerenciar. Consulte “Para instalar o Symantec Management Agent e os plug-ins da solução” na página 181.
Etapa 3	Colete o inventário.	Nesta etapa, o Notification Server coleta as informações que os agentes recém-implementados coletam dos computadores gerenciados. Consulte “Coleta de informações do inventário” na página 185.
Etapa 4	Faça o agendamento do gerenciamento de patches.	Nesta etapa, você pode agendar o download e a instalação das atualizações de software. Consulte “Para agendar gerenciamento de patches” na página 187.

Descoberta de computadores

Descoberta de computadores significa identificar os computadores que estão em seu ambiente. Antes que você possa gerenciar computadores, é necessário primeiro identificar os computadores disponíveis e selecionar aqueles que deseja gerenciar usando o Symantec Management Agent.

Para descobrir computadores, você seleciona primeiro o tipo de computador em que deseja instalar o Symantec Management Agent. Você descobre computadores Windows com a Importação do Active Directory. Você descobre computadores UNIX, Linux e Mac com uma varredura de ping para uma faixa de IP que você seleciona.

Esta tarefa é uma etapa no processo de execução de tarefas de configuração de primeira instalação.

Consulte [“Para executar as tarefas de configuração inicial”](#) na página 177.

Para descobrir computadores

- 1 No Console de gerenciamento Symantec, clique em **Início > Gerenciamento do Notification Server > Primeira instalação**.
- 2 Na página **Bem-vindo ao Console de gerenciamento Symantec**, clique em **Descobrir computadores**.
- 3 No Assistente de **Descobrir computadores**, execute as seguintes etapas:

Etapas 1 Windows Permite importar computadores Windows pelo domínio ou grupo de trabalho.

Nota: Se você preferir descobrir computadores usando uma verificação de rede, não selecione nada nesta página, mas clique em **Avançar**.

Para importar computadores Windows pelo domínio:

- 1 Marque a caixa para importar computadores Windows.
- 2 Clique em um botão de opção para optar pela importação do Microsoft Active Directory ou através da participação em domínio/WINS.
- 3 Clique na seta para baixo ao lado de **Domínio ou grupo de trabalho** para selecionar um domínio ou um grupo de trabalho. Ou, é possível digitar um nome de domínio ou um nome do grupo de trabalho manualmente.
- 4 Digite as credenciais do domínio.
- 5 Clique na opção ao lado de **Agendar importação recorrente** para **Ativar** ou **Desativar**.

Se você esperar adicionar novos computadores à sua rede, deixe esta configuração ativada. Deixar esta configuração ativada significa que, à medida que você adiciona computadores à sua rede, eles são descobertos automaticamente.

- 6 Clique em **Agendar**.
Selecione um agendamento compartilhado predefinido para a importação recorrente. Esta lista é preenchida através da página **Agendamentos compartilhados**. Você modifica, cria e usa agendamentos compartilhados em **Configurações > Notification Server > Agendamentos compartilhados**.
- 7 Clique em **Avançar**.

Etapas 2 Rede

Permite descobrir computadores usando uma verificação de rede (varredura de ping).

Nota: Se você preferir importar computadores Windows pelo domínio ou pelo grupo de trabalho, não selecione nada nesta página, mas clique em **Voltar**.

Para descobrir computadores usando uma verificação de rede:

- 1 Marque a caixa para descobrir computadores e dispositivos em rede.

- 2 Digite uma faixa de varredura de ping.

Considere se você precisa verificar todos os endereços IP. Para uma primeira instalação, poderá ser necessário incluir todas as sub-redes para garantir que você identifique cada dispositivo. Porém, é possível limitar o escopo conforme a necessidade. Por exemplo, será possível executar várias verificações nas sub-redes específicas se isso simplificar a tarefa de descoberta.

- 3 Se desejar se comunicar com dispositivos de rede e classificá-los com mais precisão, clique em **ativar faixas adicionais**.

Nota: Se você não puder conectar-se remotamente, sua rede ou seus computadores poderão ter os firewalls ativados. Poderá ser necessário desativá-los para executar a descoberta.

- 4 Se desejar continuar imediatamente para a segunda etapa da configuração de primeira instalação, marque **Executar o Assistente de Instalação do Symantec Agent**.

Consulte ["Para instalar o Symantec Management Agent e os plug-ins da solução"](#) na página 181.

- 4 Clicar em **Descobrir**.

Para instalar o Symantec Management Agent e os plug-ins da solução

O Assistente de **Instalação do agente** permite instalar o Symantec Management Agent e os plug-ins da solução nos computadores que você quer gerenciar. Ele também permite otimizar a instalação do agente com base no número de computadores em seu ambiente.

Depois de instalar o Symantec Management Agent em um computador-cliente, o agente enviará uma solicitação de registro ao Notification Server para estabelecer uma comunicação confiável. Com base nas regras que você especificar nas políticas do registro do agente, o Notification Server permitirá ou bloqueará automaticamente as solicitações de registro. Observe que a política de registro do agente padrão aceita todas as solicitações recebidas. Se você quiser permitir que somente o computador especificado possa se registrar automaticamente no Notification Server, defina políticas personalizadas de registro do agente.

Consulte [“Sobre o registro do agente”](#) na página 237.

Consulte [“Para criar uma política de registro do agente”](#) na página 243.

Você pode verificar e gerenciar as solicitações de registro na página **Status de registro do agente**, em **Relatórios > Gerenciamento do Notification Server > Registro**.

Consulte [“Para exibir e gerenciar o status do registro do agente”](#) na página 251.

Esta tarefa é uma etapa no processo de execução de tarefas de configuração de primeira instalação.

Consulte [“Para executar as tarefas de configuração inicial”](#) na página 177.

Para instalar o Symantec Management Agent e os plug-ins da solução

- 1 No Console de gerenciamento Symantec, clique em **Início > Gerenciamento do Notification Server > Primeira instalação**.
- 2 Na página **Bem-vindo ao Console de gerenciamento Symantec**, clique em **Instalação do agente**.

- 3 No Assistente de **Instalação do agente**, no painel **Etapas 1 Computadores** a selecione os computadores nos quais você quer instalar o agente e clique em **Avançar**.

Instalar automaticamente em todos os computadores descobertos

Permite instalar o agente em todos os computadores descobertos.

Esta opção de instalação permite também selecionar um agendamento recorrente de instalação de uma lista suspensa. Esta lista é preenchida através da página **Agendamentos compartilhados**. Você modifica, cria e usa agendamentos compartilhados em **Configurações > Notification Server > Agendamentos compartilhados**.

Somente em computadores descobertos selecionados

Permite digitar o nome ou pesquisar os computadores específicos nos quais instalar o agente.

Esta opção apresenta uma lista típica de opções. A coluna à esquerda, conhecida como a coluna de descoberta, permite fazer a busca ou seleção em uma lista de computadores descobertos. A coluna à direita, conhecida como a coluna selecionada, exibe uma lista de computadores selecionados na coluna de descoberta.

Na coluna de descoberta, digite todo ou parte de um nome de computador. Você também pode usar critérios de pesquisa tais como XP, Win ou outras letras que um grupo de seus nomes de computador preferidos contém. A coluna de descoberta lista os computadores descobertos que correspondem a seus critérios de pesquisa.

Use as teclas de seta para mover computadores da coluna de descoberta a coluna selecionada. À medida que você move computadores na coluna selecionada, você vê o número de computadores selecionados mudar na parte inferior direita da coluna.

Esta opção de instalação permite também adicionar critérios de pesquisa para computadores descobertos selecionados. Você pode refinar os resultados na coluna selecionada pesquisando computadores pelo nome ou endereço IP.

- 4 No painel **Etapas 2 Plug-ins**, selecione os plug-ins que você quer instalar e clique em **Avançar**.

Selecione os plug-ins para todas as soluções que tiver instalado. Você também deve selecionar os plug-ins com base nas funções de gerenciamento que deseja executar. Por exemplo, se você quiser coletar um inventário, assegure-se de que os plug-ins de inventário relevantes para seu ambiente estejam ativados.

Ativar todos Permite ativar todos os plug-ins que estão listados. Quando você ativar todos os plug-ins, você verá a proteção verde ao longo do lado esquerdo da lista. Quando você desativar todos os plug-ins, você verá a proteção vermelha.

Barra **On/Off** Permite ativar e desativar os plug-ins selecionados. A proteção vermelha ou verde indica quais plug-ins estão desativados (vermelho) e quais estão ativados (verde).

- 5 No painel **Etapas 3 Otimizar**, selecione o ambiente de instalação:

Ambiente de produção Permite otimizar a instalação do agente de acordo com o número de computadores em seu ambiente de produção.

O número de computadores em seu ambiente determinará os intervalos ideais para o download das configurações do agente e para procurar novas tarefas. Quando você selecionar o número de computadores com o regulador, o assistente ajustará automaticamente esses intervalos.

Consulte [“Opções de configuração de agente e tarefa”](#) na página 184.

Para ver detalhes das configurações do agente e de tarefa, clique em **Mostrar detalhes** e clique em seguida em **OK**.

Teste de ambiente (1 a 50 computadores) Permite testar a instalação em um subconjunto de computadores instalados.

- 6 Clique em **Instalação do agente**.

Opções de configuração de agente e tarefa

No Assistente de **Instalação do agente**, você vê um regulador que permite selecionar de 0 a 15.000 computadores. Baseado no número de computadores que você selecionar, o assistente ajustará automaticamente seu sistema para otimizar o desempenho.

Clique em **Mostrar detalhes** para ver as configurações otimizadas. A caixa de diálogo **Configurações otimizadas** mostra com que frequência uma nova configuração é obtida por download para as configurações do agente. Ela também lista o tempo máximo entre tentativas de ativação para configurações de tarefa.

Os detalhes no assistente se aplicam aos computadores descobertos nos quais você escolheu instalar o agente. Se precisar definir ou modificar opções de configuração do agente para outros computadores, você poderá fazê-lo no Console de gerenciamento Symantec, em **Configurações > Agentes/Plug-ins > Configurações direcionadas do agente**. Para otimizar as configurações da tarefa, clique em **Ajustes > Notification Server > Configurações do servidor de sites**, e, no painel esquerdo, clique em **Gerenciamento de site > Configurações > Task Service > Configurações do Task Service**. No painel direito, defina **Tempo mínimo entre tentativas de ativação**.

Consulte [“Para instalar o Symantec Management Agent e os plug-ins da solução”](#) na página 181.

Tabela 10-2 Opções para configurações ideais de agente e tarefa

Número de computadores no ambiente de produção	Configurações otimizadas de agente	Configurações otimizadas de tarefas
0 - 100	5 minutos	1 minuto
100 - 5.000	uma hora	5 minutos
5.000 - 10.000	duas horas	5 minutos
10.000 - 15.000	três horas	5 minutos
15.000 +	quatro horas	5 minutos

Coleta de informações do inventário

Coletar informações iniciais do inventário é a chave para gerenciar sua rede. Todas as soluções usam inventário e as informações que o inventário coleta preenchem as exibições do computador, do software e outras páginas e outros campos no console. Saber o que está instalado em sua rede é essencial para coletar os dados certos de modo que você possa tomar decisões de gerenciamento essenciais.

Sua rede é exclusiva. Portanto, é necessário determinar quais informações você deseja coletar, sobre quais recursos você deseja coletar as informações e com que frequência coletá-las.

Na janela da política **Coletar inventário**, você pode desativar a política ou ativá-la. Você também seleciona um agendamento padrão ou um agendamento personalizado no qual garantir que a política é atual. Antes de coletar as informações

do inventário, considere quais informações você precisa controlar e com que frequência você quer atualizá-las. Você também deve considerar se há alguma circunstância onde você desejaria desativar a política de inventário. O padrão é deixar a política ativada.

Você pode coletar os seguintes tipos de informações do inventário:

Hardware e sistema operacional	Permite coletar o inventário de CPUs, unidades de disco rígido, memória, firmware, usuários e grupos.
Software	Permite coletar o inventário sobre programas Windows e Pacotes de software UNIX/Linux/Mac.
Propriedades do arquivo	Permite coletar informações sobre fabricantes, versões, tamanho e o nome interno.
Aplicativos de servidor	Se você tiver o Inventory Pack for Servers instalado, ele permitirá coletar informações sobre aplicativos de servidor.

Esta tarefa é uma etapa no processo de execução de tarefas de configuração de primeira instalação.

Consulte [“Para executar as tarefas de configuração inicial”](#) na página 177.

Para coletar as informações de inventário

- 1 No Symantec Management Console, clique em **Início > Gerenciamento do Notification Server > Primeira instalação**.
- 2 Na página **Bem-vindo ao Symantec Management Console**, clique em **Coletar inventário**.
- 3 Na janela da política **Coletar inventário completo** ao lado de **Regras/Ações da política**, deixe a política ativada.

Se você tiver uma necessidade específica para interromper a execução da política por um tempo, clique em **Desativar** para desativar a política.

- 4 Selecione um agendamento para manter a política atual. Você pode selecionar um agendamento padrão ou criar um agendamento personalizado.

Esta lista de agendamentos é preenchida através da página **Agendamentos compartilhados**. Você modifica, cria e usa agendamentos compartilhados em **Configurações > Notification Server > Agendamentos compartilhados**.

- 5 Na janela da política **Coletar inventário completo**, verifique os detalhes do inventário e selecione os tipos de inventário para serem coletados. Faça alterações conforme a necessidade.

Para ver detalhes sobre os tipos de inventário que você selecionou, na área **Regras/Ações da política** da janela, clique em **Avançado**. Você pode selecionar os itens adicionais sobre os quais você deseja coletar dados de inventário. Se você fizer alterações, clique em **OK**.

- 6 Na janela da política **Coletar inventário completo** na área **Aplica-se a/Conformidade**, verifique os detalhes.

Esta área mostra detalhes sobre o inventário que é coletado em computadores de destino. Você pode verificar a conformidade com a política de inventário, modificar quais computadores coletam o inventário e fazer outras alterações conforme a necessidade.

- 7 Clique em **Salvar alterações**.

Para agendar gerenciamento de patches

O Assistente da opção **Agendar patch** permite especificar quando fazer o download das definições de atualização de software, com que frequência verificar os computadores em busca de atualizações disponíveis e quando instalar as atualizações. Você pode também especificar as notificações que deseja receber.

Esta tarefa é uma etapa no processo de execução de tarefas de configuração de primeira instalação.

Consulte [“Para executar as tarefas de configuração inicial”](#) na página 177.

Para agendar o gerenciamento de patches

- 1 No Console de gerenciamento Symantec, clique em **Início > Gerenciamento do Notification Server > Primeira instalação**.
- 2 Na página **Bem-vindo ao Console de gerenciamento Symantec**, clique em **Agendar patch**.

3 No assistente da opção **Agendar patch**, execute as seguintes etapas:

Etapas 1 Download Permite especificar o agendamento do download das definições de atualização de software.

Note que se você ativar o download das definições de atualização de software de um sistema operacional, todos os fornecedores deste sistema operacional serão automaticamente selecionados para o download.

Etapas 2 Notificações Permite especificar as notificações que deseja receber.

Etapas 3 Verificar e instalar atualizações Permite especificar com que frequência verificar os computadores em busca de atualizações disponíveis e quando instalar as atualizações.

4 Clique em **Agendar patch**.

Para descobrir os recursos na rede

- [Capítulo 11. Para descobrir computadores Windows](#)
- [Capítulo 12. Para importar recursos do Active Directory](#)
- [Capítulo 13. Para descobrir dispositivos de rede](#)

Para descobrir computadores Windows

Este capítulo contém os tópicos a seguir:

- [Métodos de descoberta de recursos](#)
- [Métodos de descoberta para computadores Windows](#)
- [Para descobrir computadores com descoberta de recursos de domínio](#)

Métodos de descoberta de recursos

A identificação de todos os recursos em sua rede é uma das primeiras do gerenciamento de rede bem-sucedido. O Symantec Management Platform fornece ferramentas para identificar automaticamente dispositivos em sua rede. Cria também recursos para dispositivos descobertos no banco de dados de gerenciamento de configuração, também conhecido como CMDB (Configuration Management Database). A capacidade de descobrir recursos automaticamente remove a necessidade de entradas manuais demoradas e sujeitas a erro.

Você pode executar uma descoberta manual a qualquer momento ou configurar uma agenda. Agendando a descoberta, você pode automaticamente criar recursos de CMDB para novos computadores à medida que eles são adicionados à rede.

Tabela 11-1 Métodos de descoberta de recursos

Método	Descrição
Descoberta de recursos de domínio	Se deseja descobrir rapidamente computadores Windows, você pode usar a descoberta de recursos do domínio. Este método permite descobrir os computadores que têm uma conta confiável em um domínio. Quando você instala o Notification Server, você tem a oportunidade de usar este método para descobrir computadores automaticamente. Consulte “Métodos de descoberta para computadores Windows” na página 191.
Importação do Active Directory	Você pode importar alguns ou todos os recursos de seu Microsoft Active Directory para o CMDB. Você pode configurar regras de importação dos recursos e identificar e importar os recursos que você deseja. Você pode então configurar agendas para executar importações completas e para atualizar importações nos intervalos apropriados. Consulte “Métodos de descoberta para computadores Windows” na página 191.
Descoberta de rede	Se deseja descobrir todos os recursos em todas as plataformas, use a Descoberta de rede. Usando a Descoberta de rede, você pode identificar todos os dispositivos IP que estão conectados à rede. Você pode descobrir roteadores, switches, hubs, impressoras da rede, servidores Novell NetWare e computadores Windows, UNIX, Linux e Macintosh. Consulte “Sobre a Descoberta de rede” na página 208.

Métodos de descoberta para computadores Windows

Para gerenciar computadores, faça o seguinte:

- Descubra os computadores em sua rede.
- Crie recursos para eles no CMDB.

Este processo é chamado de descoberta e permite descobrir os computadores em que você pode instalar o Symantec Management Agent e vários agentes/plug-ins da solução.

Você pode descobrir computadores Windows fazendo o seguinte:

- Pesquisar todos os computadores Windows em sua rede que estão registrados em um domínio específico
- Pesquisar todos os computadores Windows em sua rede que correspondem às unidades organizacionais que você especifica

Se deseja descobrir os computadores que estão em execução em outros sistemas operacionais, você pode usar a Descoberta de rede.

Consulte “[Métodos de descoberta de recursos](#)” na página 190.

Tabela 11-2 Métodos de descoberta para computadores Windows

Método	Descrição
Descoberta de recursos	Pesquisa o domínio especificado para todos os computadores registrados nesse domínio. Você deve escolher pelo menos uma das opções, Lista de navegação do domínio ou Participação em domínio. Consulte “Para descobrir computadores com descoberta de recursos de domínio” na página 192.
Importação do Microsoft Active Directory	Permite importar os recursos do computador que correspondem às unidades organizacionais que você especifica. Você também pode filtrar os computadores que estiveram ativos durante um número específico de dias ou que estão executando um sistema operacional Windows específico. Esse método retorna informações detalhadas sobre o sistema operacional de cada um dos computadores descobertos e é o método preferencial. Consulte “Para importar recursos usando a importação do Microsoft Active Directory” na página 199.

Você pode usar estes métodos de descoberta para identificar todos os seus computadores em domínios ou você pode descobrir computadores em um único domínio.

Para descobrir computadores com descoberta de recursos de domínio

Você pode descobrir computadores Windows pesquisando as informações dos recursos do domínio. Os computadores descobertos têm um recurso criado para eles no CMDB. Você pode executar uma descoberta manualmente ou usar uma

agenda. Depois que uma descoberta for executada, você poderá exibir os relatórios que mostram os resultados da descoberta.

Este banco de dados contém as seguintes informações sobre cada computador descoberto:

- Nome (Lista de navegação do domínio e Participação em domínio)
- Nome do sistema operacional (Lista de navegação do domínio e Participação em domínio)
- Versão principal (Lista de navegação do domínio)
- Versão secundária (Lista de navegação do domínio)
- Plataforma (Lista de navegação do domínio)

Consulte [“Métodos de descoberta para computadores Windows”](#) na página 191.

Nota: A mensagem de status na página **Descoberta de recursos** mostra a última vez em que a descoberta foi executada manualmente na página. A hora não é atualizada para mostrar uma descoberta agendada subsequente que tenha sido executada.

Para descobrir computadores com descoberta de recursos de domínio

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descobrir > Importar participação no domínio/WINS**.
- 2 Na página **Importação de Participação no domínio/WINS**, em **Domínios a pesquisar**, digite o nome de um domínio que você quer procurar e clique no ícone de adição.
- 3 (Opcional) Para inserir um nome de usuário e uma senha diferentes para o domínio para que o Notification Server tenha acesso, conclua as etapas a seguir, em ordem:
 - Selecione o domínio.
 - Clique no ícone do lápis.
 - Clique em **Usar essas credenciais**.
 - Digite o nome de usuário e a senha e clique em **OK**.
- 4 Selecione ao menos uma das seguintes opções:

Lista de navegação do domínio

Este método é projetado para ambientes pequenos, ponto a ponto.

O método usa a lista de navegação da rede para descobrir todos os computadores no domínio. A opção de navegação descobre todos os computadores que compartilham arquivos ou impressoras ou que executam o serviço Windows Messenger. Esses computadores incluem Windows NT/2000/2003/2008/95/98/98 SE/ME/XP/7/8.

Este método também pode descobrir computadores em um grupo de trabalho que cumprem os critérios de busca.

A Lista de navegação do domínio trabalha enumerando os registros na lista de navegação do computador. Esta lista de navegação do computador foi projetada para um ambiente pequeno e ponto-a-ponto; ou seja, ela não se adapta bem a grandes ambientes.

Quando o Notification Server executar uma descoberta da Lista de navegação do domínio, ele solicitará uma cópia da lista de navegação do computador. A lista de navegação inclui informações adicionais, tais como o sistema operacional e a versão do computador. Ela faz então uma pesquisa inversa do nome do computador para obter seu endereço IP.

Você pode ter problemas para descobrir computadores usando este método se as seguintes condições existirem:

- O computador não está na lista de navegação do computador.
- O computador está na lista de navegação do computador, mas não está registrado como compartilhando arquivos.
- Pode levar entre 15 e 51 minutos para que as mudanças sejam refletidas na lista de navegação do computador.

O método de descoberta da Lista de navegação para o domínio obtém o máximo possível da lista de navegação do computador e o faz o mais rapidamente possível. Este método pode sobrecarregar um PDC em um grande domínio ou em um ambiente com vários domínios. A Symantec recomenda que você execute essa ação fora do horário comercial, preferivelmente no final de semana.

Participação no domínio

Esta opção descobre todos os computadores com contas confiáveis no domínio. Ele pode descobrir computadores em domínios do Windows NT 4.0 ou em domínios do Windows 2000 e domínios posteriores do Active Directory. Este método encontra todos os computadores Windows NT/2000/2003/2008/XP/7/8 no domínio. Porém, não são encontrados computadores Windows 95/98/98 SE/ME.

Nota: Informações limitadas podem ser descobertas em computadores em domínios do NT 4.0. Por exemplo, o sistema operacional específico do computador não é conhecido.

A descoberta da participação em domínio funciona enumerando as contas de computador nos domínios especificados.

Quando você adicionar um computador Windows NT/2000/2003/2008/XP/7/8 a um domínio, uma conta de computador será criada nesse domínio. O computador usa esta conta para autenticar com o domínio, de forma que o computador possa autenticar logons do usuário usando uma conexão protegida. Os computadores Windows 9x não criam uma conta de computador, motivo pelo qual você não pode encontrar computadores Windows 9x usando este método.

Ao descobrir computadores usando o método de Participação em domínio, o Notification Server cataloga essas contas. Diferentemente do método de Lista de navegação do domínio, essas contas não têm nenhuma informação adicional além do nome do computador. O Notification Server ainda faz uma consulta reversa do nome para obter seu endereço IP.

5 Escolha uma das seguintes opções:

Descobrir agora Clique em **Descobrir agora**.

Definir
agendamento Em **Opções de agendamento**, na lista suspensa **Agendar**, especifique o agendamento da importação.

6 Clique em **Salvar alterações.**

7 Para exibir os resultados da descoberta, faça o seguinte:

- Clique em **Exibir relatórios de descoberta**.

- Na janela **Relatórios da descoberta de recursos**, clique com o botão direito do mouse em um relatório e depois clique em **Abrir em nova janela**.
- Digite os parâmetros do relatório.
- Clique em **Refresh**.

Para importar recursos do Active Directory

Este capítulo contém os tópicos a seguir:

- [Sobre a importação do Microsoft Active Directory](#)
- [Sobre a importação das associações de recursos](#)
- [Para importar recursos usando a importação do Microsoft Active Directory](#)

Sobre a importação do Microsoft Active Directory

O recurso da importação do Microsoft Active Directory do Symantec Management Platform permite importar objetos do Active Directory, como usuários, computadores, sites e sub-redes, para o CMDB. Este recurso permite aproveitar os dados que já existem no Active Directory sem o criar novamente. Você pode agendar importações regulares para manter seu CMDB preenchido com recursos atualizados, permitindo melhor gerenciamento de seu ambiente.

A importação do Microsoft Active Directory usa o Lightweight Directory Access Protocol (LDAP) para fornecer a sincronização de sentido único do Active Directory para o Symantec Management Platform. O LDAP é o mesmo protocolo usado por ferramentas de administração padrão do Active Directory. A importação do Microsoft Active Directory suporta o Windows 2000 e 2003 e os domínios do 2008.

Para usar a importação do Microsoft Active Directory, você precisa definir as regras adequadas da importação dos recursos para importar os recursos que você deseja. Você pode agendar as regras de importação de recursos para que sejam executadas em intervalos regulares e você pode executá-las manualmente a qualquer momento. Quando você executar uma regra de importação de recursos, será possível importar todos os dados adequados (uma importação completa). Como alternativa, é possível importar os dados que são novos ou alterados no

Active Directory desde a importação anterior (uma importação de atualização). Como parte do processo de importação, é possível criar automaticamente os filtros ou grupos organizacionais com base nas unidades organizacionais, nos grupos de segurança e nos grupos de distribuição que estão configurados no Active Directory. Estes filtros podem ser usados para especificar os destinos de recursos aos quais você aplica políticas e tarefas.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Consulte [“Para importar recursos usando a importação do Microsoft Active Directory”](#) na página 199.

Durante o processo de importação, os computadores do Active Directory são combinados com os computadores gerenciados no CMDB, usando o nome e o domínio do computador. Porém, a importação do Microsoft Active Directory importa todos os computadores que as regras de importação dos recursos identificam, independentemente do status de instalação de seu Symantec Management Agent. Importar todos os computadores permite importar computadores novos e não gerenciados e destiná-los para a instalação do Symantec Management Agent.

Nota: Você também pode descobrir computadores Windows novos e não gerenciados usando a descoberta de recursos.

Consulte [“Métodos de descoberta para computadores Windows”](#) na página 191.

Se há algum erro no processo da importação, é possível verificar o log do status do Symantec Management Platform para obter informações. O log do status pode ser acessado através do menu Iniciar no computador do Symantec Management Platform: **Todos os programas > Symantec > Diagnóstico > Visualizador de logs Altiris**.

O Symantec Management Platform inclui vários relatórios que fornecem informações sobre as atividades de importação do Microsoft Active Directory. Estes relatórios são armazenados na pasta **Relatórios > Gerenciamento do Notification Server > Microsoft Active Directory**.

Sobre a importação das associações de recursos

O Microsoft Active Directory não apenas armazena objetos, ele também armazena relações entre objetos. O Microsoft Active Directory Import pode extrair estas relações do Active Directory e criar os recursos adequados e as associações de recursos no CMDB. O Microsoft Active Directory Import suporta quatro associações de recursos para usuários e uma associação de recursos entre as sub-redes e os sites.

Tabela 12-1 Associações de recursos suportadas pelo Microsoft Active Directory Import

Associação de recursos	Descrição
Usuário - empresa	Cria um recurso Empresa para o usuário importado com base em seu atributo de "empresa" no Active Directory.
Usuário - departamento	Cria um recurso Departamento para o usuário importado com base em seu atributo de "departamento" no Active Directory.
Usuário - usuário	Cria um ou mais recursos Usuário para o usuário importado com base em seu atributo dos "directReports" no Active Directory.
Usuário - usuário	Cria um recurso Usuário para o usuário importado com base em seu atributo de "gerente" no Active Directory.
Site - sub-rede	Cria um ou mais recursos Sub-rede para o site importado com base em seu atributo dos "siteObjectBL" no Active Directory.
Sub-rede - site	Cria um recurso Site para a sub-rede importada com base em seu atributo de "siteObject" no Active Directory.

A janela **Ativar as associações de recursos** permite usar estas relações em uma regra de importação de recursos para importar outros recursos relacionados que não são especificados explicitamente na regra. Por padrão, todas as associações de recursos disponíveis são ativadas.

Consulte [“Para criar e modificar regras de importação de recursos”](#) na página 201.

Para importar recursos usando a importação do Microsoft Active Directory

Você pode importar todos os computadores que estão registrados no Active Directory. Como alternativa, é possível optar por importar apenas os computadores que correspondem aos critérios que você especifica.

Consulte [“Sobre a importação do Microsoft Active Directory”](#) na página 197.

Quando você instala o Symantec Management Platform, é possível usar a importação do Microsoft Active Directory para importar todos os seus computadores. Você pode então visar os computadores não gerenciados para a instalação do Symantec Management Agent. A importação do Microsoft Active Directory é o método preferido para identificar computadores novos e não gerenciados. Ele

retorna as informações detalhadas nos sistemas operacionais para cada um de seus computadores detectados.

Você também pode usar a Importação do Microsoft Active Directory para criar contas e funções do Symantec Management Platform de grupos e usuários do Windows. Você importa grupos e usuários do Windows de modo que você não tenha que criar contas e funções do Symantec Management Platform manualmente. A Importação do Microsoft Active Directory tem uma regra de importação de recursos para importar recursos de função e conta. Quando esta regra for executada, duplicará a estrutura do grupo e usuário do Windows no Symantec Management Platform. Ela cria um conta do Symantec Management Platform para todos os usuários do Windows nos grupos de segurança selecionados. Cria também funções do Symantec Management Platform para cada um dos grupos de segurança selecionados. Finalmente, coloca as contas recém-criadas de gerenciamento da Symantec nas funções do Symantec Management Platform nas quais o usuário do Windows correspondente é colocado no grupo correspondente do Windows.

Depois da importação inicial, é possível configurar as regras de importação dos recursos que verificam regularmente o Active Directory em busca de recursos novos ou alterados e depois importam os recursos apropriados para o CMDB.

Quando você configurar as regras de importação de recursos, será possível especificar a estrutura de origem do Active Directory da qual a importação será executada. Você pode aplicar restrições que filtrem os computadores importados de acordo com seus requisitos. Por exemplo, é possível importar apenas os computadores cujas contas de computador foram alteradas dentro de um número específico de dias ou aqueles que estão em execução em um sistema operacional Windows específico.

Tabela 12-2 Processo de importação de recursos usando a importação do Microsoft Active Directory

Etapa	Ação	Descrição
Etapa 1	Configure as regras apropriadas de importação de recursos.	Você pode criar qualquer nova regra de importação de recursos que você deseja e modificar as regras existentes para satisfazer seus requisitos. Você também pode excluir todas as regras que você não mais precisar. Consulte “Para criar e modificar regras de importação de recursos” na página 201.
Etapa 2	Agende as regras de importação de recursos.	Para cada regra de importação de recursos, é possível agendar importações completas e atualizar importações a ser executadas em intervalos apropriados. Consulte “Para agendar regras de importação de recursos” na página 204.

Etapa	Ação	Descrição
Etapa 3	Configure a agenda de sincronização do diretório.	O agendamento de sincronização do diretório identifica todos os recursos previamente importados que não existem mais no Active Directory e remove-os do CMDB. Consulte “Para configurar o agendamento de sincronização de diretório” na página 205.
Etapa 4	(Opcional) Execute uma regra de importação de recursos manualmente.	Você pode executar uma regra de importação de recursos manualmente a qualquer momento. Você pode executar a regra como uma importação completa ou uma importação da atualização. Consulte “Para executar manualmente regras de importação de recursos” na página 206.

Para criar e modificar regras de importação de recursos

As regras de importação de recursos permitem especificar os recursos que você deseja importar do Active Directory.

Seis regras padrão de importação de recursos são fornecidas no Symantec Management Platform, uma para cada tipo de recurso suportado: Usuário, computador, fila de impressão, site, sub-rede, função e conta. Você pode modificar estas regras para satisfazer seus requisitos ou você pode criar regras novas para importar os recursos que você deseja.

Você pode configurar uma regra para criar automaticamente filtros baseados em unidades organizacionais do Active Directory, em grupos de segurança e em grupos de distribuição dos quais a regra importará os recursos. Estes filtros podem ser usados para especificar os destinos de recurso aos quais você aplica políticas e tarefas.

Você pode agendar suas regras de importação de recursos para atualizar o CMDB em intervalos regulares ou você pode executar uma regra específica manualmente a qualquer momento. Executar suas regras de importação de recursos periodicamente assegura que todas as mudanças no Active Directory estejam refletidas no CMDB.

Esta tarefa é uma etapa do processo de importação dos recursos que usam a Importação do Microsoft Active Directory.

Consulte [“Para importar recursos usando a importação do Microsoft Active Directory”](#) na página 199.

Para criar ou modificar uma regra de importação de recursos

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, execute uma das tarefas a seguir:

Para criar uma regra nova de importação de recursos	Na barra de ferramentas, clique em Criar nova regra de importação. A regra nova é adicionada à lista de regras de importação de recursos.
Para modificar uma regra existente de importação de recursos	Na lista de regras de importação de recursos, selecione a regra apropriada.
Para excluir uma regra de importação de recursos	Na lista de regras de importação do recurso, selecione a regra apropriada e, em seguida, na barra de ferramentas, clique em Excluir a regra de importação selecionada.

- 3 Na regra de importação de recursos que você deseja modificar, para cada um dos links destacados, clique no link e especifique então as configurações apropriadas.

Tipo de recurso especificado (configuração padrão), computador, usuário, site, sub-rede	Especifica o tipo do domínio e o tipo de recurso que você deseja importar e a estrutura apropriada de origem do Active Directory.
Fonte de dados especificada (configuração padrão)	Especifica o domínio ou o servidor (controlador de domínio) e as credenciais apropriadas da conta de que você deseja importar recursos.

Nenhum (configuração padrão)	Quando você clicar neste link, uma das seguintes caixas de diálogo aparecerá: ■ Selecionar unidade organizacional (OU) Selecione as unidades organizacionais do Active Directory ou os containers (qualquer um que corresponda à estrutura da origem que você especificou na janela Seleção de recursos) de onde importar recursos. Quando você seleciona uma unidade organizacional ou container, é possível optar por incluir seus descendentes. ■ Selecionar grupos de segurança ou Selecionar grupos de distribuição Selecione os grupos específicos do Active Directory dos quais os usuários e grupos serão importados. A caixa de diálogo Selecionar grupos de segurança apenas aparecerá para a regra que importa os recursos de função e conta.
Mapeamentos de coluna especificados (configuração padrão), mapeamentos padrões da coluna	Especifica o mapeamento entre o Symantec Management Platform CMDB e os campos de dados dos recursos do Active Directory. Você pode usar estes mapeamentos para importar atributos adicionais quando o esquema do Active Directory tiver sido estendido.
Todos os computadores, Todos os usuários	Especifica os critérios apropriados para restringir os recursos importados a apenas aqueles que correspondem aos critérios especificados. Um recurso somente será importado se atender às condições dos critérios especificados.
Estas associações de recursos	Especifica as associações de recursos que você deseja usar para importar outros recursos relacionados que não são especificados explicitamente na regra de importação de recursos. Por padrão, todas as associações de recursos disponíveis são ativadas. O Microsoft Active Directory Import pode extrair estas relações do Active Directory e criar os recursos adequados e as associações de recursos no CMDB. Consulte “Sobre a importação das associações de recursos” na página 198.
Agendas especificadas	Especifica as agendas que são usadas para importar recursos. Você pode especificar agendas para importações de dados completas e de atualização. Consulte “Para agendar regras de importação de recursos” na página 204.

- 4 Marque as caixas **Ativado** apropriadas para ativar a importação do computador, do usuário, da sub-rede e dos recursos do site.
- 5 Clique em **Aplicar**.

Para agendar regras de importação de recursos

Para cada regra de importação de recurso, é possível especificar as agendas de importação completa e de importação de atualização. Uma importação completa importa todos os recursos do controlador de domínio de destino ou do domínio. Uma importação de atualização importa apenas os recursos que foram alterados desde a última vez que a regra de importação de recursos foi executada.

Uma única regra de importação de recursos pode incluir ambas as agendas ou você pode configurar diferentes regras de importação completa e de importação de atualização. Se você configurar uma regra específica de importação de atualização, recomendamos que a regra se destine a um controlador de domínio, em vez de um domínio.

Uma importação de atualização executará uma importação completa se alguma das seguintes opções for verdadeira:

- A regra é executada pela primeira vez.
- O domínio ou o servidor que está especificado na regra foi alterado.
- O controlador de domínio do qual a regra foi importada previamente não está disponível.

Caso necessário, é possível sobrepor a agenda e executar uma regra de importação de recursos manualmente a qualquer momento.

Consulte [“Para criar e modificar regras de importação de recursos”](#) na página 201.

Consulte [“Para executar manualmente regras de importação de recursos”](#) na página 206.

Esta tarefa é uma etapa do processo de importação dos recursos que usam a Importação do Microsoft Active Directory.

Consulte [“Para importar recursos usando a importação do Microsoft Active Directory”](#) na página 199.

Para agendar regras de importação de recursos

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, ao lado da regra de importação de recursos que você deseja agendar, selecione **Ativado**.

- 3 Na descrição da regra de importação de recursos, clique em **Agendas especificadas**.
- 4 Na janela **Agenda da regra**, configure qualquer uma, ou ambas, as seguintes agendas:

Agenda de importação completa	Importa todos os recursos identificados pela regra de importação de recursos.
Atualizar agendamento	Importa somente os recursos novos e modificados identificados pela regra de importação de recursos.

Consulte [“Para configurar um agendamento”](#) na página 205.

- 5 Clique em **OK** para fechar a página **Agenda da regra**.
- 6 Clique em **Aplicar**.

Para configurar um agendamento

- 1 Na agenda apropriada, selecione **Ativar**.
- 2 Na lista suspensa **Agendar**, selecione um dos seguintes agendamentos:

Na data/hora	Especificar a data e hora adequada. Se deseja que a agenda se repita, selecione Repetir a cada e especifique então o intervalo da repetição.
Agenda compartilhada	Selecione a agenda compartilhada adequada.

Para configurar o agendamento de sincronização de diretório

Para manter o CMDB sincronizado com os recursos do Active Directory, você precisa configurar a agenda adequada de sincronização do diretório. A agenda de sincronização do diretório identifica todos os recursos previamente importados que não mais existirem no Active Directory e remove-os do CMDB. Detecta também todos os recursos que forem renomeados ou movidos para fora das unidades organizacionais das quais eles foram importados inicialmente e excluir os registros correspondentes do CMDB.

Aviso: Se você mover um computador de um domínio para um grupo de trabalho, será necessário excluir o registro do computador do Active Directory para evitar a duplicação no CMDB.

Esta tarefa é uma etapa do processo de importação dos recursos que usam a Importação do Microsoft Active Directory.

Consulte [“Para importar recursos usando a importação do Microsoft Active Directory”](#) na página 199.

Para configurar a agenda de sincronização do diretório

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, em **Agenda de sincronização do diretório**, selecione **Ativado**.
- 3 Na lista suspensa **Agendar**, selecione um dos seguintes agendamentos:

Na data/hora	Especificar a data e hora adequada. Se deseja que a agenda se repita, selecione Repetir a cada e especifique então o intervalo da repetição.
Agenda compartilhada	Selecione a agenda compartilhada adequada.

- 4 Clique em **Aplicar**.

Para executar manualmente regras de importação de recursos

Se você precisa importar imediatamente recursos específicos, é possível executar a regra apropriada de importação de recursos manualmente. Você pode executar a regra de importação de recursos como uma importação completa ou uma importação de atualização. Executar uma regra de importação de recursos manualmente não tem nenhum efeito em sua agenda, se uma está ativada.

Consulte [“Para agendar regras de importação de recursos”](#) na página 204.

Esta tarefa é uma etapa do processo de importação dos recursos que usam a Importação do Microsoft Active Directory.

Consulte [“Para importar recursos usando a importação do Microsoft Active Directory”](#) na página 199.

Para executar regras de importação de recursos manualmente

- 1 No Symantec Management Console, no menu **Ações**, clique em **Descoberta > Importar Microsoft Active Directory**.
- 2 Na página **Importação do Microsoft Active Directory**, selecione a regra de importação de recursos que você deseja executar.

- 3 Clique em uma das seguintes opções:

Executar a regra de importação selecionada agora (Importação completa)	Executa uma importação completa da regra de importação de recursos selecionada.
Run the selected import rule now (Update Import)	Executa uma importação de atualização da regra selecionada de importação de recursos.

- 4 Se deseja interromper por qualquer motivo o processo de importação, clique em **Parar**.

Para descobrir dispositivos de rede

Este capítulo contém os tópicos a seguir:

- [Sobre a Descoberta de rede](#)
- [Para descobrir dispositivos de rede](#)
- [Para delegar tarefas de Descobertas de rede aos usuários não administradores](#)
- [Importação de arquivos Management Information Bases \(MIB\)](#)

Sobre a Descoberta de rede

A Descoberta de rede permite descobrir todos os dispositivos IP que estão conectados a sua rede. A Descoberta de rede permite encontrar dispositivos de rede novos e os dispositivos de rede cujas propriedades de descoberta foram alteradas.

A descoberta de rede está incluída no Symantec Management Platform.

A Descoberta de rede pode descobrir roteadores, parâmetros, hubs, impressoras de rede, servidores Novell NetWare e os computadores que executam Windows, UNIX, Linux e Macintosh. Você pode usar uma variedade de protocolos para descobrir dispositivos, como AMT, SNMP, WMI e outros.

As informações coletadas podem ajudá-lo fazer o seguinte:

- Planejar a geração de imagem
- Atualizar drivers em tipos específicos de hardware
- Configurar mudanças nos roteadores ou parâmetros

- Identificar os computadores que executam sistemas operacionais atualmente não suportados pelo Symantec Management Agent

Você também pode atualizar categorias de modo que os novos dispositivos adicionados à rede possam ser identificados durante a descoberta.

Como a Descoberta de rede integra-se ao Symantec Management Platform, quando os dispositivos forem descobertos, eles serão criados automaticamente como recursos no banco de dados central da plataforma (CMDB). Usando o componente do gerenciamento de tarefas da plataforma, você pode agendar tarefas de descoberta para que sejam executadas em um momento que melhor atenda às suas necessidades.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Você também pode descobrir computadores baseados em Windows através dos domínios ou da importação com o Microsoft Active Directory.

Consulte [“Métodos de descoberta de recursos”](#) na página 190.

Para descobrir dispositivos de rede

Para ajudá-lo a gerenciar sua rede com êxito, é necessário identificar os vários dispositivos da rede. A Descoberta de rede permite encontrar novos dispositivos de rede, identificar dispositivos de rede previamente descobertos que não são mais encontrados e encontrar os dispositivos de rede cujas propriedades de descoberta foram alteradas. A descoberta é realizada executando as tarefas que detectam dispositivos e relatando os dados ao Notification Server. Os dados da descoberta sobre os dispositivos são armazenados como recursos conhecidos no Configuration Management Database (CMDB). Para manter os dados de descoberta atualizados, configure tarefas de descoberta automatizadas para serem executadas em intervalos regulares.

Você pode descobrir todos os dispositivos em sua rede e inserir esses dispositivos no CMDB.

Consulte [“Sobre a Descoberta de rede”](#) na página 208.

Tabela 13-1 Processo de descoberta de dispositivos de rede

Etapa	Ação	Descrição
Etapa 1	(Opcional) Configure as opções da Descoberta de rede.	É possível configurar opções padrão de tarefas e as classificações de SNMP. Consulte “Para definir as configurações de descoberta” na página 210.

Etapa	Ação	Descrição
Etapa 2	Crie uma tarefa de Descoberta de rede.	Você pode criar e agendar uma tarefa para descobrir um único dispositivo ou vários dispositivos em uma rede. Você pode usar dois métodos para criar tarefas: usando o Assistente de Descoberta de rede ou criando tarefas manualmente. Consulte “Para criar tarefas de descoberta de rede usando o assistente” na página 212. Consulte “Para criar e modificar manualmente as tarefas de Descoberta de rede” na página 213.
Etapa 3	(Opcional) Modifique as configurações ou as agendas de tarefas.	Após criar uma tarefa de Descoberta de rede, você poderá modificar suas configurações ou adicionar novas agendas. Consulte “Para criar e modificar manualmente as tarefas de Descoberta de rede” na página 213.
Etapa 4	Veja os dados da descoberta.	Você pode ver o status das tarefas de Descoberta de rede e ver os relatórios que mostram os resultados da descoberta. Consulte “Para exibir dispositivos descobertos em exibições organizacionais” na página 219. Consulte “Para exibir relatórios de descoberta” na página 219.
Etapa 5	Classifique os dispositivos desconhecidos.	Se houver dispositivos com classificação desconhecida, você poderá modificar a lista de classificações de SNMP. Consulte “Para classificar dispositivos SNMP ” na página 220.

Para definir as configurações de descoberta

Você pode definir configurações globais para tarefas de Descoberta de rede. Estas configurações são usadas quando uma nova tarefa é criada.

Você pode configurar a descoberta de rede das seguintes maneiras:

Configurações das tarefas de descoberta	Nas configurações de Descoberta de rede, você pode definir o número máximo de segmentos por tarefas de descoberta. Durante o processo de descoberta, um segmento separado é usado para descobrir cada dispositivo. Este número é a contagem máxima padrão do segmento para usar quando uma nova tarefa de Descoberta de rede é criada. Você também pode configurar essa contagem para uma tarefa individual editando as propriedades avançadas da tarefa. Será conveniente reduzir esse valor se as tarefas de descoberta sobrecarregarem o desempenho do servidor.
Classificação de dispositivos SNMP	Quando que você descobre dispositivos SNMP, é possível identificar uma classificação do tipo do dispositivo de rede com o recurso. Este método permite identificar recursos como roteadores, parâmetros, impressoras, servidores etc. Você pode configurar as classificações de recursos SNMP descobertos. Consulte "Para classificar dispositivos SNMP" na página 220.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte "[Para descobrir dispositivos de rede](#)" na página 209.

Para definir as configurações de descoberta

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Descoberta e inventário** e clique em **Configurações da Descoberta de rede**.
- 3 Na página **Configurações da Descoberta de rede**, digite o número máximo de segmentos por tarefa de entrega.

Durante o processo de descoberta, um segmento separado é usado para descobrir cada dispositivo.

Este número é a contagem máxima padrão do segmento para usar quando uma nova tarefa de Descoberta de rede é criada. Você também pode configurar essa contagem para uma tarefa individual editando as propriedades avançadas da tarefa.

Será conveniente reduzir esse valor se as tarefas de descoberta sobrecarregarem o desempenho do servidor.

- 4 Clique em **Salvar alterações**.

Para criar tarefas de descoberta de rede usando o assistente

O Assistente de Descoberta de rede é uma ferramenta do administrador que guia você pela criação de tarefas de descoberta e definição de configurações. Você pode modificar as configurações avançadas e as agendas da tarefa posteriormente editando a tarefa.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Para criar tarefas de descoberta de rede usando o Assistente de Descoberta de rede

- 1 No Console de gerenciamento Symantec, no menu **Início**, clique em **Descoberta e inventário > Descoberta de rede**.
- 2 Na Web part **Ações do Início rápido da Descoberta de rede**, clique em **Iniciar o Assistente de descoberta**.
- 3 No assistente, selecione um método de descoberta e clique em **Avançar**.
Consulte [“Métodos de descoberta de dispositivos de rede”](#) na página 216.
- 4 Especifique as partes da rede a serem descobertas e clique em **Avançar**.
Consulte [“Sobre a seleção de intervalos de rede para descobrir”](#) na página 217.
- 5 Selecione um perfil de conexão e clique em **Avançar**.
Os perfis de conexão especificam os protocolos que você deseja usar para a descoberta. Você pode usar um perfil existente ou criar um perfil novo.
Consulte [“Para criar perfis de conexão com Descoberta de rede”](#) na página 214.
Consulte [“Para criar ou duplicar um perfil de conexão”](#) na página 215.
- 6 Nomeie a tarefa e clique em **Avançar**.
- 7 Agende a tarefa e clique em **Concluir**.
Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.
- 8 Para exibir as tarefas criadas pelo Assistente de Descoberta, exiba a parte inferior da **Página inicial da Descoberta de rede**.

Poderá ser necessário clicar no ícone Atualizar para exibir as tarefas criadas recentemente.

Para criar e modificar manualmente as tarefas de Descoberta de rede

Você pode criar manualmente tarefas no Portal de gerenciamento de tarefas. Esta opção permite configurar opções e agendamentos avançados. Quando criar tarefas manualmente, você poderá descobrir uma rede ou um dispositivo individual.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Para criar manualmente uma tarefa para descobrir uma rede

- 1 No Symantec Management Console, execute um dos seguintes procedimentos:
 - No menu **Início**, clique em **Descoberta e inventário > Descoberta de rede** e então, na Web part **Gerenciamento de tarefas da Descoberta de rede**, na guia **Tarefas disponíveis**, clique em **Novo(a)**.
 - No menu **Gerenciar**, clique em **Trabalhos e tarefas**. No painel esquerdo, expanda **Trabalhos e tarefas do sistema**, clique com o botão direito do mouse em **Descoberta e inventário**, e clique em **Novo(a) > Tarefa**. Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, em **Descoberta e inventário**, clique em **Descobrir rede**.
- 2 Atribuir à tarefa um nome exclusivo e descritivo.
- 3 Selecione um perfil de conexão.

Os perfis de conexão especificam os protocolos que você deseja usar para a descoberta. Você pode usar um perfil existente ou criar um perfil novo.

Consulte [“Para criar perfis de conexão com Descoberta de rede”](#) na página 214.

Consulte [“Para criar ou duplicar um perfil de conexão”](#) na página 215.
- 4 Selecione um método de descoberta.

Consulte [“Métodos de descoberta de dispositivos de rede”](#) na página 216.
- 5 Especifique as partes da rede a serem descobertas.

Consulte [“Sobre a seleção de intervalos de rede para descobrir”](#) na página 217.
- 6 (Opcional) Para configurar o número máximo de dispositivos a serem descobertos simultaneamente, clique em **Avançado**.
- 7 Clique em **OK**.

- 8 Na janela de tarefa que é aberta, agende a tarefa.
Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.
- 9 Para exibir a tarefa, no painel esquerdo, clique em **Trabalhos e tarefas > Trabalhos e tarefas do sistema > Descoberta e inventário**. Poderá ser necessário clicar no ícone Atualizar para exibir as tarefas criadas recentemente.

Para criar manualmente uma tarefa para descobrir um único dispositivo

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**. No painel esquerdo, expanda **Trabalhos e tarefas do sistema**, clique com o botão direito do mouse em **Descoberta e inventário**, e clique em **Novo(a) > Tarefa**.
- 2 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, em **Descoberta e inventário**, clique em **Descobrir dispositivo**.
- 3 Atribuir à tarefa um nome exclusivo e descritivo.
- 4 Selecione um perfil de conexão.
Os perfis de conexão especificam os protocolos que você deseja usar para a descoberta. Você pode usar um perfil existente ou criar um perfil novo.
Consulte [“Para criar perfis de conexão com Descoberta de rede”](#) na página 214.
Consulte [“Para criar ou duplicar um perfil de conexão”](#) na página 215.
- 5 Clique em **OK** para salvar a tarefa.
- 6 Na janela da tarefa que é aberta, clique em **Nova agenda**.
- 7 Na caixa de diálogo **Novo agendamento**, agende a tarefa, especifique o dispositivo que você quer descobrir digitando o endereço IP ou o nome, e clique em **Agendar**.
Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.
- 8 Para exibir a tarefa, no painel esquerdo, clique em **Trabalhos e tarefas > Trabalhos e tarefas do sistema > Descoberta e inventário**. Poderá ser necessário clicar no ícone Atualizar para exibir as tarefas criadas recentemente.

Para criar perfis de conexão com Descoberta de rede

As tarefas de Descoberta de rede usam os perfis de conexão para configurar os protocolos que são usados para se comunicar com os dispositivos de rede. Os perfis de conexão são um componente do Symantec Management Platform. O modo como você usa os protocolos e os perfis de conexão têm consequências importantes em como a Descoberta de rede detecta dispositivos.

A Descoberta de rede usa perfis de conexão para se conectar aos dispositivos de destino usando os protocolos ativados no perfil. Quando um dispositivo é descoberto, um recurso para esse dispositivo é criado no CMDB. O recurso mantém um registro dos protocolos usados para se comunicar com o dispositivo.

Se as mudanças forem realizadas nos perfis de conexão em relação aos protocolos ou às credenciais usadas para esses protocolos, e caso você queira descobrir dispositivos usando essas configurações alteradas, será necessário executar uma descoberta novamente.

É possível criar e usar perfis de conexão diferentes dependendo do tipo de dispositivos e protocolos usados em sua rede. Ao configurar tarefas de Descoberta de rede, você pode usar um perfil de conexão existente ou criar seu próprio perfil.

Consulte [“Para criar tarefas de descoberta de rede usando o assistente”](#) na página 212.

Consulte [“Para criar e modificar manualmente as tarefas de Descoberta de rede”](#) na página 213.

Para criar um perfil de conexão

- 1 Em uma tarefa de Descoberta de rede, clique no perfil de conexão **Novo(a)**.
Os protocolos relacionados são aqueles que são aceitos.
- 2 Atribua um nome ao perfil de conexão.
- 3 Ative ou desative cada protocolo e configure as opções operacionais e selecione as credenciais de acesso para cada protocolo.
Consulte [“Para gerenciar credenciais”](#) na página 115.
- 4 Clique em **OK**.
- 5 Selecione um perfil na lista suspensa.

Para criar ou duplicar um perfil de conexão

Os perfis de conexão armazenam as informações necessárias à comunicação com computadores e outros dispositivos de rede usando protocolos padrão de monitoramento da rede. Estes protocolos incluem SNMP, WMI, WSMAN e muitos outros.

Os perfis de conexão são associados aos dispositivos durante a descoberta de rede. Durante a descoberta, um perfil de conexão é selecionado para definir os protocolos e as credenciais a serem usadas. Quando a descoberta for concluída, este perfil de conexão será associado a cada recurso descoberto. Quando forem necessárias informações, o perfil de conexão associado será usado para se conectar.

Normalmente, é necessário criar um novo perfil de conexão para cada segmento da rede que usa credenciais diferentes de monitoramento de rede.

Para criar um perfil de conexão

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Monitoramento e alertas > Gerenciamento de protocolos > Perfis de conexão** e clique em **Gerenciar perfis de conexão**.
- 3 Na página **Gerenciar perfis de conexão**, clique em **Adicionar configurações** e forneça um nome para o novo perfil.
- 4 Na caixa de diálogo **Definir configurações de grupo**, digite o nome do novo perfil, ative os protocolos desejados e forneça os detalhes exigidos do protocolo.

Na parte superior direita, ao lado de cada protocolo que você quer ativar, clique no círculo colorido e em **Ativado**.

Para obter mais informações, clique na página e pressione **F1**.

- 5 Clique em **OK**.

Métodos de descoberta de dispositivos de rede

Quando fizer a descoberta de dispositivos de rede, você poderá usar um dos seguintes métodos de descoberta: ping ou ARP.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Você inicia tarefas de descoberta através do Assistente de Descoberta de rede, que você acessa da home page da descoberta de rede. É aqui que você indica qual método de descoberta deseja usar.

Consulte [“Para criar tarefas de descoberta de rede usando o assistente”](#) na página 212.

Consulte [“Para criar e modificar manualmente as tarefas de Descoberta de rede”](#) na página 213.

Tabela 13-2 Métodos de descoberta de rede

Método	Descrição
Ping	A existência do dispositivo é determinada com o envio de uma solicitação de ping ICMP a cada endereço IP possível em um intervalo especificado ou uma sub-rede. Quando um dispositivo recebe um ping, ele reage com uma resposta, relatando a presença do dispositivo ao mecanismo de descoberta. Você pode usar este método para executar uma busca detalhada que encontre todos os dispositivos. Este método não poderá ser utilizado se seu firewall de rede não permitir solicitações de ping. Este método pode não ser o melhor para sub-redes dispersas (aquelas com poucos dispositivos em seu espaço de endereço). O mecanismo pode dispendar muito tempo aguardando respostas de dispositivos que não existem. Esta situação ocorre porque o mecanismo aguarda até que o período de tempo limite especificado expire e, se aplicável, o mecanismo repete uma ou mais vezes.
ARP	A existência do dispositivo é determinada inicialmente lendo a tabela de cache do ARP de um dispositivo da infraestrutura de rede (como um parâmetro ou roteador). A tabela Cache do ARP é lida através do dispositivo e cada dispositivo na tabela é contatado e identificado individualmente. Este método de descoberta oferece ao mecanismo de descoberta um conjunto de dispositivos a serem descobertos. Porém, as entradas da tabela Cache do ARP são removidas após períodos de inatividade relativamente curtos. Isso significa que a verificação por si só não está ciente de dispositivos inativos. Você pode corrigir este problema enviando um ping para cada dispositivo em uma rede de destino. Este processo atualiza a tabela, que contém todos os dispositivos.

Sobre a seleção de intervalos de rede para descobrir

Quando criar uma tarefa de Descoberta de rede, identifique o único dispositivo de rede ou os intervalos de endereços que você quer descobrir. Isso é feito pela especificação dos endereços que você quer incluir ou excluir, ou pela combinação de ambos.

Consulte “[Para criar tarefas de descoberta de rede usando o assistente](#)” na página 212.

Consulte “[Para criar e modificar manualmente as tarefas de Descoberta de rede](#)” na página 213.

Se você tiver um dispositivo de propagação e criar um intervalo de inclusão, o dispositivo de propagação deverá ser incluído no intervalo de inclusão para que também seja descoberto.

Para usar um intervalo personalizado, é possível usar curingas ou intervalos de valores no terceiro ou quarto octeto do endereço. Os itens a seguir são exemplos de como você pode usar um intervalo personalizado:

172.16.[*].[*]	Você pode usar um asterisco como caractere curinga que será equivalente a qualquer valor de 0 a 254.
172.16.[1-24].[1-254]	É possível especificar um intervalo de valores. Qualquer endereço no intervalo será incluído ou excluído.
172.16.[3-30].[1-10]	

Você também pode importar um arquivo de texto para especificar os endereços que deseja incluir ou excluir. Ao configurar um arquivo de texto, é necessário incluir todas as informações necessárias para esse tipo de endereço ou de intervalo. Por exemplo, se você especificar um intervalo de IPs, será necessário incluir o endereço IP inicial, o endereço IP final e a máscara. Você também pode especificar intervalos personalizados de IPs em um arquivo de importação.

O item a seguir é um exemplo do formato de um arquivo de importação:

```
SingleIpAddr, Include, 192.168.0.2,
SingleIpAddr, Exclude, 192.168.0.3,

Hostname, Include, hostname1.company1.com
Hostname, Exclude, hostname2

Subnet, Include, 192.168.0.0, 255.255.255.0
Subnet, Exclude, 192.169.0.0, 255.255.255.0

CustomIpAddrRange, Include, 192.168.*.*, 255.255.0.0
CustomIpAddrRange, Exclude, 10.192.1-25.1-254, 255.0.0.0
CustomIpAddrRange, Include, 10.192.4.1-100, 255.255.254.0

IpAddrRange, Include, 192.168.0.1, 192.168.0.200, 255.255.255.0
IpAddrRange, Exclude, 192.168.0.120, 192.168.1.140, 255.255.255.0
```

Para exibir dispositivos descobertos em exibições organizacionais

Quando um dispositivo é descoberto, um recurso para esse dispositivo é criado automaticamente no Configuration Management Database (CMDB). Você pode visualizar os dispositivos usando exibições organizacionais. As exibições organizacionais mostram todos os recursos conhecidos em seu ambiente. Você pode visualizar todos os dispositivos descobertos em uma exibição, chamada Recursos de rede. Há também exibições para tipos de recursos individuais, tais como computador, impressora da rede etc.

Se o tipo de recurso do dispositivo é conhecido, o tipo de recurso é exibido como uma propriedade do recurso. Se um dispositivo tem um tipo de recurso de 'Recurso de rede', o tipo de dispositivo é desconhecido. Esses dispositivos desconhecidos são listados na exibição Recurso de rede, e não em alguma outra exibição específica de tipo de recurso. Se houver dispositivos com classificação desconhecida, você poderá modificar a lista de classificação do SNMP.

Consulte [“Para classificar dispositivos SNMP ”](#) na página 220.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Para visualizar dispositivos descobertos em exibições organizacionais

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Todos os recursos**.
- 2 No painel esquerdo, expanda **Padrão > Todos os recursos > Ativo** e clique em **Recurso de rede**.
- 3 Para exibir um tipo específico de recurso, no painel esquerdo, clique em um tipo de recurso em **Recurso de rede**.

Para exibir relatórios de descoberta

Você pode exibir os resultados da descoberta em relatórios. Você pode visualizar relatórios predefinidos ou criar seus próprios.

O relatório de descoberta de dispositivos permite filtrar os resultados que estão baseados em um intervalo de datas, no método de descoberta ou protocolo usado, ou na tarefa usada.

Os relatórios de dispositivos descobertos por grupo permitem agrupar os resultados que estão baseados em um intervalo de datas, no método de descoberta ou no protocolo usado, na tarefa usada ou no tipo do dispositivo.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Para exibir relatórios de descoberta

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, expanda **Relatórios > Descoberta e inventário** e clique no relatório que você quer exibir.
- 3 Insira os parâmetros do relatório e clique em **Atualizar**.

Consulte [“Sobre relatórios do Notification Server”](#) na página 440.

Para classificar dispositivos SNMP

Os dispositivos SNMP descobertos são identificados pelo tipo de dispositivo, tal como computador, impressora da rede etc. Para que o tipo de dispositivo seja identificado, a Descoberta de rede deve conhecer a classificação do dispositivo SNMP sobre esse tipo. A Descoberta de rede tem uma lista de dispositivos SNMP comuns predefinidos. Se o dispositivo descoberto está nessa lista, ele pode ser identificado. Se o dispositivo não estiver na lista, ele será identificado como o tipo de recurso genérico **Recurso de rede**.

Você pode exibir a lista predefinida na página **Classificações de dispositivos**. Essa página relaciona classificações de dispositivos normalmente usados. Estes dados incluem o ID de objeto SNMP, o tipo de dispositivo, o fabricante e o modelo. Se o ID de objeto SNMP descoberto corresponder a um item dessa lista, os dados serão preenchidos.

Antes de executar a tarefa Descoberta de rede, verifique a lista de classificação do dispositivo, que contém fabricantes comuns. Se a lista estiver incompleta, você poderá adicionar ou editar classificações para personalizá-la para seu ambiente de rede. Dedicar tempo para verificar e personalizar a lista de classificação de dispositivos resulta em dados de descoberta mais completos. Executar essa tarefa antes de uma descoberta não é necessário. Você pode executar essa tarefa após uma descoberta, mas é necessário executar novamente a descoberta para obter a classificação atualizada.

Se você alterar as informações para uma classificação existente do dispositivo SNMP, você precisará verificar novamente todo o dispositivo que tenha sido classificado previamente usando essa entrada. É necessário verificar novamente para que os dispositivos com informações alteradas sejam reclassificados.

Após executar a tarefa Descoberta de rede, você pode ter dispositivos com classificação desconhecida. Se você conhecer o ID de objeto desses dispositivos, poderá adicioná-los à lista de classificação. Na próxima vez em que executar uma tarefa Descoberta de rede, os dispositivos usarão a lista atualizada para serem classificados.

Você pode configurar os valores da classificação de dispositivos SNMP que são usados para identificar dispositivos SNMP. Uma lista de dispositivos comuns é fornecida em Descoberta de rede. Você pode adicionar, editar ou remover classificações para personalizar esta lista para seu ambiente de rede. Após mudar uma classificação do dispositivo, é necessário redescobri-la para que possa ser reclassificada.

Esta tarefa é uma etapa do processo para descobrir dispositivos de rede.

Consulte [“Para descobrir dispositivos de rede”](#) na página 209.

Para classificar dispositivos SNMP

- 1 No Symantec Management Console, no menu **Início**, clique em **Descoberta e inventário > Descoberta de rede**.
- 2 Na Web part **Ações do Início rápido da Descoberta de rede**, clique em **Classificações de dispositivos SNMP**.
- 3 Para adicionar uma nova classificação, clique em **Adicionar** e insira as informações sobre seu dispositivo.

O ID de objeto SNMP deve ser um valor exclusivo que você pode obter do fabricante do dispositivo.
- 4 Você também pode editar ou remover classificações para que correspondam aos dispositivos em seu ambiente de rede.
- 5 Para reclassificar os dispositivos que são baseados em configurações novas, é necessário executar novamente a descoberta.

Para delegar tarefas de Descobertas de rede aos usuários não administradores

Como um administrador de rede, é possível que você tenha uma equipe de outros administradores a quem você pode delegar determinadas tarefas de administração da rede. Independentemente de você trabalhar sozinho ou com uma equipe de administradores, pode ser necessário delegar tarefas Descoberta de rede a outros usuários não administradores.

As tarefas Descoberta de rede exigem direitos de trabalhar com perfis de conexão e credenciais. Estes direitos são concedidos através de uma combinação de permissões e de privilégios. Por padrão, as permissões são atribuídas a itens, como arquivos, tarefas e assistentes. Os privilégios são concedidos às funções de usuário, incluindo a função predefinida do administrador e as funções predefinidas de não administradores. A interseção das permissões de item e de privilégios de função determina o que os administradores e não administradores podem fazer nos itens.

Consulte [“Sobre a Descoberta de rede”](#) na página 208.

Cada uma das funções predefinidas de usuário que não seja o administrador no Symantec Management Platform inclui privilégios inerentes.

Consulte [“Funções predefinidas de segurança”](#) na página 106.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Para permitir que os usuários descubram dispositivos de rede e trabalhem com perfis de conexão e credenciais, você atribui privilégios às funções de usuário que permitem que essas funções criem perfis de conexão e credenciais. Em seguida, você seleciona uma função de usuário não administrador que será atribuída aos usuários. Em seguida, você limita ou aumenta o escopo da função, removendo ou atribuindo privilégios específicos. Para criar e executar tarefas de descoberta de rede, a função de usuário deverá ter acesso a pelo menos um perfil de conexão padrão. Este perfil pode ser o perfil de conexão padrão.

A função de Supervisores da Symantec é uma função de mais alto nível de não administrador. Outros funcionários podem ser atribuídos a uma função com direitos inerentes limitados. As funções de Atendentes de nível 1 da Symantec e de Atendentes de nível 2 da Symantec são bons exemplos. Estas funções são usadas em algumas das tarefas que estão incluídas no processo definido neste tópico. Você não está limitado a estas funções. Essas são as funções predefinidas mais úteis aos administradores.

Você pode delegar tarefas a mais de uma função de usuário. Para criar, editar ou executar tarefas, um usuário deve ser membro de uma função de segurança que tenha o privilégio de Gerenciamento de tarefas de descoberta.

A função padrão de Supervisores da Symantec inclui mais acesso à descoberta de rede do que outras funções de não administrador. Delegar tarefas à função de Supervisores da Symantec é menos complicado que delegar tarefas a funções que não têm acesso algum para executar tarefas Descoberta de rede.

Selecione uma função à qual delegar tarefas com base em ações que você deseja que os não administradores possam fazer. Delegue as tarefas concluindo, em ordem, cada etapa no processo. As tarefas relacionadas nas últimas etapas poderão depender dos direitos que foram concedidos nas etapas anteriores.

Tabela 13-3 Processo para delegar tarefas de Descobertas de rede a usuários não administradores

Etapa	Tarefa	Descrição
Etapa 1	Adicione não administradores às funções de segurança para executar tarefas Descoberta de rede.	Para delegar tarefas a usuários em funções de não administrador, é necessário atribuir usuários àquelas funções. Consulte “Para adicionar usuários não administradores às funções de segurança para executar tarefas de Descoberta de rede” na página 224.
Etapa 2	Ative funções de não administrador para criar ou executar tarefas Descoberta de rede.	Você pode delegar tarefas Descoberta de rede às funções de não administrador e atribuir usuários não administradores àquelas funções. Diversas funções padrão estão incluídas no Symantec Management Platform e cada uma tem determinados direitos inerentes. A função de Supervisores da Symantec pode executar tarefas Descoberta de rede. Outras funções de não administrador não poderão nem mesmo executar tarefas existentes até que você conceda os privilégios necessários à função. Você deve executar determinadas etapas para ativar funções de não administrador para criar e executar tarefas Descoberta de rede. Por padrão, os administradores, Supervisores da Symantec e Atendentes de níveis 1 e 2 da Symantec podem exibir a página do portal de descoberta de rede. Esta página é um local conveniente através do qual os administradores podem visualizar e executar tarefas Descoberta de rede. Por padrão, os administradores e os supervisores podem exibir todas as partes desta página. Porém, a Web part do gerenciamento de tarefas Descoberta de rede está desativada para outros usuários. Para permitir que outros usuários não administradores exibam e usem esta Web part, atribua a eles uma função de segurança que tenha o privilégio de gerenciamento de tarefas de descoberta ativado. Consulte “Funções predefinidas de segurança” na página 106. Consulte “Para ativar funções de usuário que não seja o administrador para criar ou executar tarefas de Descoberta de rede” na página 226.
Etapa 3	(Opcional, mas recomendado) Atribua privilégios de funções de usuário que não seja o administrador para criar credenciais e perfis de conexão.	Uma função de não administrador pode ser receber privilégios para descobrir dispositivos de rede e criar ou editar credenciais e perfis de conexão. A criação ou edição de credenciais e perfis de conexão pode ser necessária para executar as tarefas que serão relacionadas mais tarde neste processo. Esta etapa é opcional porque os usuários podem criar tarefas de descoberta de rede sem estes privilégios. Ele precisariam simplesmente usar os perfis de conexão existentes aos quais têm acesso. Consulte “Categorias de privilégio de segurança” na página 489. Consulte “Para conceder privilégios de funções de usuário que não seja o administrador para criar credenciais e perfis de conexão” na página 229.

Etapa	Tarefa	Descrição
Etapa 4	Forneça acesso de função de não administrador ao perfil de conexão padrão.	Para criar e executar tarefas Descoberta de rede, uma função de usuário deverá ter acesso ao perfil de conexão padrão (ou a outro perfil de conexão, mas pelo menos a um). Consulte “Para fornecer acesso de função de usuário que não seja o administrador ao perfil de conexão padrão” na página 230.
Etapa 5	Ative funções diferentes daquelas de segurança predefinidas para criar e executar tarefas usando o Assistente de Descoberta de rede.	As seguintes funções de segurança são predefinidas e, por padrão, podem criar e executar tarefas usando o Assistente de Descoberta de rede: ■ Administrador ■ Supervisores da Symantec ■ Trabalhadores do nível 2 da Symantec ■ Trabalhadores do nível 1 da Symantec Se você precisar permitir que outras funções criem e executem tarefas usando o assistente, será necessário fornecer acesso explicitamente. Consulte “Para ativar funções diferentes das funções de segurança predefinidas para criar e executar tarefas usando o Assistente de Descoberta de rede.” na página 231.
Etapa 6	(Opcional) Faça um perfil de conexão somente leitura.	Se quiser permitir a exibição de uma função específica de usuário que não seja o administrador, mas não desejar permitir a edição de um perfil de conexão, você poderá transformar o perfil em somente leitura. Consulte “Para tornar um perfil de conexão somente leitura” na página 232.

Para adicionar usuários não administradores às funções de segurança para executar tarefas de Descoberta de rede

Se desejar delegar tarefas Descoberta de rede a usuários não administradores, eles deverão ter os privilégios necessários para executar essas tarefas. Os privilégios são atribuídos às funções de usuário. Se você não criar um usuário Windows para executar tarefas Descoberta de rede, será necessário criar este usuário primeiro. Em seguida, adicione o usuário à sua função de segurança escolhida ou crie uma função personalizada. Finalmente, conceda privilégios para a função de segurança. Você pode então delegar as tarefas para as quais a função tem privilégios suficientes para executar.

A página do portal da Descoberta de rede é um local conveniente para exibir e executar tarefas de descoberta. Os administradores e supervisores da Symantec têm acesso completo a esta página por padrão. Usuários em outras funções de não administrador podem exibir esta página. Porém, a Web Part **Gerenciamento de tarefas de descoberta** é desativada a menos que você a ativar com o privilégio de Gerenciamento de tarefas de descoberta. Adicionando não administradores às

funções de segurança e concedendo direitos para o gerenciamento de tarefas. Descoberta de rede, você permite que eles exibam e trabalhem por esta página.

Consulte [“Para ativar funções de usuário que não seja o administrador para criar ou executar tarefas de Descoberta de rede”](#) na página 226.

O Symantec Management Platform inclui diversas funções de segurança de não administradores predefinidas por padrão. Você também pode criar funções de segurança personalizadas.

Consulte [“Funções predefinidas de segurança”](#) na página 106.

Consulte [“Para criar e configurar contas de usuário do Symantec Management Platform”](#) na página 225.

Esta tarefa é uma etapa no processo de delegação de tarefas de Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para adicionar usuários não administradores às funções de segurança para executar tarefas de Descoberta de rede

- 1 Faça logon no Console de gerenciamento Symantec como administrador.
- 2 Para criar um novo usuário do Windows, faça o seguinte:
 - No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
 - No painel esquerdo, clique em **Contas**.
 - Na página **Contas**, clique em **Adicionar**.
 - Na caixa de diálogo **Nova conta**, digite um nome para o novo usuário e clique em **OK**.
 - No painel direito, na guia **Geral**, em **Detalhes da conta**, no campo **Nome completo**, digite o nome completo do usuário.
Você pode deixar o campo **E-mail** vazio. Ele não é necessário para este procedimento.
 - Em **Credenciais**, clique em **Adicionar credencial > Windows**.
 - Na caixa de diálogo **Credencial do Windows**, digite o nome de logon que corresponde ao usuário do Windows associado a essa nova conta e clique em **OK**.
 - Ative a conta.
Na parte superior direita da página, clique no círculo colorido e em **Ativado**.

- 3 Para adicionar o usuário a uma função de segurança à qual você quer delegar tarefas, faça o seguinte:
 - Na guia **Membro de**, clique em **Adicionar função**.
 - Na caixa de diálogo **Selecionar função(ões)**, clique em **Atendentes de nível 1 da Symantec** ou em outra função à qual você quer atribuir este usuário, e clique em **OK**.

Se nenhuma das funções de segurança predefinidas atender às suas necessidades, será possível criar uma função de segurança personalizada. Consulte [“Para criar e configurar funções de segurança”](#) na página 88.
- 4 Clique em **Salvar alterações**.

Para ativar funções de usuário que não seja o administrador para criar ou executar tarefas de Descoberta de rede

Você pode delegar tarefas Descoberta de rede aos usuários fora do grupo Administradores da Symantec. Para delegar tarefas, você atribui privilégios às funções de não administrador. Em seguida, você adiciona usuários àquelas funções de usuário que não seja o administrador.

Este tópico descreve como delegar tarefas comuns de Descoberta de rede às seguintes funções de usuário que não seja o administrador:

- Supervisores da Symantec.

Por padrão, os usuários nesta função podem executar tarefas Descoberta de rede existentes. Porém, não podem criar tarefas, por padrão. Isso ocorre porque eles não terão acesso ao perfil de conexão padrão a menos que você conceda esse acesso explicitamente.
- Atendentes de nível 1 e nível 2 da Symantec.

Usuários nestas funções têm direitos limitados. Não podem executar tarefas existentes até que você lhes dê direitos para isso.

Você não é limitado a usar estas funções de não administrador. Elas são mostradas neste tópico como exemplos. Use qualquer função de segurança predefinida que atenda à sua finalidade.

Consulte [“Funções predefinidas de segurança”](#) na página 106.

As tarefas usam perfis de conexão, que usam credenciais. Para que uma função de não administrador crie novas tarefas (e não apenas as execute), é necessário definir permissões de acesso a um perfil de conexão. Você define em seguida um nível de controle (o nível máximo é **Controle total**) às configurações do protocolo para essa função. Após definidas estas permissões, os usuários em uma função de não administrador podem executar as tarefas que você especificou.

Para permitir que não administradores criem tarefas de Descobertas de rede, conclua os seguintes procedimentos:

- Conceda direitos a uma função de usuário que não seja o administrador para o gerenciamento de tarefas de Descoberta de rede. Este procedimento permite que usuários na função executem tarefas.
- Adicione a função de sua escolha às permissões de acesso do perfil de conexão relevante. Em seguida, permita que esta função controle configurações de protocolo. Após adicionar a função a um perfil de conexão, os usuários nessa função poderão criar e editar tarefas de Descoberta de rede.

Esta tarefa é uma etapa no processo de delegação de tarefas de Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para conceder direitos a uma função de usuário que não seja o administrador para o gerenciamento de tarefas de Descoberta de rede.

- 1 Faça login no Symantec Management Platform como administrador.
- 2 No Symantec Management Console, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 3 No painel esquerdo, em **Gerenciamento de conta**, clique em **Funções**.
- 4 Na página **Funções**, no painel esquerdo, clique na função de usuário que não seja o administrador à qual você quer delegar a criação e a execução de tarefas de Descoberta de rede.

Funções típicas às quais os administradores delegam estas tarefas são Atendentes de nível 1 da Symantec e Atendentes de nível 2 da Symantec.
- 5 À direita, na janela rotulada com a função que você selecionou, clique na guia **Privilégios**, caso não esteja ativada.
- 6 Em **Privilégios de gerenciamento**, selecione **Gerenciamento de tarefas de descoberta**.
- 7 Se a função que você selecionou também precisar criar ou editar perfis de conexão, selecione as seguintes opções adicionais:
 - Em **Privilégios do perfil de conexão**, selecione **Criar perfil de conexão**.
 - Em **Privilégios do sistema**, selecione **Exibir segurança**.
 - Em **Privilégios da credencial**, selecione **Criar credencial**.
- 8 Clique na guia **Membros**.

- 9 Assegure-se de que o usuário que você deseja adicionar à função selecionada tenha sido adicionado a esta função.

Se o usuário não for um membro desta função, será necessário criar um usuário do Notification Server e adicioná-lo à função relevante.

Consulte [“Para adicionar usuários não administradores às funções de segurança para executar tarefas de Descoberta de rede”](#) na página 224.

- 10 Clique em **Salvar alterações**.

Para conceder a uma função predefinida o controle completo (ou inferior) às configurações do protocolo

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, em **Configurações**, expanda **Monitoração e alertas > Gerenciamento de protocolos > Perfis de conexão** e clique em **Gerenciar perfis de conexão**.
- 3 Na página **Gerenciar perfis de conexão**, clique em **Perfil de conexão padrão** e clique em **Editar**.
- 4 Na caixa de diálogo **Definir configurações de grupo**, clique em **Permissões de acesso às configurações dos protocolos**.
- 5 Clique em **Adicionar**, selecione a função à qual você deseja conceder o controle e clique em **Selecionar**.

Atendentes do nível 1 da Symantec

Por padrão, os usuários nesta função têm menos direitos do que os Supervisores da Symantec. Quando esses funcionários receberem os privilégios de Gerenciamento de tarefas de descoberta e de Controle total, eles poderão criar e executar tarefas de descoberta de rede.

Atendentes do nível 2 da Symantec

Por padrão, os usuários nesta função têm menos direitos. Quando esses funcionários receberem os privilégios de Gerenciamento de tarefas de descoberta e de Controle total, eles poderão criar e executar tarefas de descoberta de rede.

Supervisores da Symantec

Por padrão, os usuários nesta função podem executar tarefas Descoberta de rede. Quando esses funcionários receberem o controle total, eles também poderão criar e editar tarefas de descoberta de rede.

- 6 Na caixa de diálogo **Seleção de permissão**, selecione as permissões de uma das seguintes maneiras:

- Marque **Uso e Leitura**. É possível marcar quaisquer caixas que correspondam às tarefas que você deseja que a função selecionada possa executar. Em seguida, clique em **Selecionar**.
 - Clique em **Controle total** para dar à função todos os direitos disponíveis que estão relacionados e clique em **Selecionar**.
- 7 Na caixa de diálogo **Configurações do descritor de segurança para: Perfil de conexão padrão**, clique em **Aplicar**.
 - 8 Na caixa de diálogo **Definir configurações de grupo**, clique em **OK** para salvar o perfil de conexão.

Para conceder privilégios de funções de usuário que não seja o administrador para criar credenciais e perfis de conexão

Quando você delegar tarefas às funções de não administrador, será necessário determinar que tarefas os usuários atribuídos àquelas funções poderão executar. Cada função de segurança predefinida do Symantec Management Platform inclui direitos inerentes.

Consulte [“Funções predefinidas de segurança”](#) na página 106.

Um exemplo é a função padrão de Supervisores da Symantec. Usuários atribuídos a esta função podem executar tarefas existentes sem que a função receba privilégios adicionais. Estes usuários também poderão criar tarefas de descoberta de rede se tiverem acesso a um perfil de conexão existente.

Porém, para permitir que funções de não administrador criem novas tarefas e perfis de conexão, conceda privilégios para aquelas funções para que criem credenciais e perfis de conexão. Estes privilégios adicionais serão necessários se for esperado que os usuários criem as novas tarefas que podem exigir credenciais e perfis de conexão diferentes das credenciais e dos perfis existentes.

Consulte [“Para definir as configurações de descoberta”](#) na página 210.

Para permitir que os usuários atribuídos às funções de não administrador criem credenciais e perfis de conexão, é necessário ativar aqueles privilégios para a função. Estes privilégios permitem que os usuários criem as credenciais e os perfis de conexão que são adequados às tarefas que você lhes delega ou que eles criam.

Esta tarefa é uma etapa no processo de delegação de tarefas Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para conceder privilégios de funções de não administrador para criar credenciais e perfis de conexão

- 1 Faça login no Console de gerenciamento Symantec como administrador.
- 2 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Gerenciamento de conta**.
- 3 Em **Gerenciamento de conta**, clique em **Funções**
- 4 Na página **Funções**, clique na função que você deseja ativar e, no painel direito, clique na guia **Privilégios**.
- 5 Vá para **Privilégios do perfil de conexão** e selecione **Criar perfil de conexão**.
- 6 Vá para **Privilégios da credencial** e selecione **Criar credencial**.
- 7 Vá para **Privilégios do sistema** e selecione **Exibir segurança**.
- 8 Clique em **Salvar alterações**.

Para fornecer acesso de função de usuário que não seja o administrador ao perfil de conexão padrão

Os usuários em funções de não administrador precisam de acesso ao perfil de conexão padrão para executar tarefas. Após conceder a estas funções o acesso ao perfil de conexão padrão, os usuários nessas funções também poderão criar tarefas. Eles não poderão criar perfis de conexão, mas poderão criar tarefas que usam perfis de conexão existentes.

Esta tarefa é uma etapa no processo de delegação de tarefas Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para conceder a uma função predefinida o controle completo (ou inferior) ao perfil de conexão padrão

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, em **Configurações**, expanda **Monitoração e alertas > Gerenciamento de protocolos > Perfis de conexão** e clique em **Gerenciar perfis de conexão**.
- 3 Na página **Gerenciar perfis de conexão**, clique em **Perfil de conexão padrão** e clique em **Editar**.
- 4 Na caixa de diálogo **Definir configurações de grupo**, clique em **Permissões de acesso às configurações dos protocolos**.

Para ativar funções diferentes das funções de segurança predefinidas para criar e executar tarefas usando o Assistente de Descoberta de rede.

O Assistente de Descoberta de rede é uma ferramenta de administrador integrada ao Symantec Management Platform. É um método para descobrir dispositivos de rede e executar outras tarefas de descoberta.

Você acessa o Assistente de Descoberta de rede pelo menu **Início** do Console de gerenciamento Symantec.

Consulte [“Para criar tarefas de descoberta de rede usando o assistente”](#) na página 212.

As seguintes funções de segurança são predefinidas e, por padrão, podem criar e executar tarefas usando o Assistente de Descoberta de rede:

- Administrador
- Supervisores da Symantec
- Trabalhadores do nível 2 da Symantec
- Trabalhadores do nível 1 da Symantec

Convém ativar outras funções para criar e executar tarefas pelo Assistente de Descoberta de rede. Neste caso, é necessário dar a essas funções os privilégios necessários para executar essas tarefas usando o assistente.

Esta tarefa é uma etapa no processo de delegação de tarefas Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para ativar funções diferentes das funções de segurança predefinidas para criar tarefas usando o Assistente de Descoberta de rede

- 1 Faça logon no Symantec Management Platform como administrador.
- 2 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Permissões**.
- 3 Em **Gerenciador de função de segurança**, na caixa suspensa **Função**, selecione a função que você deseja ativar.
- 4 Na lista suspensa **Exibir**, clique em **Configurações**.
- 5 No painel esquerdo, clique em **Edit**.

Note que, na caixa de diálogo **Seletor de itens**, se a caixa de seleção **Configurações** estiver selecionada, todas as opções restantes estarão em cinza.

- 6 Se a opção **Configurações** estiver selecionada, desmarque-a.
- 7 Em **Descoberta e inventário**, selecione a opção **Assistente de Descoberta de rede** caso já não esteja selecionada.
- 8 Selecione novamente a opção **Configurações** para ativar novamente a herança.
- 9 Clique em **Salvar alterações**.

Para ativar funções diferentes daquelas de segurança predefinidas para agendar e executar tarefas usando o Assistente de Descoberta de rede.

- 1 Faça login no Symantec Management Platform como administrador.
- 2 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Segurança > Permissões**.
- 3 Em **Gerenciador de função de segurança**, na caixa suspensa **Função**, clique na função que você deseja ativar.
- 4 Na caixa suspensa **Exibir**, clique em **Tarefas**.
- 5 No painel esquerdo, em **Tarefas**, expanda **Trabalhos e tarefas > Trabalhos e tarefas do sistema** e clique em **Descoberta e inventário**.
 Note que no painel **Descoberta e inventário**, a seção **Herdado** está em cinza e não pode ser editada.
- 6 No painel **Descoberta e inventário**, em **Não herdado**, role para baixo até **Permissões do Task Server** e selecione **Executar tarefa**.
- 7 Clique em **Salvar alterações** e feche o **Gerenciador de função de segurança**.

Para tornar um perfil de conexão somente leitura

Você pode precisar delegar tarefas Descoberta de rede aos usuários em funções de não administrador. Porém, não convém que estes usuários mudem os perfis de conexão. Convém fazer um perfil de conexão somente leitura para impedir atividades de hackers e manter a segurança e a privacidade das informações confidenciais. Outra razão para fazer um perfil de conexão somente leitura é para impedir que os usuários menos experientes modifiquem um perfil de conexão para usar protocolos não suportados.

Se quiser limitar os usuários a exibir credenciais e executar tarefas de descoberta de rede, você poderá bloquear os direitos de gravação em cada perfil de conexão. Bloqueando os direitos de gravação de uma função de não administrador, você tornará um perfil de conexão somente leitura aos usuários nessa função. Os usuários que estiverem atribuídos a essas funções de usuário que não seja o administrador cujos direitos de gravação você bloqueou ainda poderão exibir e

executar tarefas, mas não poderão mudar esse perfil de conexão nem criar um novo.

Esta tarefa é uma etapa no processo de delegação de tarefas Descoberta de rede a não administradores.

Consulte [“Para delegar tarefas de Descobertas de rede aos usuários não administradores”](#) na página 221.

Para tornar um perfil de conexão somente leitura

- 1 Faça login no Console de gerenciamento Symantec como administrador.
- 2 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 3 No painel esquerdo, em **Configurações**, expanda **Monitoração e alertas > Gerenciamento de protocolos > Perfis de conexão** e clique em **Gerenciar perfis de conexão**.
- 4 No painel **Gerenciar perfis de conexão**, clique em **Perfil de conexão padrão** e clique em **Edit**.
- 5 Na caixa de diálogo **Definir configurações de grupo**, clique em **Permissões de acesso às configurações do protocolo**.
- 6 Na caixa de diálogo **Configurações do descritor de segurança para: Perfil de conexão padrão**, selecione a função, como **Atendentes de nível 2 da Symantec** e clique em **Editar**.
- 7 Na caixa de diálogo **Seleção de permissão**, desmarque **Gravação** e clique em **Selecionar**.
- 8 Na caixa de diálogo **Configurações do descritor de segurança para: Perfil de conexão padrão**, clique em **Aplicar** para salvar as configurações e na caixa de diálogo **Definir configurações de grupo**, clique em **OK** para salvar o perfil de conexão.

Importação de arquivos Management Information Bases (MIB)

Você pode usar dois métodos para importar arquivos MIB para o banco de dados. Você pode importar manualmente os arquivos MIB um de cada vez usando o utilitário Importar MIB. Você também pode criar e agendar uma tarefa que importe um ou mais arquivos MIB.

Para importar arquivos MIB manualmente usando o utilitário Importar MIB

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Monitoramento e alertas > Navegador de importação de MIB SNMP** e clique em **Navegador de MIBs**.
- 3 Na página **Navegador de MIBs**, clique em **Importar arquivo MIB**.
- 4 Na caixa de diálogo **Importar arquivo MIB**, clique em **Procurar**, selecione o arquivo e clique em **Importar**.

Você pode importar qualquer arquivo MIB adicional que seja necessário.

Para importar arquivos MIB usando a tarefa Importar MIB

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você quer salvar a tarefa e clique em **Novo(a) > Tarefa**.
- 3 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, clique em **Monitoramento e alertas > Importar MIB**.
- 4 Renomeie a tarefa, selecione o arquivo do MIB para upload e especifique a opção de importação.

Você pode optar por importar um único arquivo MIB ou você pode optar por importar os arquivos adicionais MIB que são armazenados no local do diretório.

- 5 Clique em **Fazer upload** para fazer upload do arquivo MIB na a tarefa de importação.
- 6 Se você quiser importar vários arquivos MIB, continue a procurar e a fazer o upload de cada arquivo MIB que você precisa na tarefa.
- 7 Clique em **OK**.
- 8 Selecione uma nova tarefa de importação do MIB.

Por padrão, a nova tarefa de importação do MIB é armazenada em: **Trabalhos e tarefas do sistema > Notification Server**.

- 9 Agende a nova tarefa de importação do MIB que será executada usando o utilitário de agendamento de tarefas.

Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.

Para instalar e configurar o Symantec Management Agent

- [Capítulo 14. Introdução ao Symantec Management Agent](#)
- [Capítulo 15. Para instalar o Symantec Management Agent em computadores-cliente](#)
- [Capítulo 16. Para fazer o upgrade e desinstalar o Symantec Management Agent](#)
- [Capítulo 17. Para configurar o Symantec Management Agent](#)

Introdução ao Symantec Management Agent

Este capítulo contém os tópicos a seguir:

- [Sobre o Symantec Management Agent](#)
- [Sobre o registro do agente](#)

Sobre o Symantec Management Agent

O Symantec Management Agent é o software que estabelece a comunicação entre o computador do Notification Server e os computadores em sua rede. Os computadores que têm o Symantec Management Agent instalado são denominados computadores gerenciados. O computador do Notification Server interage com o Symantec Management Agent para monitorar e gerenciar cada computador através do Symantec Management Console.

O computador do Notification Server e o Symantec Management Agent trabalham juntos para fornecer os seguintes tipos de funcionalidades aos computadores gerenciados:

- Monitoração de hardware e de software
- Agenda de instalações de software e atualizações de arquivos
- Coleta de informações de inventário básico
- Gerenciamento de políticas e pacotes

Você pode instalar o Symantec Management Agent em computadores Windows, Linux, UNIX e Mac. O Symantec Management Agent também permite que você instale e gerencie os plug-ins dos agentes da solução que adicionam funcionalidade ao agente. Por exemplo, a instalação do plug-in de inventário permite coletar

informações detalhadas sobre hardware e software de todos os computadores gerenciados.

Consulte [“Métodos de instalação do Symantec Management Agent”](#) na página 238.

Se você quiser usar o gerenciamento habilitado para nuvem, há um procedimento especial para instalar e configurar o Symantec Management Agent para funcionar neste ambiente.

Consulte [“Sobre o gerenciamento habilitado para nuvem”](#) na página 284.

Sobre o registro do agente

Além do recurso de gerenciamento ativado na nuvem que permite gerenciar os dispositivos fora do firewall, o recurso de registro do agente foi adicionado no IT Management Suite 7.5 para garantir que somente computadores-cliente confiáveis possam se comunicar com o Notification Server.

Consulte [“Sobre o gerenciamento habilitado para nuvem”](#) na página 284.

O recurso de registro do agente exige que um computador-cliente tenha permissão de se comunicar com um Notification Server antes de poder ser gerenciado por esse Notification Server. A política padrão de registro do agente permite que todos os computadores se comuniquem com o Notification Server. Contudo, você pode criar políticas de registro do agente personalizadas que permitem ou bloqueiam determinados computadores.

Consulte [“Para criar uma política de registro do agente”](#) na página 243.

Depois que a política de registro do agente permitir ou bloquear um computador, você poderá mudar o status manualmente apenas na página de relatório **Status de registro do agente**. Por exemplo, você pode permitir ou bloquear os computadores que estão em estado pendente. Também é possível revogar o registro dos agentes que você tinha permitido anteriormente.

Consulte [“Para exibir e gerenciar o status do registro do agente”](#) na página 251.

O registro do agente é suportado em plataformas Windows, UNIX, Linux e Mac.

Para instalar o Symantec Management Agent em computadores-cliente

Este capítulo contém os tópicos a seguir:

- [Métodos de instalação do Symantec Management Agent](#)
- [Para instalar o Symantec Management Agent em computadores Windows](#)
- [Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac](#)

Métodos de instalação do Symantec Management Agent

Antes de instalar o Symantec Management Agent, recomendamos que você planeje sua instalação usando o *Guia de Planejamento de Implementação do IT Management Suite*.

Você pode instalar o Symantec Management Agent em computadores Windows, UNIX e Mac.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Depois que o Symantec Management Agent estiver instalado no computador-cliente, o agente enviará uma solicitação de registro ao Notification Server para estabelecer uma comunicação confiável.

Consulte [“Sobre o registro do agente”](#) na página 237.

Se você quiser usar o gerenciamento habilitado para nuvem, há um procedimento especial para instalar e configurar o Symantec Management Agent para funcionar neste ambiente.

Consulte [“Sobre o gerenciamento habilitado para nuvem”](#) na página 284.

Tabela 15-1 Métodos para instalar o Symantec Management Agent

Método	Descrição
Instalação por envio manual	A instalação por envio é iniciada no Console de gerenciamento Symantec e o Symantec Management Agent é instalado imediatamente. Você pode instalar o Symantec Management Agent em qualquer número de computadores na mesma operação de envio. Você também pode personalizar as opções de instalação para cada operação de envio. Em computadores UNIX, Linux e Mac, este método exige que um servidor SSH esteja em execução. Você também deve configurar o firewall para aceitar conexões SSH nos computadores de destino. Consulte “Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual” na página 246. Consulte “Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual” na página 260. Os agentes que você instalar com a instalação por envio manual ignorarão o processo de registro do agente e a comunicação entre o agente e o Notification Server será estabelecida automaticamente.
Instalação pull manual	A instalação pull manual é iniciada no computador em que o Symantec Management Agent deverá ser instalado. Esta operação permite contornar o firewall e os limites de acesso à rede que podem impedir instalações por envio em computadores remotos. Para computadores UNIX, Linux e Mac, você precisará usar este método se o SSH não estiver disponível. Consulte “Para instalar o Symantec Management Agent para Windows com uma instalação pull manual” na página 248. Consulte “Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação pull manual” na página 264.

Método	Descrição
Instalação agendada por envio	Este método está disponível apenas para computadores Windows. Uma instalação agendada do Symantec Management Agent é executada em um horário definido, diferentemente das instalações por envio manual, que são executadas imediatamente. Você pode enviar o Symantec Management Agent para os computadores em um grupo organizacional, filtro ou destino de recursos, ou para os computadores que tenham recursos selecionados. Note que os agentes que você instalar com envio agendado não ignorarão o processo de registro do agente. Consulte “Para executar uma instalação agendada do Symantec Management Agent para Windows” na página 249.
Política de upgrade do agente	A política de upgrade do Symantec Management Agent é fornecida com o Symantec Management Platform. Você pode ativar esta política e configurá-la para assegurar-se de que todos os seus computadores gerenciados tenham a versão correta do Symantec Management Agent instalada. Consulte “Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent” na página 268.

Nota: Quando você instalar o Symantec Management Agent em um computador, haverá um atraso antes que o Client Task Agent seja registrado no Notification Server. Todas as tarefas que forem selecionadas no computador durante esse tempo (normalmente, em torno de 10 minutos) ficarão com um status pendente até que o Client Task Agent seja registrado. Quando o Client Task Agent for registrado, as tarefas serão executadas imediatamente.

Para instalar o Symantec Management Agent em computadores Windows

Você pode instalar o Symantec Management Agent com uma instalação por envio manual ou uma instalação pull manual. É recomendado instalar o Symantec Management Agent enviando-o manualmente aos computadores selecionados. Porém, para instalar nos computadores remotos que têm acesso limitado à rede ou estão atrás de um firewall, pode ser necessário executar uma instalação pull manual.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Tabela 15-2 Processo para instalar o Symantec Management Agent em computadores Windows

Etapa	Ação	Descrição
Etapa 1	Verifique se os computadores cumprem os pré-requisitos da instalação.	Cada computador deve cumprir os pré-requisitos de hardware e software antes da instalação do Symantec Management Agent. Consulte “Pré-requisitos de instalação do Symantec Management Agent para Windows” na página 242.
Etapa 2	(Opcional) Defina as políticas de registro do agente.	Depois de instalar o Symantec Management Agent, ele enviará uma solicitação de registro ao Notification Server para estabelecer a confiança entre o servidor e o cliente. A política padrão de registro do agente permite o registro automático de todos os agentes. Você pode modificar a política padrão ou criar políticas personalizadas para especificar regras mais restritivas. Consulte “Para criar uma política de registro do agente” na página 243.
Etapa 3	Especifique as configurações de instalação.	Antes de executar a instalação por envio manual ou a instalação pull manual do Symantec Management Agent, especifique as configurações de instalação. Consulte “Para especificar as configurações de instalação do Symantec Management Agent para Windows” na página 246.
Etapa 4	Instale o Symantec Management Agent usando o método apropriado.	O método preferencial é enviar o Symantec Management Agent para os computadores selecionados. Porém, se um computador estiver protegido por um firewall ou for de difícil acesso para o Notification Server, você poderá realizar a instalação pull do Symantec Management Agent. Consulte “Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual” na página 246. Consulte “Para instalar o Symantec Management Agent para Windows com uma instalação pull manual” na página 248. Consulte “Para executar uma instalação agendada do Symantec Management Agent para Windows” na página 249.
Etapa 5	Exiba os relatórios de status da instalação para verificar se a instalação obteve êxito.	Os relatórios de status da instalação permitem exibir detalhes de todas as tentativas de instalações manuais remotas e das instalações agendadas do Symantec Management Agent. O relatório não inclui detalhes de nenhuma instalação por solicitação. Consulte “Para exibir relatórios de status da instalação” na página 250.

Etapa	Ação	Descrição
Etapa 6	Visualize e gerencie o status de registro do agente para verificar o registro com êxito.	O relatório Status de registro do agente permite exibir e gerenciar todas as solicitações de registro e os registros concluídos dos Symantec Management Agents. Consulte “Para exibir e gerenciar o status do registro do agente” na página 251.

Pré-requisitos de instalação do Symantec Management Agent para Windows

Para instalar o Symantec Management Agent, você precisa configurar os computadores e verificar se eles cumprem os pré-requisitos de instalação.

Consulte [“Métodos de instalação do Symantec Management Agent”](#) na página 238.

Esta tarefa é uma etapa dos processos de instalação manual do Symantec Management Agent em computadores Windows.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Tabela 15-3 Pré-requisitos de instalação do Symantec Management Agent para Windows

Pré-requisito	Descrição
Sistema operacional	Qualquer um dos seguintes itens: ■ Windows 2003 SP2 (x86, x64) ■ Windows 2003 R2 ou posterior (x86, x64) ■ Windows XP Professional SP2 (x64) ■ Windows XP Professional SP3 (x86) ■ Windows Vista SP2 ou posterior (x86, x64) ■ Windows 2008 ou posterior (x86, x64) ■ Windows 2008 R2 ou posterior (x86, x64) ■ Windows 7 ou posterior (x86, x64)
Espaço em disco rígido	Mínimo de 60 MB
RAM	Mínimo de 64 MB (128 MB recomendados)
Internet Explorer	Versão 6.0 ou superior
Direitos de acesso	Direitos locais de administrador

Pré-requisito	Descrição
Firewall	O computador deve ser capaz de comunicar-se com o Symantec Management Platform através do firewall do computador. Execute um dos seguintes procedimentos: ■ Ative Compartilhamento de arquivos e impressoras nas configurações de firewall. ■ Adicione as portas UDP 138, TCP 445, TCP 80 (ou TCP 443 para HTTPS) e ICMP tipo 8 como exceções de entrada de porta. Você pode adicionar as portas usando uma política de grupo. ■ Desative o firewall.
Compartilhamento simples de arquivos (apenas Windows XP que não seja de domínio)	Para os computadores-cliente do não sejam de domínio e que executam o Windows XP, desative também Usar compartilhamento simples de arquivo em Opções de pasta no Windows XP.
UAC (apenas Windows Vista e Windows 7 que não sejam de domínio)	Para os computadores-cliente que não sejam de domínio e que executam o Windows Vista ou Windows 7, desative também o Controle de acesso do usuário (UAC).

Para criar uma política de registro do agente

As políticas de registro do agente permitem automatizar o processo de registro do agente. Uma política de registro do agente é um conjunto de regras que determinam como as solicitações de registro de entrada serão processadas. No conteúdo da solicitação de registro, o Symantec Management Agent envia o nome do host, o endereço MAC, o endereço IP, o FQDN e os dados do usuário conectado. A política de registro do agente usa os dados da solicitação de registro e as regras que você define na política para decidir se a solicitação será permitida ou bloqueada.

Aviso: A política padrão de registro do agente permite automaticamente que todos os agentes se comuniquem com o Notification Server. Você pode modificar a política padrão ou criar políticas personalizadas para restringir os agentes que podem se comunicar com o Notification Server. Se nenhuma política ativa estiver disponível, o status de cada solicitação de registro recebida será definido como pendente.

Você pode exibir as solicitações de registro no relatório **Status de registro do agente**. É possível acessar esse relatório no Console de gerenciamento Symantec, em **Relatórios > Notification Server Management > Registro**.

Consulte [“Para exibir e gerenciar o status do registro do agente”](#) na página 251.

Essa tarefa é uma etapa opcional nos seguintes processos:

- Instalação do Symantec Management Agent em computadores do Windows.
Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.
- Instalação manual do Symantec Management Agent em computadores UNIX, Linux e Mac.
Consulte [“Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac”](#) na página 255.

Para criar uma política de registro do agente

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, em **Configurações**, expanda **Agentes/plug-ins > Symantec Management Agent > Configurações**.
- 3 Clique com o botão direito do mouse em **Políticas de registro**, depois clique em **Novo(a) > Política de registro**.
- 4 No painel direito, especifique as configurações da política de registro do agente da seguinte forma:

Regras

Permite definir tipos diferentes de máscaras para a identificação do agente usando os dados da solicitação. Por exemplo, você pode definir uma máscara para o nome de host, uma para o endereço IP e uma para o nome do usuário conectado.

Uma única política pode conter um número ilimitado de máscaras de qualquer tipo. Durante o processo de correspondência de máscara, o Notification Server tratará diferentes tipos de máscaras como a operação lógica AND e tipos semelhantes de máscaras como a operação lógica OR.

Por exemplo, uma política com as seguintes máscaras permitirá o registro de todos os agentes que tenham o nome correspondente à máscara "*test" e o respectivo endereço IP será 10.31.12.1, 10.31.12.2, ou qualquer dos 25 endereços IP da sub-rede 10.31.15.0:

- Host = *test
- IP=10.31.12.1
- IP=10.31.12.2
- IP=10.31.15.0/24

Nota: O asterisco é aceito em todas as regras, exceto em **endereço IP**. Se quiser especificar uma faixa de IP em uma regra, você deverá defini-la com a máscara de sub-rede. Por exemplo, em vez de digitar **10.31.15.***, digite **10.31.15.0/24**.

Ações

Permite definir a regra para o processamento do agente compatível com as seguintes opções:

- **Permitir**
Os agentes serão registrados automaticamente e não será preciso aceitá-los manualmente.
- **Bloquear**
As solicitações desses agentes serão recusadas.

Se duas políticas forem aplicáveis a uma solicitação de registro e uma delas permitir o registro enquanto a outra o bloqueia, a política de bloqueio será aplicada ao pedido.

5 Ative a política.

Na parte superior direita da página, clique no círculo colorido e em **Ativado**.

6 Clique em **Salvar alterações**.

Para especificar as configurações de instalação do Symantec Management Agent para Windows

As configurações de instalação permitem especificar como o Symantec Management Agent será instalado no computador-cliente. Você pode definir as opções de instalação para uma instalação manual pull ou por envio do Symantec Management Agent. Você não poderá incluir estas configurações em um arquivo .CSV quando importar nomes de computador.

Esta tarefa é uma etapa dos processos de instalação do Symantec Management Agent em computadores Windows.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para definir as opções de instalação do Symantec Management Agent para Windows

- 1 No **Console de gerenciamento Symantec**, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, em **Instalação do agente nos computadores**, clique em **Configurações**.
- 3 Na caixa de diálogo **Opções de instalação do Symantec Management Agent**, selecione as opções que você deseja usar e especifique as configurações necessárias nas caixas apropriadas; em seguida, clique em **OK**.

Para obter mais informações, clique na página e pressione **F1**.

- 4 Na página **Instalação do Symantec Management Agent**, clique em **Salvar alterações**.

Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual

Você pode enviar o Symantec Management Agent a todos os computadores Windows. Para instalar ou desinstalar manualmente o Symantec Management Agent na página **Instalação do Symantec Management Agent**, selecione os computadores apropriados. Você pode digitar os nomes dos computadores manualmente, escolher os computadores que foram descobertos com a descoberta de recursos, ou importar os computadores de um arquivo CSV. O arquivo CSV é um arquivo de texto delimitado por vírgulas. O arquivo inclui os nomes de DNS ou os endereços IP dos computadores-cliente nos quais você deseja instalar o Symantec Management Agent. Para computadores Windows, o arquivo CSV é uma lista de nomes de computador ou de endereços IP que são importados para a página **Instalação do Symantec Management Agent**. Os itens são interpretados

como os nomes ou os endereços IP dos computadores (para as entradas que estão no formato apropriado). Nenhum espaço é permitido: qualquer item que conter um espaço será ignorado.

Nota: Você apenas pode instalar manualmente o Symantec Management Agent nos computadores que foram descobertos usando a **Descoberta de recursos de domínio** ou a **Descoberta de rede**.

Esta tarefa é uma etapa dos processos de instalação do Symantec Management Agent em computadores Windows.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, na guia **Instalar agente**, em **Instalar agente nos computadores**, escolha os computadores nos quais instalar o Symantec Management Agent e clique em **Instalar**.

Para adicionar um computador manualmente

Na caixa de texto, digite o nome do computador (que deve ser um nome DNS que pode ser resolvido) ou endereço IP e clique em **Adicionar**.

Para escolher os computadores disponíveis

- 1 Clique em **Selecionar computadores**.
- 2 Clique na caixa de diálogo **Selecionar computadores**, adicione os computadores apropriados da lista **Computadores disponíveis** à lista **Computadores selecionados** e clique em **OK**.

- 1 Para importar computadores de um arquivo CSV
Em **Instalar agente nos computadores**, na barra de ferramentas, clique no símbolo de **Importar computadores de um arquivo selecionado**.
- 2 Na caixa de diálogo **Selecionar arquivo para importar**, selecione o arquivo CSV apropriado e clique em **Abrir**.
- 3 Na caixa de diálogo **Opções de instalação do Symantec Management Agent**, defina as configurações da instalação de acordo com suas necessidades e clique em **Continuar a instalação**.

Para obter mais informações, clique na página e pressione **F1**.

Na página **Instalação do Symantec Management Agent**, em **Rollout Agent to Computers**, na lista de computadores, a coluna **Status** mostra o sucesso ou a falha da instalação em cada computador. Observe que o Symantec Management Agent instalado recentemente informará seu status ao Notification Server de origem, mesmo se ele for gerenciado por outro Notification Server.

Para instalar o Symantec Management Agent para Windows com uma instalação pull manual

Se você quiser instalar o Symantec Management Agent em computadores remotos com acesso limitado à rede ou com firewall, poderá ser necessário realizar uma instalação pull do Symantec Management Agent em cada computador. Você pode fazer logon em cada computador, acessar o Notification Server com um URL, e começar o processo de instalação do Symantec Management Agent. O processo de instalação é executado automaticamente, sem a necessidade de uma interação adicional do usuário.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

A instalação pull do Symantec Management Agent usa as configurações especificadas na caixa de diálogo **Opções de instalação do Symantec Management Agent**, à exceção de **Fazer download do pacote do agente do Servidor de pacotes mais próximo**, que é irrelevante.

A URL da página **Download do Symantec Management Agent** é mostrada na página **Instalação do Symantec Management Agent**, em **URL da página de download**. Não é possível mudar esta configuração.

Esta tarefa é uma etapa dos processos de instalação do Symantec Management Agent em computadores Windows.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para visualizar a página de download do kit do Symantec Management Agent

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, em **URL da página de download**, clique em **Mostrar-me esta página**.

Para instalar o Symantec Management Agent para Windows com uma instalação pull manual

- 1 Faça login no computador como administrador.
Você pode fazer login remotamente, usando um aplicativo de acesso remoto como o pcAnywhere, ou deixar que um usuário no site remoto faça login com a conta apropriada.
- 2 No computador remoto, abra o Internet Explorer e consulte o seguinte URL:
<http://NSName/Altiris/NS/Agent/AltirisAgentDownload.aspx>
onde *NSName* é o nome de seu computador do Notification Server.
- 3 Na janela **Download do Symantec Management Agent**, clique em **Clique aqui para começar o download e a instalação**.
O processo de instalação do agente é executado silenciosamente e nenhuma ação adicional é necessária.

Para executar uma instalação agendada do Symantec Management Agent para Windows

Você pode configurar uma instalação agendada do Symantec Management Agent. Uma instalação agendada é executada em um horário definido, diferentemente das instalações por envio manual, que são executadas imediatamente. Por exemplo, se você desejar instalar o agente em um grupo específico de computadores em um horário apropriado, será possível configurar um agendamento de não repetição para ser executado na hora adequada.

Você pode também configurar um agendamento para instalar automaticamente o Symantec Management Agent em novos computadores enquanto eles são adicionados ao seu ambiente. O agendamento da descoberta de recursos é executado diariamente para detectar novos computadores e você pode configurar filtros para classificar os novos computadores em grupos apropriados. Você pode então agendar a instalação do Symantec Management Agent em todos os computadores em grupos específicos e em intervalos apropriados.

Você precisa ter cuidado ao implementar um método automático de instalação. Recomendamos que você inclua uma etapa manual para verificar se o agente está sendo instalado nos computadores apropriados.

Esta tarefa é uma etapa dos processos de instalação do Symantec Management Agent em computadores Windows.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para configurar o agendamento de instalação do Symantec Management Agent para Windows

- 1 No **Console de gerenciamento Symantec**, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, em **Agendamento do envio aos computadores**, no lado direito da página, clique no círculo colorido e, em seguida, clique em **On**.
- 3 Em **Aplicar a**, especifique os computadores nos quais o Symantec Management Agent deve ser instalado.

Você pode especificar um grupo organizacional, um filtro ou um destino de recurso existente. Você também pode selecionar recursos individuais.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.
- 4 No painel **Quando agendar**, especifique o horário agendado ou a janela de agendamento para executar a instalação e selecione as opções apropriadas.
- 5 Clique em **Salvar alterações**.

Para exibir relatórios de status da instalação

O relatório de status da instalação permite exibir detalhes de todas as tentativas de instalação por envio do Symantec Management Agent que foram realizadas. O relatório não inclui detalhes de nenhuma instalação pull.

Por padrão, os detalhes de todas as tentativas de instalação realizadas na última semana são relacionados. Você pode especificar o período para exibição e filtrar os resultados pelo nome e domínio do computador.

Esta tarefa é uma etapa dos seguintes processos:

- Instalação do Symantec Management Agent em computadores Windows.
Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.
- Instalação manual do Symantec Management Agent em computadores UNIX, Linux e Mac.

Consulte “[Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac](#)” na página 255.

Para exibir o relatório Status da instalação do agente

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, clique em **Relatório de status**.

O relatório mostra detalhes de todas as tentativas de instalação por envio para o Symantec Management Agent e o Symantec Management Agent para UNIX, Linux e Mac. O mesmo relatório está disponível nas guias **Instalar o agente** e **Instalar o agente para UNIX, Linux e Mac**.

- 3 Na janela **Status da instalação do agente**, exiba os detalhes de cada tentativa de instalação.
- 4 (Opcional) Se desejar mudar o período de tempo ou filtrar os resultados pelo nome e domínio do computador, em **Parâmetros**, defina os parâmetros apropriados do usuário:

Exibindo	Especifique o período de tempo que deseja exibir. Digite o número de unidades apropriado (horas, dias, semanas ou meses) nas caixas De e Até .
Unidades	Especifique as unidades que você deseja usar para os valores de Exibindo .
Filtrar por	Se desejar filtrar os resultados por nome ou domínio de computador (ou ambos), especifique o texto de filtro apropriado nas caixas correspondentes.

- 5 (Opcional) Se você alterou os parâmetros do usuário, clique em **Atualizar** para exibir os resultados atualizados do relatório.

Para exibir e gerenciar o status do registro do agente

O relatório do **Status de registro do agente** permite exibir todas as solicitações de registro e os registros concluídos dos agentes de gerenciamento da Symantec.

Nesse relatório, você poderá ver os computadores que a **Política de registro do agente** permitiu ou bloqueou automaticamente. Na instalação por envio direta do Symantec Management Agent, o registro é ignorado. Contudo, os computadores ainda serão exibidos no relatório e o status estará definido como **Permitido**. Se nenhuma **Política de registro do agente** for aplicável ao computador, o status será definido como **Pendente** e no menu contextual você poderá permitir ou

bloqueá-lo manualmente. O menu contextual também permite revogar a confiança dos agentes que você reservou anteriormente.

Consulte [“Para criar uma política de registro do agente”](#) na página 243.

As solicitações de registro de entrada se distinguem pelas chaves de recurso e são mescladas com base na consulta das chaves de recurso.

Em algumas situações, podem aparecer solicitações de registro duplicadas. Por exemplo, se você reinstalar o agente em um computador já registrado no Notification Server, a chave pública será alterada. Nesse caso, a Symantec recomenda aprovar a solicitação de registro para permitir que o computador mantenha a comunicação com o Notification Server. Além disso, solicitações de registro duplicadas podem aparecer se você tiver computadores com chaves de recurso idênticas em sua rede. Nesse caso, a Symantec recomenda não aprovar a solicitação de registro duplicada, pois isso pode causar problemas de conectividade para o recurso que existiu anteriormente.

Se você tiver solicitações de registro duplicadas em seu relatório, as solicitações serão controladas da seguinte forma:

- Se a solicitação inicial for permitida e a solicitação duplicada também, a solicitação duplicada será mesclada com o recurso existente e o relatório será atualizado para exibir uma única entrada.
- Se a solicitação inicial for permitida mas a solicitação duplicada for bloqueada, ambas as solicitações permanecerão na lista. A solicitação permitida representa o recurso real e a solicitação duplicada em estado bloqueado ou pendente representa a tentativa do registro de um recurso possivelmente duplicado.

O relatório **Status de registro do agente** mantém todas as solicitações para fins de auditoria e permite observá-las continuamente.

Essa tarefa é uma etapa nos seguintes processos:

- Instalação do Symantec Management Agent em computadores do Windows.
Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.
- Instalação manual do Symantec Management Agent em computadores UNIX, Linux e Mac.
Consulte [“Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac”](#) na página 255.

Para exibir e gerenciar o status de registro do agente

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, em **Relatórios**, expanda **Notification Server Management > Registro** e clique em **Status de registro do agente**.

- 3 (Opcional) Na página **Status de registro do agente**, use as opções do menu contextual para modificar o status do agente. Dependendo do status do agente, as opções do menu contextual variam.

Permitir Você pode permitir os agentes em estado **Pendente**, **Bloqueado** ou **Revogado**.

Se você permitir um agente bloqueado, a confiança será concedida na próxima vez em que o agente enviar uma solicitação de registro ao Notification Server.

Bloqueado Você pode bloquear os agentes que estão em estado **Pendente** ou **Revogado**.

Se você bloquear um computador revogado, seu status funcional não será alterado. Contudo, alterar o status permite diferenciar os computadores revogados que não podem mais se conectar ao Notification Server dos computadores revogados que ainda podem exigir sua atenção.

Os computadores com status **Bloqueado** serão removidos da lista após um período de tempo predefinido se nenhuma solicitação de novo registro for enviada do mesmo computador durante esse tempo. O período padrão é de três meses, mas você pode alterá-lo na página **Manutenção da purga**.

Revogado É possível revogar o registro dos agentes que você tinha permitido anteriormente. Por exemplo, você pode revogar o registro do computador-cliente relatado como ausente ou roubado. Após revogar o agente, você não receberá políticas do Notification Server. Além disso, um computador revogado não poderá ser usado como um servidor de sites.

Durante a revogação da confiança interna do agente, o registro da chave de criptografia do agente será marcado como revogado no Notification Server. Os agentes revogados não recebem políticas e não executam tarefas. Além disso, o agente revogado limpa as políticas armazenadas localmente para minimizar sua atividade. Após a revogação, o Symantec Management Agent é forçado a reiniciar o processo de registro.

O agente receberá as informações sobre seu status revogado na próxima vez que tentar acessar os dados protegidos. O Notification Server não notifica o agente sobre o evento de revogação quando ele ocorre.

O agente revogado permanece em estado **Revogado** mesmo que seja permitido pela política de registro do agente. Você deve gerenciar manualmente os computadores revogados se quiser alterar seu estado.

Para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac

Você pode instalar o Symantec Management Agent com uma instalação por envio manual ou uma instalação pull manual. É recomendado instalar o Symantec Management Agent enviando-o manualmente aos computadores selecionados. Porém, para instalar nos computadores remotos que têm acesso limitado à rede ou estão atrás de um firewall, pode ser necessário executar uma instalação pull manual.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Tabela 15-4 Processo para instalar manualmente o Symantec Management Agent em computadores UNIX, Linux e Mac

Etapa	Ação	Descrição
Etapa 1	Selecione os computadores nos quais você quer instalar o agente e os plug-ins.	Você tem as seguintes opções para selecionar computadores: ■ Descoberta de rede ■ Seleção manual adicionando nomes de host do cliente ou endereços IP ■ Importação do Active Directory ■ Importação usando um arquivo de valores separados por vírgula.
Etapa 2	Verifique se os computadores cumprem os pré-requisitos da instalação.	Cada computador deve cumprir os pré-requisitos de hardware e software antes da instalação do Symantec Management Agent. Consulte “Pré-requisitos de instalação do Symantec Management Agent para UNIX, Linux e Mac” na página 258.
Etapa 3	(Opcional) Defina as políticas de registro do agente.	Depois de instalar o Symantec Management Agent, ele enviará uma solicitação de registro ao Notification Server para estabelecer a confiança entre o servidor e o cliente. A política padrão de registro do agente permite o registro automático de todos os agentes. Você pode modificar a política padrão ou criar políticas personalizadas para especificar regras mais restritivas. Consulte “Para criar uma política de registro do agente” na página 243.

Etapa	Ação	Descrição
Etapa 4	Especifique as configurações de instalação.	As configurações de instalação do UNIX, Linux e Mac permitem definir as configurações de comunicação e autenticação para o Symantec Management Agent para UNIX, Linux e Mac. Se você importar nomes de computadores de um arquivo CSV, será possível especificar estas configurações no arquivo CSV. Você também pode definir ou mudar estas configurações do Console de gerenciamento Symantec. Consulte “Para especificar as configurações de instalação do Symantec Management Agent para UNIX, Linux e Mac” na página 259.
Etapa 5	Instale o Symantec Management Agent usando o método apropriado.	O método preferencial é enviar o Symantec Management Agent para os computadores selecionados. Porém, se um computador estiver protegido por um firewall ou for de difícil acesso para o Notification Server, você poderá realizar a instalação pull do Symantec Management Agent. Consulte “Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual” na página 260. Consulte “Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação pull manual” na página 264.
Etapa 6	Visualize e gerencie o status de registro do agente para verificar o registro com êxito.	O relatório Status de registro do agente permite exibir e gerenciar todas as solicitações de registro e os registros concluídos dos Symantec Management Agents. Consulte “Para exibir e gerenciar o status do registro do agente” na página 251.

Para criar um arquivo CSV para importar computadores UNIX, Linux e Mac

Se desejar instalar o Symantec Management Agent para UNIX, Linux e Mac em um grande número de computadores que exigem conexão e configurações diferentes, recomendamos que você use um arquivo CSV para importar os computadores e para definir as configurações da instalação. O CSV é um arquivo de texto delimitado por vírgulas que inclui os nomes de DNS ou os endereços IP dos computadores-cliente nos quais você deseja instalar o Symantec Management Agent. Cada linha do arquivo CSV representa uma entrada do computador que é importada para a página **Instalação do Symantec Management Agent**. O arquivo CSV também pode conter as configurações de instalação para cada computador.

Consulte [“Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual”](#) na página 260.

Um arquivo de modelo CSV para importar os computadores UNIX, Linux e Mac (`CSVTemplate.csv`) é fornecido com o Symantec Management Platform. O cabeçalho da coluna do modelo CSV indica os dados que são necessários e os valores válidos que você pode usar.

Aviso: O formato de arquivo CSV (separador de lista) deve atender às configurações regionais do servidor. Por exemplo, o arquivo de amostra `CSVTemplate.csv` utiliza as configurações regionais "Inglês (Estados Unidos)" com uma vírgula "," como separador de lista. Você pode exibir as configurações regionais do Symantec Management Platform no **Painel de Controle** do Windows.

Esta tarefa é uma etapa do processo de instalação manual do Symantec Management Agent.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para criar um arquivo CSV para importar computadores UNIX, Linux e Mac

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, na guia **Instalar o Agent para UNIX, Linux e Mac**, em **Agente de instalação para UNIX, Linux e Mac em computadores**, clique com o botão direito do mouse em **Modelo de arquivo CSV** e depois clique em **Salvar destino como**.
- 3 Na caixa de diálogo **Salvar como**, digite um nome adequado para o arquivo `CSVTemplate.csv`, procure o local apropriado e clique em **Salvar**.
- 4 Abra o arquivo salvo CSV em um editor de texto e digite as informações de cada computador no qual você deseja instalar o Symantec Management Agent para UNIX, Linux e Mac.

Não é necessário usar todos os campos. Você pode usar somente os campos dos quais necessita, como o nome do computador, nome da raiz, senha raiz etc.

As configurações que você pode especificar no arquivo CSV são idênticas às configurações que podem ser definidas na janela **Configurações da instalação** no Console de gerenciamento Symantec.

- 5 Quando você tiver concluído, salve o arquivo CSV.

Pré-requisitos de instalação do Symantec Management Agent para UNIX, Linux e Mac

Para instalar o Symantec Management Agent para UNIX, Linux e Mac, seu computador deve cumprir os pré-requisitos de hardware e software.

Consulte [“Métodos de instalação do Symantec Management Agent”](#) na página 238.

Este tópico é uma etapa do processo de instalação manual do Symantec Management Agent.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Tabela 15-5 Pré-requisitos de instalação do Symantec Management Agent para UNIX, Linux e Mac

Pré-requisito	Descrição
Sistema operacional	Qualquer um dos seguintes sistemas operacionais: ■ Solaris 9 (SPARC) ■ Solaris 10 (x86, x86_64 e SPARC) ■ Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 (x86 e x86_64) ■ Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3, 6.4 (x86 e x86_64) ■ SUSE Linux Enterprise Server 10, 11 SP1, 11 SP2 (x86 e x86_64) ■ SUSE Linux Enterprise Desktop 10, 11 SP1, 11 SP2 (x86 e x86_64) ■ Mac OS X 10.6.x, 10.7.x, 10.8.x (binário universal) ■ Mac OS X Server 10.6.x, 10.7.x, 10.8.x (binário universal) ■ HP-UX 11,11 (PA-RISC), 11,23 (PA-RISC/IA64), 11,31 (PA-RISC/IA64) ■ PPC do AIX 6.1, padrão 7.1
Espaço em disco rígido	Mínimo de 60 MB
RAM	Mínimo de 25 MB
Direitos de acesso	Os direitos de acesso do usuário-raiz são necessários em todas as plataformas UNIX/Linux. Para Mac OS X, é necessário ter direitos de acesso administrativos ou de usuário-raiz.

Pré-requisito	Descrição
Conexões remotas de SSH ativadas	As conexões remotas de SSH devem ser ativadas. Deve haver um servidor de SSH sendo executado no computador-cliente e o firewall deve estar configurado para permitir uma conexão de entrada de SSH.
Conexão de saída para o Notification Server ativada	O firewall deve estar configurado para permitir uma conexão de saída a uma porta da WEB no Notification Server.

Para especificar as configurações de instalação do Symantec Management Agent para UNIX, Linux e Mac

As configurações de instalação do Symantec Management Agent são a comunicação e as configurações de autenticação para o Symantec Management Agent para UNIX, Linux e Mac. Você deve especificar o nome e a senha de login privilegiados adequados da conta para cada computador de destino.

Consulte [“Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual”](#) na página 260.

Quando você importar computadores de um arquivo CSV, será possível especificar as configurações de instalação adequadas para cada computador no arquivo CSV. Se você não especificar nenhuma configuração no arquivo CSV ou se tiver adicionado os computadores manualmente, será preciso especificar as configurações adequadas para cada computador de destino antes de instalar o Symantec Management Agent para UNIX, Linux e Mac.

Você pode especificar configurações de instalação para um computador específico ou para vários computadores. Se você selecionar vários computadores, as mesmas configurações de instalação serão aplicadas a cada computador. Você também pode duplicar as configurações atuais de instalação de um computador e aplicá-las a outros computadores.

Consulte [“Para criar um arquivo CSV para importar computadores UNIX, Linux e Mac”](#) na página 256.

Esta tarefa é uma etapa do processo de instalação manual do Symantec Management Agent.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para especificar as configurações de instalação do Symantec Management Agent para UNIX, Linux e Mac

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, na guia **Instalar o Agent para UNIX, Linux e Mac**, em **Agente de instalação para UNIX, Linux e Mac em computadores**, na lista de computadores, clique no computador para o qual mudar as configurações de instalação do Symantec Management Agent e depois clique em **Configurações da instalação**.

Se desejar especificar configurações idênticas de instalação para vários computadores ou se duplicar as configurações atuais de instalação de outro computador, selecione os computadores apropriados.

- 3 (Opcional) Se desejar duplicar as configurações atuais de instalação de um computador específico, na caixa de diálogo **Configurações da instalação**, na lista suspensa **Carregar configurações**, selecione o computador apropriado.

A opção **Carregar configurações de** aparecerá na parte superior direita da caixa de diálogo **Configurações da instalação** se você tiver selecionado vários computadores.

- 4 Especifique as configurações apropriadas de instalação para os computadores selecionados.

Para obter mais informações, clique na página e pressione **F1**.

- 5 Na caixa de diálogo **Configurações de instalação**, clique em **OK**.

Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual

Você pode enviar o Symantec Management Agent para UNIX, Linux e Mac a qualquer computador relacionado na página de instalação do Symantec Management Agent.

Para instalar ou desinstalar manualmente o Symantec Management Agent através da página **Instalação do Symantec Management Agent**, selecione os computadores apropriados. Você pode selecionar os computadores que foram detectados com a descoberta de recursos, digitar os nomes de computador manualmente ou importar os computadores de um arquivo CSV.

Nota: Você apenas poderá instalar manualmente o Symantec Management Agent nos computadores que foram descobertos usando a **Descoberta de recursos de domínio** ou a **Descoberta de rede**.

A instalação remota do Symantec Management Agent para UNIX, Linux e Mac é executada pelo computador do Symantec Management Platform. O computador do Symantec Management Platform estabelece uma conexão com o computador de destino UNIX, Linux ou Mac, faz o upload dos arquivos necessários e os executa no computador de destino.

O processo de instalação é da seguinte maneira:

- As tentativas do Symantec Management Platform de se conectar ao computador de destino com SSH.
O protocolo SSH suporta conexão com contas privilegiadas ou do usuário não autorizado e vários senhas.
- Quando a conexão for estabelecida, o Symantec Management Platform determinará o sistema operacional e o ambiente do computador-cliente e iniciará o script apropriado de instalação por envio específico da plataforma.
- O script de instalação por envio cria uma estrutura de diretórios no computador-cliente e tenta fazer o download do utilitário `aex-bootstrap` do computador do Symantec Management Platform. O script de instalação por envio tenta cada um dos seguintes métodos, respectivamente, até que obtenha êxito: SCP/SFTP, `wget`, `curl`.
Se todos estes métodos falham, o script usa o comando `dd` para transferir o arquivo morto `aex-bootstrap.Z.uu` para o computador de destino. Ele usa então o `uudecode` para converter o arquivo morto para um formato nativo.
- O arquivo `.aex-agent-install-config.xml`, que contém todas as configurações de instalação do Symantec Management Agent, é obtido por download pelo computador-cliente.
- O script `aex-bootstrap` é executado e a conexão ao Symantec Management Platform é encerrada.
- O script `aex-bootstrap` faz o download do restante do Symantec Management Agent do computador do Symantec Management Platform e configura o Symantec Management Agent com as configurações do arquivo `.aex-agent-install-config.xml`.
- Quando o Symantec Management Agent para UNIX, Linux e Mac for executado pela primeira vez, ele coletará o inventário básico e o disponibilizará ao Symantec Management Platform.

- O Symantec Management Agent para UNIX, Linux e Mac recebe as tarefas e as políticas apropriadas do Symantec Management Platform.

Nota: Os firewalls de terceiros devem ser configurados para permitir uma conexão SSH do Symantec Management Platform ao cliente ULM para que uma instalação por envio manual funcione. A configuração dos firewalls deve usar as mesmas credenciais que você forneceu na caixa de diálogo **Configurações da instalação** na etapa 4.

Esta tarefa é uma etapa do processo de instalação manual do Symantec Management Agent.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, na guia **Instalar o Agent para UNIX, Linux e Mac**, em **Instalar o Agente para UNIX, Linux e Mac**, selecione os computadores UNIX, Linux e Mac nos quais o Symantec Management Agent será instalado:

Para adicionar um computador manualmente

Na caixa de texto, digite o nome do computador (que deve ser um nome DNS que pode ser resolvido) ou endereço IP e clique em **Adicionar**.

Para selecionar dos computadores disponíveis

Clique em **Selecionar computadores**, na caixa de diálogo **Selecionar computadores**, adicione os computadores apropriados da lista de **Computadores disponíveis** à lista de **Computadores selecionados** e clique em **OK**.

- Para importar computadores de um arquivo CSV
- 1 Na barra de ferramentas, clique em **Importar computadores de um arquivo selecionado**.
 - 2 Na caixa de diálogo **Selecionar arquivo para importar**, selecione o arquivo CSV apropriado e clique em **Abrir**.

O arquivo CSV é um arquivo de texto delimitado por vírgulas. O arquivo inclui os nomes de DNS ou os endereços IP dos computadores-cliente nos quais você deseja instalar o Symantec Management Agent. Para computadores UNIX, Linux e Mac, cada linha do arquivo CSV representa uma entrada do computador que será importada para a página **Instalação do Symantec Management Agent**. Você também pode incluir as configurações apropriadas da instalação no arquivo CSV. Estas configurações de instalação permitem configurar a comunicação e as configurações de autenticação do Symantec Management Agent para UNIX, Linux e Mac.

Se você tiver um grande número de computadores que exijam uma conexão e configurações diferentes, use um arquivo CSV para importar os computadores.

Consulte [“Para criar um arquivo CSV para importar computadores UNIX, Linux e Mac”](#) na página 256.

- 3 Clique em **Configurações da instalação** e então, na caixa de diálogo **Configurações da instalação**, especifique as configurações apropriadas da instalação.

Se tiver adicionado computadores manualmente, você precisará especificar as configurações apropriadas da instalação para cada computador de destino antes de instalar o Symantec Management Agent para UNIX, Linux e Mac. Se você tiver importado computadores de um arquivo CSV, talvez tenha especificado as configurações de instalação para cada computador no arquivo CSV. Você pode mudar estas configurações para computadores individuais ou grupos de computadores.

Consulte [“Para especificar as configurações de instalação do Symantec Management Agent para UNIX, Linux e Mac ”](#) na página 259.

- 4 (Opcional) Na caixa **Tarefas simultâneas**, especifique o número de instalações para executar simultaneamente.

Este valor define o número de segmentos executados paralelamente e que servem ao envio do Symantec Management Agent. Todos os segmentos compartilham uma fila comum de onde obtêm o próximo computador para instalação. O valor padrão é 5, mas convém usar um valor diferente para satisfazer o desempenho do Symantec Management Platform, dos computadores-cliente e da capacidade de rede. Aumentar o número de tarefas simultâneas pode reduzir o tempo total da instalação.

- 5 Clique em **Instalar**.
- 6 Na caixa de diálogo **Instalação por envio**, marque a caixa de seleção para concordar com a instalação de software de terceiros e clique em **OK**.

Nota: Se a plataforma de destino for RHEL 6.0 de 64 bits ou superior e não tiver a camada de compatibilidade com 32 bits instalada, o envio do agente falhará se você não concordar com a instalação de software de terceiros.

A coluna **Status**, na lista de computadores, mostra o sucesso ou falha da instalação em cada computador. Observe que o Symantec Management Agent recém-instalado relatará seu status ao Notification Server de origem, mesmo se for gerenciado por outro Notification Server.

- 7 Se a lista de computadores não for atualizada automaticamente, na barra de ferramentas, clique em **Atualizar** para exibir o status atual da instalação por envio de cada computador.

Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação pull manual

Se o SSH não estiver disponível ou você quiser instalar o Symantec Management Agent para UNIX, Linux e Mac nos computadores remotos que têm acesso limitado à rede ou em computadores de destino protegidos por um firewall, será possível fazer uma instalação pull do Symantec Management Agent em cada computador. Você ou qualquer pessoa com direitos de administrador pode fazer login em cada computador, acessar o Symantec Management Platform com um URL e fazer o download do programa de instalação do bootstrap que executa a instalação do Symantec Management Agent para UNIX, Linux e Mac.

O URL da página **Fazer o download do Symantec Management Agent para UNIX, Linux e Mac** é mostrado na página **Instalação do Symantec Management Agent**, em **URL da página de download para UNIX, Linux e Mac**. Você pode exibir a página, mas não pode mudar esta configuração.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Consulte [“Symantec Management Agent para comandos de solução de problemas de UNIX, Linux e Mac”](#) na página 512.

Esta tarefa é uma etapa do processo de instalação manual do Symantec Management Agent.

Consulte [“Para instalar o Symantec Management Agent em computadores Windows”](#) na página 240.

Para visualizar a página Fazer download do Symantec Management Agent para UNIX, Linux e Mac

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, na guia **Instalar o Symantec Management Agent para UNIX, Linux e Mac**, em **URL da página de download para usuários de UNIX, Linux e Mac**, na lista suspensa **Selecione a plataforma**, clique na plataforma apropriada e depois clique em **Exibir página**.

Para fazer a instalação pull do Symantec Management Agent para UNIX, Linux e Mac em computadores remotos

- 1 Faça logon no computador remoto como administrador.
- 2 No computador remoto, abra um navegador da Web e vá para o seguinte URL:
`http://Nome_do_SMP/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=Plataforma`
onde *Nome_do_SMP* é o nome de seu computador do Symantec Management Platform e *Plataforma* é a plataforma apropriada.
- 3 Siga as instruções que são exibidas na página **Fazer o download do Symantec Management Agent para UNIX, Linux e Mac** para fazer o download e executar o programa de instalação do bootstrap no computador remoto.

Para fazer o upgrade e desinstalar o Symantec Management Agent

Este capítulo contém os tópicos a seguir:

- [Métodos para fazer upgrade do Symantec Management Agent](#)
- [Métodos de desinstalação do Symantec Management Agent](#)
- [Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent](#)
- [Sobre a comunicação do agente legado](#)
- [Para configurar o pacote do Symantec Management Agent](#)
- [Para remover manualmente o Symantec Management Agent para Windows](#)

Métodos para fazer upgrade do Symantec Management Agent

Você precisa instalar a versão apropriada do Symantec Management Agent em seus computadores gerenciados. Se algum computador tiver versões antigas do agente instaladas, será necessário fazer upgrade das versões.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Tabela 16-1 Métodos de upgrade do Symantec Management Agent

Método	Descrição
Enviar manualmente o Symantec Management Agent aos computadores apropriados.	Você pode fazer o upgrade do Symantec Management Agent manualmente enviando-o aos computadores apropriados. Você pode enviá-lo para um computador que tenha uma versão mais antiga do Symantec Management Agent instalada. Consulte “Para instalar o Symantec Management Agent para Windows com uma instalação por envio manual” na página 246. Consulte “Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual” na página 260.
Use a política de upgrade do Symantec Management Agent.	A política de upgrade do Symantec Management Agent é fornecida com o Notification Server. Você pode ativar esta política e configurá-la para assegurar-se de que todos os seus computadores gerenciados tenham a versão correta do Symantec Management Agent instalada. Consulte “Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent” na página 268. Nota: Durante a transição do IT Management Suite das versões anteriores à versão 7.5, o modo de Comunicação do agente legado (LAC, Legacy Agent Communication) ativado permitirá que um Notification Server com upgrade execute um conjunto limitado de funções de gerenciamento em endpoints com versões mais antiga do Symantec Management Agent. Você pode gerenciar o modo Comunicação do agente legado no Console de gerenciamento Symantec, na página Configurações do Notification Server, guia Processamento. Consulte “Sobre a comunicação do agente legado” na página 272. Consulte “Para definir configurações do Notification Server” na página 66.

Métodos de desinstalação do Symantec Management Agent

É possível remover o Symantec Management Agent de um computador gerenciado quando não precisar mais do programa. Você não precisa remover nenhum agente da solução instalado no computador porque ele é removido automaticamente como parte do processo de desinstalação do Symantec Management Agent.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

Tabela 16-2 Métodos para desinstalar o Symantec Management Agent

Método	Descrição
Desinstalação manual.	A desinstalação manual é iniciada no Symantec Management Console e remove o Symantec Management Agent imediatamente. Você pode remover o Symantec Management Agent de qualquer número de computadores Windows na mesma operação de desinstalação. Também é possível personalizar as opções de desinstalação para cada operação. Esta opção está disponível apenas para computadores Windows. Consulte “Para remover manualmente o Symantec Management Agent para Windows” na página 274.
Use a política de desinstalação do Symantec Management Agent.	A política de desinstalação do Symantec Management Agent é fornecida com o Symantec Management Platform. Você pode ativar esta política e configurá-la para assegurar-se de que o Symantec Management Agent seja removido dos computadores apropriados. Esta opção está disponível para computadores Windows, UNIX, Linux e Mac. Consulte “Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent” na página 268.

Para configurar as políticas de upgrade e de desinstalação do Symantec Management Agent

Você pode configurar o upgrade do Symantec Management Agent e as políticas de desinstalação do Symantec Management Agent para satisfazer seus requisitos.

Ambas as políticas usam o pacote apropriado do Symantec Management Agent, mas com programas diferentes.

Consulte [“Sobre o Symantec Management Agent”](#) na página 236.

O Notification Server fornece filtros padrão que você pode usar em operações de instalação agendadas do agente e também em políticas de upgrade e de desinstalação do agente. Estes filtros são armazenados na pasta Symantec Management Agent, na subpasta apropriada. Você não pode modificar os filtros padrão, mas pode duplicá-los para criar novos filtros que poderá editar para atender a seus requisitos.

Contudo, você deve ser cuidadoso quando executar upgrades do Symantec Management Agent baseados em destinos de recursos. Em um ambiente grande, é recomendável agendar os upgrades usando primeiro um destino de teste e depois fazer a distribuição agendada por meio dos destinos apropriados em vez de executar todos ao mesmo tempo. Por exemplo, pode haver alguns problemas com o upgrade; assim, você poderá testá-lo em um pequeno número de computadores e identificar e resolver os problemas sem afetar todos os computadores. Um upgrade escalonado também ajuda a gerenciar a carga na rede, pois os agentes normalmente precisam solicitar dados do Notification Server logo que seus upgrades são concluídos

Nota: Durante a transição do IT Management Suite das versões anteriores à versão 7.5, o modo de **Comunicação do agente legado** (LAC, Legacy Agent Communication) ativado permitirá que um Notification Server com upgrade execute um conjunto limitado de funções de gerenciamento em endpoints com versões mais antiga do Symantec Management Agent. Você pode gerenciar o modo **Comunicação do agente legado** no Console de gerenciamento Symantec, na página **Configurações do Notification Server**, guia **Processamento**.

Consulte [“Sobre a comunicação do agente legado”](#) na página 272.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

Para configurar as políticas de upgrade e desinstalação do agente

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Agentes/Plug-ins > Symantec Management Agent** e execute em seguida uma das seguintes ações:

Para configurar a política de upgrade do Symantec Management Agent.	■ Em computadores Windows x64, expanda Windows > Servidor não de sites e clique em Symantec Management Agent para Windows x64 (servidores não de site) - Upgrade para Symantec Management Agent de 64 bits. ■ Em computadores Windows x86, expanda Windows > Servidor não de sites e clique em Symantec Management Agent para Windows x86 (servidores não de site) - Upgrade para Symantec Management Agent de 32 bits.
Para configurar a política que faz o upgrade do Symantec Management Agent nos computadores que contêm um ou vários serviços de site.	■ Em computadores Windows x64, expanda Windows > Servidor de sites e clique em Symantec Management Agent para Windows x64 (somente servidores de site) - Upgrade para Symantec Management Agent de 64 bits. ■ Em computadores Windows x86, expanda Windows > Servidor de sites e clique em Symantec Management Agent para Windows x86 (somente servidores de site) - Upgrade para Symantec Management Agent de 32 bits.
Para configurar a política de desinstalação do Symantec Management Agent.	Expandir a pasta Windows e clicar em Symantec Management Agent para Windows - Desinstalação.
Para configurar a política de upgrade do Symantec Management Agent para UNIX/Linux/Mac.	Expandir a pasta UNIX/Linux/Mac e clicar em Symantec Management Agent para UNIX/Linux/Mac - Fazer upgrade.
Para configurar a política de desinstalação do Symantec Management Agent para UNIX/Linux/Mac.	Expandir a pasta UNIX/Linux/Mac e clicar em Symantec Management Agent para UNIX/Linux/Mac - Desinstalar.

3 No painel direito, faça as mudanças de configuração apropriadas:

Nome do programa

O nome do programa do pacote do Symantec Management Agent que será executado quando a política for acionada. A configuração padrão é o programa apropriado para a política e não é preciso alterá-la. Porém, se você adicionou um novo programa ao pacote do Symantec Management Agent, convém usá-lo em seu lugar.

Consulte [“Gerenciamento de programas do pacote”](#) na página 374.

Ativar a geração de relatórios detalhados dos eventos de status

Ativar o envio de eventos de status do pacote ao Notification Server.

As configurações de **Captura de eventos do Notification Server** na política de **Configurações globais do Symantec Management Agent** têm prioridade sobre a configuração de **Ativar geração de relatórios detalhados de eventos de status** aqui. Os eventos serão enviados somente se forem ativados na política de **Configurações globais do Symantec Management Agent**.

Consulte [“Para definir as configurações globais de agentes”](#) na página 277.

Aplicado a

Especifique os computadores aos quais a política se aplica.

Você pode usar filtros predefinidos que são fornecidos com o Notification Server ou criar seus próprios.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Multicast de pacotes

Desativa o download de pacotes pelo multicast.

Normalmente, o multicast torna mais lenta a instalação de um pacote; assim, convém desativá-lo para um patch urgente. Além disso, em alguns ambientes, o multicast não funciona. Por exemplo, pode ser desativado em roteadores e em switches.

As configurações do **Multicast de pacotes** na política de **Configurações globais do Symantec Management Agent** têm prioridade sobre essas configurações.

Agendamento

Especifique o agendamento da política.

Consulte [“Especificação de um agendamento de política”](#) na página 388.

4 Ative a política.

Na parte superior direita da página, clique no círculo colorido e em **Ativado**.

5 Clique em **Salvar alterações**.

Sobre a comunicação do agente legado

O modo **Comunicação do agente legado** (LAC, Legacy Agent Communication) permite controlar se os computadores que usam versões anteriores do Symantec Management Agent podem se comunicar com o Notification Server que passou por um upgrade. Esta opção permite fazer o upgrade dos agentes em seu ambiente em etapas, em vez de atualizar todos eles imediatamente após o upgrade do Notification Server.

Dependendo do modo LAC, o Notification Server pode gerenciar os agentes da seguinte forma:

O modo LAC é desativado.

O Notification Server pode gerenciar de maneira ativa somente os computadores que têm a versão do Symantec Management Agent idêntica à do Notification Server.

Além disso, o Notification Server pode fazer o upgrade do Symantec Management Agent nos computadores que eram gerenciados anteriormente pelo mesmo Notification Server.

O modo LAC é ativado.

O Notification Server pode executar um conjunto limitado de funções de gerenciamento nos computadores que têm uma versão do Symantec Management Agent anterior à do Notification Server.

Nota: Se o modo LAC estiver ativado, os usuários que forem associados com a função **Administradores da Symantec** verão um banner de notificação no canto superior direito do Console de gerenciamento Symantec, a menos que especifiquem para que ele não seja exibido.

Para o Symantec Management Agent 7.1 SP1b e superior, o modo **Comunicação do agente legado** suporta o gerenciamento de agentes legados com os seguintes plug-ins:

Windows	Gerenciamento de software, Gerenciamento de patches, inventário e pcAnywhere.
UNIX e Linux	Gerenciamento de software e inventário.
Mac OS X	Inventário.

A Symantec recomenda desativar o modo LAC após o período de transição da versão anterior do IT Management Suite para a 7.5, para que você não fique limitado a um subconjunto das funcionalidades que o produto oferece quando o modo LAC estiver ativado.

Você pode configurar o modo **Comunicação do agente legado** no Console de gerenciamento Symantec, na página **Configurações do Notification Server**, guia **Processamento**.

Consulte [“Para definir configurações do Notification Server”](#) na página 66.

O modo LAC padrão em diferentes cenários é o seguinte:

- Se você executar uma instalação limpa do IT Management Suite 7.5, o LAC estará desativado.
- Se você fizer upgrade do IT Management Suite 7.0 ou 7.1 para o IT Management Suite 7.5, o LAC estará ativado.
- Se você fizer upgrade do Notification Server 6.x para o IT Management Suite 7.5, o LAC estará ativado.

Para configurar o pacote do Symantec Management Agent

As políticas de instalação do Symantec Management Agent usarão o pacote apropriado quando você fizer upgrade ou desinstalar um agente. Recomendamos que não haja alteração de configurações neste pacote.

Após configurar um pacote do Symantec Management Agent, você precisará atualizar os pontos de distribuição de pacotes para atualizar as informações do pacote em cada servidor de pacotes.

Consulte [“Atualização dos pontos de distribuição para um pacote”](#) na página 372.

Para configurar um pacote do Symantec Management Agent

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Agentes/Plug-ins > Symantec Management Agent**.

- 3 Na pasta **Windows** ou **UNIX/Linux/Mac**, clique no pacote do Symantec Management Agent que você deseja configurar.
- 4 Na página **Pacote do Symantec Management Agent**, faça as alterações necessárias de configuração nas guias apropriadas.
Para obter mais informações, clique na página e pressione **F1**.
- 5 Clique em **Salvar alterações**.

Para remover manualmente o Symantec Management Agent para Windows

Você pode remover manualmente o Symantec Management Agent de qualquer computador selecionado.

Para remover manualmente o Symantec Management Agent

- 1 No Console de gerenciamento Symantec, no menu **Ações**, clique em **Agentes/Plug-ins > Enviar Symantec Management Agent**.
- 2 Na página **Instalação do Symantec Management Agent**, selecione os computadores Windows dos quais o Symantec Management Agent será removido.
- 3 Na página **Instalação do Symantec Management Agent**, em **Instalar agente nos computadores**, clique em **Desinstalar**.

- 4 Na caixa de diálogo **Opções de desinstalação do Symantec Management Agent**, selecione as opções que você deseja usar e especifique as configurações necessárias nas caixas apropriadas.

Usar proxy (se estiver configurado no computador alvo)

Use esta opção se o computador em que você está fazendo a instalação por envio precisar conectar-se ao Notification Server através de um servidor proxy. As mesmas configurações de proxy são usadas para conectar-se ao Notification Server, bem como as configurações de proxy que são usadas pelo Internet Explorer.

Usar a seguinte conta de administrador

Uma conta de administrador é necessária para iniciar o serviço de desinstalação no computador de onde o Symantec Management Agent será removido. A identidade do aplicativo Notification Server é usada por padrão. Se esta conta não tiver permissão para acessar o computador, outra conta precisará ser usada.

É necessário especificar o nome do usuário e a senha da conta de administrador apropriados.

- 5 Clique em **Continuar a desinstalação**.

Para configurar o Symantec Management Agent

Este capítulo contém os tópicos a seguir:

- [Para configurar o Symantec Management Agent](#)

Para configurar o Symantec Management Agent

As configurações padrão do Symantec Management Agent são apropriadas para um ambiente pequeno do Symantec Management Platform. Conforme seu ambiente cresce ou se sua organização tem requisitos específicos, você precisa fazer as alterações de configuração apropriadas.

As configurações do agente são aplicadas aos computadores gerenciados apropriados usando as políticas de configuração do agente. Você pode modificar essas políticas para alterar as configurações a qualquer momento. As configurações novas são aplicadas aos agentes quando os computadores gerenciados obtêm suas próximas atualizações da política (uma vez por dia, normalmente).

Tabela 17-1 Tipos de políticas de configuração de agente

Tipo	Descrição
Configurações globais	As configurações globais se aplicam a todos os Symantec Management Agents em todos os computadores gerenciados. Essas configurações são aplicadas como uma única política que se destina automaticamente a cada computador gerenciado. Consulte “Para definir as configurações globais de agentes” na página 277.

Tipo	Descrição
Configurações de destino	As configurações direcionadas do agente são os parâmetros gerais que controlam o Symantec Management Agent, incluindo como o agente se comunica com o Notification Server. Você pode modificar as políticas padrão fornecidas com o Symantec Management Platform. Você pode criar suas próprias políticas de configurações direcionadas do agente e aplicá-las aos computadores gerenciados apropriados. Consulte “Para definir as configurações do agente de destino” na página 278.
Janelas de manutenção	Uma janela de manutenção é um horário e uma duração agendados nos quais as operações de manutenção podem ser executadas em um computador gerenciado. Uma política de janela de manutenção define uma ou mais janelas de manutenção. Você pode modificar a política padrão fornecida com o Symantec Management Platform. Você pode criar suas próprias políticas de janela de manutenção e aplicá-las aos computadores gerenciados apropriados. Consulte “Para configurar políticas de janela de manutenção” na página 280.

As políticas de configurações de destino e as políticas de janela de manutenção são aplicadas aos computadores gerenciados incluídos nos destinos especificados da política. Esses destinos não são mutuamente exclusivos. Duas ou mais políticas do mesmo tipo podem ser aplicadas ao mesmo computador gerenciado.

Se um computador gerenciado tiver duas ou mais políticas de configurações de destino aplicadas, o Notification Server selecionará a política a ser usada. A seleção é baseada na GUID da política e não é transparente ao usuário. Você não pode determinar com antecedência qual política é escolhida. Porém, após fazer a seleção, ela será usada consistentemente para garantir que a mesma política seja aplicada a cada atualização de política.

Se duas ou mais políticas de janela de manutenção forem aplicadas ao mesmo computador gerenciado, as políticas serão mescladas. Todas as janelas de manutenção especificadas são usadas.

Para definir as configurações globais de agentes

As configurações globais são aquelas que você não precisaria definir distintamente em computadores diferentes; assim, elas se aplicam a todos os Symantec Management Agents em todos os computadores gerenciados. Essas configurações

são aplicadas como uma política de configurações globais de agentes; assim, elas são atualizadas da mesma maneira como qualquer outra política. Por padrão, a política de configurações globais de agentes é atualizada de hora em hora. Você não pode excluir ou desativar a política de configurações globais de agentes ou criar versões alternativas dela.

Se deseja especificar configurações do agente para grupos específicos de computadores gerenciados, você precisará configurar as políticas apropriadas de configurações direcionadas do agente.

Para definir as configurações globais do agente

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Agentes/Plug-ins > Configurações globais**.
- 2 Defina as configurações apropriadas nas seguintes guias:

Geral	Especifique as configurações de ativação/gerenciamento de energia e multicast de pacotes.
Autenticação	Especifique o nome de usuário e a senha que o Symantec Management Agent usará quando se conectar ao Notification Server ou a um servidor de pacotes.
Eventos	Especifique os eventos do Notification Server que você deseja capturar.

Para obter mais informações, clique na página e pressione **F1**.

- 3 Clique em **Salvar alterações**.

Consulte [“Para configurar o Symantec Management Agent”](#) na página 276.

Para definir as configurações do agente de destino

A política de configurações direcionadas do agente permite definir os parâmetros gerais que controlam o Symantec Management Agent, inclusive como o agente se comunica com o Notification Server. Você pode aplicar estas configurações a grupos específicos de computadores. Por exemplo, alguns grupos de computadores podem ter finalidades diferentes ou talvez tratem de modo diferente os servidores de outros computadores gerenciados. Você pode modificar as políticas padrão fornecidas com o Notification Server ou criar suas próprias políticas de configurações direcionadas do agente.

Se desejar especificar algumas configurações que se aplicam a todos os Symantec Management Agents em todos os computadores gerenciados, você precisará configurar a política de configurações globais de agentes.

Para definir as configurações de agente de destino

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Agentes/Plug-ins > Configurações de agente de destino**.
- 2 No painel esquerdo, execute um desses procedimentos:
 - Para criar uma nova política de configurações direcionadas do agente, clique em **Criar nova**.
 - Para definir ou mudar o nome da política, clique na política apropriada e depois em **Renomear**.
 Na caixa de diálogo **Renomear o item**, digite o nome novo e clique em **OK**.
- 3 No painel direito, faça as configurações apropriadas nas seguintes guias:

Geral	As configurações gerais incluem as frequências de download da política e da coleta do inventário, além dos computadores, usuários ou destinos de recursos aos quais a política se aplica.
UNIX/Linux/Mac	Se o Symantec Management Agent para UNIX, Linux e Mac estiver instalado, esta guia estará disponível e fornecerá configurações gerais para computadores gerenciados UNIX, Linux e Mac.
Downloads	As configurações de download controlam como cada agente faz o download de pacotes durante entregas do software. Você pode ativar o download do multicast e configurar o multicast para sessões do mestre e de cliente. Você pode substituir estas configurações para políticas e tarefas individuais de entrega do software.
Bloqueios	Os períodos de bloqueio são os momentos em que toda a comunicação entre o agente e o Notification Server é desativada. Você pode configurar qualquer quantidade de períodos de bloqueio.
Controle do usuário	As configurações do controle do usuário são as opções que afetam o que o usuário do computador gerenciado pode ver.
Avançado	Permite especificar um URL alternativo para ser usado pelo Symantec Management Agent para acessar o Notification Server e ativar os recursos de gerenciamento de energia.

Para obter mais informações, clique na página e pressione **F1**.

- 4 (Opcional) Para restaurar a política a suas configurações padrão, clique em **Restaurar padrões**.
- 5 Clique em **Salvar alterações**.

Consulte “[Para configurar o Symantec Management Agent](#)” na página 276.

Para configurar políticas de janela de manutenção

Uma janela de manutenção é um horário e uma duração agendados nos quais as operações de manutenção podem ser executadas em um computador gerenciado. Uma operação de manutenção altera o estado de um computador, fazendo com que ele reinicie ou interfira na capacidade de um usuário operá-lo. Por exemplo, instalar patches de software e sistema operacional ou executar uma verificação de vírus.

Uma política de janela de manutenção define uma ou mais janelas de manutenção e é aplicada a um destino de recurso da mesma maneira como qualquer outra política. Essas políticas fornecem a flexibilidade máxima para atribuir janelas de manutenção a computadores, sem complicar o gerenciamento de configurações do agente. Se várias políticas de janela de manutenção se aplicarem a um único computador, as alterações no computador serão permitidas durante algumas das janelas de manutenção.

O uso de janelas de manutenção permite agendar o trabalho de manutenção em computadores gerenciados com efeito mínimo no fluxo de trabalho e na produtividade. Além disso, você pode agendar o trabalho de manutenção em servidores críticos em diferentes momentos. Assim, não acontecerá de dois servidores serem reiniciados ao mesmo tempo. Uma janela de manutenção pode ser agendada para determinadas vezes, tais como diariamente, semanalmente ou mensalmente. A janela de manutenção pode estar disponível indefinidamente ou restrita a um intervalo específico de datas.

Quando você aplica uma janela de manutenção a um computador gerenciado, as tarefas de manutenção, tais como patches e entregas de software, podem ser realizadas neles somente no período de tempo agendado. Os Symantec Management Agents podem fazer o download de pacotes de entrega de software a qualquer momento, mas os programas associados podem ser executados somente durante as janelas de manutenção.

O Symantec Management Agent processa a política e fornece a funcionalidade que as soluções usam para determinar se uma janela de manutenção está atualmente aberta. A funcionalidade também é fornecida para permitir que as soluções informem o Notification Server que uma tarefa de manutenção foi executada.

Se o Symantec Management Agent estiver executando uma tarefa como parte de um trabalho quando a janela de manutenção expirar, a janela de manutenção será estendida automaticamente até que todas as tarefas contidas no trabalho sejam concluídas.

Você pode criar e modificar as políticas de janela de manutenção que você precisa e aplicá-las aos destinos apropriados. A política padrão de janela de manutenção é aplicada a todos os computadores gerenciados.

Para configurar políticas de janela de manutenção

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Agentes/Plug-ins > Janelas de manutenção**.
- 2 No painel esquerdo, execute um desses procedimentos:
 - Para criar uma nova política de janela de manutenção, clique com o botão direito do mouse na pasta **Janelas de manutenção** e em **Novo(a) > Janela de manutenção**.
 - Para modificar uma política de janela de manutenção existente, clique na política apropriada.
- 3 No painel direito, na lista suspensa **Fuso horário**, clique na opção apropriada:

Usar hora do agente Os horários são especificados sem informações sobre o fuso horário e aplicados no horário local em cada computador gerenciado. As janelas de manutenção são abertas e fechadas em horários diferentes, dependendo dos fusos horários dos computadores gerenciados.

Usar hora do servidor Os horários são especificados com informações de fuso horário, onde o deslocamento de fuso horário é aquele do fuso horário do servidor no qual a política é definida. As janelas de manutenção são abertas simultaneamente, independentemente dos fusos horários, e são compensadas para o horário de verão.

Esta opção garante que as janelas de manutenção sejam sempre coordenadas com o horário local especificado no servidor em que a política é criada.

Coordenar usando UTC Os horários são especificados com informações de fuso horário, onde o deslocamento do fuso horário é 0. As janelas de manutenção são abertas simultaneamente, independentemente dos fusos horários, e não são afetadas pelo horário de verão.

O fuso horário aplica-se a todas as janelas de manutenção especificadas nesta política.

- 4 Se desejar que a política entre em vigor em uma data específica em vez de assim que for ativada, no canto direito superior, clique em **Avançado** e, em seguida, na caixa de diálogo **Opções avançadas**, defina a data de início e a data de término e clique em **OK**.

Início	A data em que a política entra em vigor. A política deve ser ativada assim como qualquer outra política. Você pode ativar a política a qualquer momento antes ou depois da data de início.
Término	Se desejar que a política esteja disponível por um período de tempo limitado, defina a data final apropriada. A política estará indisponível após essa data, esteja ela ativada ou não. Esta configuração é opcional. Se nenhuma data de final for especificada, a política estará disponível indefinidamente.

- 5 Para criar as janelas de manutenção que você quer incluir na política, clique em **Adicionar janela de manutenção**.

- 6 Em cada janela de manutenção, faça o seguinte:

- Em **Horas diárias**, especifique o horário de início e de término da janela de manutenção ou sua duração nas caixas correspondentes.
Como alternativa, você pode arrastar as setas verdes (hora de início) e vermelhas (hora de término) para os locais apropriados na linha de tempo.
- Em **Agendamento de repetições**, na caixa **Repetir a cada**, selecione um agendamento e especifique os filtros de agendamento apropriados.

- 7 Em **Aplicado a**, especifique o destino da política de janela de manutenção.

Você pode selecionar um grupo organizacional, um filtro ou um destino de recurso existente. Você também pode selecionar recursos individuais.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Detalhes dos itens selecionados são exibidos na grade. Você pode exibir a lista por destinos, recursos, computadores ou usuários e fazer todas as adições e exclusões necessárias.

- 8 Clique em **Salvar alterações**.

Consulte [“Para configurar o Symantec Management Agent”](#) na página 276.

Para implementar o gerenciamento habilitado para nuvem

- [Capítulo 18. Introdução ao gerenciamento habilitado para nuvem](#)
- [Capítulo 19. Para preparar o ambiente para o gerenciamento habilitado para nuvem](#)
- [Capítulo 20. Para configurar o gerenciamento habilitado para nuvem](#)
- [Capítulo 21. Para executar tarefas de gerenciamento habilitado para nuvem](#)

Introdução ao gerenciamento habilitado para nuvem

Este capítulo contém os tópicos a seguir:

- [Sobre o gerenciamento habilitado para nuvem](#)

Sobre o gerenciamento habilitado para nuvem

O gerenciamento habilitado para nuvem permite gerenciar endpoints pela Internet mesmo se os computadores-cliente estiverem fora do ambiente corporativo e não puderem acessar os servidores de gerenciamento diretamente. Os computadores gerenciados não precisam usar uma conexão VPN à rede da sua organização.

Você pode aplicar o gerenciamento habilitado para nuvem nos seguintes cenários:

- Uma organização com muitos funcionários que viajam ou que trabalham fora do escritório (fora da intranet corporativa).
- Um provedor de serviços gerenciados (MSP) que gerencia empresas externas.
- Empresas altamente distribuídas, com muitos escritórios pequenos ou funcionários que trabalham remotamente em casa.

Quando você implementar o gerenciamento habilitado para nuvem, o computador do Notification Server e os servidores de sites não serão expostos diretamente à Internet. Consequentemente, o Symantec Management Agent fará a comunicação com o computador do Notification Server e os servidores de sites através de um gateway da Internet. Geralmente dois ou mais gateways da Internet devem estar disponíveis para manter o gerenciamento seguro de clientes ativados na nuvem

e para fornecer opções de failover. Cada gateway da Internet pode suportar o roteamento para vários Notification Servers independentes.

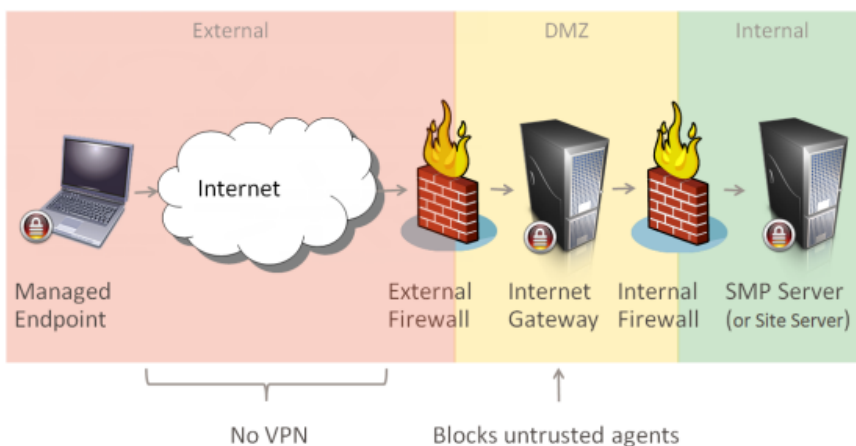
Para usar o gerenciamento habilitado para nuvem, instale um servidor de gateway da Internet. O gateway da Internet funciona como um proxy de encapsulamento. Ele assegura a privacidade e a segurança dos dados que são transmitidos entre um agente e um servidor de gerenciamento com comunicações HTTPS. O gateway da Internet é localizado em uma zona desmilitarizada (DMZ) entre dois firewalls. Ele aceita conexões de entrada dos computadores-cliente autorizados na Internet e as encaminha aos Notification Servers e aos servidores de sites apropriados em sua rede. O gateway da Internet bloqueia todas as tentativas de conexão feitas por clientes não autorizados.

O Symantec Management Agent determina automaticamente se o roteamento da comunicação através do gateway da Internet é necessário. Se um computador habilitado para nuvem tiver acesso direto à rede local usando o VPN, o agente alternará automaticamente para uma comunicação direta com o Notification Server. Se um computador habilitado para nuvem estiver fora da rede da empresa, o agente roteará toda a comunicação na Internet para o Notification Server através do gateway da Internet.

Nota: O gerenciamento habilitado para nuvem é suportado somente em computadores-cliente Microsoft Windows.

O gerenciamento habilitado para nuvem estará disponível no Symantec Management Platform somente quando uma ou mais soluções instaladas suportarem o gerenciamento habilitado para nuvem. Nem todas as soluções da Symantec suportam o gerenciamento habilitado para nuvem no IT Management Suite 7.5. Para obter mais informações sobre o suporte ao gerenciamento habilitado para nuvem para uma solução particular, consulte a documentação da solução.

Figura 18-1 Gerenciamento habilitado para nuvem



Para aproveitar o recurso de gerenciamento habilitado para nuvem, execute as tarefas a seguir:

- Configure a infraestrutura e configure seus servidores e computadores-cliente para usar SSL.
Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.
- Instale e configure os gateways da Internet, configure as políticas de gerenciamento habilitado para nuvem e configure os agentes de gerenciamento da Symantec para suportar o ambiente de gerenciamento habilitado para nuvem.
Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.
- (Opcional) Execute a solução de problemas e as tarefas de manutenção.
Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Para preparar o ambiente para o gerenciamento habilitado para nuvem

Este capítulo contém os tópicos a seguir:

- [Para preparar o ambiente para o gerenciamento habilitado para nuvem](#)

Para preparar o ambiente para o gerenciamento habilitado para nuvem

Configurar seu ambiente para usar SSL é um pré-requisito para configurar o gerenciamento habilitado para nuvem. Depois de configurar seu ambiente para usar SSL, você poderá começar configurar o gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Tabela 19-1 Processo para preparar seu ambiente para o gerenciamento habilitado para nuvem

Etapa	Ação	Descrição
Etapa 1	Configure seus Notification Servers e Symantec Management Agents para usar HTTPS.	Primeiramente, certifique-se de que os Notification Servers estejam configurados para acesso HTTPS e que seus Symantec Management Agents usem HTTPS. O Notification Server será configurado automaticamente para usar HTTPS se você selecionar Exigir HTTPS para acessar o Management Platform na página Configuração do Notification Server, no Symantec Installation Manager, durante a instalação do IT Management Suite. Quando você instalar os Symantec Management Agents de um Notification Server que use HTTPS, os Symantec Management Agents também serão configurados automaticamente para usar HTTPS. Se instalar o Notification Server sem suporte a HTTPS, você poderá configurá-lo manualmente mais tarde. Você também deve redirecionar os Symantec Management Agents para usar HTTPS para comunicar-se com o Notification Server. Consulte “Para configurar o Notification Server para usar o HTTPS” na página 290. Consulte “Para aplicar uma autoridade de certificação raiz a um computador gerenciado” na página 292. Consulte “Para redirecionar o Symantec Management Agent para usar HTTPS” na página 295.

Etapa	Ação	Descrição
Etapa 2	Prepare seus computadores locais.	Os computadores-cliente habilitados para nuvem devem verificar a identidade dos servidores de sites. Para este objetivo, você pode usar um certificado comercial, sua própria infraestrutura de chave pública (PKI, public key infrastructure) ou o Notification Server pode atuar como uma autoridade de certificação (CA, certificate authority) e gerar certificados de seus servidores de site da Internet. O gerenciamento habilitado para nuvem não atribui certificados de servidor aos servidores de sites. Você precisa aplicar certificados de servidor aos servidores de sites para que eles fiquem acessíveis usando HTTPS. Um certificado de servidor é um pré-requisito para qualquer servidor de sites que atenda aos Symantec Management Agents na Internet. A ferramenta de geração de certificados do servidor de sites (<code>AeXGenSiteServerCert.exe</code>) permite criar um certificado de servidor. O nome do certificado deve corresponder ao nome do servidor de sites. Este certificado é assinado pela autoridade de certificação (CA) especial do Notification Server para clientes ativados na nuvem. Se você não tiver sua própria autoridade de certificação da empresa, esta ferramenta permitirá configurar facilmente o HTTPS em seus servidores de sites. Para certificar-se de que o agente no servidor de sites possa se comunicar com o Notification Server usando HTTPS, você deverá também aplicar a autoridade de certificação raiz ao servidor local. Consulte “Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem” na página 296. Consulte “Para aplicar uma autoridade de certificação raiz a um computador gerenciado” na página 292.
Etapa 3	Instale os serviços de site.	Depois de preparar os servidores locais, você poderá instalar os serviços de site. Nota: A execução do Task Server em um computador-cliente habilitado para nuvem e gerenciado na Internet não é suportada e pode conduzir a comportamento indesejável. Consulte “Para gerenciar servidores de sites” na página 131.

Etapa	Ação	Descrição
Etapa 4	Configure os servidores de pacotes para publicar bases de código do pacote HTTPS.	Você precisa assegurar-se de que seus agentes ou servidores de pacotes ativados na nuvem possam receber pacotes do Notification Server ou dos servidores de pacotes internos. Para permitir que façam o download de pacotes, o Notification Server e os servidores de pacotes internos devem publicar bases de código do pacote HTTPS. Consulte “Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS” na página 302. Consulte “Configurações suportadas para servidores de pacotes em um ambiente misto” na página 517. Nota: Os servidores de pacotes publicam bases de códigos usando o FQDN interno. Se você usar um certificado SSL digital atribuído ao Symantec Management Platform, poderá encontrar um problema de conectividade. Para resolver esse problema, consulte o seguinte artigo: TECH210809 (em inglês).
Etapa 5	Configure sites e servidores de sites para atender a agentes ativados na nuvem.	Os agentes ativados na nuvem que estiverem atrás do gateway da Internet usarão sites da Internet para determinar os serviços de site. No Console de gerenciamento Symantec, adicione seus servidores de sites a um Site padrão predefinido ou a outras páginas da internet que você quiser usar. Você deve também atribuir os computadores ativador na nuvem aos sites que baseados nos destinos dos recursos. Esta atribuição manual garante que cada computador permaneça um membro do site apropriado, independentemente de sua localização física. Consulte “Para configurar sites e servidores de sites para atender agentes habilitados para nuvem” na página 304.
Etapa 6	Certifique-se de que o site da internet esteja configurado corretamente.	Na página do site da Internet, certifique-se de que os serviços de site necessários estejam configurados corretamente e de que as configurações se apliquem aos destinos de recursos apropriados. Você pode acessar a página do site da Internet no Console de gerenciamento Symantec, na página Configurações do servidor de sites, em Gerenciamento de site > Sites.

Para configurar o Notification Server para usar o HTTPS

Se durante a instalação do IT Management Suite você não configura seu Notification Server para usar o HTTPS, deverá configurá-lo manualmente.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para configurar o Notification Server para usar o HTTPS

1 No computador do Notification Server, inicie o gerenciador de Serviços de Informações da Internet (IIS, Internet Information Services).

2 Edite as **propriedades do site do Altiris**.

Siga o procedimento que corresponde ao sistema operacional do computador do Notification Server:

Windows 2003	1 Na janela Propriedades do Altiris, na guia Segurança do diretório, em Comunicações seguras, clique em Editar. 2 Na janela Comunicações seguras, selecione Exigir canal seguro (SSL) e clique em OK.
Windows 2008	1 No painel central, em IIS, clique em Configurações do SSL. 2 Selecione Exigir SSL. 3 No painel Ações, clique em Aplicar.

3 Se o Notification Server não iniciar as bases de código de publicação do HTTPS, faça o seguinte:

- Reinicie o IIS no Notification Server.
- Reinicie o serviço do Altiris no Notification Server.
- No Notification Server, execute o agendamento de atualização de pacotes nas tarefas agendadas do Windows.

Para concluir esta etapa, você também deve realizar o seguinte:

Consulte [“Para aplicar uma autoridade de certificação raiz a um computador gerenciado”](#) na página 292.

Consulte [“Para redirecionar o Symantec Management Agent para usar HTTPS”](#) na página 295.

Para aplicar uma autoridade de certificação raiz a um computador gerenciado

Para migrar um computador gerenciado para o gerenciamento habilitado para nuvem, certifique-se de que o agente possa se comunicar com o Notification Server e com os servidores de sites usando HTTPS. Para usar o HTTPS para comunicação, o agente deverá confiar no Notification Server e nos servidores de sites. Caso necessário, será possível adicionar os certificados da autoridade de certificação raiz apropriada (CA) ao armazenamento **Autoridades de certificação raiz confiáveis** da conta de **Computador local** no computador gerenciado.

Você pode exportar o certificado autoassinado apropriado do Notification Server. Se o Notification Server não usar um certificado autoassinado, você precisará exportar a CA raiz para a cadeia de certificados que o Notification Server usa.

Para aplicar o certificado da CA exportado a um computador-cliente, você pode usar uma linha de comando ou o Console de Gerenciamento Microsoft. Como alternativa, você pode usar a política de grupo do Active Directory para instalar o certificado ou para reinstalar o Symantec Management Agent com a entrega automática de certificado ativada.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para concluir esta etapa, você também deve realizar o seguinte:

Consulte [“Para configurar o Notification Server para usar o HTTPS”](#) na página 290.

Consulte [“Para redirecionar o Symantec Management Agent para usar HTTPS”](#) na página 295.

Para exportar um certificado raiz da CA do Notification Server

- 1 No computador do Notification Server, inicie o Console de Gerenciamento Microsoft.
- 2 Adicione o snap-in **Certificados** de **Conta de computador > Computador local** e navegue até **Raiz do console > Certificados (computador local) > Autoridades de certificação raiz confiáveis > Certificados**.

- 3 Clique com o botão direito do mouse na autoridade de certificação que deseja exportar:

SMP <NS_Name> Agent CA	Esta autoridade de certificação emite certificados do agente. Os Symantec Management Agents usam esses certificados quando se comunicam com o Notification Server e com os servidores de sites através de um gateway da Internet. O gateway da Internet deve ter esta CA instalada para confiar nos clientes de conexão.
SMP <NS_Name> Server CA	Esta autoridade de certificação emite certificados de servidor. Servidores de sites usam estes certificados para se autenticarem. Quando os Symantec Management Agents contatam o servidor de sites, eles verificam o certificado de servidor.

- 4 Clique em **Todas as tarefas > Exportar**.
- 5 No Assistente de Exportação de certificados, especifique as seguintes configurações:
 - Selecione **Não, não exportar a chave privada**.
 - Selecione **X.509 binário codificado por DER (*.cer)**.
 - Especifique o caminho e o nome do arquivo do certificado exportado.
- 6 Clique em **Concluir** e feche a janela pop-up de confirmação da exportação.

Você pode, em seguida, levar o arquivo a um computador gerenciado e aplicar o certificado manualmente. Como alternativa, você pode distribuir o certificado aos computadores gerenciados usando uma tarefa de entrega de pacotes ou uma política de grupo do Active Directory.

Para aplicar manualmente uma certificado raiz da CA a um computador gerenciado usando uma linha de comando

- 1 No computador gerenciado apropriado, coloque o arquivo do certificado na pasta de instalação do Symantec Management Agent.

A pasta padrão é *C:\Arquivos de programas\Altiris\Altiris Agent*.
- 2 Abra uma janela de prompt de comando e digite a linha de comando a seguir:

```
[Pasta de instalação do agente]\AeXNSAgent.exe  
/rootca=certificateFile.cer
```

Este comando insere o certificado especificado no armazenamento de certificados de Autoridades de certificação raiz confiáveis.

Por exemplo:

```
C:\Arquivos de programas\Altiris\Altiris Agent\AeXNSAgent.exe  
/rootca=myClientCert.cer
```

Para aplicar manualmente um certificado raiz da CA a um computador gerenciado usando o Console de Gerenciamento Microsoft

- 1 Coloque o arquivo do certificado em um local acessível pelo computador gerenciado.
- 2 No computador gerenciado, inicie o Console de Gerenciamento Microsoft.
- 3 Adicione o snap-in **Certificados** para a conta do **Computador local** e abra a pasta **Raiz do console > Certificados (computador local)**.
- 4 Clique com o botão direito do mouse em **Autoridades de certificação raiz confiáveis** e selecione, em seguida, **Todas as tarefas > Importar**.
- 5 Em **Assistente de Importação de Certificado**, especifique o caminho e o nome de arquivo do certificado que deseja importar.
- 6 Clique em **Avançar** para aceitar o local padrão e outras configurações e clique em **Concluir**.

Para aplicar um certificado raiz da CA aos computadores gerenciados reinstalando o Symantec Management Agent

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Agentes/Plug-ins > Symantec Management Agent > Configurações** e clique em **Instalação do Symantec Management Agent**.
- 3 Na página **Instalação do Symantec Management Agent**, na guia **Instalar agente**, em **Instalar agente nos computadores**, clique em **Configurações**.

- 4 Na caixa de diálogo **Opções de instalação do Symantec Management Agent**, selecione **Instalar certificado do servidor no computador cliente** e clique em **OK**.
- 5 Na página **Instalação do Symantec Management Agent**, na guia **Instalar agente**, em **Instalar agente nos computadores**, selecione os computadores nos quais instalar o Symantec Management Agent e clique em **Instalar**.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Para redirecionar o Symantec Management Agent para usar HTTPS

Para colocar o Symantec Management Agent sob o gerenciamento habilitado para nuvem, você precisa garantir que o agente use HTTPS para se comunicar com o Notification Server. Você pode redirecionar o agente para usar HTTPS usando a política de **Configurações direcionadas do agente**.

A Symantec recomenda criar uma política direcionada personalizada para clientes habilitados para nuvem e excluir estes clientes de outras políticas direcionadas.

Consulte [“Para definir as configurações do agente de destino”](#) na página 278.

Aviso: Você precisa garantir que o agente confie no certificado SSL do servidor usado pelo Notification Server para comunicações HTTPS. Para aplicar o certificado apropriado a um computador-cliente, você pode usar uma linha de comando ou o Console de Gerenciamento Microsoft. Como alternativa, você pode reinstalar o Symantec Management Agent com a entrega automática de certificado ativada.

Consulte [“Para aplicar uma autoridade de certificação raiz a um computador gerenciado”](#) na página 292.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para concluir esta etapa, você também deve realizar o seguinte:

Consulte [“Para configurar o Notification Server para usar o HTTPS”](#) na página 290.

Consulte [“Para aplicar uma autoridade de certificação raiz a um computador gerenciado”](#) na página 292.

Para redirecionar um Symantec Management Agent para usar HTTPS

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Agentes/Plug-ins > Configurações direcionadas do agente**.
- 2 No painel esquerdo, selecione a política que se aplica aos computadores que você deseja colocar sob o gerenciamento habilitado para nuvem.
- 3 No painel direito, na guia **Avançado**, em **URL alternativo para acessar o NS**, marque a caixa de seleção.
- 4 Especifique o URL HTTPS apropriado para o Symantec Management Agent usar para acessar o Notification Server:

Nome do servidor O nome do computador do Notification Server.

Web do servidor O endereço da Web do Notification Server. O endereço deve estar no seguinte formato:

`https://NS_FQDN[:port]/Altiris/`

- 5 Clique em **Salvar alterações**.

Quando a política for atualizada no computador gerenciado, ela redirecionará o agente para usar HTTPS para comunicar-se com o Notification Server.

A próxima etapa é preparar seus computadores do servidor de sites.

Consulte [“Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem”](#) na página 296.

Para obter um processo completo e detalhado sobre como preparar seu ambiente para o gerenciamento habilitado para nuvem, consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem

Para poder realizar esta etapa, certifique-se de ter configurado seu Notification Server e os Symantec Management Agents para usar HTTPS.

Consulte [“Para configurar o Notification Server para usar o HTTPS”](#) na página 290.

Consulte [“Para redirecionar o Symantec Management Agent para usar HTTPS”](#) na página 295.

O gerenciamento habilitado para nuvem não atribui certificados de servidor aos servidores de sites. Você precisa aplicar certificados de servidor aos servidores de sites para que eles fiquem acessíveis usando HTTPS. Um certificado de servidor é um pré-requisito para que qualquer servidor de sites atenda aos Symantec

Management Agents na Internet. Por razões de segurança, a Symantec recomenda usar os certificados autoassinados.

Você deve usar sua própria autoridade de certificação da empresa (CA) para criar os certificados de servidor de que você precisa para configurar o HTTPS em seus servidores de sites. Porém, se você não tiver sua própria autoridade de certificação da empresa, o Symantec Management Platform fornecerá uma ferramenta de linha de comando que permitirá gerar certificados de servidor.

A ferramenta de geração de certificados de servidor de sites, `AeXGenSiteServerCert.exe`, permite criar o certificado de servidor de que você precisa. Uma autoridade de certificação especial do servidor no Notification Server emite o certificado do servidor. A parte pública do certificado é armazenada no banco de dados de gerenciamento de configuração (CMDB). Ambas as partes, pública e privada, são adicionadas a um arquivo PKCS#12 (PFX) que contém toda a cadeia de certificados.

Nota: A ferramenta `AeXGenSiteServerCert.exe` suporta apenas IIS.

Após gerar o arquivo do certificado de servidor, você precisará instalar o certificado no servidor de sites apropriado. O procedimento de instalação dependerá se o certificado de servidor for protegido por senha ou não. Também dependerá do sistema operacional do computador do servidor local.

Note que os computadores do servidor de tarefas devem ter os recursos IIS 6.0 ou IIS 7.0 e .NET Framework 3.5 ativados.

Nota: Aplicar um certificado de servidor regenerado a um gateway da Internet afeta os Symantec Management Agents existentes. Os agentes existentes não poderão se conectar ao gateway da Internet até que recebam detalhes atualizados da impressão digital do certificado do gateway. Se nenhum gateway da Internet alternativo estiver disponível, os Symantec Management Agents poderão ser incapazes de se conectar à rede interna. Você precisaria atualizar manualmente a configuração do agente.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para gerar um certificado de servidor para um servidor de sites

- 1 No computador do Notification Server, abra uma janela do prompt de comando e acesse o seguinte diretório:

```
C:\Arquivos de programas\Altiris\Notification Server\bin\Tools
```

- 2 Digite a seguinte linha de comando com os parâmetros apropriados:

```
AeXGenSiteServerCert.exe <SiteServerFQDN> [-o  
CertificateChain.pfx] [-p senha]
```

SiteServerFQDN

O nome usado pelo Symantec Management Agent para se conectar ao servidor de sites.

Este nome é tipicamente o nome de domínio totalmente qualificado (FQDN) do computador do servidor de sites. Por exemplo, seu servidor de sites pode ser nomeado **myhost.mydomain.com**.

O nome no certificado deve corresponder ao nome usado pelo agente para se conectar ao servidor de sites. Se o nome ou o endereço não corresponder, o agente não poderá se conectar ao servidor de sites.

CertificateChain.pfx

O nome do arquivo PFX que você deseja gerar.

Se você omitir este parâmetro, o nome de arquivo gerado do certificado será o nome comum especificado com a extensão .pfx aplicada a ele (**NomeComum.pfx**).

senha

A senha que deseja usar.

Se você omitir este parâmetro, a senha ficará vazia. Nenhuma senha padrão é fornecida.

O Gerenciador do IIS espera que um arquivo PFX seja protegido por senha quando você o importar. Se seu arquivo PFX não tiver senha, você precisará primeiro importar o arquivo no computador servidor local que usa o Console de Gerenciamento Microsoft (MMC). Você poderá em seguida usar o Gerenciador do IIS para aplicar o certificado optando por atribuir um certificado existente.

O arquivo do certificado de servidor será criado no mesmo diretório onde você executar o comando.

Para aplicar um certificado de servidor a um servidor de sites do Windows Vista/7/2008

- 1 Coloque o arquivo PFX do certificado de servidor no computador do servidor de sites ou em um local acessível.
- 2 No computador do servidor de sites, inicie o Gerenciador dos serviços de informações da Internet (IIS) e, no painel esquerdo, clique em **Nome do computador**.
- 3 No painel central, clique duas vezes em **Certificados de servidor** e depois, no painel **Ações**, clique em **Importar**.
- 4 Na caixa de diálogo **Importar certificado**, especifique o caminho e o arquivo do certificado que você quer importar, digite a senha, se tiver criado o certificado com uma senha, e clique em **OK**.
- 5 No Gerenciador dos serviços de informações da Internet (IIS), no painel esquerdo, em **Nome do computador > Sites**, clique em **Site padrão**.
- 6 No painel **Ações**, clique em **Ligações**.
- 7 Na lista de ligações, execute um destes procedimentos:

Crie uma nova ligação Clique em **Adicionar** e defina o tipo para **HTTPS**.

Edite uma ligação de HTTPS existente Selecione a ligação e clique em **Editar**.

- 8 Na caixa de diálogo **Adicionar ligação do site** ou **Editar ligação do site**, especifique o número da porta para usar, as interfaces de rede para escutar e o certificado SSL que você quer usar, e clique em **OK**.

Espera-se que o certificado esteja no armazenamento Pessoal da conta do computador local.

- 9 No computador do servidor de sites, reinicie o **IIS** e os **Altiris Object Host Services**.

Para aplicar um certificado de servidor protegido por senha a um servidor de sites do Windows 2003

- 1 Coloque o arquivo PFX do certificado de servidor no computador do servidor de sites ou em um local acessível.
- 2 No computador do servidor de sites, inicie o Gerenciador do IIS e, no painel esquerdo, em **Nome do computador > Sites**, clique com o botão direito do mouse em **Site padrão** e clique em **Propriedades**.
- 3 Na janela **Propriedades de site padrão**, na guia **Segurança do diretório**, clique em **Certificado do servidor**.

- 4 No **Assistente de Certificado do IIS**, faça o seguinte:
 - Na página **Certificado do servidor**, clique em **Importar um certificado de um arquivo .pfx** e em **Avançar**.
 - Na página **Importar certificado**, especifique o caminho e o nome do arquivo de certificado e clique em **Avançar**.
 - Na página **Importar senha do certificado**, digite a senha do certificado que você quer importar.
 - Na página **Porta SSL**, especifique o número da porta para usar e clique em **Avançar**.
 - Na página **Resumo do certificado importado**, verifique os dados do certificado e clique em **Avançar**.
 - Clique em **Concluir**.
- 5 Clique em **OK** para fechar a janela **Propriedades do site padrão**.
- 6 No computador do servidor de sites, reinicie o **IIS** e os **Altiris Object Host Services**.

Para aplicar um certificado de servidor que não tenha a senha para um servidor de sites do Windows 2003

- 1 No computador do servidor de sites, inicie o Console de Gerenciamento Microsoft.
- 2 Adicione o snap-in **Certificados** à conta do **Computador local** e abra a pasta **Raiz do console > Certificados > Pessoal**.
- 3 Clique com o botão direito do mouse em **Certificados** e depois clique em **Todas as tarefas > Importar**.
- 4 Em **Assistente de Importação de Certificado**, especifique o arquivo do certificado de servidor que deseja importar.
- 5 Clique em **Avançar** para aceitar as configurações padrão de todas as páginas restantes em **Assistente de Importação de Certificado** e, em seguida, clique em **Concluir**.

O certificado é adicionado ao armazenamento de certificados Pessoal.
- 6 Inicie o Gerenciador dos serviços de informações da Internet (IIS) e, no painel esquerdo, em **Nome do computador > Sites**, clique com o botão direito do mouse em **Site padrão** e clique em **Propriedades**.
- 7 Na janela **Propriedades de site padrão**, na guia **Segurança do diretório**, clique em **Certificado do servidor**.

- 8 No **Assistente de certificado de servidor Web**, na página **Certificado do servidor**, clique em **Atribuir um certificado existente** e em **Avançar**.
- 9 Selecione o certificado que você importou e clique em **Avançar** para aceitar as configurações padrão de todas as páginas restantes.
- 10 Clique em **Concluir** e em **OK** para fechar a janela **Propriedades do site padrão**.

Para aplicar um certificado de servidor a um servidor de sites do Windows XP

- 1 Coloque o arquivo PFX do certificado de servidor no computador do servidor de sites ou em um local acessível.
- 2 No computador do servidor de sites, inicie o Console de Gerenciamento Microsoft.
- 3 Adicione o snap-in **Certificados** à conta do **Computador local** e abra a pasta **Raiz do console > Certificados > Pessoal**.
- 4 Clique com o botão direito do mouse em **Certificados** e depois clique em **Todas as tarefas > Importar**.
- 5 No **Assistente de Importação de Certificado**, especifique o nome e o caminho do arquivo de certificado que você quer importar, digite a senha, especifique o armazenamento de certificados, verifique as configurações, e clique em **Concluir**.
- 6 No Gerenciador dos serviços de informações da Internet (IIS), em **Nome do computador > Sites**, clique com o botão direito do mouse em **Site padrão** e clique em **Propriedades**.

Note que você deve ter os recursos IIS 6.0 ou IIS 7.0 e .NET Framework 3.5 ativados.
- 7 Na janela **Propriedades de site padrão**, na guia **Segurança do diretório**, clique em **Certificado do servidor**.
- 8 No **Assistente de Certificado do IIS**, faça o seguinte:
 - Na página **Certificado do servidor**, clique em **Atribuir um certificado existente** e clique em **Avançar**.
 - Na página **Certificados disponíveis**, clique no arquivo de certificado e em **Avançar**.
 - Na página **Porta SSL**, especifique o número da porta para usar e clique em **Avançar**.
 - Na página **Resumo do certificado**, verifique os dados do certificado e clique em **Avançar**.
 - Clique em **Concluir**.

9 Clique em **OK** para fechar a janela **Propriedades do site padrão**.

10 No computador do servidor de sites, reinicie o **IIS** e os **Altiris Object Host Services**.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

A próxima etapa é instalar serviços de site.

Consulte [“Para gerenciar servidores de sites”](#) na página 131.

Para obter um processo completo e detalhado sobre como preparar seu ambiente para o gerenciamento habilitado para nuvem, consulte [Consulte “Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS

Para poder realizar esta tarefa, certifique-se de ter instalado os serviços de site.

Consulte [“Para gerenciar servidores de sites”](#) na página 131.

Você pode configurar o HTTPS em seus servidores de pacotes usando a página **Configurações do serviço de pacotes**. Esta página especifica as configurações globais do serviço do pacote que serão aplicadas a todos os servidores de pacotes que servem o Symantec Management Platform.

Cada computador de servidor de pacotes deve ter seu IIS configurado para aceitar conexões HTTPS. Você pode usar sua autoridade de certificação interna da empresa para fornecer os certificados apropriados. Se você não tiver uma autoridade de certificação interna da empresa, será possível usar uma ferramenta de linha de comando do Notification Server para gerar os certificados necessários para a configuração do HTTPS.

Consulte [“Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem”](#) na página 296.

Você precisa assegurar-se de que seus servidores de pacotes habilitados para nuvem possam servir como a fonte do download para os pacotes. Os agentes e os servidores de pacotes habilitados para nuvem têm permissão apenas para fazer o download de pacotes usando HTTPS através do gateway da Internet. Para permitir que servidores de pacotes desconectados façam download de pacotes, o Notification Server e os servidores de pacotes no mesmo site devem publicar bases de código do pacote de HTTPS. Esta configuração é necessária porque quando um servidor de pacotes não tem fontes do pacote disponíveis dentro de seu próprio site, ele deve solicitá-las de outro lugar. O servidor de pacotes tenta primeiro obter pacotes dos servidores de pacotes que estão localizados no mesmo site que o Notification

Server. Se nenhum servidor de pacotes estiver disponível, ele tentará obter pacotes do próprio Notification Server.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS

- 1 Para configurar o HTTPS globalmente em todos os servidores de pacotes, faça o seguinte:
 - No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
 - No painel esquerdo, expanda **Gerenciamento de site > Configurações > Serviço de pacote** e clique em **Configurações do serviço de pacotes**.
 - Na página **Configurações do serviço de pacotes**, em **Configurações globais do serviço de pacotes**, clique em **Publicar a base de código HTTPS**.
 - Clique em **Salvar alterações**.
- 2 Para configurar um servidor de pacotes individual para usar HTTPS, crie as seguintes chaves do registro e valores em cada computador do servidor de pacotes localizado no mesmo site que o Notification Server:
 - **Local do registro:** HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Package Server
 - **Tipo de chave:** DWORD
 - **Nome** EnableHTTPOverride
 - **Valor:** 1

Esta chave do registro sobrepõe a configuração da base de código HTTP no servidor de pacotes e faz com que ela publique bases de código HTTPS.

A etapa seguinte é configurar sites e servidores de sites para servir agentes habilitados para nuvem.

Consulte [“Para configurar sites e servidores de sites para atender agentes habilitados para nuvem”](#) na página 304.

Para obter um processo completo e detalhado sobre como preparar seu ambiente para o gerenciamento habilitado para nuvem, consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para configurar sites e servidores de sites para atender agentes habilitados para nuvem

Para poder realizar esta etapa, certifique-se de que você tenha configurado servidores de pacotes para que publiquem bases de códigos HTTPS.

Consulte [“Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS”](#) na página 302.

Os computadores que você deseja gerenciar pela Internet devem ser organizados em um ou mais sites. Estes sites devem ser dedicados aos agentes habilitados para nuvem e não devem conter agentes gerenciados diretamente. Você deve atribuir os servidores de sites apropriados a cada site.

O gerenciamento habilitado para nuvem dá suporte aos servidores de pacotes da Internet e aos servidores de tarefas da Internet, os quais o Symantec Management Agent acessa através de um gateway da Internet. O gerenciamento habilitado para nuvem suporta também servidores de pacotes desconectados, que são servidores de pacotes localizados no mesmo site que os agentes habilitados para nuvem. Apenas os agentes locais podem acessar um servidor de pacotes desconectado e usam uma conexão direta. Porém, os servidores de tarefas desconectados não são suportados.

Os computadores habilitados para nuvem devem ser atribuídos manualmente aos sites que estão baseados nos destinos de recursos. Os agentes habilitados para nuvem não reconhecem as atribuições do site com base em endereços IP e sub-redes. A atribuição manual garante que cada computador permaneça membro do site apropriado, independentemente da localização física do computador.

Consulte [“Para gerenciar sites”](#) na página 129.

Você pode atribuir manualmente um agente habilitado para nuvem a vários sites ou servidores de sites. Os servidores de sites que estão disponíveis para o agente são uma união de todos os servidores de sites nos sites atribuídos.

Você pode definir as configurações do servidor de sites para agentes habilitados para nuvem das seguintes maneiras:

Crie e configure um site.

Você pode criar e configurar tantos sites quantos forem necessários para satisfazer sua configuração do ambiente. Um servidor de pacotes ou agente habilitado para nuvem atribuído a vários sites recebe a união de todos os servidores de sites nos sites atribuídos.

Atribua os agentes habilitados para nuvem diretamente aos servidores de sites.	Você atribui um destino de recursos diretamente ao servidor de sites para garantir que os membros de destino tenham acesso apenas a esse servidor de sites específico. A atribuição pelo método do site disponibiliza todos os servidores de sites que são membros do site atribuído aos agentes de destino habilitados para nuvem.

Nota: Caso necessário, é possível usar estes dois métodos de atribuição em conjunto.

Esta tarefa é uma etapa do processo de preparação de seu ambiente para o gerenciamento habilitado para nuvem.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para criar e configurar um site da Internet para servir aos agentes habilitados para nuvem

- 1 No Console de gerenciamento Symantec, crie um site novo.
Consulte [“Para gerenciar sites”](#) na página 129.
- 2 Atribua manualmente o destino de recursos apropriado ao site.
Este destino de recursos contém os agentes e os servidores de pacotes habilitados para nuvem. Você pode reutilizar o mesmo destino de recursos que é aplicado à política de **Configurações do gerenciamento habilitado para nuvem**
- 3 Atribua os servidores de sites apropriados ao site de uma das seguintes maneiras:

Para atribuir manualmente o servidor de sites ao site	1 No Console de gerenciamento Symantec, no menu Configurações, clique em Notification Server > Configurações do servidor de sites. 2 No painel esquerdo, expanda Gerenciamento de site > Servidores de sites > nome_do_servidor_de_sites e clique em Sites. 3 No painel direito, em Informações detalhadas, clique em Novo(a). 4 Na caixa de diálogo Selecionar um site, clique no site da Internet ao qual você quer atribuir o servidor de sites, e clique em OK.

Para atribuir as sub-redes dos servidores de sites local ao site

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 No painel esquerdo, clique em **Gerenciamento de site > Sub-redes**.
- 3 No painel direito, selecione a sub-rede apropriada.
- 4 Na barra de ferramentas, clique em **Atribuir ao site**.
- 5 Na janela **Selecione um site**, escolha o site ao qual você deseja atribuir o servidor de sites.

Nota: Um servidor de sites local é aquele que existe no mesmo site desconectado que os agentes habilitados para nuvem aos quais ele serve.

Este tipo de atribuição exige que o site desconectado tenha uma sub-rede exclusiva que não coincida com as sub-redes de clientes internos, se houver. Esta configuração não é comum; portanto, esta abordagem geralmente não é recomendada.

Consulte [“Para atribuir um servidor de sites a um site manualmente”](#) na página 133.

Para atribuir diretamente agentes habilitados para nuvem a um servidor de sites

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Configurações do servidor de sites**.
- 2 No painel esquerdo, expanda o site ou o servidor de sites que você deseja modificar e clique em **Agentes atribuídos manualmente**.
- 3 No painel direito, clique em **Novo(a)**, especifique o destino de recursos que contém os agentes habilitados para nuvem apropriados, e clique em **OK**.

Consulte [“Seleção de destinos de recurso nomeados”](#) na página 386.

A próxima etapa é certificar-se de que o site da Internet tenha sido configurado adequadamente.

Para obter um processo completo e detalhado sobre como preparar seu ambiente para o gerenciamento habilitado para nuvem, consulte Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Para configurar o gerenciamento habilitado para nuvem

Este capítulo contém os tópicos a seguir:

- [Para configurar o gerenciamento habilitado para nuvem](#)

Para configurar o gerenciamento habilitado para nuvem

Para que você possa aproveitar da funcionalidade que o gerenciamento habilitado para nuvem oferece, instale e configure os gateways da Internet. Em seguida, você deve configurar as políticas de gerenciamento habilitado para nuvem e também configurar os Symantec Management Agents para suportar o ambiente do gerenciamento habilitado para nuvem.

Para que você possa configurar o gerenciamento habilitado para nuvem, configure seu ambiente para usar o SSL.

Consulte [“Para preparar o ambiente para o gerenciamento habilitado para nuvem”](#) na página 287.

Tabela 20-1 Processo para configurar o gerenciamento habilitado para nuvem

Etapa	Ação	Descrição
Etapa 1	Certifique-se de que as configurações do pool de aplicativos estejam corretas.	O Gerenciamento habilitado para nuvem exige que o DefaultAppPool do computador do Notification Server use a configuração Integrado no Modo gerenciado de canal. Para poder continuar com a configuração do Gerenciamento habilitado para nuvem, certifique-se de que a configuração Integrado tenha sido usada. Consulte “Para configurar o DefaultAppPool para suar o Modo integrado de canal gerenciado” na página 310.
Etapa 2	Definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem .	Um site separado do agente no Notification Server é exigido para agentes habilitados para nuvem. Este site contém somente interfaces do agente e não fornece acesso a páginas do Console de gerenciamento Symantec. Também executa o certificado adicional e verificações de acesso do recurso para aplicar medidas de segurança para os agentes que se conectam através da Internet. Você deve configurar o gateway da Internet para permitir o acesso somente ao site do agente no Notification Server. Consulte “Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.” na página 311.

Etapa	Ação	Descrição
Etapa 3	Preparar o computador gateway da Internet.	O computador gateway da Internet deve estar localizado na zona desmilitarizada (DMZ, demilitarized zone) de sua organização para garantir que esteja protegido das redes externas e internas. Você precisa configurar o firewall no computador gateway para permitir conexões de entrada da Internet apenas para a porta apropriada do gateway. Você precisa também configurar o firewall para permitir as conexões de saída apenas para servidores específicos em sua rede interna. Se o gateway for executado em uma máquina virtual VMware, você deverá usar o adaptador de rede VMXNET 3. Note que VMXNET 3 estará disponível somente quando você tiver o VMware Tools instalado em sua máquina virtual. Para obter mais informações sobre o adaptador de rede VMXNET 3, consulte o artigo da base de conhecimento da VMware: KB1001805 (em inglês). O computador deve ter o sistema operacional Windows Server 2008 R2 SP1 com o recurso .NET Framework 3.5.1 ativado. O Symantec Management Platform não precisa gerenciar o computador gateway. O gateway da Internet é normalmente não gerenciado. Para poder iniciar a instalação, é necessário verificar se o computador gateway pode acessar o computador do Notification Server e todos os servidores locais necessários. Quando você verificar a conexão, use os nomes do host ou os endereços IP aos quais os agentes gerenciados pela Internet tentam se conectar. Consulte “Sobre a preparação do computador gateway da Internet” na página 313.
Etapa 4	Fazer o download e executar o pacote de instalação de gateway da Internet.	Para instalar o gateway da Internet, você precisa fazer o download e executar o pacote de instalação de gateway da Internet do Console de gerenciamento Symantec. Consulte “Download e execução do pacote de instalação de gateway da Internet” na página 315.

Etapa	Ação	Descrição
Etapa 5	Configure o gateway da Internet usando o Assistente de Configuração do gateway da Internet do Symantec Management Platform e o Gerente do gateway da Internet do Symantec Management Platform .	No assistente de Configuração do gateway da Internet do Symantec Management Platform, você especifica a porta para conexões de entrada, as informações do certificado SSL e a conta do usuário. Em Gerente do gateway da Internet do Symantec Management Platform, você adiciona seu Notification Server e seus servidores de sites à lista de servidores que podem se comunicar com o gateway da Internet. Você também precisa copiar a Impressão digital do certificado do Gateway necessária para configurar a política de Ajustes do gerenciamento habilitado para nuvem. Consulte “Para configurar o gateway da Internet” na página 317.
Etapa 6	Configurar a política de Configurações do gerenciamento habilitado para nuvem .	A política de Configurações do gerenciamento habilitado para nuvem permite direcionar os computadores que você deseja gerenciar pela Internet. A política também contém a lista de gateways da Internet que estão disponíveis para uso pelos computadores-cliente de destino. Consulte “Para configurar a política de Configurações do gerenciamento habilitado para nuvem” na página 320. Para colocar os Symantec Management Agents existentes no gerenciamento habilitado para nuvem, certifique-se de adicionar estes computadores à política de Configurações do gerenciamento habilitado para nuvem.
Etapa 7	Instalar o Symantec Management Agent em computadores desligados.	Em alguns casos, um computador que você deseja gerenciar pode não ter acesso à rede que hospeda o Symantec Management Platform. Para instalar o Console de gerenciamento Symantec em um computador desligado, você deve fazer o download do pacote de instalação do agente de seu Console de gerenciamento Symantec, salvá-lo em uma mídia apropriada e então instalá-lo nos computadores apropriados. Consulte “Para instalar o Symantec Management Agent em um computador desconectado” na página 324.

Para configurar o DefaultAppPool para suar o Modo integrado de canal gerenciado

O Gerenciamento habilitado para nuvem exige que o **DefaultAppPool** do computador do Notification Server use a configuração **Integrado** no **Modo gerenciado de canal**.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para definir o DefaultAppPool para usar o Modo integrado de canal gerenciado

- 1 No computador do Notification Server, abra o **Gerenciador dos Serviços de Informações da Internet (IIS)**.
- 2 No **Gerenciador dos Serviços de Informações da Internet (IIS)**, no painel **Conexões**, clique em **(nome do computador do Notification Server) > Pools de aplicativos**.
- 3 No painel **Pools de aplicativos**, clique em **DefaultAppPool**, e, no painel **Ações**, clique em **Configurações básicas**.
- 4 Na janela **Editar pool de aplicativos**, em **Modo de canal gerenciado**, selecione **Integrado**. Clique em **OK**.

A próxima etapa é configurar a política de **Configurações do site do IIS do agente de gerenciamento habilitado para nuvem**.

Consulte [“Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.”](#) na página 311.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.

Para poder realizar esta tarefa, certifique-se de ter definido o **DefaultAppPool** para usar o **Modo integrado de canal gerenciado**.

Consulte [“Para configurar o DefaultAppPool para usar o Modo integrado de canal gerenciado”](#) na página 310.

Um site separado do agente no Notification Server é exigido para agentes habilitados para nuvem. Este site contém somente interfaces do agente e não fornece acesso a páginas do Console de gerenciamento Symantec. Também executa o certificado adicional e verificações de acesso do recurso para aplicar medidas de segurança para os agentes que se conectam através da Internet.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Gerenciamento habilitado para nuvem**.
- 2 No painel esquerdo, expanda **Configuração** e clique em **Configurações do site do IIS do agente de gerenciamento habilitado para nuvem**.
- 3 Na página **Configurações do site do IIS do agente de gerenciamento habilitado para nuvem**, selecione **Adicione o site do IIS para conexões do agente de gerenciamento habilitado para nuvem** e especifique as seguintes configurações:

Nome	Permite especificar o nome sob o qual o site é exibido no Gerenciador dos Serviços de Informações da Internet (IIS) .
Porta	Permite especificar a porta na qual o site estará disponível. Para configurar o Gerenciamento habilitado para nuvem, é necessário que a porta selecionada possa ser acessada pelo computador gateway da Internet.
FQDN	Permite ver o FQDN atual do computador do Notification Server.
Certificado	Permite criar um certificado SSL autoassinado ou importar um comercial.

- 4 Clique em **Salvar alterações**.

Nota: Uma tarefa de atualização de pacotes faz parte do processo de criação de sites. Em ambientes com grande quantidade destes, pode levar um tempo considerável. Você pode fechar com segurança o Console de gerenciamento da Symantec assim que as seguintes mensagens forem registradas em log:

```
Tarefa de criação de site de agente {Task_Guid} iniciada.

Iniciando atualização do pacote para todos os pacotes.
```

O site do IIS do agente de gerenciamento habilitado para nuvem exige uma conexão que seja protegida com um certificado SSL. Você pode importar um certificado comercial ou criar um certificado autoassinado. Para usar um certificado comercial, ele tem que cumprir os seguintes requisitos:

Tabela 20-2 Requisitos do Symantec Management Platform para certificados SSL

Assinatura digital	O certificado tem uma assinatura digital válida.
Confiança	O certificado é emitido pela autoridade de certificação que é confiada pelo computador do Notification Server.
Validade	O certificado é válido pelo menos por 30 dias da data da importação.
Uso aprimorado da chave	O valor do Uso aprimorado da chave do certificado é o OID da autenticação do servidor (1.3.6.1.5.5.7.3.1).
Nome do sujeito ou nome alternativo sujeito	O sujeito ou o nome alternativo do sujeito corresponde ao nome de domínio totalmente qualificado do computador do Notification Server.
Algoritmo de hashing	O certificado usa um dos seguintes algoritmos de hashing: ■ SHA1 ■ SHA256 ■ SHA384 ■ SHA512
Algoritmo assimétrico	O certificado usa o algoritmo assimétrico do RSA.
Formato de arquivo	.pfx

A próxima etapa é preparar o computador gateway da Internet.

Consulte [“Sobre a preparação do computador gateway da Internet”](#) na página 313.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Sobre a preparação do computador gateway da Internet

Para poder realizar a próxima tarefa, certifique-se de ter definido as configurações do site IIS do Agente de gerenciamento habilitado para nuvem.

Consulte [“Para definir as Configurações do site do IIS do agente de gerenciamento habilitado para nuvem.”](#) na página 311.

O gateway da Internet permite que os Symantec Management Agents na Internet comuniquem-se com o Symantec Management Platform. O gateway da Internet encaminha solicitações dos Symantec Management Agents autenticados para números de porta específicos em instâncias ou em servidores de sites do Notification

Server no gateway. Por padrão, todas as solicitações são encaminhadas da porta HTTPS 443 padrão no gateway para a porta 4726 no computador do Notification Server.

O gateway da Internet cria um túnel virtual no firewall interno. Ele permite que os clientes autorizados na Internet acessem os servidores internos apropriados, mas impede a entrada de todos os clientes não autorizados. O Symantec Management Agent habilitado para nuvem comunica-se com o gateway diretamente através da Internet. Não é necessária VPN. Quando um agente habilitado para nuvem é conectado, o gateway e o agente trocam e verificam os certificados de cada um. O gateway confirma se um Notification Server conhecido emitiu o certificado do agente. O gateway cria um túnel que o agente pode usar para se comunicar diretamente ao Notification Server e aos servidores de sites apropriados que usam HTTPS. Quando o agente encerrar a comunicação com o servidor de destino, fechará sua conexão com o gateway, e o gateway destruirá o túnel.

O recurso do gerenciamento habilitado para nuvem não suporta o uso de servidores proxy. Você não pode configurar um proxy entre o Symantec Management Agent habilitado para nuvem e o gateway da Internet.

A Symantec recomenda configurar pelo menos dois gateways da Internet para fornecer opções de failover, balanceamento de carga, e para manter a continuidade de uma comunicação. Cada gateway da Internet pode servir vários Notification Servers. Esta configuração será suportada mesmo se os servidores de notificação forem organizados em uma estrutura de hierarquia. Cada gateway da Internet suporta de 1 a 60.000 endpoints e 3.000 conexões simultâneas.

Os seguintes exemplos ajudam a decidir quantos gateways da Internet você precisa em seu ambiente:

- Quando você tiver 20.000 clientes em um Notification Server e 30% deles forem habilitado para nuvem, a melhor prática é ter dois gateways da Internet para assegurar a alta disponibilidade. Contudo, mesmo um gateway da Internet pode controlar facilmente esta configuração.
- Se você tiver 180.000 clientes divididos em duas hierarquias com 70% deles habilitados para nuvem, você precisará de pelo menos quatro gateways da Internet: três para controlar a carga do nó e um para a tolerância a falhas.

Antes de instalar o gateway da Internet, você precisa configurar o computador-host. O computador gateway deve estar localizado na zona desmilitarizada (DMZ) de sua organização para garantir que esteja protegido de redes externas e internas. Você precisa configurar o firewall no computador gateway da Internet para permitir conexões de entrada da Internet apenas às portas apropriadas do gateway. Você precisa também configurar o firewall para permitir as conexões de saída apenas para servidores específicos em sua rede interna.

Se o gateway for executado em uma máquina virtual VMware, você deverá usar o adaptador de rede VMXNET 3. Note que VMXNET 3 estará disponível somente quando você tiver o VMware Tools instalado em sua máquina virtual. Para obter mais informações sobre o adaptador de rede VMXNET 3, consulte o artigo da base de conhecimento da VMware: [KB1001805](#) (em inglês).

Nota: O computador gateway da Internet deve ter o sistema operacional Windows Server 2008 R2 SP1 com o recurso .NET Framework 3.5.1 ativado.

O Symantec Management Platform não precisa gerenciar o computador gateway. O gateway da Internet é normalmente não gerenciado.

Antes de começar a instalação, verifique se o computador gateway da Internet pode acessar o computador do Notification Server e todos os servidores locais exigidos. Quando você verificar a conexão, use os nomes do host ou os endereços IP aos quais os agentes habilitados para nuvem tentam se conectar.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Consulte [“Sobre o balanceamento de carga do gateway da Internet”](#) na página 521.

A próxima etapa é fazer o download do pacote de instalação do gateway da Internet.

Consulte [“Download e execução do pacote de instalação de gateway da Internet”](#) na página 315.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Download e execução do pacote de instalação de gateway da Internet

Para poder realizar esta tarefa, certifique-se de ter preparado o computador gateway da Internet.

Consulte [“Sobre a preparação do computador gateway da Internet”](#) na página 313.

Se quiser instalar um novo gateway da Internet, você precisará primeiro obter o pacote de instalação apropriado do gateway da Internet. O pacote de instalação é um arquivo EXE que você pode obter por download no Console de gerenciamento Symantec. O pacote contém um instalador que guia você no processo de instalação.

Se puder acessar o Console de gerenciamento Symantec remotamente no computador gateway, você poderá optar por executar diretamente o pacote de

instalação do gateway da Internet. Como alternativa, você pode salvar o arquivo em outra mídia, copiá-lo no computador gateway da Internet apropriado, e executá-lo.

Aviso: Saia de todos os programas Windows antes de executar o pacote de instalação de gateway da Internet.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para fazer o download e executar o pacote de instalação de gateway da Internet

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Gerenciamento habilitado para nuvem**.
- 2 No painel esquerdo, expanda **Configurar** e clique em **Configuração do gerenciamento habilitado para nuvem**.
- 3 Na página **Configuração do gerenciamento habilitado para nuvem**, na guia **Configuração do gateway da Internet**, clique em **Faça o download do pacote de instalação do gateway da Internet**.
- 4 Se você estiver no computador gateway, será possível clicar em **Executar** para executar imediatamente o instalador.

Se você quiser salvar o pacote como um arquivo para executá-lo mais tarde ou para executá-lo em um computador diferente, clique em **Salvar**, especifique a pasta apropriada, e clique em **OK**.
- 5 Navegue até o pacote de instalação de gateway da Internet do SMP obtido por download e clique duas vezes em `SMP_Internet_Gateway`.
- 6 Na caixa de diálogo **Abrir arquivo - Aviso de segurança**, clique em **Executar**.
- 7 Na caixa de diálogo **Configuração do gateway da Internet do Symantec Management Platform**, clique em **Avançar**.
- 8 Clique em **Aceito o contrato de licença** e em **Avançar**.
- 9 Especifique o caminho da pasta de destino onde você quer instalar os arquivos do gateway da Internet, clique em **Avançar** e em **Avançar**.
- 10 Certifique-se de que a opção **Iniciar o Assistente de Configuração** esteja selecionada e clique em **Concluir**.

A próxima etapa é configurar o gateway da Internet.

Consulte [“Para configurar o gateway da Internet”](#) na página 317.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para configurar o gateway da Internet

Para poder realizar esta tarefa, certifique-se de ter feito o download do pacote de instalação do gateway da Internet.

Consulte [“Download e execução do pacote de instalação de gateway da Internet”](#) na página 315.

Depois que o gateway da Internet é instalado com êxito, você deve configurá-lo para funcionar junto com o Symantec Management Platform. Você configura o gateway da Internet usando o assistente de **Configuração do gateway da Internet do Symantec Management Platform** e o **Gerente do gateway da Internet do Symantec Management Platform**.

No assistente de **Configuração do gateway da Internet do Symantec Management Platform**, você especifica a porta para conexões de entrada, as informações do certificado SSL e a conta do usuário.

Em **Gerente do gateway da Internet do Symantec Management Platform**, você adiciona seu Notification Server e seus servidores de sites à lista de servidores que podem se comunicar com o gateway da Internet. Você também obtém a **Impressão digital do certificado do Gateway** necessária para configurar a política de **Ajustes do gerenciamento habilitado para nuvem**.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para configurar o gateway da Internet usando o Assistente de Configuração do gateway da Internet do Symantec Management Platform

- 1 No computador do gateway da Internet, no Assistente de **Configuração do gateway da Internet do Symantec Management Platform**, na página **Portas e endereços IP**, especifique o endereço IP e as portas apropriados e clique em **Avançar**.

Por padrão, a porta para conexões de entrada é 443. Porém, é possível especificar um número de porta diferente, caso necessário. Todos os números de portas especificadas devem ser de portas do TCP (numeradas de 1 a 65535).

Você deve usar o endereço IP do computador gateway da Internet. Você pode especificar um número de porta apenas e somente um endereço IP. Se você escolher usar todos os endereços IP disponíveis, o mesmo número de portas será usado para todos os endereços IP. Se você exigir um controle mais granular dos endereços IP e dos números de porta, você precisará editar diretamente o arquivo de configuração Apache.

- 2 Na página **Informações do certificado SSL**, especifique as informações apropriadas do certificado e clique em **Avançar**.

O gateway da Internet deve ter um certificado SSL disponível de modo que os Symantec Management Agents possam se comunicar com ele. O Assistente de configuração gera um certificado SSL autoassinado com base nas informações que você fornece.

Se apropriado, você poderá usar seu próprio certificado em vez do certificado autoassinado gerado. Você precisa substituir manualmente o certificado e os arquivos chaves após a instalação.

Crie ou receba um certificado e uma chave privada de uma autoridade de certificação. Armazene o certificado e a chave nos arquivos

`%diretóriodeinstalação%\Apache\certs\server.crt` e

`%diretóriodeinstalação%\Apache\certs\server.key` respectivamente. O certificado e a chave devem ser armazenados em formatos diferentes de DES PEM e conter uma cadeia de certificação completa. Então reinicie o Apache (`httpd.exe`) ou use a interface do usuário para reiniciar o serviço.

- 3 Na página **Conta do usuário**, especifique as informações apropriadas da conta do usuário e clique em **Avançar**.

Por razões de segurança, você deve executar o serviço do gateway da Internet como uma conta do usuário dedicada. A Symantec recomenda usar uma conta de **Serviço local**.

- 4 Na página **Resumo**, verifique sua configuração, e clique em **Concluir**.

Para configurar o gateway da Internet no assistente de Gerenciador do gateway da Internet do Symantec Management Platform

- 1 Para abrir o **Gerenciador do gateway da Internet do Symantec Management Platform**, clique em **Iniciar > Programas > Symantec > Gerente do gateway da Internet**.

Note que depois que o assistente de **Configuração do gateway da Internet do Symantec Management Platform** for concluído, o **Gerenciador do gateway da Internet do Symantec Management Platform** será aberto automaticamente.

- 2 Para adicionar seus servidores de sites e servidores da notificação à lista de servidores que podem se comunicar com o gateway da Internet, faça o seguinte:

- Em **Gerente do gateway da Internet de Symantec Management Platform**, na guia **Servidores**, clique em **Adicionar servidor**.

- Na caixa de diálogo **Adicionar servidor**, adicione um **Nome do host** e edite o número da **Porta SSL** caso necessário. Se você adicionar o Notification Server, certifique-se de que a opção **Este é um servidor SMP** está selecionada. Clique em **OK**.

Note que a **Porta SSL** do computador do Notification Server deve ser a mesma que você especifica na página **Configurações de site do agente do CEM**, no Console de gerenciamento Symantec.

- Se a caixa de diálogo **Aviso de certificado** for exibida, clique em **Ignorar**.
- Na caixa de diálogo **Reiniciar o serviço?**, clique em **Sim**.

- 3 Para copiar a **Impressão digital do certificado do Gateway** que você precisa para a configuração da política de **Ajustes do gerenciamento habilitado para nuvem** no Console de gerenciamento Symantec, clique em **Copiar para a área de transferência** na aba **Geral** do **Gerenciador de gateway de Internet do Symantec Management Platform**.

Consulte "[Para configurar a política de Configurações do gerenciamento habilitado para nuvem](#)" na página 320.

Consulte "[Scripts de gerenciamento de gateway da Internet](#)" na página 520.

A próxima etapa é configurar a política de **Configurações do gerenciamento habilitado para nuvem**.

Consulte "[Para configurar a política de Configurações do gerenciamento habilitado para nuvem](#)" na página 320.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem” na página 307.](#)

Para configurar a política de Configurações do gerenciamento habilitado para nuvem

Para poder realizar esta tarefa, certifique-se de ter configurado o gateway da Internet.

Consulte [“Para configurar o gateway da Internet”](#) na página 317.

A política de **Configurações do gerenciamento habilitado para nuvem** permite direcionar os computadores que você deseja gerenciar pela Internet. A política contém a lista de gateways da Internet que estão disponíveis para uso pelos computadores-cliente de destino. Você pode especificar os gateways da Internet disponíveis digitando os detalhes apropriados de cada gateway.

Você configuraria normalmente somente uma política de **Configurações do gerenciamento habilitado para nuvem**. Você apenas precisará de várias políticas se quiser ter um controle mais detalhado sobre os gateways da Internet que servem computadores habilitados para nuvem específicos ou se quiser executar o balanceamento de carga manual.

Para gerar um pacote de instalação do agente, você precisa criar ou selecionar uma política de **Configurações do gerenciamento habilitado para nuvem** e aplicá-la aos computadores de destino apropriados. A lista dos gateways da Internet disponíveis para a política selecionada está incluída no pacote de instalação do agente. Esta lista permite que o agente instalado recentemente inicie a comunicação com o Notification Server imediatamente. O novo computador habilitado para nuvem é adicionado automaticamente ao destino de recursos da política selecionada.

Quando o Symantec Management Agent receber a política de **Configurações do gerenciamento habilitado para nuvem** e não estiver conectado diretamente ao Notification Server, ele tentará se conectar através do gateway da Internet. Quando o agente tiver se conectado com êxito, ele se tornará um agente habilitado para nuvem. O Symantec Management Agent alternará para o modo habilitado para nuvem apenas quando fizer uma conexão bem-sucedida através de um gateway.

Note que um computador habilitado para nuvem será revertido automaticamente para uma comunicação direta com o Notification Server local quando o acesso direto à rede estiver disponível. Ele também mudará automaticamente para o modo habilitado para nuvem quando a conexão direta não estiver mais disponível. Por exemplo, um laptop que normalmente é usado em locais remotos pode ser usado ocasionalmente no escritório e ser conectado à rede interna.

Embora a política de **Configurações do gerenciamento habilitado para nuvem** seja direcionada a um computador, o computador continuará comunicando-se através dos gateways da Internet apropriados. Se a rede interna estiver configurada corretamente, todo o tráfego entre o agente, o gateway da Internet e o Notification Server ficará na rede interna. No entanto, se a política de **Configurações do gerenciamento habilitado para nuvem** for desativada ou não for mais direcionada ao computador, o computador vai parar de usar o gateway da Internet. O computador reverterá para comunicação direta com o Notification Server local.

Um agente habilitado para nuvem mantém uma lista dos gateways da Internet que estão disponíveis para uso. Além disso, mantém uma lista de servidores de site locais e remotos que podem ser usados. Estas listas são atualizadas no agente sempre que a política de **Configurações do gerenciamento habilitado para nuvem** for atualizada.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para configurar a política de Configurações do gerenciamento habilitado para nuvem

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Gerenciamento habilitado para nuvem**.
- 2 No painel esquerdo, expanda **Política** e clique em **Configurações do gerenciamento habilitado para nuvem**.
- 3 Na página **Configurações do gerenciamento habilitado para nuvem**, configure a política da seguinte forma:

Configure a lista de gateways da Internet que aceitam o tráfego externo do agente.

Para adicionar um gateway da Internet, na caixa de diálogo **Editar servidor gateway**, especifique os parâmetros da seguinte forma:

- **Servidor**

O nome de domínio totalmente qualificado (FQDN) do computador gateway da Internet.

- **Porta**

O número da porta que o Symantec Management Agent deve usar para se conectar ao gateway da Internet. A porta padrão é a 443.

- **Impressão digital**

Cole o valor da **Impressão digital do certificado do gateway** que você copiou no computador gateway da Internet, em **Gerenciador de gateway da Internet do Symantec Management Platform**, na guia **Geral**.

Consulte [“Para configurar o gateway da Internet”](#) na página 317.

Especifique os computadores de destino aos quais a política se aplica.

Se você quiser trazer os Symantec Management Agents existentes para o gerenciamento habilitado para nuvem, adicione estes computadores à política. Depois que o agente em um computador-cliente receber a política de **Configurações do gerenciamento habilitado para nuvem**, ele será conectado ao Notification Server e solicitará seu certificado de cliente exclusivo. Quando o agente tiver recebido seu certificado e não tiver nenhuma conexão direta ao Notification Server, ele tentará se conectar através dos gateways da Internet disponíveis que foram especificados na política. Quando o agente tiver se conectado com êxito, ele será alternado do modo diretamente gerenciado e se tornará um agente habilitado para nuvem.

Aviso: Se você planejar usar o pacote de instalação para instalar agentes em computadores desconectados, inclua aqueles clientes na política. Caso contrário, as configurações do gateway para estes clientes serão excluídas quando eles se conectarem diretamente à rede local. As configurações do gateway para os clientes são excluídas porque não são automaticamente membros da política de **Configurações do gerenciamento habilitado para nuvem**. Portanto, você deve definir o escopo dos clientes antes de instalar o pacote de instalação.

Consulte ["Especificação dos destinos de uma política ou tarefa"](#) na página 380.

4 Ative a política.

Na parte superior direita da página, clique no círculo colorido e em **Ativado**.

5 Clique em **Salvar alterações**.

Depois que o Symantec Management Agent receber a política, ele estará pronto para usar o recurso de gerenciamento habilitado para nuvem. Até que o computador-cliente esteja conectado à rede interna, o modo de gerenciamento habilitado para nuvem permanecerá desativado. Quando você desconectar o computador-cliente da rede interna, e o Symantec Management Agent puder se conectar ao Notification Server através de um gateway da Internet, o gerenciamento habilitado para nuvem ficará ativo automaticamente.

Você pode verificar o status do modo de gerenciamento habilitado para nuvem no Symantec Management Agent do computador-cliente, na guia **Configurações do Symantec Management Agent**, em **Status da rede**.

A próxima etapa é instalar o Symantec Management Agent em um computador desconectado.

Consulte [“Para instalar o Symantec Management Agent em um computador desconectado”](#) na página 324.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para instalar o Symantec Management Agent em um computador desconectado

Para poder realizar a próxima tarefa, certifique-se de ter configurado a política de Configurações do gerenciamento habilitado para nuvem.

Consulte [“Para configurar a política de Configurações do gerenciamento habilitado para nuvem ”](#) na página 320.

Em alguns casos, um computador que você deseja gerenciar pode não ter acesso à rede que hospeda o Symantec Management Platform. Para instalar o Symantec Management Agent em um computador desconectado, você precisa fazer o download do pacote de instalação do agente no Console de gerenciamento Symantec.

Consulte [“Parâmetros do pacote de instalação do agente habilitado para nuvem”](#) na página 522.

Depois de gerar o pacote de instalação do agente da instância apropriada do Symantec Management Platform, você precisa enviá-lo ao site remoto desconectado. Você pode enviar o pacote por e-mail ou enviá-lo em uma mídia física, como CD ou unidade flash. Os usuários no site remoto executam o pacote de instalação do agente para instalar o Symantec Management Agent em seus computadores. O Symantec Management Agent recentemente instalado se conecta imediatamente ao Notification Server através do gateway da Internet apropriado. Você pode usar o mesmo pacote de instalação para instalar o Symantec Management Agent em todos os computadores em um site remoto específico. Porém, todos os agentes instalados recentemente compartilham as mesmas configurações; por isso, use os mesmos gateways da Internet e conecte-se ao mesmo Notification Server.

Nota: Se você quiser usar o pacote de instalação para instalar agentes no computador desconectado, crie uma política que inclua aqueles clientes. Se você não fizer isso, as configurações do gateway para estes clientes serão excluídas quando eles se conectarem diretamente à rede local. As configurações do gateway para os clientes serão excluídas porque elas não são membros da política de **Configurações do gerenciamento habilitado para nuvem**. Você deve consequentemente definir o escopo dos clientes antes do instalar do pacote de instalação.

Esta tarefa é uma etapa do processo de configuração do gerenciamento habilitado para nuvem.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para instalar o Symantec Management Agent em um computador desconectado

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Notification Server > Gerenciamento habilitado para nuvem**.
- 2 No painel esquerdo, expanda **Configurar** e clique em **Configuração do gerenciamento habilitado para nuvem**.
- 3 Na página **Configuração do gerenciamento habilitado para nuvem**, na guia **Configuração do Symantec Management Agent**, clique em **Gerar e fazer o download do pacote de instalação do Symantec Management Agent**.
- 4 Na caixa de diálogo **Pacote de instalação do Agent habilitado para nuvem**, especifique os parâmetros apropriados do pacote.

Para obter mais informações, clique na página e pressione **F1**.

Consulte [Tabela C-5](#) na página 522.

- 5 Clique em **Gerar pacote de instalação de agente**.

A geração do pacote pode levar alguns minutos. Quando o pacote estiver pronto, você será alertado para executar ou salvar o arquivo.

O pacote de instalação gerado é um pacote de instalação de agente extraído automaticamente que inclui os seguintes componentes e configurações:

- Instalador do Symantec Management Agent para a plataforma apropriada.
- Endereço do Notification Server (incluindo o protocolo e o número da porta que serão usados).
- Certificado do Notification Server com cadeia da CA.
O gateway da Internet certifica a impressão digital e o certificado do local. O certificado do local é usado para conectar-se pela primeira vez ao gateway. O certificado do local é essencial porque é usado para gerar uma solicitação permanente de certificação do cliente.

- Lista de gateways da Internet que estão disponíveis para uso pelo agente habilitado para nuvem.
- Destino de recursos ao qual o computador é adicionado automaticamente.
- Grupo organizacional ao qual o computador é adicionado automaticamente.
- Scripts para configurar o Symantec Management Agent para usar as configurações especificadas.

Aviso: O pacote de instalação do Symantec Management Agent é válido para um período limitado (por padrão, sete dias) da hora em que foi gerado. O certificado do local temporário incluído no pacote expira após este período. Se você usar o pacote depois que seu certificado do local tiver expirado, o agente instalado não poderá usar o gateway da Internet para comunicações. Você precisa reinstalar o agente usando um pacote de instalação recém-gerado que contenha um certificado válido do local.

- 6 Na caixa de diálogo **Download do arquivo**, clique em **Salvar** e especifique o local onde salvar o arquivo.
- 7 Quando o download do pacote for concluído, clique em **Fechar**.
- 8 Na caixa de diálogo **Pacote de instalação do Agent habilitado para nuvem**, clique em **Fechar**.
- 9 Coloque o pacote de instalação do Symantec Management Agent no computador desconectado apropriado.
- 10 Execute o pacote de instalação do agente no computador desconectado.

O pacote do agente é um arquivo executável autoextraível e sua instalação é executada silenciosamente.

Após a instalação, o Symantec Management Agent configura-se automaticamente e faz-se o seguinte:

- O agente renegocia seu certificado.
O agente solicita e recebe um novo certificado do Notification Server: o novo certificado é específico a esse computador-cliente e substitui o certificado do local temporário que foi incluído no pacote de instalação do agente.

- O agente é atribuído automaticamente aos destinos de recursos e aos grupos organizacionais apropriados no Symantec Management Platform.
- 11** Verifique se a instalação foi bem-sucedida. Você pode usar o Console de gerenciamento Symantec para exibir os relatórios a fim de verificar se o computador gerenciado está presente.

Se você especificar um grupo organizacional no pacote de instalação, você também poderá verificar se o computador novo foi adicionado ao grupo apropriado.

Consulte [“Para exibir relatórios do gerenciamento habilitado para nuvem”](#) na página 339.

Para obter um processo completo e detalhado sobre como configurar o gerenciamento habilitado para nuvem, consulte [Consulte “Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Para executar tarefas de gerenciamento habilitado para nuvem

Este capítulo contém os tópicos a seguir:

- [Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem](#)

Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem

Esta seção esboça algumas tarefas de solução de problemas e manutenção que podem ser necessárias.

Consulte [“Sobre o gerenciamento habilitado para nuvem”](#) na página 284.

Tabela 21-1 Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem

Tarefa	Descrição
Aplicação de uma autoridade de certificação raiz a um computador gerenciado.	Para migrar um computador gerenciado diretamente ao gerenciamento habilitado para nuvem, assegure-se de que o agente possa se comunicar com o Notification Server usando HTTPS. O agente deve confiar no Notification Server para usar HTTPS para comunicação. Caso necessário, é possível adicionar uma autoridade de certificação (CA, certificate authority) raiz ao armazenamento de Autoridades de certificação raiz confiáveis no computador gerenciado. Consulte “Para aplicar uma autoridade de certificação raiz a um computador gerenciado” na página 292.

Tarefa	Descrição
Geração de um certificado temporário do cliente.	O gerenciamento de cliente habilitado para nuvem atribui certificados do cliente aos computadores gerenciados e aos servidores de sites de modo que possam se identificar no Notification Server. Talvez seja necessário gerar um certificado temporário do cliente para um computador gerenciado. Uma ferramenta de geração de certificado do cliente (<code>AeXGenClientCert.exe</code>) está disponível no Notification Server. Consulte “Para gerar um certificado temporário do cliente” na página 330.
Instalação de um certificado temporário de cliente em um computador gerenciado.	Se o Symantec Management Agent parar de se comunicar através dos gateways da Internet, seu certificado poderá estar danificado. Você pode restaurar a comunicação instalando um certificado temporário do cliente no computador gerenciado apropriado. O Symantec Management Agent usa o certificado temporário para reparar a conectividade ao gateway da Internet. Você pode adicionar ou remover os certificados do armazenamento de certificados do serviço do agente em caso de necessidade. Consulte “Para instalar um certificado temporário em um computador gerenciado” na página 332.
Revogação de um certificado do cliente em um computador gerenciado.	Se você acreditar que um certificado específico do cliente tenha sido comprometido e não deve mais ser confiado, será possível revogar o certificado. Por exemplo, se um computador laptop habilitado para nuvem for perdido ou roubado, você precisará revogar imediatamente seu certificado. Revogar o certificado impede que o computador gerenciado acesse sua rede no modo habilitado para nuvem. Consulte “Para revogar um certificado do gerenciamento habilitado para nuvem” na página 333.
Para forçar um agente habilitado para nuvem a usar um gateway da Internet especificado.	Se o agente não tiver uma lista válida de gateways da Internet, será possível forçar a comunicação através de um conjunto específico de gateways. Você pode adicionar e remover gateways da Internet na lista, caso seja necessário. Consulte “Para forçar o Symantec Management Agent a usar um gateway da Internet especificado” na página 336.
Para fazer backup e restaurar o gateway da Internet.	Você pode fazer o backup de suas configurações de gateway da Internet e restaurar seu estado original no caso de falha. Consulte “Para fazer backup e restaurar um gateway da Internet” na página 337.
Para exibir relatórios do gerenciamento habilitado para nuvem.	Um conjunto de relatórios predefinidos é fornecido para ajudá-lo a monitorar e gerenciar seus computadores habilitados para nuvem. Consulte “Para exibir relatórios do gerenciamento habilitado para nuvem” na página 339.

Para gerar um certificado temporário do cliente

O gerenciamento de cliente habilitado para nuvem atribui certificados do cliente aos computadores gerenciados e aos servidores de sites de modo que possam se identificar no Notification Server. A ferramenta de geração de certificados do cliente (`AeXGenClientCert.exe`) permite criar os certificados do cliente de que você precisa. O certificado de autoridade de certificação (CA) do agente do Notification Server emite estes certificados. A parte pública do certificado é armazenada no banco de dados de gerenciamento de configuração (CMDB). Ambas as partes, pública e privada, são adicionadas a um arquivo PKCS#12 (PFX).

Nota: O certificado gerado é válido por um período limitado. Por padrão, este período é de sete dias, mas você pode mudá-lo, caso necessário.

Talvez seja necessário gerar um certificado temporário para um computador gerenciado. Você precisa gerar o arquivo PFX apropriado e instalar o arquivo no computador gerenciado ou no servidor de sites.

Para gerar um certificado do cliente

- ◆ No computador do Notification Server, abra um prompt de comando e execute a linha de comando a seguir com os parâmetros apropriados:

```
\Arquivos de programas\Altiris\Notification
Server\bin\Tools\AeXGenClientCert <Nome_comum> [-o
Certificate.pfx] [-p senha]
```

CommonName	O identificador que você deseja exibir na linha de assunto do certificado. Este identificador é usado para propósitos de geração de relatórios e diagnóstico. Este identificador deve ser o mesmo que o parâmetro Nome da instalação que foi especificado no pacote de instalação do Symantec Management Agent. Consulte “Parâmetros do pacote de instalação do agente habilitado para nuvem” na página 522.
Certificate.pfx	O caminho completo e o nome do arquivo PFX que você deseja gerar. Se você omitir este parâmetro, o certificado gerado será salvo no diretório local. O arquivo do certificado é nomeado com base no nome comum especificado com a extensão .pfx aplicada a ele (CommonName.pfx).
senha	A senha que deseja usar. Se você omitir este parâmetro, a senha ficará vazia. Nenhuma senha padrão é aplicada.

O nome e o caminho do arquivo gerado são mostrados no prompt de comando.

Você precisa copiar o arquivo gerado do certificado na mídia apropriada e colocá-lo na pasta-raiz do computador-cliente apropriado. Em seguida, no computador-cliente, use o parâmetro da linha de comando `/importcert` para que o Symantec Management Agent use esse certificado.

Consulte [“Para instalar um certificado temporário em um computador gerenciado”](#) na página 332.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem ”](#) na página 328.

Para instalar um certificado temporário em um computador gerenciado

Se o Symantec Management Agent parar de se comunicar através dos gateways da Internet, seu certificado poderá estar danificado. Você pode resolver este problema instalando um certificado temporário no computador-cliente apropriado.

O Symantec Management Agent usa o certificado temporário para se conectar ao Notification Server através do gateway da Internet apropriado. Assim, ele pedirá um novo certificado exclusivo a esse computador.

O arquivo do certificado deve incluir uma chave privada e não ter nenhuma senha associada.

Para instalar um certificado temporário em um computador gerenciado

- 1 Gere um certificado temporário do cliente, *tempcert.pfx*.

Você pode usar uma ferramenta de linha de comando no computador do Notification Server para gerar um certificado temporário do cliente. A ferramenta de linha de comando gera um arquivo PFX que contém o certificado e a chave privada.

Consulte [“Ferramentas de linha de comando do Notification Server”](#) na página 516.

Nota: Por padrão, o arquivo gerado não tem nenhuma senha. Não especifique uma senha porque o Symantec Management Agent não pode usar arquivos PFX protegidos por senha.

Consulte [“Para gerar um certificado temporário do cliente”](#) na página 330.

- 2 Coloque o arquivo PFX gerado na pasta-raiz no computador gerenciado.
- 3 Abra um prompt de comando e execute a linha de comando a seguir:

```
[Pasta de instalação do agente]\AeXNSAgent.exe  
/importcert=tempcert.pfx
```

Por exemplo:

**\Arquivos de programas\Altiris\Altiris
Agent\AeXNSAgent.exe/importcert=myRootCert.pfx**

- 4 Reinicie o Symantec Management Agent para que as novas configurações entrem em vigor.

Para remover um certificado de um computador gerenciado

- ◆ No computador gerenciado, abra um prompt de comando e execute a linha de comando a seguir:

```
[Pasta de instalação do agente]\AeXNSAgent.exe /removecert
```

Este comando remove o certificado atual do Symantec Management Agent.

Por exemplo:

\Arquivos de programas\Altiris\Altiris Agent\AeXNSAgent.exe /removecert

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Consulte [“Parâmetros da linha de comando para a configuração de agente habilitado para nuvem”](#) na página 523.

Para revogar um certificado do gerenciamento habilitado para nuvem

Revogar um certificado de gerenciamento habilitado para nuvem (CEM) impede que o computador gerenciado acesse sua rede no modo habilitado para nuvem. Por exemplo, se um computador laptop habilitado para nuvem for perdido ou roubado, você precisará revogar imediatamente seu certificado.

O agente tem dois certificados de CEM. Um certificado permite que o agente crie a conexão ao gateway da Internet e o outro certificado permite que o agente se conecte ao Notification Server. Se o certificado que permite que o agente se conecte ao Notification Server for revogado, o Notification Server recusará a conexão de tal cliente. Contudo, o gateway da Internet não tem capacidade para receber as informações sobre certificados revogados diretamente do Notification Server. Para revogar um certificado particular no gateway da Internet, você precisa adicionar os detalhes do certificado à Lista de revogação de certificados (CRL, Certificate Revocation List) no Notification Server, gerar um arquivo atualizado de CRL e aplicar então o arquivo atualizado de CRL ao gateway da Internet apropriado.

Nota: Você precisa aplicar o arquivo atualizado de CRL a cada gateway da Internet que o agente revogado possa usar.

Note que a revogação do certificado habilitado para nuvem apenas bloqueia o computador gerenciado de acessar o Notification Server no modo habilitado para nuvem. Se a confiança do agente não for revogada, o agente poderá continuar a operar no modo local.

Para revogar um certificado do gerenciamento habilitado para nuvem

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, em **Relatórios**, expanda **Gerenciamento do Notification Server > Certificados** e clique em **Certificado por impressão digital**.
- 3 Na página do relatório **Certificado por impressão digital**, clique com o botão direito do mouse no certificado que você quer revogar e depois clique em **Revogar certificado**.

Se você revogar o certificado na página do relatório **Certificado por impressão digital**, os detalhes do certificado serão adicionados ao arquivo de CRL automaticamente.

O CRL é armazenado no armazenamento do computador raiz, embora os certificados sejam armazenados no banco de dados de gerenciamento de configuração (CMDB). A ferramenta de revogação de certificados (AeXRevokeCertificate.exe) carregará primeiro o CRL existente, se houver. Se nenhuma CRL existir no armazenamento de certificados, a ferramenta criará uma. A ferramenta, em seguida, adicionará o número de série do certificado à lista e vai gerar um arquivo codificado em PEM que contenha a CRL atualizada. Você coloca, em seguida, o arquivo da CRL gerado no computador gateway da Internet e executa um script para aplicar a lista atualizada ao gateway da Internet.

Por padrão, o arquivo de CRL está no seguinte local no Notification Server:

```
\Arquivos de programas\Altiris\Notification  
Server\bin\Tools\AeXRevokeCertificate\EMEncodedFile.CRL
```

Para adicionar manualmente um certificado do gerenciamento habilitado para nuvem ao CRL

- 1 Obtenha o número de série e a impressão digital do certificado do cliente que você deseja revogar.

Se você tiver acesso ao computador-cliente, será possível usar o Console de Gerenciamento Microsoft (MMC) para localizar os detalhes do certificado do cliente.

Se você não tiver acesso ao computador-cliente, será possível usar alguns dos seguintes métodos:

- No Console de gerenciamento Symantec, abra o Gerenciador de recursos e visualize as informações do inventário básico do computador-cliente. O caminho do menu é **Exibir > Classes de dados > Inventário > Inventário básico > Certificado AeX AC**. Os detalhes completos do certificado do cliente são mostrados, incluindo o número de série e a impressão digital.

- Consulte esses detalhes no CMDB do Symantec Management Platform usando uma consulta SQL. Os certificados do cliente são armazenados na tabela **CertificateRegistration**.
 - No gateway da Internet, abra o arquivo de log de acesso e procure uma entrada que se relacione ao cliente. O arquivo access.log é armazenado na pasta Apache\logs na pasta de instalação do gateway da Internet. Cada entrada no arquivo de log inclui o nome do computador que acessou o gateway da Internet e o número de série correspondente do certificado.
- 2 No computador do Notification Server, abra uma janela do prompt de comando e execute a linha de comando a seguir com os parâmetros apropriados:

```

\Arquivos de programas\Altiris\Notification
Server\bin\Tools\AeXRevokeCertificate -o <PEMEncodedFile.CRL> <-t
Sha1ThumbPrint | -s Número_de_série>

```

PEMEncodedFile.CRL O nome e o caminho completo do arquivo da CLR codificado em PEM que deseja gerar. Se você omitir este parâmetro, o arquivo gerado será salvo no diretório local.

Sha1ThumbPrint O identificador exclusivo do certificado.

SerialNumber Se mais de um certificado no banco de dados tiver o mesmo número de série, use um SHA-1 thumbprint para identificar o certificado. Inversamente, se dois certificados tiverem a mesma impressão digital, identifique o certificado pelo número de série.

Nota: Em alguns lugares, a impressão digital e o número de série podem ser exibidos como octetos separados por espaço. Porém, quando você os especificar como parâmetros de linha de comando, eles não deverão incluir nenhum caractere de espaço.

O arquivo atualizado de CRL é gerado.

Para aplicar o CRL a um gateway da Internet

- 1 Coloque o CRL gerado no seguinte local do computador gateway da Internet:

[Pasta de instalação do gateway da Internet]\Apache\certs\crl

A pasta de instalação padrão é \Arquivos de programas x86\Symantec\SMP Internet Gateway. Porém, o caminho depende do diretório de destino que foi especificado durante a instalação do gateway da Internet.

- 2 Na mesma pasta, clique duas vezes em **UpdateCrlHashes.cmd** para executar o script de **Atualização de CRL**.

Este script executa a configuração necessária e reinicia o gateway da Internet para que as mudanças entrem em vigor.

Consulte “[Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem](#)” na página 328.

Para forçar o Symantec Management Agent a usar um gateway da Internet especificado

Se o agente não tiver uma lista válida de gateways da Internet, será possível forçar a comunicação através de um conjunto específico de gateways. Você força uma lista específica de gateways pela linha de comando ou modificando as configurações do registro. Uma linha de comando está disponível para adicionar gateways individuais.

Se você quiser remover um gateway da Internet da configuração do Symantec Management Agent, será possível fazer isso editando o registro.

Os detalhes do gateway da Internet são armazenados no registro. Você pode adicionar ou remover gateways da Internet editando as entradas na seguinte chave:

HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Secure Gateways

Cada gateway da Internet tem um conjunto de valores na chave <GatewayName>.

Nota: Você precisa reiniciar o Symantec Management Agent para que estas configurações entrem em vigor.

Para forçar o Symantec Management Agent a usar um gateway da Internet especificado

- ◆ No computador-cliente, abra um prompt de comando e execute a linha de comando a seguir:

```
\Arquivos de programas\Altiris\Altiris Agent\AeXNSAgent.exe
/gw=gatewayName,port,thumbprint
```

gatewayName	O nome ou o endereço IP do computador gateway.
porta	O número da porta que o Symantec Management Agent deve usar para se conectar ao gateway. A porta padrão é 443.
Impressão digital	A impressão digital do certificado que o gateway usa para conexões seguras. Nota: Em alguns lugares, a impressão digital pode ser exibida como octetos separados por espaço. Porém, quando você a especificar como um parâmetro de linha de comando, ela não deverá incluir nenhum caractere de espaço.

Cada parâmetro precisa ser separado com uma vírgula. Nenhum espaço ou outra pontuação é permitido.

Por exemplo:

```
\Arquivos de programas\Altiris\Altiris Agent\AeXNSAgent.exe
/gw=myGateWay.symantec.com,443,0f8753ef3da6bc4
```

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Consulte [“Parâmetros da linha de comando para a configuração de agente habilitado para nuvem”](#) na página 523.

Para fazer backup e restaurar um gateway da Internet

Para fazer backup seu gateway da Internet permite restaurar seu estado original em caso de uma falha. Você poderá executar uma restauração parcial se alguns arquivos da lista de backup estiverem ausentes ou corrompidos. Você pode também executar uma restauração completa em caso de corrupções fatais na configuração do gateway da Internet. Por exemplo, você substituiu um disco rígido em seu computador gateway da Internet.

Você pode executar um backup sem interromper o serviço do gateway da Internet.

Você deve fazer backup dos arquivos em pastas dadas da seguinte forma:

- arquivos `openssl.cnf`, `server.crt` e `server.key` na pasta `C:\Arquivos de programas\Symantec\SMP Internet Gateway\Apache\certs`
- Todos os arquivos na pasta `C:\Arquivos de programas\Symantec\SMP Internet Gateway\Apache\certs\client`
- Todos os arquivos na pasta `C:\Arquivos de programas\Symantec\SMP Internet Gateway\Apache\certs\crl`
- Todos os arquivos na pasta `C:\Arquivos de programas\Symantec\SMP Internet Gateway\Apache\conf`

Para executar uma restauração parcial

- 1 Abra o **Gerenciador de gateway de Internet do Symantec Management Platform** e na guia **Geral**, em **Serviço do gateway da Internet**, clique em **Parar** para interromper o serviço do gateway da Internet.
- 2 Restaurar itens do problema da lista de backup.
- 3 No **Gerenciador de gateway de Internet do Symantec Management Platform** e na guia **Geral**, em **Serviço do gateway da Internet**, clique em **Iniciar** para iniciar o serviço do gateway da Internet.

Depois que você inicia o serviço, certifique-se de que as configurações do gateway da Internet estejam corretas e o recurso esteja funcionando corretamente.

Para executar uma restauração completa

- 1 Execute uma instalação nova do gateway da Internet.
Ao final da instalação, desmarque **Iniciar o Assistente de Configuração**.
- 2 Restaure todos os itens da lista de backup para locais apropriados no computador do gateway da Internet.
- 3 Abra o **Gerenciador de gateway de Internet do Symantec Management Platform** e na guia **Configurações**, clique em **Executar o assistente**.
- 4 No Assistente de **Configuração do gateway da Internet do Symantec Management Platform**, navegue pelas páginas e certifique-se de que todos os dados tenham sido pré-preenchidos corretamente.

- 5 Na página **Conta do usuário**, especifique as credenciais de serviço do gateway da Internet.
- 6 Na página **Resumo**, verifique as configurações, certifique-se de que **Reiniciar serviços automaticamente?** esteja selecionado e clique em **Concluir**.

Depois de o serviço ter sido iniciado, certifique-se de que as configurações do gateway da Internet estejam corretas e o recurso esteja funcionando corretamente.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Para exibir relatórios do gerenciamento habilitado para nuvem

Um conjunto abrangente de relatórios é fornecido para ajudar a monitorar e gerenciar seus computadores ativados na nuvem. Você também pode criar relatórios personalizados para satisfazer a seus requisitos.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para exibir relatórios do gerenciamento habilitado para nuvem

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, clique em **Relatórios > Gerenciamento do Notification Server > Agente > Gerenciamento habilitado para nuvem** e depois clique no relatório que você deseja exibir.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Para gerenciar recursos do Symantec Management Platform

- [Capítulo 22. Para configurar a segurança dos recursos](#)
- [Capítulo 23. Para configurar filtros e destinos de recursos](#)
- [Capítulo 24. Para configurar pacotes](#)
- [Capítulo 25. Para usar políticas](#)
- [Capítulo 26. Para usar tarefas e trabalhos](#)
- [Capítulo 27. Para usar o Gerenciador de recursos](#)
- [Capítulo 28. Para usar relatórios do Notification Server](#)
- [Capítulo 29. Para criar relatórios personalizados do Notification Server](#)
- [Capítulo 30. Para exibir informações dos recursos](#)

Para configurar a segurança dos recursos

Este capítulo contém os tópicos a seguir:

- [Para configurar a segurança dos recursos](#)
- [Considerações sobre o escopo do recurso](#)

Para configurar a segurança dos recursos

O modelo de segurança de recursos foi alterado significativamente no Notification Server 7.0. Recursos, que incluem todos os computadores, usuários e tudo mais que é definido no CMDB ou no modelo do recurso, obtêm agora todas as suas concessões de permissão das exibições organizacionais e dos grupos aos quais pertencem. Isto substitui a implementação do Notification Server 6.0, que exigia a proteção de coleções padrão e de pastas de recursos.

Nota: Há algumas exceções, tais como os pacotes, que são recursos, mas também itens, que aparecem na estrutura da pasta do Symantec Management Console. As opções de segurança para esses itens são desativadas na estrutura da pasta. A segurança deles é definida da mesma maneira que para outros recursos.

Uma exibição organizacional é um agrupamento hierárquico de recursos (como grupos organizacionais) que reflete uma exibição ou estrutura real de sua organização. Por exemplo, você pode criar exibições organizacionais para agrupar seus recursos por local geográfico, por departamento ou pela estrutura de rede. Como no mundo real, um recurso pode (mas não necessariamente) aparecer apenas uma vez em uma exibição organizacional.

A atribuição de recursos a grupos organizacionais é automática e você não pode mudá-la. Observe que pode haver um atraso entre os recursos que estão sendo descobertos e os que são mostrados no grupo organizacional apropriado. Cada recurso recém-descoberto é colocado no grupo organizacional de nível superior e permanece lá até que seja movido para o grupo organizacional apropriado quando a atualização da agenda da Exibição organizacional é executada.

Você pode remover recursos de qualquer exibição organizacional, exceto a exibição **Padrão**. Quando um recurso é excluído do CMDB, ele é removido automaticamente de todas as exibições organizacionais usando a agenda de atualização delta.

Consulte [“Agendamento de atualizações da participação em recursos”](#) na página 368.

Você configura a segurança atribuindo as permissões apropriadas a cada função de segurança nas exibições organizacionais e nos grupos organizacionais dentro de cada exibição. Uma permissão atribuída a um grupo organizacional aplica-se a todos os recursos nesse grupo e, por padrão, aplica-se a todos os seus grupos filho. Você não pode atribuir permissões diretamente a recursos específicos.

As concessões de permissão em um recurso são acumuladas nas exibições organizacionais. As permissões que uma função de segurança tem em um recurso específico são a união de todas as permissões atribuídas ao recurso nos grupos organizacionais a que pertencem. Se uma função de segurança tem a permissão de executar uma ação em um recurso em uma exibição organizacional, a função pode executar essa ação independentemente de a permissão ser aplicada a outras exibições organizacionais que contêm o mesmo recurso. Por exemplo, se uma função de segurança tiver acesso de leitura a um recurso em uma exibição organizacional, acesso de gravação ao mesmo recurso em uma outra exibição organizacional, mas nenhum acesso ao recurso em uma terceira exibição organizacional, a função terá acesso de leitura e gravação ao recurso.

Implementar a segurança de recursos dessa maneira fornece a cada função de segurança sua própria exibição exclusiva ou “escopo” dos recursos disponíveis. A função de segurança determina quais recursos seus membros podem acessar e quais ações podem ser executadas nesses recursos. Filtros, destinos e resultados de relatório são dinâmicos e têm seu escopo determinado automaticamente de acordo com a função do usuário que os possui. Consequentemente, os filtros, os destinos e os resultados do relatório sempre conterão apenas os recursos aos quais esse usuário tem a permissão de acesso necessária.

A configuração da segurança de recursos é uma etapa opcional no processo de configuração da segurança do Symantec Management Platform.

Consulte [“Para configurar a segurança do Symantec Management Platform”](#) na página 84.

Nota: Quando um destino é avaliado, apenas os recursos aos quais o usuário tem acesso de leitura está disponível. Consequentemente, a única permissão de segurança que um usuário necessita para aplicar uma tarefa ou uma política a um recurso é a permissão de leitura.

Tabela 22-1 Processo para configurar a segurança de recursos

Etapa	Ação	Descrição
Etapa 1	Identifique seu gerenciamento de recursos e requisitos de segurança.	É necessário determinar o gerenciamento de recursos e requisitos de segurança e planejar as estruturas de exibição organizacional que melhor atendem a seus requisitos. Você pode usar a estrutura que desejar. Por exemplo, talvez você queira usar exibições organizacionais baseadas na geografia, função de negócios ou estrutura de gerenciamento. Para obter mais informações, consulte o <i>Guia de Planejamento de Implementação do IT Management Suite</i>.
Etapa 2	Crie as exibições organizacionais desejadas.	Crie as exibições organizacionais que você precisa para modelar as estruturas lógicas apropriadas em sua organização. Consulte “Para criar e configurar uma exibição organizacional” na página 344. Consulte “Para criar e preencher um grupo ou exibição organizacional” na página 345.
Etapa 3	Em cada exibição organizacional, crie os grupos organizacionais que você deseja e atribua os recursos apropriados a cada grupo organizacional.	Em cada exibição organizacional, você pode criar uma hierarquia de grupos para representar a estrutura organizacional que você deseja modelar. Os novos recursos são adicionados automaticamente à exibição organizacional Padrão. É possível movê-los para os grupos apropriados em cada uma de suas exibições organizacionais. Consulte “Para criar e configurar um grupo organizacional” na página 346. Consulte “Para exibir recursos em um grupo organizacional” na página 347.

Etapa	Ação	Descrição
Etapa 4	Atribua as funções de segurança apropriadas a cada grupo organizacional.	Atribuir uma função de segurança a um grupo organizacional oferece aos usuários que tenham essa função acesso a todos os recursos diretamente incluídos nesse grupo. É preciso especificar as permissões que cada função tem no grupo. Por padrão, as configurações de segurança em um grupo aplicam-se a todos os grupos filho. Você pode interromper a herança quando necessário. Consulte “Para definir a segurança da configuração em um grupo organizacional” na página 348.

Para criar e configurar uma exibição organizacional

Uma exibição organizacional é um agrupamento hierárquico de recursos (como grupos organizacionais) que reflete uma exibição ou estrutura real de sua organização. Por exemplo, você pode criar exibições organizacionais para agrupar seus recursos por local geográfico, por departamento ou pela estrutura de rede. Como no mundo real, um recurso pode (mas não necessariamente) aparecer apenas uma vez em uma exibição organizacional.

As exibições organizacionais fornecem meios seguros de separar seus recursos em unidades bem estruturadas e gerenciáveis. Uma exibição organizacional não pode conter nenhum recurso diretamente. Todos os recursos devem estar contidos em grupos organizacionais. Você pode usar exibições e grupos organizacionais para modelar um grande variedade de requisitos organizacionais. Você pode proteger suas exibições organizacionais usando o modelo de herança de segurança NT familiar que é usado em todo o Symantec Management Platform.

Você poderá usar exibições e grupos organizacionais nos destinos quando desejar aplicar uma política ou tarefa aos computadores, usuários ou aos recursos selecionados. A exibição ou o grupo organizacional é usado da mesma maneira que um filtro, mas fornece a segurança necessária para garantir que somente os recursos aos quais o proprietário de destino tem permissão sejam incluídos.

Esta tarefa é uma etapa do processo de configuração da segurança do recurso.

Consulte [“Para configurar a segurança dos recursos”](#) na página 341.

Para criar um grupo organizacional

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Exibições e grupos organizacionais**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta **Exibições organizacionais** e depois clique em **Novo(a) > Exibição organizacional**.

- 3 (Opcional) No painel direito, edite o nome e a descrição da exibição organizacional.
- 4 Para especificar os grupos organizacionais que são exibidos, faça o seguinte:
 - No painel direito, clique em **Filtro**.
 - Na caixa de diálogo **Filtrar grupos visíveis**, selecione os grupos organizacionais que você quer tornar visíveis para esta exibição organizacional e depois clique em **OK**.

Para criar e preencher um grupo ou exibição organizacional

Na exibição aprimorada **Computadores**, você pode facilmente criar e preencher grupos e exibições organizacionais.

Para criar e preencher um grupo ou exibição organizacional

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Computadores**.
- 2 Clique com o botão direito do mouse em **Todas as exibições de computador** e em **Novo(a) > Exibição organizacional**.
- 3 Na caixa de diálogo **Exibição organizacional**, digite o nome da exibição organizacional e clique em **OK**.
- 4 Clique com o botão direito do mouse na nova exibição organizacional, e clique em **Novo(a) > Grupo organizacional**.

Observe que você não pode adicionar grupos organizacionais à exibição organizacional padrão **Todos os computadores**.

- 5 Na caixa de diálogo **Grupo organizacional**, digite o nome do novo grupo e clique em **OK**.
- 6 Para preencher o novo grupo organizacional, faça o seguinte:
 - Em **Todas as exibições de computador**, clique em **Todos os computadores**.
 - No painel de listas, selecione os computadores que você quer adicionar a este grupo organizacional.
Você pode usar as teclas **Shift** ou **Ctrl** para selecionar vários computadores.
 - Arraste os computadores selecionados para o novo grupo organizacional ou clique com o botão direito do mouse em um dos computadores selecionados, e depois clique em **Adicionar a grupo organizacional**. Na caixa de diálogo **Adicionar a grupo organizacional**, clique no grupo ao qual você deseja adicionar os computadores e clique em **OK**.

Para criar e configurar um grupo organizacional

Cada exibição organizacional contém um ou mais grupos organizacionais, e cada um pode conter recursos e grupos organizacionais filho. A estrutura hierárquica dos grupos organizacionais pode ter tantos níveis quanto for necessário para representar a maneira como os recursos estão organizados em seu ambiente. A participação de um grupo organizacional inclui os recursos contidos em todos os seus grupos filho.

O Console de gerenciamento Symantec tem uma exibição organizacional **Padrão** predefinida na qual todos os recursos são colocados automaticamente. A estrutura padrão é uma hierarquia de grupos organizacionais baseada no tipo de recurso. Não é possível adicionar ou remover grupos organizacionais da exibição organizacional **Padrão**. Todos os recursos descobertos recentemente são colocados automaticamente no grupo apropriado da exibição organizacional **Padrão**.

Esta tarefa é uma etapa do processo de configuração da segurança do recurso.

Consulte [“Para configurar a segurança dos recursos”](#) na página 341.

Para criar e configurar um grupo organizacional

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Exibições e grupos organizacionais**.
- 2 No painel esquerdo, clique com o botão direito do mouse na exibição organizacional para a qual você quer adicionar um grupo organizacional e clique em **Novo(a) > Grupo organizacional**.
- 3 No painel direito, edite o nome e a descrição do grupo organizacional.
Os nomes dos grupos não têm nenhuma restrição; portanto, você pode ter vários grupos com o mesmo nome.
- 4 Para adicionar recursos ao grupo, faça o seguinte:
 - No painel direito, clique em **Adicionar** e depois clique no item que você quer adicionar ao grupo.
 - Na caixa de diálogo **Editar grupo**, selecione os recursos apropriados e clique em **OK**.
- 5 Para remover um recurso do grupo, clique com o botão direito do mouse no recurso e depois clique em **Excluir**.

Aviso: Quando você excluir um recurso, ele será removido do CMDB. Você não deve excluir nenhum recurso que seja crítico à atividade e à funcionalidade do Symantec Management Platform. Os recursos críticos incluem o computador do Notification Server, os sites e as sub-redes.

Para exibir recursos em um grupo organizacional

O painel Recursos exibe todos os recursos diretamente incluídos no grupo organizacional e todos os recursos incluídos em qualquer um de seus grupos filho. Você pode mudar a exibição para ver somente os computadores que estão no grupo.

Consulte [“Para configurar a segurança dos recursos”](#) na página 341.

Você pode exibir a lista dos recursos que estão disponíveis para uma função de segurança específica. Por exemplo, convém verificar se você configurou corretamente a segurança dos recursos para uma função específica. As funções de segurança atribuídas a um grupo organizacional determinam o acesso a todos os recursos que são diretamente incluídos nesse grupo. Cada função de segurança tem acesso somente aos recursos diretamente incluídos nos grupos aos quais a função é atribuída.

Quando exibe os recursos para uma função de segurança específica, você visualiza somente os recursos que estão disponíveis para a função selecionada e a sua função. Se sua função é a função Administrador (que tem acesso a todos os recursos), você visualizará sempre todos os recursos que estão disponíveis à função selecionada. Porém, se você tem outra função (que pode não ter acesso a todos os recursos), não é possível ver todos os recursos que estão disponíveis à função selecionada.

Nota: Se você não pertence a uma função (isto é, a segurança baseada em usuário foi aplicada, em vez da baseada em função), escolha **Nenhum** para não ter nenhuma função de segurança selecionada. Isto garante que todos os recursos aos quais você tem acesso sejam mostrados. Se você selecionar uma função à qual você não pertence, todos os recursos serão filtrados e nada poderá ser visto.

Você pode executar ações de gerenciamento em recursos em um grupo organizacional. As ações disponíveis incluem a abertura do Gerenciador de recursos, a exportação dos recursos para um arquivo XML, a exibição das propriedades dos recursos, a adição dos recursos a um grupo diferente e a exclusão dos recursos do grupo.

Para exibir recursos em um grupo organizacional

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Exibições e grupos organizacionais**.
- 2 No painel esquerdo, expanda a pasta **Exibições organizacionais** e selecione o grupo organizacional apropriado.
- 3 (Opcional) Para exibir recursos para uma função de segurança particular, no painel direito, em **Recursos**, na lista suspensa **Função**, clique na função apropriada.

Para definir a segurança da configuração em um grupo organizacional

Você define a segurança em um grupo organizacional atribuindo-lhe as funções de segurança apropriadas. Quando uma função de segurança for atribuída a um grupo, os membros dessa função de segurança terão acesso aos recursos que estão no grupo. Por padrão, todos os grupos filho herdam todas as atribuições de segurança em um grupo organizacional. A herança dá à função o mesmo acesso a todos os recursos naqueles grupos filho. Você pode interromper a herança em qualquer nível e restaurá-la quando necessário.

Para definir a segurança em grupos organizacionais, é necessária a permissão do sistema **Alterar permissões**.

Quando você instalar o Symantec Management Platform, a configuração padrão será a de que todas as funções tenham permissão completa na exibição organizacional **Padrão**. A configuração padrão dá a todas as funções acesso total a todos os recursos. Se desejar configurar a segurança dos recursos (que é opcional), você poderá usar a exibição organizacional **Padrão** para definir permissões padrão em todos os recursos ou tipos específicos de recursos. É necessário desativar a herança para as funções apropriadas de segurança e limpar as permissões abaixo da estrutura do grupo organizacional.

Você pode atribuir uma função de segurança a um grupo organizacional com as permissões apropriadas a essa função. Por exemplo, uma função de administrador exige direitos totais de gerenciamento a todos os recursos em um grupo, mas uma função de usuário final pode exigir somente acesso de leitura a esses recursos. Por padrão, atribuir algumas permissões a uma função de segurança em um grupo organizacional dá a essa função as mesmas permissões em todos os seus grupos filho.

Esta tarefa é uma etapa do processo de configuração da segurança do recurso.

Consulte [“Para configurar a segurança dos recursos”](#) na página 341.

Para definir a segurança em um grupo organizacional

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Exibições e grupos organizacionais**.
- 2 No painel esquerdo, clique com o botão direito do mouse no grupo organizacional, clique em **Gerenciar segurança** e depois execute uma das seguintes ações:

Para atribuir todas as permissões disponíveis

- Clique em **Atribuir direitos de gerenciamento**.
- Na caixa de diálogo **Atribuir direitos de gerenciamento**, selecione as funções de segurança apropriadas e clique em **OK**.

Para atribuir a permissão de "Leitura" ao sistema da Symantec

- Clique em **Atribuir leitura**.
- Na caixa de diálogo **Atribuir direitos de leitura**, selecione as funções de segurança apropriadas e clique em **OK**.

Para definir permissões de segurança personalizadas

- Clique em **Atribuir personalizado**.
- No **Gerenciador de Função de Segurança**, na lista suspensa **Função**, selecione a função de segurança para a qual você deseja definir permissões.
- Na lista suspensa **Exibir**, clique em **Todos os itens**.
- No painel esquerdo, selecione a exibição ou o grupo organizacional para o qual você deseja definir permissões.
- No painel direito, em **Não herdado**, faça as mudanças apropriadas nas configurações de permissão.
- (Opcional) Se você quiser configurar a herança de permissão, clique em **Avançadas**. Consulte ["Para personalizar a herança de permissões"](#) na página 104.
- Clique em **Salvar alterações**.

- 3 Clique em **Salvar alterações**.

Considerações sobre o escopo do recurso

O escopo do recurso fornece meios seguros de separar recursos em unidades gerenciáveis e bem estruturadas. Estas unidades são genéricas por natureza; assim, elas podem ser organizadas para adequarem-se a vários requisitos organizacionais.

Na maioria dos casos, a avaliação dos requisitos de escopo de recursos em seu planejamento resultará nas seguintes perguntas:

- Quem deve ter acesso total à infraestrutura do Symantec Management Platform?
- Quais são as funções de gerenciamento existentes para operações rotineiras?
- Que áreas de funcionalidade exigem funções e direitos específicos?
- O Active Directory reflete exatamente nosso modelo de gerenciamento e negócios?
- Existem grupos do Active Directory que reflitam as funções na arquitetura do Symantec Management Platform?
- Quais são os tipos de recursos que precisam de gerenciamento?

Quando projetar sua estrutura de recursos, use a seguinte lista de verificação para garantir que ela seja concluída na ordem correta:

- Identifique usuários, funções de segurança e direitos.
- Crie funções de segurança.
Atribua direitos e a participação do usuário.
- Crie a estrutura de grupos e exibições organizacionais.
Siga as melhores práticas de importação do Active Directory. Agrupe por tipo de recurso (usuário, computador).
- Atribua funções e permissões a exibições e grupos organizacionais específicos.
- Gere relatórios para a exibição do sistema da linha de base dos recursos.
- Faça o backup da estrutura do grupo e da exibição organizacional usando um XML de exportação.

Tabela 22-2 Considerações do planejamento para o escopo de recursos

Item	Considerações de planejamento
Segurança	■ Você deve configurar funções de segurança antes de executar outra tarefa de segurança do console e antes que o Notification Server seja implementado em seu ambiente de produção. ■ A segurança do recurso é a combinação do escopo, da função de segurança e das permissões. ■ Os recursos obtêm todas as suas concessões de permissão das coleções de escopos das quais são membros. As concessões são cumulativas por natureza. Com a permissão de executar uma ação em um recurso em uma coleção de escopo, você garante que o usuário/função possa continuar a executar esta ação independentemente de a permissão ser aplicada a outras coleções de escopo que contenham o recurso. ■ As funções de segurança são grupos de usuários que permitem que você atribua privilégios para responsabilidades administrativas e de funcionários, permitindo também atribuir permissões para pastas ou itens que podem ser exibidos pelos administradores ou funcionários no Symantec Management Console. ■ As funções integradas são fornecidas com uma variedade de concessões de privilégio, e as funções podem ser atribuídas em qualquer local dentro da estrutura da exibição organizacional ou do grupo organizacional, dependendo do escopo administrativo que você optou por conceder. ■ As concessões de segurança são atribuídas aos grupos organizacionais e são herdadas do grupo organizacional acima dele.

Item	Considerações de planejamento
Exibições organizacionais	■ Uma exibição organizacional é uma hierarquia independente e segura de grupos organizacionais que contêm recursos. ■ As exibições organizacionais fornecem um meio simplificado e seguro de agrupar e gerenciar recursos. ■ Considere uma exibição organizacional para representar um limite ou uma estrutura de segurança administrativa que se alinhe ao seu ambiente de TI. ■ Faça o espelhamento de seu modelo organizacional do Active Directory usando a opção Importação do Active Directory para impedir a criação e o preenchimento manuais. ■ Todos os recursos em uma exibição organizacional (gerenciada e não gerenciada) estão no escopo, por padrão. ■ As exibições organizacionais apenas contêm recursos através dos grupos organizacionais. Uma exibição organizacional não pode conter nenhum recurso diretamente. Todos os recursos recentemente descobertos são importados automaticamente para a exibição organizacional padrão. ■ Um item do recurso pode pertencer a apenas um grupo organizacional em cada exibição organizacional. Quando você adicionar um recurso a um grupo organizacional, ele será removido automaticamente de qualquer outro grupo ao qual esteja atribuído. ■ Use os grupos organizacionais para aplicar uma política ou tarefa a computadores, usuários e recursos selecionados. Para fazer isso, use um grupo organizacional em um destino. Nesta instância, um grupo organizacional funciona como um filtro, mas fornece segurança para garantir que apenas o recurso ao qual o proprietário de destino tem permissão seja incluído. ■ O Symantec Management Platform permite várias exibições organizacionais porque os administradores podem ter várias maneiras de organizar recursos. Portanto, é possível ter uma visão por função e por região. ■ Com a exibição organizacional padrão, todos os recursos têm escopo e estão seguros nesta exibição. Os recursos (gerenciados e não gerenciados) são agrupados por tipo e a participação do recurso é dinâmica. ■ A participação do recurso na exibição padrão do sistema é atualizada dinamicamente e definida em um intervalo de atualização de 5 minutos. Dependendo de como você planeja a criação e a participação dos recursos de sua estrutura organizacional, mantenha isso em mente quando identificar o impacto geral de atualizações da participação de recursos.

Item	Considerações de planejamento
Filtros	■ Os filtros são conceitualmente semelhantes às coleções do Notification Server 6. Eles são implementados de maneira diferente, pois são aplicados aos destinos, não às políticas. Eles são recursos unidos por um conjunto definido de critérios. ■ Os filtros devem ser criados de um único atributo. Os filtros podem ser combinados para criar destinos complexos e com a utilização de menos critérios você obterá uma maior possibilidade de reutilização e menor complexidade, resultando em um Notification Server mais eficiente.
Destinos	■ Os destinos são a intersecção de grupos organizacionais e filtros. Por exemplo, computadores no Financeiro (Grupo) que têm menos do que o 1 GB de RAM (Filtro). ■ Os destinos são aplicados a políticas e tarefas e podem ser criados com antecedência ou no momento da aplicação. ■ Os destinos apenas podem conter os recursos aos quais o criador de destino tem acesso. Eles não são visíveis como objetos em nenhum local no console, mas são acessíveis usando a opção Aplicar rapidamente em uma tarefa ou política.

Para configurar filtros e destinos de recursos

Este capítulo contém os tópicos a seguir:

- [Sobre filtros de recursos](#)
- [Criação ou modificação de um filtro](#)
- [Execução de ações em recursos do filtro](#)
- [Exibição das dependências do filtro](#)
- [Sobre destinos de recursos](#)
- [Agendamento de atualizações da participação em recursos](#)

Sobre filtros de recursos

Um filtro, também conhecido como filtro de recursos, é uma definição dinâmica de um conjunto de recursos. Os recursos podem ser agrupados por alguns parâmetros especificados e também podem ser explicitamente incluídos ou excluídos de um filtro. Um filtro normalmente isola apenas um aspecto de um recurso, como seu sistema operacional, o espaço disponível em disco ou RAM. Filtros são usados com grupos organizacionais para identificar os recursos (destinos de recurso) aos quais uma tarefa ou uma política se aplica.

Consulte [“Sobre destinos de recursos”](#) na página 367.

Um filtro não contém nenhum recurso específico. Todos os recursos estão contidos nos grupos organizacionais configurados nas exibições organizacionais. Os grupos e as exibições organizacionais são os mesmos que são usados para a segurança do recurso. Um filtro opera em uma exibição ou grupo organizacional específico para identificar os recursos apropriados. Consequentemente, os filtros são portáteis

e podem ser aplicados a qualquer exibição ou grupo organizacional e podem ser usados com outros filtros. Por exemplo, você pode aplicar uma política a todos os computadores com Windows XP em um departamento específico de sua organização. Neste caso, para selecionar apenas os computadores nos quais é executado o Windows XP, é possível aplicar um filtro ao grupo organizacional que representa o departamento apropriado.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Criação ou modificação de um filtro

Você pode criar um filtro novo do zero ou clonar um filtro existente e modificá-lo para satisfazer seus requisitos. Você pode modificar qualquer filtro que criar ou em que tiver permissão para gravar. Você não pode modificar nenhum dos filtros padrão que são fornecidos com o Notification Server. Você não pode modificar nenhum filtro que é adicionado por replicação de hierarquia de um Notification Server pai. Somente os filtros que forem criados em seu Notification Server podem ser editados localmente.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Você também pode criar um filtro salvando um relatório. Um filtro criado dessa maneira é um filtro estático e não tem nenhuma consulta. A participação em filtro é uma lista fixa de inclusões que é determinada quando o filtro é criado. Você pode modificar um filtro estático adicionando inclusões ou exclusões que possam ser filtros dinâmicos. Porém, você não pode adicionar uma consulta diretamente a um filtro estático.

Consulte [“Para criar um filtro estático dos resultados do relatório do Notification Server”](#) na página 447.

Tabela 23-1 Processo para criar ou modificar um filtro

Etapa	Ação	Descrição
Etapa 1	Crie um filtro novo ou selecione um filtro existente para modificar.	Você pode criar um filtro novo do zero ou modificar um filtro existente para satisfazer seus requisitos. Consulte “Para criar um novo filtro” na página 357. Consulte “Para modificar um filtro existente” na página 357.

Etapa	Ação	Descrição
Etapa 2	Selecione o tipo de consulta.	Esta etapa aplica-se somente a um filtro novo. Você não pode mudar o tipo de consulta quando modifica um filtro existente. Se deseja criar um filtro dinâmico, você precisa selecionar o tipo apropriado de consulta. Se você não escolhe nenhuma consulta, a participação em filtro é composta pelas inclusões e exclusões especificadas. Consulte “Para selecionar o tipo de consulta de filtros” na página 358.
Etapa 3	Especifique a consulta a ser usada.	Você mesmo pode escrever a consulta SQL ou usar o Criador de consulta para criar a consulta de filtro. O Criador de consultas é uma ferramenta simples que permite selecionar as tabelas e os campos que você quer usar. Ele ajuda a definir a consulta para satisfazer a seus requisitos. Consulte “Para definir uma consulta de recursos para um filtro” na página 359. Consulte “Para definir uma consulta SQL para um filtro” na página 361.
Etapa 4	Especifique as inclusões e as exclusões.	Você pode especificar recursos ou filtros específicos para incluir ou excluir no filtro. Os filtros que você inclui ou exclui podem conter filtros adicionais. Você pode selecionar entre os recursos e os filtros que estão disponíveis no CMDB e importar recursos de um arquivo CSV. Consulte “Para especificar inclusões e exclusões de filtros” na página 362.
Etapa 5	Verifique a configuração do filtro visualizando a participação em filtro.	A associação de um filtro é determinada executando a consulta do filtro no CMDB para extrair os recursos apropriados. Você pode atualizar a associação para verificar se o filtro está corretamente definido. Consulte “Para atualização a associação de um filtro” na página 364.
Etapa 6	Salve o filtro.	Você pode salvar a nova definição do filtro ou a definição modificada do filtro. Depois que um filtro novo é salvo, você não pode mudar seu tipo de consulta. Consulte “Para criar um novo filtro” na página 357. Consulte “Para modificar um filtro existente” na página 357.

Para criar um novo filtro

Você pode criar novos filtros que sejam necessários e pode especificar a consulta, as inclusões e as exclusões para definir a participação desejada.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para criar um filtro novo

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta para a qual você deseja adicionar o filtro novo e clique em **Novo(a) > Filtro**.
- 3 No painel direito, especifique o nome e a descrição do filtro.
- 4 Selecione o tipo de consulta.

Consulte [“Para selecionar o tipo de consulta de filtros”](#) na página 358.

- 5 Execute uma das seguintes ações:

Defina a consulta	Consulte “Para definir uma consulta de recursos para um filtro” na página 359. Consulte “Para definir uma consulta SQL para um filtro” na página 361.
Especifique todas as inclusões e exclusões necessárias	Consulte “Para especificar inclusões e exclusões de filtros” na página 362.
Atualize a participação em filtro	Consulte “Para atualização a associação de um filtro” na página 364.

- 6 Clique em **Salvar alterações**.

Para modificar um filtro existente

Você pode modificar qualquer filtro que criar ou em que tiver permissão para gravar. Você não pode modificar nenhum dos filtros padrão que são fornecidos com o Notification Server. Você não pode modificar nenhum filtro que é adicionado por replicação de hierarquia de um Notification Server pai. Somente os filtros que foram criados em seu Notification Server podem ser editados localmente. A única ação que você pode executar em um filtro somente leitura é atualizar a participação em filtro.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Se deseja modificar um filtro somente leitura, clone-o para criar um filtro novo e então modifique o filtro novo para satisfazer seus requisitos. Quando modifica um filtro, você pode modificar a consulta do filtro e as inclusões ou exclusões específicas, mas não pode mudar o tipo de consulta.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para modificar um filtro existente

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja modificar.
- 3 (Opcional) No painel direito, mude o nome do filtro e a descrição.
- 4 No canto superior direito, clique em **Editar**.

Se a opção Editar está indisponível, o filtro é somente leitura e você não pode modificá-lo.

- 5 Execute uma das seguintes ações:

Modifique a consulta

Consulte [“Para definir uma consulta de recursos para um filtro”](#) na página 359.

Consulte [“Para definir uma consulta SQL para um filtro”](#) na página 361.

Modifique as inclusões e exclusões

Consulte [“Para especificar inclusões e exclusões de filtros”](#) na página 362.

Atualize a participação em filtro

Consulte [“Para atualização a associação de um filtro”](#) na página 364.

- 6 Clique em **Salvar alterações**.

Para selecionar o tipo de consulta de filtros

Quando cria um filtro novo, você precisa especificar o tipo de consulta para usar. Você pode usar o Criador de consulta para definir a consulta do filtro ou você mesmo pode escrever a consulta SQL. Você também pode escolher não ter nenhuma consulta no filtro. Você não pode mudar o tipo de consulta depois que o filtro for salvo.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para selecionar o tipo de consulta do filtro

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta para a qual você deseja adicionar o filtro novo e clique em **Novo(a) > Filtro**.
- 3 Na página **Novo filtro**, na lista suspensa **Definição do filtro**, selecione o tipo de consulta que você quer usar:

Nenhum	O filtro não usa uma consulta. As inclusões e exclusões de recursos e filtros específicos definem a participação em filtro.
Criador de consulta	Use o Criador de consulta para construir a consulta do filtro. O Criador de consulta é uma ferramenta simples que permite selecionar as tabelas e os campos que você quer usar. Ele ajuda a definir a consulta para satisfazer a seus requisitos. Consulte “Para definir uma consulta de recursos para um filtro” na página 359.
SQL bruta	Escreva sua própria consulta SQL. Por exemplo, convém copiar uma consulta de outro filtro ou relatório e modificá-la para satisfazer seus requisitos. Consulte “Para definir uma consulta SQL para um filtro” na página 361.

Para definir uma consulta de recursos para um filtro

Uma consulta de recursos é baseada nas tabelas que estão disponíveis no CMDB. O Criador de consulta é uma ferramenta simples que fornece um modelo padrão e permite selecionar as tabelas e os campos que você deseja usar. Ele ajuda a definir a consulta para satisfazer a seus requisitos. Você não precisa de nenhum conhecimento em SQL para definir uma consulta de recursos. A consulta de recursos é convertida em SQL automaticamente e o SQL é executado no CMDB para extrair os recursos apropriados.

Consulte [“Para selecionar o tipo de consulta de filtros”](#) na página 358.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para definir uma consulta de recursos para um filtro

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja modificar.
- 3 No painel direito, no painel **Definição do filtro**, especifique os detalhes da consulta de recursos nas guias apropriadas.

Consulta	A sintaxe de consulta de recursos. Consulte "Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta " na página 530.
Campos	Os campos e os atributos da classe de dados para usar na consulta. Consulte "Página de edição do relatório personalizado: guia Fonte de dados : guia Campos " na página 533.
Parâmetros da consulta	Os parâmetros que são usados na consulta. Esses são parâmetros internos para uso do SQL, não parâmetros do usuário. Parâmetros não são usados geralmente em consultas de filtro, mas podem ser úteis para obter as informações do registro. Por exemplo, um número de versão do agente para um upgrade. Consulte "Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta " na página 535.
Expressões do filtro	As instruções condicionais que são usadas para refinar mais os resultados da consulta. Cada instrução ou instrução agrupada pode ser considerada um filtro. Você precisa criar as instruções que deseja usar e agrupá-las de maneira apropriada. Consulte "Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro " na página 536.
Consulta resolvida	O código do SQL que é executado no CMDB para extrair os resultados do filtro. Consulte "Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida " na página 538.

Para definir uma consulta SQL para um filtro

Você pode gravar uma consulta SQL para definir os recursos que deseja incluir no filtro. Você pode gravar o código SQL do zero. Como alternativa, você pode copiar o SQL de outro filtro ou relatório e modificá-lo para satisfazer seus requisitos. Por exemplo, você pode criar uma consulta de recursos usando o Criador de consulta e copiar o SQL gerado da guia Consulta resolvida. Também é possível usar o Criador de consulta para definir a estrutura básica de sua consulta, convertê-la para SQL e modificá-la diretamente no SQL para criar a consulta desejada.

Você precisa do privilégio Editar SQL para criar ou modificar consultas SQL e ter boa compreensão sobre a estrutura da tabela do CMDB.

Consulte [“Para selecionar o tipo de consulta de filtros”](#) na página 358.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para definir uma consulta SQL para um filtro

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja modificar.

- 3 No painel direito, no painel **Definição do filtro**, especifique os detalhes da consulta SQL nas guias apropriadas.

Consulta com parâmetros	O código SQL para a consulta. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta parametrizada” na página 534.
Parâmetros da consulta	Os parâmetros que são usados na consulta. Esses são parâmetros internos para uso do SQL, não parâmetros do usuário. Parâmetros não são usados geralmente em consultas de filtro, mas podem ser úteis para obter as informações do registro. Por exemplo, um número de versão do agente para um upgrade. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta” na página 535.
Consulta resolvida	O código do SQL que é executado no CMDB para extrair os resultados do filtro. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida” na página 538.

- 4 Clique em **Salvar alterações**.

Para especificar inclusões e exclusões de filtros

Você pode especificar recursos ou filtros específicos para incluir ou excluir no filtro. Os filtros que você inclui ou exclui podem conter filtros adicionais. Você pode selecionar recursos e filtros da lista dos disponíveis no CMDB e também pode importar recursos de um arquivo .csv.

Se você importar recursos de um arquivo .csv, o arquivo pode identificar um computador pelo nome, nome de domínio totalmente qualificado ou pelo endereço IP. Todo item que não for encontrado no CMDB será ignorado.

A participação em filtro é determinada adicionando as inclusões aos resultados da consulta e depois removendo as exclusões. Os filtros e os recursos não têm nenhuma diferença em prioridade.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte “[Criação ou modificação de um filtro](#)” na página 355.

Para especificar recursos a serem incluídos ou excluídos

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja modificar.
- 3 No painel direito, no painel **Definição do filtro**, em **Inclusões e exclusões explícitas**, realize uma das seguintes tarefas:

Para incluir recursos selecionados	1	Em Inclusões , clique em Selecione um recurso .
	2	Na janela Selecionar recursos , selecione os recursos que você deseja incluir e clique em OK .
Para incluir os recursos listados em um arquivo	1	Em Inclusões , clique em Importar de um arquivo .
	2	Na janela Selecionar arquivo para importar , selecione o arquivo .CSV apropriado e clique em Abrir .
Para excluir recursos selecionados	1	Em Exclusões , clique em Selecione um recurso .
	2	Na janela Selecionar recursos , selecione os recursos que você deseja excluir e clique em OK .
Para excluir os recursos listados em um arquivo	1	Em Exclusões , clique em Importar de um arquivo .
	2	Na janela Selecionar arquivo para importar , selecione o arquivo .CSV apropriado e clique em Abrir .

Os recursos selecionados são relacionados ao lado dos campos apropriados.

Para especificar filtros a serem incluídos ou excluídos

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja modificar.
- 3 No painel direito, no painel **Definição do filtro**, em **Inclusões e exclusões explícitas**, realize uma das seguintes tarefas:

Para incluir filtros selecionados	1	Em Inclusões , clique em Selecionar um filtro .
	2	Na janela Selecionar filtros , selecione os filtros que você deseja incluir e clique em OK .
Para excluir filtros selecionados	1	Em Exclusões , clique em Selecionar um filtro .
	2	Na janela Selecionar filtros , selecione os filtros que você deseja excluir e clique em OK .

Os filtros selecionados são relacionados ao lado dos campos apropriados.

Para atualização a associação de um filtro

A associação de um filtro é determinada executando a consulta do filtro no CMDB para extrair os recursos apropriados. Para manter a associação de filtro atualizada conforme mudam as informações dos recursos no CMDB, é necessário atualizar a associação em intervalos apropriados. Você pode usar as atualizações agendadas do filtro para atualizar a associação de filtro ou executar a atualização manualmente em momentos apropriados. Por exemplo, quando você cria ou modifica um filtro, pode atualizar a associação para verificar se o filtro está corretamente definido.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Consulte [“Agendamento de atualizações da participação em recursos”](#) na página 368.

O painel Associação de filtro na página *Nome do filtro* mostra detalhes dos recursos em seu escopo que são identificados atualmente como membros do filtro. A participação em filtro pode ser diferente para funções de usuário diferentes. Somente os recursos para os quais o usuário tem permissão de leitura são visíveis a esse usuário. Porém, quando um usuário atualiza manualmente a associação de um filtro, a consulta do filtro é executada em todos os recursos no CMDB. O console restringe os resultados para mostrar somente os recursos que estão dentro do escopo de visualização do usuário.

Esta tarefa é uma etapa do processo de criação ou modificação de um filtro.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Para atualizar a associação de um filtro

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro para o qual você quer atualizar a associação.
- 3 No painel direito, no painel **Participação em filtro**, execute um destes procedimentos:

Para atualizar imediatamente a participação em filtro

Clique em **Atualizar participação**.

Para atualizar a participação em filtro usando as agendas de atualização do filtro

Clique em **Atualizar participação > Automático**.

Para permitir somente atualizações manuais da participação em filtro

Clique em **Atualizar participação > Manual**.

Esta opção desativa as atualizações agendadas da associação de filtro. Por exemplo, o filtro contém uma consulta complexa que você quer executar somente quando necessário.

Execução de ações em recursos do filtro

Você pode executar ações em recursos selecionados do filtro. Estas opções são iguais às que estão disponíveis no menu contextual (menu de clique com o botão direito do mouse). As ações disponíveis dependem do tipo de recurso que é selecionado; assim, algumas opções podem não estar disponíveis para todos os recursos.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Para executar uma ação em um recurso do filtro

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro que você deseja usar.

- 3 No painel direito, no painel **Participação em filtro**, selecione o recurso em que deseja executar uma ação.
- 4 Clique em **Ações** e clique na opção apropriada:

Gerenciador de recursos	Abre o recurso no Console do gerenciador de recursos.
Exportar	Exporta o recurso para um arquivo XML.
Propriedades	Exibe as propriedades do recurso.
Definir o status do ativo > Ativo	Define o status de um ativo a Ativo. Esta configuração é relevante para a solução do Ativo.
Definir o status do ativo > Removido	Define o status de um ativo a Removido. Esta configuração é relevante para a solução do Ativo.
Adicionar a grupo organizacional	Atribui o recurso a um grupo organizacional.
Excluir	Exclui o recurso do filtro.
Tarefa de gerenciamento de energia	Agende ou execute a tarefa de gerenciamento de energia.

Exibição das dependências do filtro

Antes de modificar um filtro, convém descobrir a relação de dependência de outros filtros em relação a esse que será alterado. Você pode exibir uma lista de todos os filtros, destinos, tarefas e políticas que usam um filtro específico.

Consulte [“Sobre filtros de recursos”](#) na página 354.

A lista de dependências contém todos os destinos que incluem o filtro especificado diretamente ou em um filtro incluído. A lista contém também todas as políticas e tarefas que são aplicadas àqueles destinos. A inclusão do filtro no destino define a dependência. A dependência não significa necessariamente que a política ou a tarefa estão aplicadas atualmente a recursos no filtro.

Para exibir as dependências de um filtro

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Filtros**.
- 2 No painel esquerdo, clique no filtro do qual deseja exibir dependências.
- 3 No painel direito, no painel **Participação em filtro**, clique em **Referenciado por**.

- 4 Na caixa de diálogo **Itens aplicados a este filtro**, veja a lista dos filtros, dos destinos, das tarefas e das políticas que usam o filtro.
- 5 Clique em **Fechar**.

Sobre destinos de recursos

Um destino de recurso, geralmente conhecido como destino, é uma estrutura que permite aplicar tarefas e diretivas a uma coleção dinâmica de recursos. Um destino consiste em ao menos uma exibição ou grupo organizacional e em um grande número de filtros. Os filtros refinam os recursos disponíveis para identificar aqueles que você quer. A exibição ou o grupo organizacional atuam como um filtro de segurança. Isso assegura que a diretiva ou a tarefa seja aplicada apenas a recursos com os quais a função de segurança do usuário permite que ele trabalhe.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Os destinos são armazenados em cache no CMDB e avaliados dinamicamente quando a tarefa ou a diretiva são executadas. O destino é avaliado em relação ao escopo do usuário atual. Apenas os recursos que aparecem na exibição ou no grupo organizacional ou nos filtros são retornados. O destino inclui apenas os recursos aos quais o usuário tem acesso de leitura. Os recursos fora do escopo do usuário atual nunca são visíveis.

Os filtros do sistema que são fornecidos com o Notification Server contêm apenas recursos gerenciados, mas destinos, exibições e grupos organizacionais podem conter recursos não gerenciados. Você também pode criar seus próprios filtros personalizados que incluem recursos não gerenciados. Porém, quando você aplicar um destino a uma diretiva ou a uma tarefa, apenas os computadores gerenciados no destino poderão solicitar a diretiva ou executar a tarefa.

Há dois tipos de destinos que você pode aplicar a uma diretiva ou a uma tarefa:

Destinos de recurso
autogerados

Estes são os destinos que não foram explicitamente nomeados e salvos. Os destinos autogerados são usados apenas pela diretiva ou pela tarefa na qual você os cria. Por exemplo, se você usar a opção **Aplicar rapidamente** para selecionar um filtro ou a caixa de diálogo **Selecionar recursos** para selecionar um conjunto de recursos, o destino correspondente será criado e adicionado à diretiva ou à tarefa. É dado um nome padrão ao destino autogerado com base no grupo organizacional, no filtro ou no conjunto de recursos que ele contém.

Você pode editar estes destinos quando você modifica a diretiva ou a tarefa, mas você não pode aplicá-los a nenhuma outra diretiva ou tarefa.

Destinos de recurso nomeados

Estes são destinos que foram explicitamente salvos como destinos de recurso nomeados. Os destinos nomeados podem ser aplicados a qualquer número de tarefas e de diretivas e podem ser modificados por qualquer usuário que tiver as permissões adequadas.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Agendamento de atualizações da participação em recursos

Você pode manter todos os seus filtros de recursos, grupos organizacionais e destinos de recursos atualizados configurando os agendamentos apropriados de atualização de filtros. Estes agendamentos permitem atualizar os filtros, grupos organizacionais e os destinos de que você precisa em intervalos adequados. Esses agendamentos ajudam a gerenciar a carga de processamento imposta no Notification Server.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Os agendamentos predefinidos de atualização da participação em recursos são fornecidos com o Symantec Management Platform. Esses agendamentos são apropriados para a maioria das finalidades e você não deve precisar alterá-los. Porém, como os requisitos de sua organização mudam, você pode fazer as alterações necessárias.

Tabela 23-2 Agendamentos de atualização da participação em recursos

Agendar	Descrição
Agendamento de atualização delta	Atualiza a participação dos seguinte recursos: ■ Filtros que tiveram alterações de participação desde a última atualização. ■ Todos os grupos organizacionais dinâmicos. ■ Todos os destinos inválidos. Um destino pode ser invalidado pelos seguintes eventos: ■ Sua definição é salva. ■ Um filtro usado que tem alterações de participação. ■ Um grupo organizacional usado que tem alterações de participação. ■ A segurança aplicada a um grupo organizacional usado é alterada. Por padrão, esse agendamento é executado a cada cinco minutos.
Agendamento de atualização completa	Recria completamente a participação em todos os filtros, grupos organizacionais e destinos, independentemente do status do inventário ou de todas as alterações nas políticas. A atualização completa pode impor uma carga significativa ao Notification Server e deve ser agendada de maneira apropriada. Por padrão, esse agendamento é executado uma vez por dia.
Agendamento de atualização de política	Atualiza a participação dos filtros usados por uma política, caso a política tenha sido alterada desde a última atualização. Este agendamento garante que quando você atualiza ou cria uma política, todos os filtros incluídos nos destinos novos ou modificados da política são atualizados automaticamente. Por padrão, esse agendamento é executado a cada cinco minutos.

Consulte [“Componentes de um agendamento do Symantec Management Platform”](#) na página 119.

Consulte [“Para exibir do calendário de agendamento interno do Notification Server”](#) na página 124.

Para configurar os agendamentos de atualização da participação em recursos

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Notification Server > Atualização da associação a recurso**.
- 2 Na página Atualização de participação em recursos, configure os agendamentos de atualização que você deseja usar.
Consulte "[Especificação de um agendamento de política](#)" na página 388.
- 3 Se deseja executar imediatamente um agendamento de atualização, no painel apropriado, clique em **Executar**.
Por exemplo, você pode garantir que todas as alterações em seus filtros entrem em vigor imediatamente, em vez de aguardar até a atualização agendada.
- 4 Clique em **OK**.

Para configurar pacotes

Este capítulo contém os tópicos a seguir:

- [Alteração das configurações de um pacote](#)
- [Atualização dos pontos de distribuição para um pacote](#)
- [Como ativar o acesso a um pacote em um local de origem do UNC](#)
- [Gerenciamento de programas do pacote](#)

Alteração das configurações de um pacote

Um pacote inclui um conjunto de arquivos que podem ser fornecidos a um recurso gerenciado. Por exemplo, o pacote do Symantec Management Agent inclui o arquivo AeXClientUpgrade.exe. O arquivo AeXClientUpgrade.exe instala o agente nos recursos gerenciados.

A página **Pacote** permite definir as configurações do pacote, como a fonte do pacote, local do pacote e como o pacote é executado.

Para alterar as configurações de um pacote

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, selecione o pacote que você deseja modificar.

- 3 Na página **Pacote**, faça as mudanças de configuração necessárias nas guias apropriadas:

Pacote

Programas Consulte "[Gerenciamento de programas do pacote](#)" na página 374.

Servidores de pacotes

Avançadas

- 4 Clique em **Salvar alterações** para confirmar as configurações novas.
 Você precisa atualizar os pontos de distribuição de pacotes para atualizar as informações do pacote em cada servidor de pacotes.
 Consulte "[Atualização dos pontos de distribuição para um pacote](#)" na página 372.

Atualização dos pontos de distribuição para um pacote

Os pontos de distribuição de pacotes são os locais onde o pacote é armazenado, como locais dos servidores de pacotes ou da fonte de UNC. As informações em cada pacote estão contidas em um arquivo XML armazenado com o pacote. Estas informações devem ser atualizadas sempre que o pacote é modificado. O Notification Server e os servidores de pacotes usam estas informações para fornecer os arquivos apropriados quando um computador gerenciado solicita o pacote. As informações do pacote são atualizadas de acordo com um agendamento, mas você poderá executar uma atualização manual quando for necessário. Por exemplo, é possível manualmente atualizar os pontos de distribuição para que um pacote modificado tenha imediatamente as informações do pacote atualizadas em todos os seus pontos de distribuição.

Consulte "[Alteração das configurações de um pacote](#)" na página 371.

Você pode atualizar pontos de distribuição de um pacote no catálogo de software ou de um pacote que seja acessado do menu **Configurações**.

Para atualizar os pontos de distribuição de pacotes para um pacote no catálogo de software

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Catálogo de software**.
- 2 Na janela **Catálogo de software**, execute uma das seguintes ações:

- Para componente de software indefinido, na lista **Software recém-descoberto/indefinido**, selecione-o e clique no símbolo de **Edit**. Se o componente de software indefinido não estiver na lista, clique em **Show all software**, na parte inferior da lista.
 - Para um componente de software definido, localize o produto de software ao qual o componente de software está associado na lista **Produtos de software gerenciados** ou **Software não gerenciado**. Depois, clique no sinal de **Plus** que precede o produto de software e, em seguida, clique no link do componente de software que aparece abaixo do produto de software.
- 3 Na página de recursos de software, na guia **Pacote**, no painel **Pacotes**, clique no pacote em que você deseja atualizar os pontos de distribuição.
 - 4 Clique em **Ações > Atualizar pontos de distribuição**.

Para atualizar os pontos de distribuição de pacotes de um pacote acessado do menu **Configurações**

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, selecione o pacote em que você deseja atualizar os pontos de distribuição.
- 3 Na página **Pacote**, na parte inferior da página, clique em **Atualizar pontos de distribuição**.

Como ativar o acesso a um pacote em um local de origem do UNC

O Symantec Management Agent usa as credenciais da conectividade do agente (ACC) para se conectar ao IIS no Notification Server para fazer o download de pacotes de UNC com HTTP. O IIS autentica então a origem do UNC usando as credenciais do ponto de distribuição (DPC). O Symantec Management Agent usa o ACC para se conectar e fazer o download de origens. Certifique-se de que o ACC tenha acesso de leitura quando o Symantec Management Agent for obtido por download diretamente da origem do pacote de UNC.

O DPC não será usado se o Symantec Management Agent fizer o download de um pacote de um servidor de pacotes. O servidor de pacotes aplica qualquer acesso anônimo ou o ACC aos arquivos de pacote obtidos por download.

Para ativar o acesso a um pacote em um local de origem do UNC

- 1 Especifique as credenciais do ponto de distribuição de pacotes que você deseja usar.

Você especifica estas credenciais na guia **Credenciais de ponto de distribuição** da página **Configurações do Notification Server**.

Recomendamos selecionar **Usar credencial de conectividade do agente** ao especificar as credenciais do ponto de distribuição de pacotes. Esta opção assegura que apenas uma credencial, a ACC, precise existir nos locais de origem do pacote do UNC.

Consulte [“Configurações da credencial de ponto de distribuição”](#) na página 74.

- 2 Forneça acesso de leitura a essas credenciais na pasta de origem do UNC.

Gerenciamento de programas do pacote

Um pacote pode ter mais de um programa. Você pode gerenciar os programas em um pacote para atender a seus requisitos. Você pode alterar detalhes do programa, adicionar programas novos ao pacote e excluir todos os programas que não são mais necessários.

Consulte [“Alteração das configurações de um pacote”](#) na página 371.

Para exibir detalhes de um programa do pacote

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, selecione o pacote que você deseja modificar.
- 3 Na página Pacote, na guia **Programas**, selecione o programa que você deseja exibir

Para criar um novo programa no pacote

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, selecione o pacote que você deseja modificar.
- 3 Na página Pacote, na guia **Programas**, clique em **Novo**.
- 4 Especifique os detalhes do programa nos campos apropriados.
- 5 Clique em **Aplicar**.

Para remover um programa de um pacote

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, selecione o pacote que você deseja modificar.
- 3 Na página Pacote, na guia **Programas**, selecione o programa que você deseja remover e clique em **Excluir**.
- 4 Clique em **Aplicar**.

Para usar políticas

Este capítulo contém os tópicos a seguir:

- Sobre políticas do Symantec Management Platform
- Sobre políticas baseadas em usuário
- Gerenciamento de políticas do Symantec Management Platform
- Para aplicar uma política usando o recursos de arrastar e soltar
- Especificação dos destinos de uma política ou tarefa
- Modificação de um destino de recurso
- Como criar um alvo do recurso
- Seleção de um destino de recurso existente
- Como salvar um destino de recurso nomeado
- Especificação de regras de filtragem para destinos de recurso
- Seleção de destinos de recurso nomeados
- Especificação de um agendamento de política
- Para configurar as políticas de instalação, de upgrade e de desinstalação do agente/plug-in
- Sobre as políticas de automação
- Componentes-chave das políticas de automação
- Gerenciamento de políticas de automação
- Criação ou modificação de políticas de automação agendadas
- Criação ou modificação de políticas de automação baseadas em mensagens

- [Para criar e modificar tarefas de política de automação](#)

Sobre políticas do Symantec Management Platform

Uma política do Symantec Management Platform é um conjunto de regras que se aplicam a um recurso ou a um conjunto de recursos (conhecidos como o destino da política). Uma política pode ser avaliada com base em uma agenda ou em dados de entrada. Quando uma política é avaliada, a ação apropriada é tomada. Esta ação inclui tipicamente tarefas em execução nos recursos de destino para assegurar que todos cumpram a política.

Tabela 25-1 Tipos comuns de políticas do Symantec Management Platform

Tipo de política	Descrição
Agente	Especifica as configurações do Symantec Management Agent em computadores-cliente. Consulte “Para configurar o Symantec Management Agent” na página 276.
Automação	Especifica ações automatizadas a serem executadas em computadores-cliente ou no computador do Notification Server. Estas políticas são dinâmicas. Elas visam os computadores apropriados quando a política é ativada e executam a ação que for necessária com base no estado atual de cada computador de destino. Os destinos da política de automação podem ser baseados nos resultados do relatório ou em uma consulta, em vez de basearem-se em filtros e destinos de recursos como em outros tipos de políticas. Consulte “Sobre as políticas de automação” na página 392.
Usuário	Especifica as configurações que se aplicam a usuários específicos. Estas configurações são aplicadas aos computadores em que os usuários estão conectados. Consulte “Sobre políticas baseadas em usuário” na página 377.
Solução	As soluções podem fornecer suas próprias políticas que são dirigidas a computadores ou usuários dessas soluções.

Sobre políticas baseadas em usuário

As políticas baseadas em usuário podem ser aplicadas a usuários específicos ou grupos de usuários. Elas também podem (mas não necessariamente) ser aplicadas a computadores específicos.

Consulte [“Sobre políticas do Symantec Management Platform”](#) na página 377.

Por exemplo, algumas organizações têm um grande número de grupos de segurança do Active Directory e querem atribuir suas políticas usando estes grupos de segurança. Os grupos de segurança que contêm computadores gerenciados ou usuários são importados para o CMDB. Usar políticas com base no usuário permite ao administrador gerenciar computadores usando a infraestrutura existente do Active Directory. Grupos de trabalho e usuários locais são suportados.

As políticas baseadas em usuário serão aplicadas somente quando um usuário estiver conectado em um computador gerenciado. Essas políticas são aplicadas somente ao usuário que faz logon na sessão do console. Cada vez que um usuário fizer logon em um computador gerenciado, o Symantec Management Agent buscará as políticas com base no usuário que se aplicarem a esse usuário. As políticas são armazenadas em cache no computador por uma semana. O Symantec Management Agent executa também solicitações regulares de configuração para todas as políticas ativas que usam o SID do usuário atualmente conectado, além do GUID do computador gerenciado, para receber políticas com base no usuário e no computador. O agente fará esta solicitação na primeira vez que o usuário fizer logon em um computador gerenciado. O agente repetirá a solicitação sempre que executar sua solicitação normal de configuração.

Nota: Os usuários que fizerem logon em computadores gerenciados pelos serviços de terminal não receberão as políticas destinadas a eles. Todos os usuários vêm as políticas que se aplicam ao usuário que fez logon na sessão do console.

Talvez você queira excluir alguns computadores ou usuários das políticas baseadas no usuário. Por exemplo, um computador gerenciado compartilhado por muitos usuários ou um administrador que pode fazer logon em muitos computadores diferentes a cada dia. Se tal computador ou usuário era um destino para uma política baseada em usuário, as alterações orientadas por políticas frequentes poderiam impor uma sobrecarga significativa aos computadores afetados.

Você pode criar uma lista de computadores aos quais as políticas com base no usuário não se aplicam. Você pode criar uma lista de usuários a quem as políticas com base no usuário não devem ser direcionadas. Você pode usar essas listas como exclusões nos filtros apropriados.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Consulte [“Criação ou modificação de um filtro”](#) na página 355.

Gerenciamento de políticas do Symantec Management Platform

A exibição Políticas coleta todas as políticas disponíveis em uma única estrutura de pastas. Esta estrutura padrão permite facilmente acessar as políticas que deseja exibir ou modificar.

Consulte [“Sobre políticas do Symantec Management Platform”](#) na página 377.

Consulte [“Sobre as políticas de automação”](#) na página 392.

Para gerenciar políticas

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas**.
- 2 No painel esquerdo, na pasta Políticas, selecione a política ou o grupo de políticas que você deseja gerenciar.

Para aplicar uma política usando o recursos de arrastar e soltar

Na exibição **Políticas**, você pode pesquisar, exibir e aplicar políticas. Esta exibição aprimorada tem um campo de pesquisa que permite encontrar rapidamente as políticas com as quais você quer trabalhar. Você pode procurar pelo nome ou pelo tipo da política.

Consulte [“Sobre a exibição Políticas ”](#) na página 43.

Você pode iniciar políticas arrastando-as e soltando-as em um ou mais computadores. Além disso, você pode usar a opção **Aplicar rapidamente** para visar uma política sem pesquisar manualmente.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Nota: Você deve ter uma das seguintes soluções ou séries instaladas para executar esta tarefa: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para aplicar uma política usando o recurso de arrastar e soltar

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Políticas**.
- 2 No painel de navegação, clique na política que você quer executar e arraste-a para a direita para iniciar a operação de arrastar e soltar.

Os resultados de sua pesquisa mais recente de computador aparecerão no painel de listas. Se você tiver filtrado sua pesquisa mais recente de computador, a lista exibirá os resultados da pesquisa filtrada.

Consulte [“Para pesquisar um computador e salvar a pesquisa como um filtro”](#) na página 38.
- 3 Para selecionar os computadores nos quais você quer executar a política, execute um destes procedimentos:
 - Para executar a política em todos os computadores relacionados, solte-a no ícone do título, no painel de listas.
 - Para executar a política em um computador específico, solte-a no computador na lista.
 - Para executar a política em uma pesquisa salva, exibição ou grupo organizacional, arraste-a para a blade **Computadores** e solte-a em uma pesquisa salva, em uma exibição ou um grupo organizacional
- 4 Na caixa de diálogo **Aplicar política**, clique em **OK**.

Especificação dos destinos de uma política ou tarefa

Você precisa especificar um ou mais destinos de uma política ou tarefa. Um destino define os computadores, usuários e recursos aos quais a política ou a tarefa se aplicam. Uma política ou uma tarefa podem ter vários destinos.

Você pode aplicar os seguintes tipos de destinos a uma política ou a uma tarefa:

Destinos de recurso
autogerados

Estes destinos não foram explicitamente nomeados e salvos. Os destinos autogerados são usados apenas pela política ou pela tarefa na qual você os cria. Você pode editar estes destinos quando você modificar a política ou a tarefa, mas você não poderá aplicá-los a nenhuma outra política ou tarefa.

Destinos de recurso nomeados

Estes destinos foram explicitamente salvos como destinos de recurso nomeados. Os destinos nomeados podem ser aplicados a qualquer número de tarefas e de políticas e podem ser modificados por qualquer usuário que tiver as permissões adequadas.

Consulte [“Como salvar um destino de recurso nomeado”](#) na página 384.

Os destinos não são mostrados como itens em nenhum lugar no Symantec Management Console. Porém, é possível usar a opção **Aplicar rapidamente** para selecionar destinos nomeados existentes que serão aplicados a uma política ou tarefa. Você também pode exibir a lista de destinos nomeados disponíveis na caixa de diálogo **Salvar como** quando você criar ou modificar um destino nomeado.

Consulte [“Sobre destinos de recursos”](#) na página 367.

Para especificar o destino de uma política ou de uma tarefa

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas**.
- 2 No painel esquerdo, na pasta Políticas, selecione a política ou o grupo de políticas que você deseja gerenciar.
- 3 Na página *Nome da política* ou na página *Nome da tarefa*, em **Aplica-se a/Conformidade**, clique em **Aplicar a** e, em seguida, clique em uma das seguintes opções:

Aplicar rapidamente	1 Na caixa de diálogo Aplicar rapidamente, na lista suspensa, selecione o destino nomeado, o grupo organizacional ou o filtro adequado. 2 (Opcional) Digite as primeiras letras do item que você quer. As opções na lista são reduzidas àquelas que correspondem à sua pesquisa. 3 Clique em Aplicar.

Computadores	Na janela Selecionar computadores, selecione os computadores que você quer. Consulte “Como criar um alvo do recurso” na página 383.

Usuários	Na janela Selecionar usuários, selecione os usuários que você quer. Consulte “Como criar um alvo do recurso” na página 383.

Recursos Na janela **Selecionar recursos**, selecione os recursos que você quer.

Consulte [“Como criar um alvo do recurso”](#) na página 383.

Note que algumas opções podem não estar disponíveis para todas as políticas.

Cada seleção é adicionada à lista de destinos na grade **Aplicar a**.

Repita esta etapa para adicionar quantos destinos quiser.

- 4 (Opcional) Na lista suspensa **View**, clique na opção apropriada: **Computadores e usuários**, **Applied by**, ou **Execuções de tarefas**.

A lista mostra somente os itens que foram claramente selecionados. Por exemplo, se visualizar os computadores, você poderá ver somente os computadores que selecionou na janela **Selecionar computadores**. Você não pode ver nenhum computador adicional contido nos destinos que selecionou na caixa de diálogo **Aplicar rapidamente**.

- 5 Se desejar modificar um destino ou excluí-lo da lista, selecione-o na grade **Aplica-se a/Conformidade** e, então, clique em **Editar** ou **Excluir**, o que for adequado.

Consulte [“Modificação de um destino de recurso”](#) na página 382.

- 6 Clique em **Salvar alterações**.

Modificação de um destino de recurso

Quando você modificar uma política ou uma tarefa, será possível modificar todos os destinos gerados automaticamente que ela contiver e quaisquer destinos de recurso nomeados a que você tiver acesso.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Consulte [“Gerenciamento de políticas do Symantec Management Platform”](#) na página 379.

Para modificar um destino de recurso

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas**.
- 2 No painel esquerdo, na pasta Políticas, selecione a política ou o grupo de políticas que você deseja gerenciar.
- 3 Na página *Nome da política* ou página *Nome da tarefa*, no painel **Aplica-se a/Conformidade**, na lista suspensa **View**, clique em **Computadores e usuários**.

- 4 Na grade **Aplica-se a/Conformidade**, selecione o destino que você deseja modificar.
 - 5 Clique em **Editar**.
 - 6 Na janela **Editar grupo selecionado**, faça as mudanças necessárias ao destino.
- Consulte [“Como criar um alvo do recurso”](#) na página 383.

Como criar um alvo do recurso

As janelas **Selecionar computadores**, **Selecionar usuários** e **Selecionar recursos** permitem selecionar os itens que você deseja incluir em um novo destino de recurso. A janela **Editar o grupo selecionado** permite alterar a seleção de um destino de recurso existente.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Para criar um destino de recurso

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas**.
- 2 No painel esquerdo, na pasta Políticas, selecione a política ou o grupo de políticas que você deseja gerenciar.
- 3 Na página *Nome da política* ou na página *Nome da tarefa*, no painel **Aplica-se a/Conformidade**, clique duas vezes no recurso que você quer gerenciar.
- 4 Se você quiser basear o destino do recurso em um destino nomeado existente, na caixa de diálogo **Adicionar destino**, clique em **Open** e, em seguida, na janela **Open** e selecione o destino apropriado.

Consulte [“Seleção de um destino de recurso existente”](#) na página 384.

- 5 Em **Regras de filtragem**, especifique as regras com que você deseja filtrar os computadores, usuários ou recursos disponíveis.

Consulte [“Especificação de regras de filtragem para destinos de recurso”](#) na página 385.

- 6 Se deseja salvar o destino de recurso como um destino nomeado, clique em **Gravar como**.

Consulte [“Como salvar um destino de recurso nomeado”](#) na página 384.

- 7 Quando a lista **Itens que atualmente correspondem às regras** mostrar os itens que você deseja incluir no destino, clique em **OK**.

O destino de recurso especificado é adicionado à política ou à tarefa. Se o destino for autogerado (um que não tenha sido salvo como um destino nomeado), é dado a ele um nome padrão baseado nos nomes dos grupos organizacionais e nos filtros usados.

Seleção de um destino de recurso existente

A caixa de diálogo **Abrir** permite selecionar um destino de recurso nomeado existente ou um grupo nomeado de destinos de recurso (que é um destino de recurso). Se você acessar esta caixa de diálogo através do Construtor do destino de recurso (janela geralmente chamada de **Selecionar recursos**) ou o Seletor do destino de recurso (geralmente chamado de janela **Selecionar um destino de recurso** ou **Selecionar um grupo**), o destino ou o grupo de destinos que você selecionar aqui substituirá a seleção atual na janela. Se você acessar esta caixa de diálogo através da janela do seletor dos recursos (**Selecionar computadores** ou **Selecionar recursos**), a participação de destino será adicionada à seleção atual na janela.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Consulte [“Como salvar um destino de recurso nomeado”](#) na página 384.

Para selecionar um destino de recurso existente

- 1 Nas janelas **Selecionar computadores/recursos**, **Selecionar um grupo** ou **Editar o grupo selecionado**, clique em **Abrir**.
- 2 Na caixa de diálogo **Abrir**, na lista de destinos de recurso nomeados ou de grupos, clique no destino adequado ou no grupo.
- 3 Clique em **OK**.

Como salvar um destino de recurso nomeado

Se deseja usar um destino de recurso em várias tarefas e políticas ou torná-lo disponível para outros usuários, será possível salvar o destino como um destino de recurso nomeado. Os destinos nomeados podem ser aplicados a qualquer número de tarefas e políticas. Qualquer usuário que tiver as permissões adequadas poderá acessar ou modificar quaisquer destinos nomeados que você criar. Você

também poderá salvar grupos nomeados de destinos de recurso quando apropriado, como para a inclusão nas regras de replicação.

Consulte “[Especificação dos destinos de uma política ou tarefa](#)” na página 380.

Consulte “[Seleção de destinos de recurso nomeados](#)” na página 386.

Consulte “[Seleção de um destino de recurso existente](#)” na página 384.

Se você acessar a janela **Gravar como** através do seletor do destino de recurso (geralmente chamado de janela **Selecionar destino dos recursos** ou **Selecionar um grupo**), será possível salvar os destinos de recurso selecionados como um grupo nomeado de destinos de recurso. Se você acessar a janela **Gravar como** através do construtor do destino de recurso (geralmente chamado de janela **Selecionar computadores** ou **Selecionar recursos**), será possível salvar os recursos selecionados (que poderão ser explicitamente especificados ou dinamicamente selecionados usando uma consulta) como um destino de recurso nomeado.

Para salvar um destino de recurso nomeado

- 1
- Na janela **Selecionar computadores/recursos**, na janela **Selecionar um grupo** ou **Editar o grupo selecionado**, clique em **Gravar como**.
- 2
- Na caixa de diálogo **Gravar como**, execute uma das seguintes ações:

Para criar um novo destino ou grupo	Na caixa Nome , digite o nome adequado para o destino ou grupo.
Para sobrescrever um destino ou um grupo existente	Na lista de destinos ou grupos nomeados, clique no nome adequado. Apenas os destinos ou os grupos aos quais você tem acesso para gravação são selecionáveis. Todos os destinos ou grupos somente leituras ficarão em cinza.

- 3
- Clique em **OK**.

Especificação de regras de filtragem para destinos de recurso

As regras de filtragem permitem filtrar computadores, usuários e recursos para identificar os itens que você deseja selecionar. As regras são aplicadas na ordem em que são listadas; assim, todos os itens excluídos podem ser incluídos novamente por uma regra posterior. A lista **Itens que atualmente correspondem às regras** mostra os itens selecionados pelas regras especificadas. A lista é atualizada automaticamente enquanto você adiciona e modifica as regras de filtragem.

Consulte “[Especificação dos destinos de uma política ou tarefa](#)” na página 380.

Para especificar uma regra de filtragem

- 1 Na janela **Selecionar itens**, em **Regras de filtragem**, clique em **Adicionar regra**.
- 2 Na primeira lista suspensa, clique na operação apropriada:

Excluir itens em	Exclui os itens que estão no filtro ou no grupo organizacional especificado ou recursos selecionados da lista de itens.
Excluir itens que não estejam em	Exclui os itens que não estão no filtro ou no grupo organizacional especificado ou recursos selecionados da lista de itens.

- 3 Na segunda lista suspensa, clique na opção apropriada:

Filtro	Aplicar a operação a um filtro específico.
Grupo	Aplicar a operação a um grupo organizacional específico.
Lista de itens	Aplicar a operação aos computadores, usuários ou recursos especificados.

- 4 Na terceira lista suspensa, selecione o item apropriado:

Para selecionar um filtro ou grupo	Digite as primeiras letras do filtro ou do grupo organizacional que você deseja. As opções na lista são reduzidas àquelas que correspondem à sua pesquisa.
Para selecionar itens específicos	Clique nas elipses (...) e depois, na janela Selecionar item , selecione os itens apropriados.

Para gerenciar a lista de regras de filtragem

- 1 Se você deseja mover para cima ou para baixo a lista de regras de filtragem, clique na seta para cima ou a seta para baixo.
- 2 Se você deseja remover uma regra de filtragem da lista, clique em **Excluir**.

Seleção de destinos de recurso nomeados

A janela **Selecionar destinos de recursos** ou **Selecionar um grupo** permite selecionar os destinos de recurso nomeados que você deseja usar. O painel

esquerdo exibe a lista de destinos de recurso disponíveis e o painel direito exibe a lista de destinos de recurso selecionados.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Você pode filtrar os destinos de recursos selecionados no painel esquerdo por exibição organizacional ou por um grupo organizacional específico. O filtro restringe a participação dos destinos selecionados aos recursos contidos na exibição ou no grupo organizacional especificado. Você também pode criar novos destinos de recurso nomeados.

Você precisa adicionar os destinos de recursos que deseja selecionar à lista de destinos de recursos no painel direito. Você também pode salvar os destinos de recurso selecionados como um grupo nomeado de destinos de recurso.

Para selecionar destinos de recurso nomeados

- 1 (Opcional) Se deseja filtrar a participação dos destinos de recurso selecionados por uma exibição ou por um grupo organizacional específico, na lista suspensa **Grupo**, selecione a exibição ou o grupo organizacional adequado.
- 2 (Opcional) Se você quiser criar um novo destino de recurso nomeado, clique em **Criar destino**.

Consulte [“Como criar um alvo do recurso”](#) na página 383.

- 3 No painel esquerdo, selecione os destinos de recurso que você quer e clique em > para adicioná-los à lista de destinos de recursos selecionados no painel direito.
- 4 (Opcional) Se você quer selecionar os destinos de recursos contidos em um grupo de destinos de recursos nomeado existente, clique em **Abrir** e, na caixa de diálogo **Abrir**, selecione o grupo adequado.

Consulte [“Seleção de um destino de recurso existente”](#) na página 384.

Os destinos de recursos no grupo selecionado são adicionados à lista no painel direito.

- 5 (Opcional) Se você quiser remover todos os destinos de recursos da lista de destinos selecionados, selecione os destinos de recursos apropriados e clique em <.
- 6 (Opcional) Se você quiser salvar os destinos de recurso como um grupo nomeado na lista de recursos selecionados para reutilização posterior, clique em **Gravar como** e, na caixa de diálogo **Gravar como**, especifique o nome apropriado.

Consulte [“Como salvar um destino de recurso nomeado”](#) na página 384.

- 7 Clique em **OK**.

Especificação de um agendamento de política

Você precisa especificar os horários em que uma política será acionada configurando os agendamentos apropriados. É possível especificar tantos agendamentos quanto precisar e ter qualquer quantidade de agendamentos ativos ao mesmo tempo.

Consulte [“Sobre políticas do Symantec Management Platform”](#) na página 377.

Este tópico aplica-se também a algumas outras agendas, como o agendamento da atualização de participação dos recursos. Algumas opções descritas aqui podem não estar disponíveis para todas as diretivas.

Para especificar uma agenda de diretiva

- 1 Na página da diretiva, em **Agenda**, clique em **Adicionar agenda** e clique em um dos seguintes itens:
- Horário agendado

1 Na caixa Iniciar, especifique o horário apropriado.

2 Se desejar que o agendamento seja repetido, clique em **Nenhuma repetição** e, na caixa de diálogo **Repetir agendamento**, especifique a frequência apropriada.

Janela Agendamento

1 Nas caixas Início, Fim e Duração, especifique os horários apropriados.

2 Na janela **Durante**, selecione todas as caixas e especifique o intervalo apropriado.

3 Se desejar que o agendamento seja repetido, clique em **Nenhuma repetição** e, na caixa de diálogo **Repetir agendamento**, especifique a frequência apropriada.

No login do usuário

A política será acionada quando um usuário fizer logon no computador gerenciado.

Na inicialização do computador

A política será acionada quando o computador gerenciado for iniciado.

Cada agendamento é adicionado à lista de agendamentos da política. Repita esta etapa para adicionar quantos agendamentos desejar.

2 Na lista suspensa **Fuso horário**, selecione o fuso horário apropriado:

Usar hora do agente	Os horários são especificados sem informações sobre o fuso horário e aplicados no horário local em cada computador gerenciado. Os agendamentos são executados em momentos diferentes segundo os fusos horários dos computadores gerenciados.
Usar hora do servidor	Os horários são especificados com informações de fuso horário, em que o deslocamento de fuso horário é o mesmo do fuso horário do servidor em que a política é definida. Os agendamentos são executados simultaneamente, independentemente dos fusos horários, e são ajustados para o horário de verão. Esta opção garante que os agendamentos de manutenção sejam sempre coordenados com o horário local especificado no servidor em que a política é criada.
Coordenação com UTC	Os horários são especificados com informações de fuso horário, onde o deslocamento do fuso horário é 0. Os agendamentos são executados simultaneamente, independentemente dos fusos horários, e não são afetados pelo horário de verão.

3 Clique em **Avançar** e, na caixa de diálogo **Opções avançadas**, faça as mudanças apropriadas:

Apenas executar verificação se:	Selecionar as opções apropriadas: ■ O computador estiver conectado à rede ■ O computador estiver disponível no horário agendado exato ■ Um usuário fizer logon no computador ■ Um usuário não fizer logon no computador

Para configurar as políticas de instalação, de upgrade e de desinstalação do agente/plug-in

Datas de início e fim

A data de início é o dia em que a política terá efeito. Essa política deve ser ativada assim como qualquer outra política. Você pode ativar a política a qualquer momento antes ou depois da data de início.

Se desejar que a política esteja disponível por um período de tempo limitado, defina a data final apropriada. A política estará indisponível após essa data, esteja ela ativada ou não.

A configuração da data de fim é opcional. Se nenhuma data de final for especificada, a política estará disponível indefinidamente.

- 4 Clique em **OK** para fechar a caixa de diálogo Opções avançadas.
- 5 (Opcional) Se desejar remover um agendamento da lista, selecione-o e clique em **Excluir**.

Para configurar as políticas de instalação, de upgrade e de desinstalação do agente/plug-in

Você pode configurar as políticas de instalação, upgrade e desinstalação do agente para satisfazer seus requisitos. Estas políticas usam o mesmo pacote do agente, mas cada política usa um programa diferente.

Para configurar as políticas de instalação, de upgrade e de desinstalação do agente/plug-in

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda a pasta apropriada e selecione a política que você deseja configurar.
- 3 (Opcional) Para ativar ou desativar a política, na página **Instalação do agente**, **Upgrade do agente** ou **Desinstalação do agente**, clique no símbolo de status e clique em **Ativar** ou **Desativar**.
- 4 Faça as alterações de configuração apropriadas:

Nome do programa	O nome do programa do pacote do agente que é executado quando a política é acionada. A configuração padrão é o programa apropriado para a política e não deve ser necessário alterá-la. Porém, se você adicionou um programa novo ao pacote do agente, talvez você queira usá-lo em seu lugar. Consulte “Gerenciamento de programas do pacote” na página 374.
Ativar relatórios detalhados de eventos de status	Ativar o envio de eventos de status do pacote ao Notification Server. As configurações de Captura de eventos do Notification Server na política de configurações do Symantec Management Agent têm prioridade sobre a configuração Ativar relatórios detalhados aqui. Os eventos serão enviados somente se forem ativados na política de configurações globais do Symantec Management Agent. Consulte “Para definir as configurações globais de agentes” na página 277.
Aplica-se a	Especifique os computadores aos quais a política se aplica. Você pode usar filtros predefinidos que são fornecidos com o Notification Server ou criar seus próprios. Consulte “Especificação dos destinos de uma política ou tarefa” na página 380.
Multicast de pacotes	Desativa o download do pacote pelo multicast. Normalmente, o multicast torna mais lenta a instalação de um pacote; assim, convém desativá-lo para um patch urgente. Além disso, em alguns ambientes, o multicast não funciona. Por exemplo, pode ser desativado em roteadores e em switches. As configurações do multicast de pacotes na política de configurações globais do Symantec Management Agent têm prioridade sobre estas configurações.
Agendar	Especifique a agenda da política. Consulte “Especificação de um agendamento de política” na página 388.

Opções de
agendamento
adicionais

As opções adicionais de agenda são as seguintes:

- **Executar uma vez logo que possível**
- **O usuário pode executar**
- **Notificar o usuário quando a tarefa estiver disponível**
- **Avisar antes de executar**

5 Clique em **Salvar alterações**.

Sobre as políticas de automação

As políticas de automação são conjuntos de regras, definidos pelo sistema ou pelo administrador, que governam a execução de ações automatizadas. Os exemplos de ações automatizadas incluem a execução de um relatório usando os parâmetros que foram obtidos pela política, o envio de um alerta ao administrador e a execução de um comando ou a execução de uma tarefa em computadores gerenciados.

Consulte [“Sobre políticas do Symantec Management Platform”](#) na página 377.

Consulte [“Gerenciamento de políticas de automação”](#) na página 394.

Consulte [“Componentes-chave das políticas de automação”](#) na página 393.

As políticas de automação podem ser executadas em um agendamento ou ser acionadas por mensagens do Notification Server. A política determina quando uma ação deve iniciar e quem ou o que deve ser notificado dos resultados. As políticas de automação são executadas no computador do Notification Server; portanto, elas não estão relacionadas com a atividade relativa ao agente em computadores gerenciados. Porém, algumas políticas de automação podem ser acionadas pelas mensagens geradas pela atividade do agente.

As políticas de automação não são aplicadas aos destinos dos recursos, diferentemente dos outros tipos de políticas do Notification Server. Elas são ações do Notification Server executadas nos computadores gerenciados apropriados. Algumas ações, tais como enviar um e-mail ao administrador que contém um relatório ou uma fonte de dados como um arquivo HTML, não afetam nenhum computador gerenciado.

Muitas das soluções que funcionam com o Notification Server vêm com políticas de automação. Essas políticas permitem que o Notification Server realize uma variedade de ações quando as condições definidas ocorrem. As políticas de automação podem ser definidas em um único processo iniciando em um computador. As políticas de automação também podem ser definidas em cenários complexos, como vários processos em uma ampla gama de computadores. As soluções que definem políticas de automação especificam seus próprios critérios para o tipo de condições que conduzem às ações que estão sendo iniciadas.

Por exemplo, o Inventory Solution usa dados do CMDB e a medição de aplicativos usa a lista de processos monitorados. Nesta solução, porém, há conjuntos comuns de ações que podem ser executadas automaticamente.

Componentes-chave das políticas de automação

Consulte [“Sobre as políticas de automação”](#) na página 392.

As políticas de automação têm os mesmos componentes-chave.

Tabela 25-2 Componentes-chave das políticas de automação

Componente	Descrição
Acionador	Inicia a avaliação de uma política de automação. O Notification Server possui os seguintes acionadores: ■ Agenda Uma agenda do Notification Server, como uma agenda compartilhada ou uma agenda personalizada especificada. Você não pode usar as janelas de manutenção (que são definidas nos computadores gerenciados) como acionadores da política de automação. ■ Mensagem Uma mensagem interna do Notification Server. Elas são enviadas quando eventos de interesse ocorrem. Por exemplo, um recurso criado, um recurso descoberto, um recurso excluído, um computador novo descoberto ou um serviço do Notification Server iniciado.
Fonte de dados	Fornece as informações que a política de automação usa depois de ser acionada. A fonte de dados é tipicamente um relatório ou uma consulta que retorna uma lista de computadores, junto com informações sobre o estado de cada computador e de suas configurações atuais que são relevantes à política. O relatório ou a consulta são executados quando a política é acionada para se assegurar de que os dados mais recentes sejam extraídos. A fonte de dados define os computadores gerenciados que são visados pela política e as ações que são executadas neles. Uma política de automação também pode extrair parâmetros da fonte de dados e usá-los como parâmetros de entrada para tarefas ou trabalhos. O Notification Server fornece as seguintes fontes de dados: ■ Relatório ■ Consulta SQL bruta Se selecionar esta opção, você precisará do privilégio Editar SQL diretamente para editar a consulta da fonte de dados e exibir os resultados da consulta. Consulte “Privilegios do sistema” na página 494. ■ Consulta de recursos ■ Mensagem ■ Nenhum As soluções podem acrescentar fontes de dados adicionais.

Componente	Descrição
Regra de avaliação	Avalia os dados contidos na fonte de dados e determina se uma ação precisa ser executada. O Notification Server fornece as seguintes regras de avaliação: ■ Execução para dados não vazios ■ Executar para cada registro ■ Processamento de mensagens ■ Executar sempre
Ação	Especifica a tarefa ou o trabalho que a política executa. Estas são tarefas do agente padrão ou do servidor. A ação pode incluir os parâmetros de entrada que são aprovados da fonte de dados.

Gerenciamento de políticas de automação

Você pode configurar e gerenciar as políticas de automação disponíveis no Notification Server. É possível criar novas políticas, editar políticas existentes, ativar ou desativar uma política quando necessário, definir a segurança apropriada em uma política e excluir uma política quando ela não for mais necessária.

Consulte [“Sobre as políticas de automação”](#) na página 392.

Para gerenciar políticas de automação

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 Na página **Políticas de automação**, selecione a guia apropriada:

Agendas	Gerenciar políticas de automação que são executados em uma agenda definida.
Mensagem do sistema	Gerenciar políticas de automação que são executadas quando uma mensagem específica do sistema é recebida.

3 Execute uma das seguintes opções:

Crie ou modifique uma política	Consulte “Criação ou modificação de políticas de automação agendadas” na página 396. Consulte “Criação ou modificação de políticas de automação baseadas em mensagens” na página 399.
Ative ou desative uma política	No painel esquerdo, selecione a política de automação que você deseja ativar ou desativar e clique em Ativar ou Desativar , a opção que for apropriada.
Exclua uma política	No painel esquerdo, selecione a política de automação que você deseja excluir e clique em Excluir. Você pode excluir todas as políticas de automação que você criou. Não é possível excluir nenhuma das políticas de automação padrão fornecidas com o Notification Server.
Defina a segurança em uma política	No painel esquerdo, selecione a política de automação na qual você deseja definir a segurança e clique em Ações > Segurança. No Gerenciador de Função de Segurança, defina a segurança apropriada.
Execute outras ações em uma política	No painel esquerdo, selecione a política de automação na qual você deseja executar uma ação, clique em Ações e, em seguida, clique na opção apropriada. As ações disponíveis são as mesmas do menu contextual.
Teste uma política	No painel esquerdo, selecione a política de automação que você deseja testar e, no painel direito, clique em Testar política de automação. Você pode usar o teste de política de automação para verificar se todos os componentes da política são consistentes e se os parâmetros de entrada estão mapeados corretamente. O teste executa a política e os resultados da ação são exibidos no log de trabalhos/tarefas.

Criação ou modificação de políticas de automação agendadas

As políticas de automação podem usar qualquer agenda do Notification Server, como uma agenda compartilhada ou uma agenda personalizada especificada. As

Consulte “Sobre as políticas de automação” na página 392.

Nota: Este tópico abrange as opções padrão que são fornecidas no Notification Server. As soluções podem ampliar ou adicionar novas opções. Para obter mais informações, consulte a documentação apropriada da solução.

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 Na página **Políticas de automação**, na guia **Agendamentos**, execute um destes procedimentos:

- Para modificar uma política existente No painel esquerdo, selecione a nova política.

- Na data/hora Especifique a data, o horário e a repetição da agenda nos campos apropriados.

Agenda compartilhada

Na lista suspensa **Selecionar agendamento compartilhado**, selecione o agendamento apropriado.

Consulte “[Para gerenciar agendamentos compartilhados](#)” na página 122.

- 5 No painel **Detalhes**, em **Fonte de dados**, especifique a origem dos dados que deseja usar.

Consulte “[Especificação da fonte de dados da política de automação](#)” na página 401.
- 6 Em **Condições**, na lista suspensa **Regra de avaliação**, selecione a regra de avaliação apropriada:

Execução para dados não vazios	Trata a tabela da fonte de dados como uma única unidade. Quando a política for acionada, a ação será executada somente se a tabela contiver uma ou mais linhas e será executada apenas uma vez. Você precisa usar esta opção se a fonte de dados contiver as informações em um arquivo HTML em vez de uma tabela. Esta opção permite visar tudo em uma única coluna, como uma lista de GUIDs. Não é possível definir parâmetros dinâmicos para distinguir computadores de destino. Se desejar fazer isso, use a opção Executar para cada registro.
Executar para cada registro	Avalia a linha da tabela da fonte de dados por linha, o que permite usar campos por linha como parâmetros dinâmicos para as ações especificadas. A ação é executada uma vez por linha.
Executar sempre	Executa as ações especificadas sem usar uma fonte de dados. Esta opção está disponível somente quando nenhuma fonte de dados é especificada.
- 7 Em **Ações**, especifique a tarefa ou o trabalho a ser executado e defina todos os parâmetros de entrada necessários.

Consulte “[Como especificar a ação da política de automação](#)” na página 402.
- 8 Clique em **Aplicar** para salvar as configurações de política.
- 9 (Opcional) Se deseja certificar-se de que todos os componentes da política são consistentes e que os parâmetros de entrada estão mapeados corretamente, clique em **Testar política de automação**.

O teste é apenas uma verificação interna e não afeta os recursos.

Criação ou modificação de políticas de automação baseadas em mensagens

As políticas de automação podem usar uma mensagem interna do Notification Server como um acionador. As mensagens disponíveis para essa finalidade são predefinidas. Estas mensagens relacionam-se a eventos do Notification Server, como recursos descobertos, criados ou excluídos, novos computadores descobertos ou serviços do Notification Server que são iniciados. As soluções podem disponibilizar mensagens adicionais específicas da solução. Quando uma política de automação é acionada, as ações apropriadas são executadas imediatamente. Você não pode configurar uma política de automação para que seja executada posteriormente, depois que ela foi acionada.

Consulte “Sobre as políticas de automação” na página 392.

Consulte “Gerenciamento de políticas de automação” na página 394.

Nota: Este tópico abrange as opções padrão que são fornecidas no Symantec Management Platform. As soluções podem ampliar ou adicionar novas opções. Para obter mais informações, consulte a documentação apropriada da solução.

Para criar ou modificar uma política de automação baseada em mensagens

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 Na página **Políticas de automação**, na guia **Mensagens do sistema**, execute um destes procedimentos:

Para criar uma nova política 1 Clique em **Nova política.**

- 2 Na caixa de diálogo **Nome da política de automação**, digite o novo nome da política e clique em **OK**.

Para modificar uma política existente No painel esquerdo, selecione a nova política.

- 3 (Opcional) No painel direito, edite o nome e a descrição da política clicando nos campos apropriados e digitando os novos detalhes.
- 4 Na lista suspensa **Mensagem do NS**, selecione a mensagem que você deseja usar.

- 5 No painel **Detalhes**, em **Fonte de dados**, especifique a origem dos dados que deseja usar.

Consulte [“Especificação da fonte de dados da política de automação”](#) na página 401.
- 6 Em **Condições**, na lista suspensa **Regra de avaliação**, selecione a regra de avaliação apropriada:

Execução para dados não vazios	Trata a tabela da fonte de dados como uma única unidade. Quando a política for acionada, a ação será executada somente se a tabela contiver uma ou mais linhas e será executada apenas uma vez. Você precisa usar esta opção se a fonte de dados contiver as informações em um arquivo HTML em vez de uma tabela. Esta opção permite visar tudo em uma única coluna, como uma lista de GUIDs. Não é possível definir parâmetros dinâmicos para distinguir computadores de destino. Se desejar fazer isso, use a opção Executar para cada registro.
Executar para cada registro	Avalia a linha da tabela da fonte de dados por linha, o que permite usar campos por linha como parâmetros dinâmicos para as ações especificadas. A ação é executada uma vez por linha.
Processamento de mensagens	Avalia o texto da mensagem da fonte de dados e usa os parâmetros apropriados nas ações especificadas. Esta opção está disponível somente quando uma fonte de dados da mensagem é usada.
Executar sempre	Executa as ações especificadas sem usar uma fonte de dados. Esta opção está disponível somente quando nenhuma fonte de dados é especificada.
- 7 Em **Ações**, especifique a tarefa ou o trabalho a ser executado e defina todos os parâmetros de entrada necessários.

Consulte [“Como especificar a ação da política de automação”](#) na página 402.
- 8 Clique em **Salvar alterações** para salvar as configurações da política.
- 9 (Opcional) Se deseja certificar-se de que todos os componentes da política são consistentes e que os parâmetros de entrada estão mapeados corretamente, clique em **Testar política de automação**.

O teste é apenas uma verificação interna e não afeta os recursos.

Especificação da fonte de dados da política de automação

A fonte de dados da política de automação determina que computadores visar e que ações executar neles. Uma política de automação pode extrair parâmetros da fonte de dados e usá-los como parâmetros de entrada para tarefas ou trabalhos.

Consulte [“Criação ou modificação de políticas de automação agendadas”](#) na página 396.

Consulte [“Criação ou modificação de políticas de automação baseadas em mensagens”](#) na página 399.

Você pode usar fontes de dados externas, como relatórios e mensagens, ou usar uma consulta para extrair dados do CMDB. Uma fonte de dados externa, como um relatório, pode ser usada por qualquer número de políticas de automação. Você precisa ser cuidadoso ao usar relatórios, porque eles podem ser modificados mais tarde e os parâmetros dos quais algumas ações dependem podem ser alterados ou removidos. Se uma ação não puder determinar um parâmetro necessário através de um relatório da fonte de dados, ela usará o valor padrão definido na política de automação.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

As consultas SQL e as consultas de recursos são incorporadas na definição da política de automação. Você não pode compartilhar consultas entre as políticas de automação e não é possível acessar diretamente as consultas (também conhecidas como fontes de dados) que são componentes dos relatórios. Se deseja usar uma consulta de relatório, você poderá copiar o SQL do relatório e colá-lo na política de automação.

Uma política de automação que não define um destino para sua ação não exige uma fonte de dados. Por exemplo, uma política que envia uma mensagem ao administrador ou executa uma tarefa no computador do Notification Server.

Para especificar a fonte de dados da política de automação

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 Na página **Políticas de automação**, na guia **Mensagem do sistema**, selecione uma política de automação existente ou crie uma nova.
- 3 No painel direito, em **Details**, em **Data Source**, na lista suspensa **Data Source**, selecione a opção apropriada:

Relatório	Use os resultados de um relatório. 1 No campo Relatório, clique em Nome do relatório. 2 Na janela Selecionar relatório, selecione os relatórios apropriados e clique em OK.
Consulta SQL bruta	Use os resultados de uma consulta SQL. 1 Clique em Editar consulta. 2 Na janela Fonte de dados, especifique a consulta SQL que você deseja usar e clique em OK. Consulte “Para definir uma consulta SQL para um filtro” na página 361. Se deseja reutilizar uma consulta de um filtro ou relatório existente, você pode copiar o conteúdo da guia Consulta resolvida, do filtro ou da consulta de relatório apropriada. Você pode colar o conteúdo na guia Consulta resolvida, na janela Fonte de dados. Você pode então modificar o SQL conforme a necessidade. Observe que a consulta na guia Consulta resolvida tem todos os parâmetros substituídos pelos valores especificados do teste.
Consulta de recursos	Use os resultados de uma consulta de recursos. 1 Clique em Editar consulta. 2 Na janela Fonte de dados, especifique a consulta de recursos que você deseja usar e clique em OK. Consulte “Para definir uma consulta de recursos para um filtro” na página 359.
Mensagem	Use as informações contidas na mensagem que acionou a política.
Nenhum	Nenhuma fonte de dados é necessária. A política de automação não precisa definir um destino para sua ação.

Como especificar a ação da política de automação

As ações da política de automação são trabalhos e tarefas. O Symantec Management Platform fornece um conjunto de tarefas que você pode usar, e as soluções podem adicionar mais. Você pode criar suas próprias tarefas e estender as opções para satisfazer seus requisitos. Se seu Symantec Management Platform faz parte de uma hierarquia, tarefas e trabalhos adicionais podem ser replicados de maneira decrescente do Symantec Management Platform pai.

Consulte “Criação ou modificação de políticas de automação agendadas” na página 396.

Consulte “Criação ou modificação de políticas de automação baseadas em mensagens” na página 399.

Uma política de automação pode conter somente uma ação, que pode ser uma tarefa ou um trabalho, que é aplicada a todos os computadores aos quais a política se destina. Se quiser incluir várias tarefas, você precisa colocá-las em um trabalho apropriado. Como alternativa, você precisa criar várias políticas de automação com os acionadores, as fontes de dados e as ações apropriadas.

Aviso: Qualquer número de políticas de automação pode compartilhar um trabalho ou uma tarefa. Quando você modificar uma tarefa que deseja usar em uma política de automação, suas mudanças poderão afetar muitas outras políticas. Você pode preferir duplicar a tarefa relevante e usar a duplicata modificada na política.

As tarefas podem conter parâmetros estáticos e dinâmicos de entrada. Os parâmetros dinâmicos serão definidos com valores extraídos da fonte de dados quando a política for acionada. Os parâmetros estáticos têm valores definidos dentro da tarefa, para que sejam os mesmos sempre que a tarefa é executada.

As ações de falha ou os códigos de retorno não podem ser definidos em uma política de automação; assim, se algum for necessário, será preciso configurá-los na tarefa.

Para especificar a ação da política de automação

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Políticas de automação**.
- 2 Na página **Políticas de automação**, na guia **Mensagem do sistema**, selecione uma política de automação existente ou crie uma nova.
- 3 No painel direito, em **Actions**, no campo **Executar tarefa/tarefa**, clique em **Selecione um trabalho ou uma tarefa**.
- 4 Na caixa de diálogo **Selecionar tarefa**, no painel esquerdo, selecione o trabalho ou a tarefa apropriada e clique em **OK**.

Consulte “Para selecionar um trabalho ou tarefa à política de automação” na página 404.

- 5 (Opcional) Clique em **Editar parâmetro de entrada** e, na caixa de diálogo Editar parâmetros de entrada de trabalho/tarefa, especifique o seguinte para cada parâmetro da ação:

- 4 Na caixa de diálogo **Selecionar tarefa**, no painel esquerdo, selecione a tarefa apropriada e depois, no painel direito, faça todas as mudanças de configuração necessárias à tarefa ou ao trabalho.
- 5 Clique em **OK**.

Para criar e modificar tarefas de política de automação

Um conjunto de tarefas da política de automação é fornecido com o Symantec Management Platform. Você pode usá-las em suas políticas de automação e usá-las como um modelo para criar suas próprias tarefas e trabalhos personalizados.

Consulte [“Como especificar a ação da política de automação”](#) na página 402.

As tarefas permitem executar as seguintes ações:

Atribuir ao grupo organizacional	Permite atribuir recursos a um grupo organizacional.
Enviar um relatório por e-mail	Permite enviar um relatório especificado por e-mail como um anexo. Convém usar esta tarefa como parte de um trabalho que inclua também uma tarefa de execução de relatório para criar o relatório apropriado.
Enviar um e-mail	Permite enviar um e-mail com informações que você define a usuários especificados. O e-mail pode incluir status, licença do produto ou outras informações.
Executar um relatório	Convém usar esta tarefa como parte de um trabalho que inclua também uma tarefa de envio de relatório por e-mail aos usuários apropriados ou ao administrador do Notification Server

Para criar ou modificar uma tarefa de política de automação

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, expanda a pasta **Trabalhos e tarefas > Trabalhos e tarefas do sistema > Notification Server > Tarefas de política de automação** e execute um destes procedimentos:

- Para criar do zero um novo trabalho ou tarefa

1

Clique com o botão direito do mouse na pasta **Tarefas de política de automação**, clique em **Novo(a)** e depois clique na opção apropriada.
- 2

Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, selecione a tarefa.
- 3

No painel direito, especifique as opções e clique em **OK**.

Para criar um novo trabalho ou tarefa usando trabalhos ou tarefas existentes como modelo

Clique com o botão direito do mouse no trabalho ou na tarefa e clique em **Clonar**.

Para modificar um trabalho ou tarefa existente

Clicar no trabalho ou na tarefa.

- 3

No painel direito, especifique os detalhes apropriados para o trabalho ou a tarefa.
- 4

Clique em **Salvar alterações**.

Para usar tarefas e trabalhos

Este capítulo contém os tópicos a seguir:

- [Sobre o Gerenciamento de tarefas](#)
- [Componentes do gerenciamento de tarefas](#)
- [Como o servidor de tarefas usa o mecanismo de ativação](#)
- [Sobre quando usar tarefas, trabalhos e políticas](#)
- [Sobre tarefas em execução na hierarquia](#)
- [Sequenciamento de tarefas](#)
- [Exibição e edição das permissões em um tipo de tarefa](#)
- [Para criar tarefas para propriedades de entrada ou saída de tarefas](#)
- [Para limpar dados de tarefas](#)
- [Para limpar dados da versão da tarefa](#)
- [Alteração das configurações do Client Task Agent](#)
- [Acesso ao Portal de trabalhos e tarefas](#)

Sobre o Gerenciamento de tarefas

O Gerenciamento de tarefas possibilita a organização das tarefas em sequência e sua automação para soluções da Symantec. Arranjar tarefas em sequência permite executar operações de gerenciamento complexas em um único trabalho. As tarefas podem ser arranjadas em sequência em um trabalho, o que lhe oferece

grande flexibilidade no trabalho. A funcionalidade é semelhante àquela oferecida pelo software do Symantec Deployment Solution com seu mecanismo de trabalhos. Porém, o Gerenciamento de tarefas foi desenvolvido sobre o Symantec Management Platform e permite que o restante do catálogo da solução da Symantec utilize seus eficazes recursos.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Você pode executar as tarefas automaticamente com base em eventos do sistema ou em alterações no banco de dados. Você também pode executar tarefas automaticamente para manter a conformidade dos computadores com as políticas.

Os servidores de tarefas são semelhantes a servidores de pacotes, pois foram projetados para residir em um servidor separado e são leves. Os servidores de pacotes e tarefas são serviços de site e são instalados em um servidor de sites. Os computadores podem ser atribuídos a um servidor de sites específico pelo nome de computador ou pela sub-rede.

Consulte [“Sobre os serviços de site”](#) na página 127.

Você pode criar, executar ou agendar trabalhos e tarefas no portal de Trabalhos e tarefas. Os componentes de tarefa organizam estes trabalhos e tarefas sem problemas.

Consulte [“Componentes do gerenciamento de tarefas”](#) na página 409.

O Gerenciamento de tarefas inclui os seguintes recursos:

- Executa várias tarefas em uma sequência definida denominada trabalho.
Consulte [“Criação de trabalhos”](#) na página 420.
- Permite que os usuários forneçam uma lógica para controlar erros da tarefa ou outros códigos de retorno.
- Inclui a eficaz linha de comando e recursos VBScript.
- Fornece as tarefas predefinidas de gerenciamento de energia.
- Executa as tarefas do cliente e servidor.
Consulte [“Para implementar um servidor de tarefas”](#) na página 418.
- Fornece os recursos de ação rápida para a execução de trabalhos, como as opções Executar agora e o feedback do status praticamente em tempo real.
Consulte [“Execução de um trabalho ou uma tarefa”](#) na página 422.
Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.
Consulte [“Exibição do status da tarefa no Symantec Management Agent”](#) na página 426.
- Reutiliza as tarefas em vários trabalhos ou permite duplicar e modificar tarefas conforme desejado.

Componentes do gerenciamento de tarefas

O Gerenciamento de tarefas funciona aproveitando diversos componentes. Estes componentes organizam a atribuição e o desempenho de trabalhos e tarefas nos computadores-cliente conectados.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Tabela 26-1 Componentes do gerenciamento de tarefas

Componente	Descrição
Task Server	Este componente distribui trabalhos e tarefas na rede e pode ser executado no Notification Server ou em um computador remoto. O servidor de tarefas tem a capacidade de ativar os computadores-cliente registrados. Esta capacidade de ativar é separada do componente do Tickle Server no computador do Notification Server. O servidor de tarefas envia as informações de status ao carregador de dados. Envia também as ativações, as informações de trabalhos e tarefas ao Client Task Agent.
Servidor de ativação	O Tickle Server notifica o Task Server quando e onde há tarefas a executar em seus computadores-cliente conectados. O servidor de ativação Server então ativa os computadores-cliente conectados e envia a eles o XML que contém as informações sobre o trabalho ou a tarefa usando HTTP(S). O Tickle Server também coleta as informações de status e as encaminha ao banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database) usando HTTP(S). Este componente é sempre executado no computador do Notification Server. Ele enviará um pacote de ativação de IP aos servidores de tarefas quando qualquer um de seus clientes tiver um trabalho ou uma tarefa para executar. Consulte “Como o servidor de tarefas usa o mecanismo de ativação” na página 410.

Componente	Descrição
Carregador de dados	Este componente recebe informações de status dos Task Servers e as coloca em um cache de memória até que elas possam ser enviadas para o CMDDB. O carregador de dados melhora a escalabilidade ao permitir que as informações de status de centenas de clientes sejam recebidas de uma vez sem sobrecarregar o SQL Server. Este componente também é executado em cada servidor de tarefas remoto e coloca em fila os dados em espera até que eles possam ser enviados ao Notification Server.
Client Task Agent	Este agente é executado em computadores-cliente e executa as seguintes ações: ■ Aceita ativações de um Task Server. ■ Recebe as informações de trabalhos e tarefas. ■ Passa as informações a um controlador. ■ Envia as informações de status de volta ao Task Server. Este agente é instalado automaticamente com o Symantec Management Agent. Nota: Quando você instalar o Symantec Management Agent em um computador, haverá um atraso antes que o Client Task Agent seja registrado no Notification Server. Todas as tarefas que forem selecionadas no computador durante esse tempo (normalmente, em torno de 10 minutos) ficarão com um status pendente até que o Client Task Agent seja registrado. Quando o Client Task Agent for registrado, as tarefas serão executadas imediatamente.

Como o servidor de tarefas usa o mecanismo de ativação

O Tickle Server é um componente do Gerenciamento de tarefas. O componente do Servidor de ativação é executado somente no computador do Notification Server e é responsável por notificar os servidores de tarefas sobre as tarefas pendentes para seus computadores-cliente. Os Task Servers têm também a capacidade nativa de ativar seus computadores-cliente registrados. Esta capacidade de ativar é separada do componente do Tickle Server no computador do Notification Server.

Consulte [“Componentes do gerenciamento de tarefas”](#) na página 409.

O Servidor de ativação envia pacotes de ativação de IP aos Task Servers quando quaisquer de seus computadores-cliente registrados têm um trabalho ou tarefa

para executar. Depois que o pacote de ativação é recebido, o Task Server solicita imediatamente as informações da tarefa ou do trabalho do Notification Server para seus computadores-cliente registrados. Ele também ativa seus computadores-cliente. Quando o Client Task Agent recebe o pacote de ativação, ele solicita informações do trabalho ou tarefa de seu Task Server registrado. Somente depois que o Client Task Agent recebe as informações da tarefa, ela é executada. Os eventos de status das tarefas concluídas são enviados de volta ao Task Server registrado na conclusão.

Se os pacotes de ativação forem bloqueados ou não puderem atingir o destino, o Client Task Agent voltará a verificar automaticamente seu Task Server registrado para obter todas as novas informações do trabalho. Ele executa essa verificação a cada 5 minutos. Este intervalo de solicitação de tarefas é configurável no Symantec Management Console. A tarefa do Task Server e as informações do trabalho não são recebidas pela política de configuração do Symantec Management Agent. Elas são recebidas diretamente pelo Client Task Agent de seu Task Server registrado. Se você forçar o Symantec Management Agent para atualizar a política de configuração, ele não forçará o Client Task Agent para receber as informações das tarefas pendentes.

Consulte [“Alteração das configurações do Client Task Agent”](#) na página 431.

Por padrão, o Servidor de ativação usa a porta 50123 para Task Servers e os Task Servers usam a porta 50124 para habilitar os Client Task Agents.

Consulte [“Sobre o Gerenciamento de tarefas ”](#) na página 407.

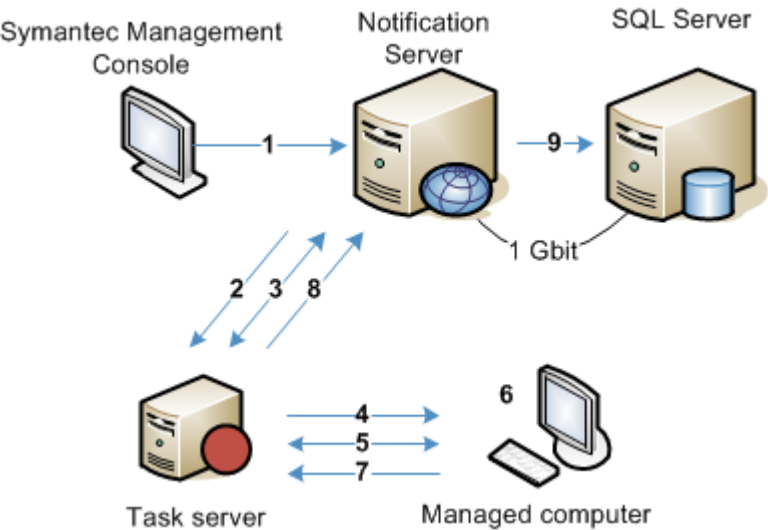
O seguinte exemplo assume que o Client Task Agent do ComputerA está registrado com o RemoteTaskServer1.

Tabela 26-2 Sequência para como a ativação do servidor de tarefas funciona

Sequência	Descrição
Um	Um administrador do Notification Server atribui uma tarefa para executar imediatamente no ComputerA.
Dois	O Servidor de ativação no computador do Notification Server envia um pacote de ativação para notificar o RemoteTaskServer1 da tarefa pendente.
Três	O RemoteTaskServer1 verifica se o cliente de destino tem permissão para receber tarefas. Se o modo Comunicação de agente legado estiver desativado e o destino for um agente legado, a tarefa falhará imediatamente. Ela também falhará se o agente receber um upgrade, mas estará no estado Não permitido . Consulte “Sobre o registro do agente” na página 237.

Sequência	Descrição
Quatro	O RemoteTaskServer1 recebe o pacote de ativação e solicita imediatamente as informações do trabalho do Notification Server.
Cinco	O RemoteTaskServer1 ativa o ComputerA para notificá-lo da tarefa pendente.
Seis	O ComputerA recebe o pacote de ativação e solicita imediatamente as informações do trabalho do servidor de tarefas registrado – RemoteTaskServer1.
Sete	O ComputerA recebe as informações do trabalho e executa a tarefa.
Oito	Na conclusão da tarefa, o ComputerA envia um evento de status de volta ao RemoteTaskServer1.
Nove	O RemoteTaskServer1 armazena o evento de status em cache e tenta imediatamente encaminhá-lo de volta ao Notification Server.
Dez	O Notification Server recebe o evento de status do RemoteTaskServer1 e registra as informações no banco de dados.

Figura 26-1 Sequência de como a ativação do servidor de tarefas funciona



Sobre quando usar tarefas, trabalhos e políticas

As tarefas, os trabalhos e as políticas têm usos diferentes no Notification Server. A decisão sobre qual usar depende do que você deseja realizar.

Uma política é um conjunto de regras que se aplicam a um recurso ou a um conjunto de recursos (conhecidos como o destino da política). Uma política pode ser avaliada com base em um agendamento ou em dados de entrada. Quando uma política é avaliada, a ação apropriada é tomada. Esta ação inclui tipicamente tarefas em execução nos recursos de destino para assegurar que todos cumpram a política. O uso de uma política permite aplicar ações a recursos específicos, que você define como o destino da política.

Consulte [“Sobre políticas do Symantec Management Platform”](#) na página 377.

Uma tarefa é uma ação separada que não tem ações contínuas e que você implementa em computadores selecionados. Você pode executar as tarefas automaticamente com base em eventos do sistema ou em alterações no banco de dados. Você também pode executar tarefas automaticamente para manter a conformidade dos computadores com as políticas.

Uma tarefa é uma sequência de tarefas que são executadas em ordem específica.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Em geral, use políticas para o gerenciamento contínuo e use tarefas para aplicar políticas ou executar ações não repetidas.

Tabela 26-3 Sobre quando usar tarefas, trabalhos e políticas

Opção	Critérios
Tarefa	Use uma tarefa quando os seguintes critérios forem verdadeiros: ■ Você precisa executar uma ação que seja concluída rapidamente (sem ações pendentes).
Trabalho	Use um trabalho quando os seguintes critérios forem verdadeiros: ■ Você precisa executar ações em uma ordem específica. ■ Uma ação pode ser útil para que um usuário crie uma sequência ou estabeleça um vínculo com uma mensagem do Notification Server.
Política	Use uma política quando os seguintes critérios forem verdadeiros: ■ Você tem dados de configuração estáticos para enviar ao Symantec Management Agent. ■ Você tem ações pendentes sem um final definido.

Sobre tarefas em execução na hierarquia

O Symantec Management Platform permite criar tarefas no Notification Server pai e executá-las em todos os computadores-cliente na hierarquia. Tais tarefas também são replicadas ao Notification Server filho e executadas em todos os computadores gerenciados aplicáveis.

Consulte [“Sobre a hierarquia do Notification Server”](#) na página 153.

Consulte [“Sobre o Gerenciamento de tarefas ”](#) na página 407.

Quando executar tarefas na hierarquia, você deverá considerar as seguintes informações específicas do projeto:

Os computadores-cliente relatam as informações de status da tarefa somente ao Notification Server a que estão atribuídos. A informações de status da tarefa para os computadores-cliente atribuídos a um Notification Server filho não são sempre exatas no Notification Server pai.

Se você criar uma tarefa no Notification Server pai e executá-la em todos os computadores-cliente no ambiente, nem todos os computadores a relatarão ao Notification Server pai. Os computadores-cliente que são atribuídos ao relatório do Notification Server filho relatam as informações de status da tarefa somente ao Notification Server filho. Além disso, as informações de status da tarefa não são replicadas do Notification Server filho ao respectivo pai.

Por consequência, a página **Trabalhos/Tarefas** no Notification Server pai exibirá informações de status da tarefa imprecisas para as tarefas executadas nos computadores-cliente atribuídos a um Notification Server filho.

Você pode ver as informações exatas de status da tarefa para cada computador separadamente no Notification Server pai, na janela **Detalhes da instância da tarefa**. A janela **Detalhes da instância da tarefa** abre um URL do Notification Server filho e exige as credenciais do Notification Server filho.

Além disso, a janela **Detalhes da instância da tarefa** exibe as informações corretas de status da tarefa somente nos seguintes casos:

- Se você criar uma tarefa no Notification Server pai, clique em **Execução rápida** ou **Novo agendamento > Agora**, e adicione computadores-cliente do Notification Server filho como destinos da tarefa.
- Se você criar uma tarefa no Notification Server pai, adicione um agendamento para a tarefa e adicione computadores-cliente do Notification Server filho como um destino da tarefa.

Se você replicar a tarefa ao Notification Server filho e iniciar a tarefa através dele, não será possível exibir os detalhes do status da tarefa no Notification Server pai.

Um trabalho do servidor que contém tarefas do cliente não é replicado corretamente do Notification Server pai para o filho.

Se você criar um trabalho do servidor que contenha tarefas do cliente e replicá-lo de um Notification Server pai para um filho, as tarefas do cliente no trabalho do servidor serão replicadas ao Notification Server filho, mas as tarefas do servidor e o próprio trabalho do servidor não o serão. Além disso, as tarefas do servidor desse trabalho específico serão executadas no Notification Server pai, enquanto as tarefas do cliente serão executadas no Notification Server filho.

Para solucionar esse problema, você pode criar um trabalho do servidor no Notification Server filho e adicionar-lhe as tarefas replicadas do cliente. Como alternativa, é possível criar um trabalho do cliente no pai. O trabalho do cliente que contém tarefas do cliente será replicado corretamente.

Se você aplicar um trabalho do servidor que contenha tarefas do cliente do Notification Server pai ao Notification Server filho, o status de execução da tarefa estará disponível somente no Notification Server pai. No Notification Server filho, a instância desse trabalho em particular não será criada.

A Symantec não recomenda a criação de um trabalho de servidor que contenha tarefas do cliente.

Para obter mais informações sobre trabalhos e tarefas, consulte o seguinte artigo da base de conhecimento:

<http://www.symantec.com/docs/HOWTO9671>

Se você excluir a tarefa no Notification Server pai, a opção **Replicar agora** não excluirá a tarefa no Notification Server filho.

Se você excluir uma tarefa no Notification Server pai e usar a opção **Replicar agora** para replicar a operação ao Notification Server filho, a tarefa no Notification Server filho não será excluída.

Somente replicações diferenciais ou completas excluem a tarefa com êxito no Notification Server filho.

Para trabalhos que contêm somente tarefas do servidor e para tarefas do servidor, o agendamento não é replicado do Notification Server pai ao filho.

Se você criar e agendar uma nova tarefa do servidor no Notification Server pai e replicá-la ao Notification Server filho, o agendamento não será replicado ao filho. Será preciso agendar essa tarefa separadamente no Notification Server filho.

Sequenciamento de tarefas

Arranjar tarefas em sequência permite executar operações de gerenciamento complexas em um único trabalho. As tarefas podem ser arranjadas em sequência em um trabalho, o que lhe oferece grande flexibilidade no trabalho.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Tabela 26-4 Processo para arranjar tarefas em sequência

Etapa	Ação	Descrição
Etapa 1	(Opcional) Distribuir servidores de tarefas.	Os Task Servers permitem distribuir trabalhos e tarefas aos computadores em sua rede. Assim, os trabalhos e as tarefas podem ser executados em computadores gerenciados. A Symantec recomenda implementar pelo menos um servidor de tarefas por Notification Server. Após implementar o servidor de tarefas dedicado inicial, adicione servidores de tarefas adicionais para cada 5000 a 7500 computadores-cliente. O número de computadores gerenciados que podem ser atendidos por um Task Server depende do hardware do computador do Task Server. Consulte “Para implementar um servidor de tarefas” na página 418.
Etapa 2	Criar uma tarefa.	Tarefas executadas no Notification Server ou em computadores gerenciados. Consulte “Para criar uma tarefa” na página 419.
Etapa 3	Criar um trabalho.	Trabalhos executam tarefas, outros trabalhos e condições. Consulte “Criação de trabalhos” na página 420.

Etapa	Ação	Descrição
Etapa 4	Executar trabalhos ou tarefas.	Os trabalhos e as tarefas podem ser executados no Notification Server ou em computadores gerenciados. Consulte “Para executar um trabalho ou uma tarefa usando o recurso de arrastar e soltar” na página 421. Consulte “Execução de um trabalho ou uma tarefa” na página 422. Consulte “Para reexecutar uma tarefa com falha” na página 423. Consulte “Para adicionar um agendamento a uma política, tarefa ou trabalho” na página 425.
Etapa 5	Exiba o status em tempo real dos trabalhos ou das tarefas.	Você pode exibir o status do trabalho ou da tarefa no Console de gerenciamento Symantec e também em um computador-cliente, no Symantec Management Agent. Nota: Para obter melhor desempenho, no Console de gerenciamento Symantec, o status da tarefa é atualizado cada cinco minutos. Consulte “Exibição do status da tarefa no Symantec Management Agent” na página 426.

Para implementar um servidor de tarefas

Os servidores de tarefas permitem distribuir os trabalhos e as tarefas em diferentes computadores na rede para que os Symantec Management Agents possam executá-los. Quando distribuir tarefas e trabalhos, você reduzirá o tráfego na rede e a carga no Notification Server. O Symantec Management Agent acessa o servidor de tarefas mais próximo para os downloads de trabalhos e tarefas.

Consulte [“Componentes do gerenciamento de tarefas”](#) na página 409.

Cada Notification Server transforma-se em um Task Server quando o componente Task Server é instalado. Assim, você poderá distribuir mais Task Servers conforme necessário.

O servidor de tarefas pode apenas ser instalado em um computador que tenha o IIS instalado.

Os requisitos para um computador de servidor de tarefas são:

- Microsoft .NET Framework versão 3.5

- Os sistemas operacionais mínimos suportados são o Windows XP x86 SP3, o Windows x64 SP2 ou o Windows Server 2003 SP2
- Serviços de Informações da Internet (IIS) da Microsoft
- Symantec Management Agent

As recomendações mínimas de hardware para um computador de servidor de tarefas são:

- Processador Intel Pentium 4 ou equivalente
- 1 GB de RAM
- 1 GB de espaço em disco

A Symantec recomenda implementar pelo menos um servidor de tarefas por Notification Server. Após implementar o servidor de tarefas dedicado inicial, adicione servidores de tarefas adicionais para cada 5000 a 7500 computadores-cliente. O número de computadores gerenciados que podem ser atendidos por um Task Server depende do hardware do computador do Task Server.

Consulte [“Sobre os serviços de site”](#) na página 127.

Esta tarefa é uma etapa no processo de sequenciamento de tarefas.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para distribuir um Task Server usando serviços de site

- ◆ Distribua um Task Server como um servidor de sites.

Consulte [“Para gerenciar servidores de sites”](#) na página 131.

Para criar uma tarefa

Você cria e distribui tarefas para computadores gerenciados usando tipos predefinidos de tarefas. O tipo de tarefa escolhido depende do que você deseja realizar. Muitos tipos de tarefas são fornecidos com o Gerenciamento de tarefas. Algumas soluções da Symantec fornecem também tipos de tarefas e tarefas de amostra.

Esta tarefa é uma etapa no processo de sequenciamento de tarefas.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para criar uma tarefa

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você quer criar a tarefa e clique em **Novo(a) > Tarefa**.

- 3 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, selecione um tipo de tarefa.
- 4 No painel direito, defina as configurações.
- 5 Clique em **OK**.

Criação de trabalhos

Você pode criar trabalhos que executem várias tarefas ou trabalhos. Os dois tipos de trabalhos são trabalhos de servidor e trabalhos de cliente. Os trabalhos de servidor são executados no Notification Server. Os trabalhos de cliente são distribuídos nos computadores gerenciados por um servidor de tarefas. Em seguida, o computador gerenciado executa o trabalho e informa o Notification Server.

Os trabalhos podem conter várias tarefas, trabalhos e condições, o que lhe fornece grande flexibilidade para configurar a sequência de trabalhos necessária.

Esta tarefa é uma etapa no processo de sequenciamento de tarefas.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para criar um trabalho

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você quer criar a tarefa e depois clique em **Novo(a) > trabalho do servidor** ou **Novo(a) > Trabalho do cliente**.
- 3 No painel direito, configure o trabalho:

Edite o nome do trabalho	Clique no texto do nome e digite o novo nome.

Crie uma nova tarefa
adicionar um trabalho

- 1 Clique em **Novo(a) > Tarefa**.
- 2 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, selecione uma tarefa.
- 3 No painel direito, defina as configurações.
- 4 Clique em **OK**.

Adicione uma tarefa ou um trabalho existente a um trabalho	1 Clique em Adicionar existente. 2 Na caixa de diálogo Adicionar tarefa existente, no painel esquerdo, selecione a tarefa ou trabalho que deseja adicionar. 3 Clique em OK. Um recurso de arrastar e soltar está disponível e permite alterar a ordem das tarefas ou trabalhos adicionados a um trabalho. Você também pode usar as setas para cima e para baixo no menu para mover tarefas, trabalhos e condições.
Adicione uma condição a um trabalho	1 Clique em Nova > Condição. 2 Na caixa de diálogo Editar condição, a regra fornece uma cláusula Where que permite selecionar uma tarefa ou um trabalho, uma operação a executar e uma condição para executar a operação na tarefa ou no trabalho. 3 Na primeira lista suspensa, selecione ou digite a tarefa ou o trabalho e o código de retorno para a condição. 4 Na segunda lista suspensa, selecione a operação que a regra executará. 5 No terceiro campo, digite a condição. 6 (Opcional) Para adicionar mais regras, clique em Adicionar regra. 7 Clique em OK. Você pode adicionar uma ou mais tarefas ou trabalhos para serem executados como resultado da condição em Else.

- 4 Clique em **Salvar alterações**.

Para executar um trabalho ou uma tarefa usando o recurso de arrastar e soltar

Na exibição aprimorada **Trabalhos / Tarefas**, você pode exibir, executar e agendar trabalhos e tarefas com facilidade.

Consulte [“Sobre a exibição Trabalhos/Tarefas”](#) na página 43.

Você pode executar trabalhos e tarefas arrastando e soltando os itens em um ou mais computadores. Você pode também usar a opção **Execução rápida** para visar a um trabalho ou uma tarefa sem precisar exibir os detalhes manualmente.

Consulte [“Especificação dos destinos de uma política ou tarefa”](#) na página 380.

Nota: Você deve ter uma das seguintes soluções ou séries instaladas para executar esta tarefa: Deployment Solution (produto autônomo), IT Management Suite, Server Management Suite ou Client Management Suite.

Para executar um trabalho ou uma tarefa usando o recurso de arrastar e soltar

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel de navegação, clique no trabalho ou na tarefa que você quer executar e arraste-os para a direita para iniciar a operação de arrastar e soltar.

Os resultados de sua pesquisa mais recente de computador aparecerão no painel de listas. Se você tiver filtrado sua pesquisa mais recente de computador, a lista exibirá os resultados da pesquisa filtrada.

Consulte [“Para pesquisar um computador e salvar a pesquisa como um filtro”](#) na página 38.

- 3 Para selecionar os computadores nos quais você quer executar o trabalho ou a tarefa, execute um destes procedimentos:
 - Para executar o trabalho ou a tarefa em todos os computadores relacionados, solte-os no ícone do título, no painel de listas.
 - Para executar o trabalho ou a tarefa em um computador específico, solte-os no computador, dentro da lista.
 - Para executar o trabalho ou a tarefa em uma pesquisa salva, exibição organizacional ou o grupo organizacional, arraste-os para a blade **Computadores** e solte-os então em uma pesquisa salva, em uma exibição organizacional ou em um grupo organizacional.
- 4 Na caixa de diálogo **Novo agendamento**, especifique o agendamento do trabalho ou da tarefa e clique em **Agendar**.

Execução de um trabalho ou uma tarefa

Os trabalhos e as tarefas que você cria podem ser executados no Notification Server ou em computadores gerenciados, dependendo de serem tarefas do servidor ou tarefas do cliente. As tarefas do servidor são tarefas que são executadas em

um computador do Notification Server. As tarefas do cliente são tarefas executadas em um computador-cliente.

Se mais de uma tarefa for adicionada a um trabalho, elas serão executadas uma após a outra. Se uma condição for adicionada, as tarefas executadas serão baseadas nos resultados da condição. O servidor deve receber o status de uma tarefa anterior que tenha sido concluída antes que a próxima tarefa no trabalho seja iniciada. Poderá haver um atraso de alguns segundos antes de iniciar a próxima tarefa.

Esta tarefa é uma etapa no processo de sequenciamento de tarefas.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para executar um trabalho ou uma tarefa

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, selecione o trabalho ou a tarefa que você deseja executar.
- 3 Adicione uma agenda para executar o trabalho ou a tarefa.

Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.

Para reexecutar uma tarefa com falha

Você pode reexecutar uma tarefa em computadores com falha.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

A nova execução da tarefa funciona da seguinte forma:

- Você pode selecionar várias instâncias da tarefa para reexecutar. Todos os computadores com falha das instâncias da tarefa incluídas serão incluídos na nova execução da instância da tarefa.
- Você pode reexecutar somente tarefas com falhas do cliente, não tarefas com falhas do servidor.
- **Falha ao executar novamente** ignora os destinos que foram usados na instância de tarefa anterior, não importa como tenham sido criados (Execução rápida, Agendamento em relação a uma lista de computadores ou agendamento em relação a um destino). Ela é reexecutada em relação à lista de computadores com falha da tarefa recém executada.

Nota: Use a função de nova execução da tarefa somente no nível do Notification Server filho, onde é possível ver indicadores do status da tarefa. Recomendamos não reexecutar tarefas através de um Notification Server pai em uma hierarquia, devido ao tempo de atraso na replicação dos dados.

Para reexecutar uma tarefa com falha

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Computadores**.

Nota: Você também pode acessar **Gerenciar > Trabalhos e tarefas** e ignorar as etapas 2 e 3.

- 2 Clique nas setas duplas (>>) na parte superior do painel de listas para navegar ao resumo do container de **Entregas de software**.
- 3 Em **Tarefas de entrega rápida**, clique em uma instância de tarefa que falhou em alguns computadores e que você deseja reexecutar nesses computadores.
- 4 No painel **Status da tarefa**, clique em **Falha ao executar novamente** para reexecutar as instâncias de tarefa na lista de computadores que retornou um status **Falhas**.
- 5 Essa ação inicia a janela **Novo agendamento**. Ela pré-preenche o campo **Dispositivos selecionados** com os computadores nos quais as instâncias de tarefa não foram executadas.

Nota: Se você clicar em **Falha ao executar novamente** em uma instância de tarefa sem computadores com falha, uma mensagem pop-up indicará que não há computadores com falha na instância de tarefa. Quando você clicar em **Falha ao executar novamente** em uma instância de tarefa que estiver em estado pendente ou em execução, nenhum computador será relacionado, porque a tarefa ainda não obteve êxito nem falhou.

- 6 Clique em **Agendar** para agendar a tarefa a ser reexecutada nos computadores com falha.

Isso criará uma nova instância da tarefa. A instância antiga ainda estará lá.

Nota: Você pode encontrar uma mensagem de erro onde se lê: “Esta execução da tarefa foi excluída e não pode ser exibida ou reexecutada. Somente os dados de resumo existem”. O gerenciamento de tarefas tem uma tarefa diária de limpeza que é executada por especificações do usuário, para limitar o número de linhas em funcionamento no banco de dados. Isso impede que o desempenho do gerenciamento de tarefas se torne lento demais. Por padrão, todas as noites, a tarefa de limpeza retém somente as 200,000 instâncias de tarefa mais recentes. A contagem do computador ainda mostra todos os computadores em que a tarefa foi executada. Contudo, se os detalhes de uma das instâncias de tarefa tiverem sido excluídos, **Falha ao executar novamente** não incluirá essas tarefas. Como resultado, pode haver uma discrepância entre a contagem do computador com falha na tarefa e a contagem quando você clicar em **Falha ao executar novamente**.

- 7 Esse novo agendamento aparecerá então na página do flipbook **Entregas de software**. Você pode exibir qual instância da tarefa foi executada ou reexecutada mais recentemente. Também é possível ver em quantos computadores a tarefa foi executada com êxito ou sem êxito.

Para adicionar um agendamento a uma política, tarefa ou trabalho

Ao agendar uma política, tarefa ou trabalho para execução, você tem duas opções: execução rápida e agenda. A opção de execução rápida executa imediatamente a política, tarefa ou trabalho atual em um computador especificado. A opção de agenda fornece diversas opções de agenda e de computador de destino. A opção de agenda permite definir uma agenda. O destino deve ser definido em outra parte.

Para adicionar uma agenda de execução rápida

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, selecione a política, tarefa ou trabalho ao qual deseja aplicar a execução rápida.
- 3 No painel direito, em **Status da tarefa**, clique em **Execução rápida**.
- 4 Na caixa de diálogo **Execução rápida agora**, selecione o nome do computador em que você deseja executar a política, tarefa ou trabalho.
- 5 Clique em **Executar**.

Para adicionar um novo agendamento

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, selecione a política, tarefa ou trabalho que deseja agendar.
- 3 No painel direito, em **Status da tarefa**, clique em **Novo agendamento**.
- 4 Na caixa de diálogo **Novo agendamento**, configure a agenda.
- 5 Clique em **Agendar**.

Quando as tarefas ou os trabalhos são selecionados para execução, eles aparecem na seção Status do trabalho e da tarefa.

Exibição do status da tarefa no Symantec Management Agent

O status da tarefa (que inclui o histórico da tarefa) é registrado no Symantec Management Agent. Para exibir o status da tarefa em um computador, abra o Symantec Management Agent. O status da tarefa permite visualizar quais tarefas foram executadas e o resultado.

Esta tarefa é uma etapa no processo de sequenciamento de tarefas.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para exibir o status da tarefa no Symantec Management Agent

- 1 No computador no qual você quer exibir o status, clique duas vezes no ícone na bandeja do sistema para abrir o Symantec Management Agent.
- 2 Na janela **Symantec Management Agent**, clique na guia **Status da tarefa**.

Exibição e edição das permissões em um tipo de tarefa

Você pode exibir e editar as permissões nas propriedades do tipo de tarefa. Alterar as permissões no tipo de tarefa permite que você controle quais usuários podem criar tarefas novas. Os usuários que têm permissão para Criar nova tarefa podem criar novas tarefas desse tipo.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Consulte [“Permissões do servidor de tarefas”](#) na página 507.

Para exibir e editar permissões em um tipo de tarefa

- 1 No Symantec Management Console, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Notification Server > Configurações de tarefas > Tipos de tarefas**.
- 3 Procure e clique no tipo de tarefa que você quer exibir.
- 4 No painel direito, clique em **Ver permissões**.
- 5 Para editar permissões, no Gerenciador de função de segurança edite as permissões no tipo de tarefa.

Consulte [“Para atribuir permissões de segurança a pastas e itens”](#) na página 103.

Para criar tarefas para propriedades de entrada ou saída de tarefas

As propriedades de entrada são as propriedades passadas para uma tarefa de alguma fonte. As tarefas podem receber propriedades de entrada de um valor definido, de outras tarefas ou do tempo de execução. As tarefas podem usar as propriedades de entrada (semelhantes às variáveis) para executar suas funções. Todas as propriedades disponíveis para uma tarefa (tanto as propriedades de entrada como as propriedades criadas pela tarefa) são denominadas propriedades da tarefa.

Uma tarefa pode enviar as propriedades da tarefa a outras tarefas. Se você tiver uma tarefa que envia propriedades, todas as tarefas subsequentes nesses trabalhos podem usar as propriedades de saída para as propriedades de entrada. As tarefas não precisam ser simultâneas.

Você não precisa de uma tarefa de saída para cada tarefa de entrada. As tarefas de entrada também podem receber a entrada de um valor definido ou do tempo de execução.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Consulte [“Para criar uma tarefa”](#) na página 419.

Para criar uma tarefa que envie propriedades

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você quer criar a tarefa e clique em **Novo(a) > Tarefa**.

- 3 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, selecione a tarefa que tem a opção **Avançadas** (por exemplo: **Executar script**).
- 4 No painel direito, clique em **Avançadas**.
- 5 Selecione **Salvar o script output com status da tarefa** e clique em **OK**.
Quando uma tarefa estiver selecionada nesta caixa, todas as propriedades da tarefa se tornarão visualizáveis e disponíveis para as tarefas subsequentes de um trabalho.
- 6 Configure a tarefa.
- 7 Na caixa de diálogo **Criar nova tarefa**, clique em **OK**.

Para criar uma tarefa com propriedades de entrada de outra tarefa

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você quer criar a tarefa e clique em **Novo(a) > Tarefa**.
- 3 Na caixa de diálogo **Criar nova tarefa**, no painel esquerdo, selecione uma tarefa de script.
As tarefas de script recebem propriedades de entrada.
- 4 Para usar esta tarefa com o objetivo de passar as propriedades para outra tarefa, clique em **Avançadas**, selecione **Salvar saída do script com status da tarefa** e clique em **OK**.
- 5 Na caixa de diálogo **Criar nova tarefa**, na seção de comando do script, insira um ou mais tokens (por exemplo: `%!input!%`) que capturem a saída.
- 6 Clique em **OK**.

Para configurar tarefas em um trabalho para entrada

- 1 Crie um trabalho e o coloque nas tarefas criadas para saída e entrada. Cada tarefa de saída deve preceder uma tarefa que recebe sua saída.
Consulte "[Criação de trabalhos](#)" na página 420.
- 2 Configure cada tarefa de entrada no trabalho.
A entrada da tarefa será exibida no lado direito quando você clicar na tarefa nas seguintes situações: quando uma tarefa do cliente tiver entrada e estiver em um trabalho do cliente ou quando houver uma tarefa do cliente dentro de um trabalho do servidor.

Solicitar a entrada da tarefa sempre que esse trabalho for executado Selecione para inserir a entrada manualmente quando o trabalho for executado.

Inserir a entrada da tarefa agora Selecione para inserir a entrada da tarefa neste momento:

- **Usar um valor definido**

Selecione para usar um valor que não seja alterado. Insira o valor no campo exibido quando a tela é atualizada. Se esta tarefa for uma tarefa do cliente dentro de um trabalho do servidor, será necessário selecionar o computador ou os computadores que executam a tarefa do cliente. Todas as tarefas do cliente têm este parâmetro como um parâmetro padrão de entrada quando são trabalhos internos do servidor.

- **Use uma saída anterior da tarefa**

Selecione para usar uma saída anterior da tarefa. Use este parâmetro se houver uma tarefa de saída neste trabalho que você deseja usar. Quando a tela é atualizada, o nome da variável é exibido, bem como uma lista de tarefas de saída disponíveis. Selecione a tarefa cuja saída você deseja usar para esta tarefa.

- **Solicitar no tempo de execução**

Selecione para ser solicitado para fornecer a entrada no tempo de execução.

3 Clique em **OK**.

Para limpar dados de tarefas

Para diminuir a carga em seus recursos do sistema, dados da tarefa pode ser arquivados ou excluídos usando opções de limpeza.

Consulte “[Sobre o Gerenciamento de tarefas](#)” na página 407.

Consulte “[Sequenciamento de tarefas](#)” na página 417.

Para limpar dados de tarefas

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Notification Server > Configurações de tarefas > Limpar dados da tarefa**.

- 3 Na página **Limpar dados da tarefa**, edite os detalhes necessários.

Todas as noites, os dados de tarefas atuais e os dados de tarefas arquivados são movidos ou excluídos de acordo com as seguintes configurações.

Número máximo de linhas do banco de dados de trabalho	Depois que o número de linhas do banco de dados de trabalho atinge o número máximo, as linhas mais antigas são arquivadas até que o número máximo não seja excedido.

As linhas do banco de dados de trabalho são as linhas do banco de dados que foram usadas recentemente. Recomendamos manter esse número pequeno para diminuir a carga nos recursos do sistema.

Executar a tarefa de limpeza sob demanda	Se você selecionar esta opção e o número de linhas usado for excedido, a tarefa da limpeza será começada imediatamente.

- 4 (Opcional) Adicione um agendamento para limpar os dados da tarefa.

Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.

- 5 Clique em **Salvar alterações**.

Para limpar dados da versão da tarefa

Para diminuir a carga nos recursos do sistema, o histórico da versão da tarefa pode ser arquivado ou excluído usando as opções de limpeza.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Para limpar dados da versão da tarefa

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Notification Server > Configurações de tarefas > Limpar dados de versão**.

- 3 Na página **Limpar dados de versão**, edite os detalhes necessários.

Por padrão, toda semana, as versões da tarefa são excluídas de acordo com as seguintes configurações.

Número máximo de versões da tarefa a manter no banco de dados	Depois que o número de versões atinge o número selecionado, as mais antigas são excluídas para melhorar o desempenho do banco de dados.

Você pode selecionar manter 1, 5, 10 ou 20 versões de uma tarefa no banco de dados.

- 4 (Opcional) Adicione um agendamento para limpar os dados da tarefa.

Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.

- 5 Clique em **Salvar alterações**.

Alteração das configurações do Client Task Agent

O Client Task Agent faz parte do Symantec Management Agent. Ele recebe trabalhos e tarefas do Task Server e as executa em computadores gerenciados. Em seguida, ele relata ao Notification Server.

Nota: Quando você instalar o Symantec Management Agent em um computador, haverá um atraso antes que o Client Task Agent seja registrado no Notification Server. Todas as tarefas que forem selecionadas no computador durante esse tempo (normalmente, em torno de 10 minutos) ficarão com um status pendente até que o Client Task Agent seja registrado. Quando o Client Task Agent for registrado, as tarefas serão executadas imediatamente.

Nota: Geralmente, o Client Task Agent abre uma conexão direta com o servidor de tarefas na porta 50124. O servidor de tarefas usa esta conexão para informar ao agente quando as tarefas novas estão disponíveis. Porém, se um proxy estiver sendo usado, uma conexão direta será impossível; assim, o Task Server não pode dizer ao agente quando as tarefas novas se tornam disponíveis. Para manter atualizado, você precisa definir o valor adequado de **Verificar novas tarefas no Task Server** no campo de **Atualização de tarefa**.

Consulte [“Sobre o Gerenciamento de tarefas”](#) na página 407.

Consulte [“Sequenciamento de tarefas”](#) na página 417.

Consulte [“Componentes do gerenciamento de tarefas”](#) na página 409.

Você pode alterar as configurações do Client Task Agent para melhorar a eficiência do trabalho entre o Client Task Agent e o servidor de tarefas. Para melhorar a eficiência, é possível definir o intervalo de tempo em que você deseja que o Client Task Agent solicite tarefas do servidor de tarefas. Você pode definir o método padrão pelo qual o Notification Server seleciona o servidor de tarefas. Você também pode definir a ação que desejará executar se vários servidores de tarefa estiverem disponíveis em um site.

Para alterar as configurações do Client Task Agent

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, clique em **Notification Server > Configurações de tarefas > Configurações do Task Agent**.
- 3 Na página **Configurações do Task Agent**, edite os detalhes necessários.

Verificar no Task Server se há novas tarefas a cada O intervalo, em minutos, no qual que você deseja que o agente solicite tarefas do Task Server.

Quando mais de um Task Server estiver disponível em um site A ação que você deseja executar se vários Task Servers estiverem disponíveis em um site.

- 4 Selecione os destinos, os computadores ou os usuários aos quais as mudanças serão aplicadas.
- 5 Clique em **Salvar alterações**.

Acesso ao Portal de trabalhos e tarefas

O Portal de trabalhos e tarefas permite criar e agendar tarefas para execução em seus recursos gerenciados. Você pode acessar o Portal de trabalhos e tarefas do Symantec Management Console.

O Portal de Trabalhos e tarefas dá acesso fácil à maioria das ações de trabalhos e tarefas, que são fornecidas pelo Gerenciamento de tarefas.

Diversas Web Parts são fornecidas nesta página:

Início rápido - Trabalhos e Tarefas Permite criar, executar ou agendar trabalhos e tarefas.

Servidores de tarefas Permite exibir seus servidores de tarefas e o número de computadores-cliente conectados a cada servidor de tarefas.

Dispositivos e computadores da tarefa	Permite exibir seus servidores de tarefas e computadores gerenciados.

Você pode também configurar a página para mostrar as Web parts desejadas. A opção **Editar**, no canto superior direito, permite alterar as Web Parts exibidas neste portal.

Para acessar o Portal de trabalhos e tarefas

- 1 No **Symantec Management Console**, no menu **Configurações**, clique em **Console > Páginas do portal**.
- 2 No painel esquerdo, clique em **Portal de trabalhos e tarefas**.
- 3 (Opcional) No **Portal de trabalhos e tarefas**, clique no ícone **Atualizar** na Web Part que você deseja atualizar.

Se você quiser configurar uma atualização automática para uma Web part, clique no ícone **Atualizar**, selecione **Atualizar a cada** e, na lista suspensa, clique no intervalo de atualização desejado.

Para usar o Gerenciador de recursos

Este capítulo contém os tópicos a seguir:

- [Sobre gerenciamento de recursos](#)
- [Acesso ao Gerenciador de recursos](#)
- [Exibição dos dados de inventário para uma classe de dados](#)
- [Exibição dos dados de evento para uma classe de dados](#)
- [Adição de recursos a um grupo organizacional](#)
- [Tarefas do Gerenciador de recursos](#)

Sobre gerenciamento de recursos

Você pode gerenciar os recursos no Configuration Management Database (CMDB) usando o Gerenciador de recursos. O Gerenciador de recursos permite exibir as informações e executar várias tarefas em recursos. As informações disponíveis e as tarefas que você pode executar dependem do tipo dos recursos que são selecionados.

Quando você acessar o Gerenciador de recursos, a **Página do portal Recurso base** será exibida para todos os recursos, exceto computadores e pacotes de software. Para um recurso de computador ou um pacote de software, a página **Gerenciador de recursos** é exibida. A página exibida para recursos não relacionados a computador contém a Web part **Item Property Summary**. Esta Web part exibe as informações de propriedades do recurso selecionado (como GUID e nome do produto). Para um recurso de computador, é exibida uma página de resumo do recurso de computador. Se clicar em **Portal do Gerenciador de**

recursos, no menu **Home**, você poderá acessar a Web part **Item Property Summary** de um recurso de computador.

Consulte [“Tarefas do Gerenciador de recursos”](#) na página 438.

Você pode acessar o Gerenciador de recursos de diversas maneiras. Os diferentes métodos facilitam o acesso ao Gerenciador de recursos, independentemente de onde você está no Symantec Management Console.

Consulte [“Acesso ao Gerenciador de recursos”](#) na página 435.

Acesso ao Gerenciador de recursos

É possível acessar o Gerenciador de recursos das seguintes maneiras:

- Usando o menu **Gerenciar** no Symantec Management Console
- Clicando com o botão direito do mouse no recurso em uma lista ou em um relatório
- Clicando duas vezes no recurso em uma lista ou em um relatório
- Digitando um URL em seu navegador da Web

Consulte [“Sobre gerenciamento de recursos”](#) na página 434.

Para acessar o Gerenciador de recursos do menu Gerenciar

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Recurso**.
- 2 Na caixa de diálogo **Selecionar recurso**, selecione os recursos que você deseja gerenciar e clique em **OK**.

A página do Gerenciador de recursos abre com as informações resumidas sobre os recursos selecionados.

Para acessar o Gerenciador de recursos em um menu, clique com o botão direito do mouse

- ◆ Em uma lista de recursos ou em um relatório do Symantec Management Console, clique com o botão direito do mouse nos recursos que você deseja gerenciar e clique em **Gerenciador de recursos**.

Em algumas listas, recursos ou relatórios, a opção de clique com o botão direito do mouse do Gerenciador de recursos pode não estar disponível. Nestes casos, use outro método para acessar o Gerenciador de recursos.

Para acessar o Gerenciador de recursos clicando duas vezes em um recurso

- ◆ Em uma lista de recursos ou em um relatório no Symantec Management Console, clique duas vezes no recurso que deseja gerenciar.

Para acessar o Gerenciador de recursos de URL

- ◆ Em uma janela do navegador, digite o seguinte URL:

`http://NS Name/Altiris/Console/Dashboard/DashboardView.aspx?name=Nome do recurso de destino`

Nome do NS é o nome do computador do Notification Server. *Nome do recurso de destino* pode ser o nome do recurso, o GUID dos recursos ou o GUID do item. Se você omitir o “?name=Nome do recurso de destino”, o Gerenciador de recursos será aberto com o seguinte erro:

Nenhum GUID de recurso fornecido.

Ao usar um banco de dados que diferencia maiúsculas e minúsculas, certifique-se de que o nome recurso de destino corresponda ao nome dos recursos no banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database), inclusive diferenciando maiúsculas de minúsculas.

Exibição dos dados de inventário para uma classe de dados

Usando o Gerenciador de recursos, você pode exibir os dados de evento para uma classe de dados específica. Os dados de inventário que são exibidos dependem da classe de dados selecionada. Em geral, é possível exibir status e dados atuais. Quando aplicável, os dados de histórico também estão disponíveis.

Consulte “[Acesso ao Gerenciador de recursos](#)” na página 435.

Para exibir os dados de inventário para uma classe de dados

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Recurso**.
- 2 Na caixa de diálogo **Selecionar recurso**, selecione os recursos que você deseja gerenciar e clique em **OK**.
- 3 No **Gerenciador de recursos**, no menu **Exibir**, clique em **Inventário**.
- 4 Na árvore, selecione a classe de dados da qual você quer exibir os dados de inventário.
- 5 No painel direito, selecione a guia que contém as informações que deseja exibir.

Exibição dos dados de evento para uma classe de dados

Usando o Gerenciador de recursos, você pode exibir os dados de evento para uma classe de dados específica. Os dados do evento que são exibidos dependem da classe de dados selecionada. Em geral, você pode visualizar o status e os dados atuais sobre os eventos da classe de dados.

Para exibir os dados de evento para uma classe de dados

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Recurso**.
- 2 Na caixa de diálogo **Selecionar recurso**, selecione os recursos que você deseja gerenciar e clique em **OK**.
- 3 No **Gerenciador de recursos**, no menu **Exibir**, clique em **Eventos**.
Consulte [“Acesso ao Gerenciador de recursos”](#) na página 435.
- 4 Na árvore, selecione a classe de dados da qual você quer exibir os dados de evento.
- 5 No painel direito, selecione a guia que contém as informações que deseja exibir.

Adição de recursos a um grupo organizacional

A caixa de diálogo Adicionar ao grupo organizacional permite adicionar os recursos selecionados a um grupo organizacional. Um recurso pode aparecer apenas uma vez em cada exibição organizacional.

Para adicionar recursos a um grupo organizacional

- 1 No Symantec Management Console, no menu **Gerenciar**, clique em **Recurso**.
- 2 Na caixa de diálogo **Selecionar recurso**, selecione os recursos que você deseja gerenciar e clique em **OK**.
- 3 No painel esquerdo do **Gerenciador de recursos**, clique em **Adicionar ao link do grupo organizacional**.
- 4 Na caixa de diálogo **Adicionar ao grupo organizacional**, selecione o grupo organizacional ao qual deseja adicionar os recursos.
- 5 Clique em **OK**.

Consulte [“Tarefas do Gerenciador de recursos”](#) na página 438.

Tarefas do Gerenciador de recursos

O Gerenciador de recursos permite executar diversas tarefas em um recurso. Estas tarefas estão disponíveis através do menu **Tarefas** do Gerenciador de recursos. As tarefas disponíveis dependem do tipo de recurso selecionado.

Consulte [“Sobre gerenciamento de recursos”](#) na página 434.

Tabela 27-1 Tarefas do Gerenciador de recursos

Tarefa	Descrição
Acessar o portal de gerenciamento de tarefas	Se a tarefa que deseja executar não estiver listada no painel esquerdo, você poderá acessar o portal de gerenciamento de tarefas para encontrar tarefas adicionais.
Adicionar recursos a um grupo organizacional	Você pode adicionar os recursos selecionados a um grupo organizacional ou movê-los para um novo grupo organizacional. Se você selecionar um grupo organizacional dentro de uma exibição organizacional da qual o recurso ainda não seja membro, o recurso será adicionado ao grupo organizacional. Se você escolher um grupo organizacional dentro da exibição organizacional da qual o recurso já seja membro, o grupo organizacional recém-selecionado substituirá o grupo organizacional anterior.
Excluir um recurso	Você pode excluir o recurso selecionado do banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database).
Mesclar recursos duplicados da empresa	(apenas recursos da empresa) Se houver duas entradas para a mesma empresa, você pode usar esses recurso para mesclar as entradas.
Fazer ping nos computadores	Você pode usar a opção Enviar ping para computador , do menu Tarefa , para fazer ping no computador selecionado.
Agendar tarefa	Você pode usar a opção Agendar tarefa , do menu Tarefa , para agendar a execução de um trabalho ou de uma tarefa.
Exibir um resumo organizacional	Você pode exibir (Resumos > Resumo organizacional) os grupos organizacionais dos quais o recurso selecionado é parte.

Tarefa	Descrição
Exibir calendário	Você pode usar a opção Calendário, do menu Exibir, para exibir as informações de agendamento do Notification Server. Consulte “Para exibir do calendário de agendamento interno do Notification Server” na página 124.
Exibir eventos	Você pode exibir os dados de eventos para uma classe de dados, inclusive as informações gerais sobre a classe de dados e o status da classe de dados. Consulte “Exibição dos dados de evento para uma classe de dados” na página 437.
Exibir inventário	Você pode exibir os dados de inventário de uma classe de dados, inclusive as informações gerais sobre a classe de dados e o status da classe de dados. Consulte “Exibição dos dados de inventário para uma classe de dados” na página 436.
Exibir associações de recursos	Você pode exibir os recursos aos quais o recurso selecionado está associado no painel esquerdo. Se você selecionar o recurso associado no painel esquerdo, o Gerenciador de recursos permitirá gerenciar esse recurso.
Exibir detalhes dos recursos	Quando o Gerenciador de recursos é aberto, o painel direito fornece detalhes sobre o recurso selecionado.
Exibir as associações de recursos	Você pode usar a opção Associação de recursos, do menu Exibir, para exibir as informações da associação do recurso. A página de associação dos recursos exibe informações sobre o tipo da associação do recurso e os nomes dos tipos de recursos que estão associados ao recurso selecionado. Consulte “Para exibir e gerenciar dados de recursos com relatórios do Notification Server” na página 441.

Para usar relatórios do Notification Server

Este capítulo contém os tópicos a seguir:

- [Sobre relatórios do Notification Server](#)
- [Para exibir e gerenciar dados de recursos com relatórios do Notification Server](#)

Sobre relatórios do Notification Server

Você pode exibir e gerenciar os dados de recursos nos relatórios do Notification Server. Estes relatórios apresentam informações sobre os computadores gerenciados e não gerenciados e sobre a configuração do Notification Server. As soluções instaladas fornecem também relatórios com informações específicas sobre essa solução. Por exemplo, você pode usar esses relatórios para obter mais informações sobre os eventos e as políticas de automação executadas pelo Notification Server e quanto tempo elas demoram.

Os relatórios podem ser protegidos de modo que somente os usuários apropriados possam executá-los. Além disso, os relatórios retornam somente os dados que o usuário que executa o relatório tem permissão para visualizar. Por exemplo, se um gerente executa um relatório de salários, ele obtém apenas os salários de seus funcionários.

Os relatórios permitem exibir as informações de várias maneiras. Você pode exibir suas informações em tabelas ou gráficos. Você também pode fazer uma busca detalhada em itens específicos de um relatório para obter informações adicionais.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Uma ampla gama de relatórios é fornecida com o Notification Server. Não é possível modificar esses relatórios padrão, mas você pode duplicá-los e editar o clone para atender a seus requisitos. Também é possível criar novos relatórios personalizados.

Para exibir e gerenciar dados de recursos com relatórios do Notification Server

Você pode usar relatórios para exibir e gerenciar dados de recursos. Os relatórios recuperam dados do CMDB.

Consulte [“Sobre relatórios do Notification Server”](#) na página 440.

Tabela 28-1 Processo para exibir e gerenciar dados de recursos com relatórios do Notification Server

Etapa	Ação	Descrição
Etapa 1	Extraia os resultados do relatório.	Você deve selecionar o relatório que será usado e, opcionalmente, definir os parâmetros de usuário e selecionar a captura de imagem que será usada. Consulte “Para extrair resultados do relatório do Notification Server” na página 442.
Etapa 2	Veja os resultados do relatório.	Você pode configurar a exibição do relatório para atender aos seus requisitos: ■ Selecione a exibição em grade ou em gráfico para usar, caso outras exibições tenham sido configuradas para o relatório. ■ Agrupe e ordene as colunas na exibição em grade. ■ Exiba os resultados em uma exibição de gráfico, caso elas tenham sido definidas para o relatório. Consulte “Para exibir resultados do relatório do Notification Server” na página 444.
Etapa 3	(Opcional) Use os resultados do relatório.	Você pode usar os resultados do relatório das seguintes maneiras: ■ Clicar duas vezes nos itens selecionados para obter informações mais detalhadas. Clicar duas vezes em um item abre a exibição apropriada, a qual pode ser outro relatório ou o console do Gerenciador de recursos. ■ Executar ações nos itens selecionados. ■ Imprimir os resultados do relatório. Consulte “Para usar resultados do relatório do Notification Server” na página 445.

Etapa	Ação	Descrição
Etapa 4	(Opcional) Salve os resultados do relatório.	Os resultados do relatório podem ser salvos nos seguintes formatos: ■ Arquivo Planilha (.csv), arquivo HTML e arquivo XML são fornecidos com o Notification Server. As soluções instaladas podem fornecer opções para tipos de arquivo adicionais. Consulte “Para salvar os resultados do relatório do Notification Server como um arquivo” na página 446. ■ Filtro estático Consulte “Para criar um filtro estático dos resultados do relatório do Notification Server” na página 447. ■ Captura de imagem Consulte “Para salvar os resultados do relatório do Notification Server como uma captura de imagem” na página 448. ■ Web part Consulte “Para salvar os resultados do relatório do Notification Server como uma Web part” na página 449.

Para extrair resultados do relatório do Notification Server

Um conjunto de relatórios é fornecido com o Notification Server e as soluções instaladas podem acrescentar relatórios adicionais.

Alguns relatórios têm parâmetros do usuário que podem ser definidos ao extrair os resultados do relatório. Os parâmetros de usuário são variáveis na consulta de relatório e tornam os relatórios mais flexíveis e potentes. Por exemplo, a lista Computador por relatório do tipo de sistema e nome do sistema operacional tem os parâmetros do usuário definidos para o tipo de sistema e o nome do sistema operacional. Ao extrair resultados do relatório, é possível especificar a combinação do tipo e do nome do sistema operacional que você deseja usar definindo os parâmetros apropriados. Sem parâmetros de usuário, os relatórios teriam valores definidos na consulta. Você precisaria para ter um relatório diferente para cada combinação de tipo de sistema e do nome do sistema operacional. Como alternativa, você precisaria modificar a consulta de relatório cada vez que quisesse extrair resultados.

Para minimizar a carga no Notification Server, relatórios grandes ou frequentemente usados são geralmente agendados para serem executados em intervalos apropriados e são salvos como capturas de imagem. A criação de capturas de imagem permite que os usuários restantes exibam os resultados do relatório na captura de imagem mais recente em vez de cada usuário executar o relatório novamente. Os relatórios agendados são executados normalmente no escopo de

Administrador para garantir que todos os dados disponíveis sejam incluídos. Quando você exibir o conjunto de resultados do relatório, os dados da captura de imagem recebem o escopo apropriado. Quando você exibir resultados do relatório, poderá escolher a captura de imagem a ser utilizado. Caso você não escolha uma captura de imagem, os resultados serão extraídos executando a consulta de relatório no CMDB.

Em grandes ambientes, a Symantec recomenda usar a funcionalidade **SuppressReportAutorun**. Quando **SuppressReportAutorun** estiver ativado e você abrir algum relatório, esse não será executado imediatamente. Para ver os resultados do relatório, clique em **Atualizar**. Por padrão, a funcionalidade **SuppressReportAutorun** está desativada. Você pode ativá-la no **Configurador do NS**, em **Configurações principais > Interface do usuário > Relatório > SuppressReportAutorun**.

Consulte [“Como definir as configurações do Notification Server com o configurador do NS”](#) na página 75.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para extrair resultados do relatório do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 (Opcional) No painel direito, em **Parâmetros**, defina os parâmetros apropriados do usuário.

Consulte [“Para definir provedores de valores e parâmetros para um relatório personalizado”](#) na página 460.

- 4 Se desejar usar uma captura de imagem, na lista suspensa **Exibir**, selecione a captura de imagem apropriada.

As opções são predefinidas como:

- Atual
- Captura de imagem mais recente

Todas as capturas de imagem adicionais que você criar serão relacionadas. Cada um é rotulado com a data e a hora de criação.

Para exibir resultados do relatório do Notification Server

Você pode visualizar os resultados do relatório usando as seguintes exibições, se elas estiverem configuradas para o relatório:

Exibição em grade	As exibições em grade são tabelas com os itens dos resultados exibidos em linhas separadas. As colunas disponíveis são definidas no relatório. Você pode mudar a ordem da coluna e agrupar os resultados de acordo com os valores de uma coluna específica. Por exemplo, talvez convenha agrupar uma lista de computadores pelo tipo de sistema operacional ou pela sub-rede.
Exibição de gráfico	As exibições em gráfico são formatos gráficos, como gráficos de barra, de linha, de pizza e de área. Várias exibições de gráfico podem ser definidas no relatório, mas você pode exibir somente um de cada vez.

Cada gráfico ou grade é uma exibição específica dos resultados do relatório; assim, uma exibição pode conter um subconjunto de resultados. Um relatório pode ter várias exibições disponíveis para personalizar a saída para usuários diferentes, em vez de criar relatórios distintos para cada usuário. Por exemplo, um relatório que relacione computadores gerenciados pode incluir as propriedades de cada computador, como o sistema operacional, o tipo de processador e o tamanho do disco. O relatório pode ter várias exibições diferentes, com cada exibição contendo um subconjunto das propriedades disponíveis para cada computador. Quando você verifica o relatório, você pode optar pela exibição que contém as propriedades que o interessam.

Quando você salva um relatório, todos os resultados em seu escopo são salvos. Você não fica restrito aos dados exibidos na exibição atual. Quando você imprime um relatório, a exibição atual é impressa.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para exibir resultados do relatório do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 No painel direito, na lista suspensa **Exibir**, selecione a exibição apropriada. Todas as exibições em grade e em gráfico que foram criadas serão listadas.

- 4 (Opcional) Se desejar agrupar os resultados, na lista suspensa **Agrupar por**, selecione a coluna apropriada.
- 5 (Opcional) Para alterar a ordem das colunas, clique em um cabeçalho de coluna e arraste-a para a posição apropriada.

Para usar resultados do relatório do Notification Server

Você pode fazer uma busca detalhada nos resultados do relatório para obter informações adicionais. Clicar duas vezes em um item abre a exibição apropriada, que pode ser outro relatório ou o Gerenciador de recursos.

Você pode executar ações em recursos diretamente dos resultados do relatório. Por exemplo, você pode executar um relatório que liste todos os computadores que cumprem critérios específicos. Você pode então executar uma ação em alguns ou em todos os computadores. As ações disponíveis são aquelas que se aplicam ao tipo de recurso selecionado e que você tem permissão para executar.

Você pode imprimir as linhas de resultados selecionadas ou todos os resultados do relatório.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para expandir os resultados do relatório

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 No painel direito, na lista suspensa **Exibir**, selecione a exibição apropriada.
- 4 Nos resultados do relatório, clique no item para o qual deseja obter informações adicionais

Observe que a ação de detalhamento pode variar: pode ser uma ação de um só clique ou de dois cliques.

Para executar ações nos recursos listados nos resultados do relatório

- 1 Nos resultados do relatório, selecione os recursos nos quais deseja executar uma ação.
- 2 Clique em **Ações** e selecione a opção apropriada.

Observe que esta função não está sempre disponível.

Para imprimir os resultados de um relatório

- 1 Se necessário, nos resultados do relatório, selecione as linhas de resultados do relatório que deseja imprimir.
- 2 Clique em **Imprimir**.
- 3 Na caixa de diálogo **Imprimir**, especifique as seguintes configurações:

Parâmetros Se deseja incluir as configurações do parâmetro do usuário nos resultados impressos, selecione **Incluir parâmetros**.

Intervalo de dados Escolha uma das seguintes opções:

- Imprimir tudo - Inclui todos os resultados do relatório.
- Imprimir as linhas selecionadas - Inclui somente as linhas selecionadas de resultados do relatório.

- 4 Clique em **Imprimir**.

Uma visualização da impressão do relatório é mostrada em uma nova janela do navegador e a caixa de diálogo Impressão do Windows aparece. A visualização é o mesmo que você vê ao salvar o relatório como HTML.

- 5 Na caixa de diálogo **Impressão do Windows**, selecione as opções apropriadas e clique em **Imprimir**.

Para salvar os resultados do relatório do Notification Server como um arquivo

Você pode salvar os resultados do relatório como um arquivo. Você pode salvar todos os resultados ou selecionar os resultados que deseja incluir. Opções para planilha (.csv), arquivo HTML e arquivo XML são fornecidas com o Notification Server. As soluções instaladas podem fornecer opções para tipos de arquivo adicionais.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para salvar os resultados do relatório do Notification Server como um arquivo

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.

- 3 (Opcional) No painel direito, selecione as linhas de resultados do relatório que deseja incluir no arquivo.
- 4 Clique em **Salvar como** e clique no tipo de arquivo apropriado.
- 5 Na caixa de diálogo **Salvar como**, especifique as seguintes configurações:

Parâmetros Se deseja incluir as configurações do parâmetro do usuário no arquivo, selecione **Incluir parâmetros**.

Intervalo de dados Escolha uma das seguintes opções:

- Salvar tudo - Inclui todos os resultados do relatório no filtro.
- Salvar as linhas selecionadas - Inclui somente as linhas selecionadas de resultados do relatório no filtro.

- 6 Clique em **Salvar**.
- 7 Na caixa de diálogo **Salvar relatório**, selecione a pasta para salvar o arquivo e clique em **Salvar**.

Para criar um filtro estático dos resultados do relatório do Notification Server

Você pode criar um novo filtro estático salvando os resultados de um relatório. Você pode incluir todos os resultados ou selecionar os resultados que deseja incluir.

Consulte [“Sobre filtros de recursos”](#) na página 354.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para criar um filtro estático dos resultados do relatório do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 (Opcional) No painel direito, selecione as linhas de resultados do relatório que deseja incluir no filtro.
- 4 Clique em **Salvar como > Filtro estático**.
- 5 Na caixa de diálogo **Salvar como filtro estático**, especifique as configurações apropriadas:

Nome	O padrão é o nome do relatório. Se desejar mudar o nome, digite o nome apropriado do filtro.
Escolha um recurso a ser usado como base do filtro.	Esta opção aplica-se somente a relatórios dos recursos. Na lista suspensa, selecione a opção apropriada.
Intervalo de dados	Escolha uma das seguintes opções: ■ Salvar tudo - Inclui todos os resultados do relatório no filtro. ■ Salvar as linhas selecionadas - Inclui somente as linhas selecionadas de resultados do relatório no filtro.

6 Clique em **Salvar**.

O novo filtro é armazenado na árvore Filtros da pasta Filtros com base em relatórios.

Para salvar os resultados do relatório do Notification Server como uma captura de imagem

Você pode salvar os resultados atuais do relatório como uma captura de imagem. Por exemplo, talvez você queira salvar um conjunto específico de resultados e torná-los disponíveis a outros usuários sem extraí-los novamente do CMDB. Quando você salvar um relatório como uma captura de imagem, ele será salvo de acordo com seu escopo. Somente os usuários que compartilham a mesma função de segurança podem visualizar a captura de imagem.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte “[Para exibir e gerenciar dados de recursos com relatórios do Notification Server](#)” na página 441.

Para salvar os resultados do relatório do Notification Server como uma captura de imagem

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 No painel direito, clique em **Salvar como > Captura de imagem**.

Na próxima vez em que você abrir o relatório, a nova captura de imagem estará disponível na lista suspensa **Exibição**.

Para salvar os resultados do relatório do Notification Server como uma Web part

Você pode salvar um relatório como uma Web part que poder ser usada em uma página do portal. O relatório da Web part é uma cópia dinâmica e totalmente funcional do relatório. O conjunto de resultados exibido na página do portal é atualizado quando você abre a página; assim, ele está sempre atualizado. O relatório da Web part é independente do relatório original; assim, nenhuma mudança realizada em um relatório é propagada para os outros.

Consulte [“Para criar e modificar Web parts”](#) na página 60.

Esta tarefa é uma etapa do processo de exibição e gerenciamento de dados de recursos nos relatórios do Notification Server.

Consulte [“Para exibir e gerenciar dados de recursos com relatórios do Notification Server”](#) na página 441.

Para salvar os resultados do relatório do Notification Server como uma Web part

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja usar.
- 3 No painel direito, clique em **Salvar como > Web part**.
- 4 (Opcional) Na caixa de diálogo **Salvar como Web part** edite o nome da nova Web part.

O nome padrão deve ser apropriado para a maioria das finalidades.

- 5 (Opcional) Na lista suspensa **Escolher um tamanho de Web part**, selecione o tamanho apropriado.

O padrão é Pequeno.

- 6 Clique em **Salvar**.

A nova Web part é salva na pasta Configurações\Configurações do console\Webparts.

Para criar relatórios personalizados do Notification Server

Este capítulo contém os tópicos a seguir:

- [Componentes de um relatório personalizado do Notification Server](#)
- [Para criar e modificar relatórios personalizados do Notification Server](#)

Componentes de um relatório personalizado do Notification Server

Os relatórios do Notification Server são criados de um conjunto padrão de componentes.

Tabela 29-1 Os componentes de um relatório personalizado do Notification Server

Componente	Descrição
Fonte de dados	A fonte de dados é o componente que fornece os dados do relatório. Relatórios personalizados e filtros dinâmicos usam as consultas SQL que são executadas no CMDDB para extrair os dados apropriados. As soluções podem fornecer relatórios que usam outras fontes de dados, como planilhas ou arquivos CSV. Relatórios personalizados e filtros dinâmicos usam uma consulta SQL como a fonte de dados. Você pode definir uma consulta escrevendo o SQL do zero ou usando o Criador de consulta. Consulte “Para definir uma consulta de recursos para um relatório personalizado” na página 457. Consulte “Para definir uma consulta SQL para um relatório personalizado” na página 459.
Exibições	Uma exibição de relatório é a maneira específica como os dados do relatório são exibidos. Uma exibição contém tipicamente um subconjunto dos dados do relatório. Os dados são apresentados de uma maneira que seja apropriada a uma função de usuário específico. Você pode escolher as colunas de dados que serão incluídas na exibição e especificar que dados devem ser usados como eixo primário. Os tipos disponíveis de exibições são: ■ Exibição em grade Exiba os resultados do relatório em formato tabular, com cada item exibido em uma linha separada. ■ Exibição em gráfico Exiba os dados do relatório em formato de gráfico, como gráficos de barra, de linha, de pizza e de área. ■ Texto de modelo Configurar várias exibições para um relatório permite personalizar seus dados para diferentes usuários. Você pode usar um único relatório para todos os usuários em vez de criar vários relatórios para atender a exigências de diferentes usuários. Consulte “Para criar ou modificar uma exibição em gráfico para um relatório personalizado” na página 462. Consulte “Para criar ou modificar uma exibição em grade para um relatório personalizado” na página 464.

Componente	Descrição
Parâmetros	Parâmetros são variáveis na consulta de relatório que o usuário pode definir quando executar o relatório. O uso de parâmetros pode fazer com que os relatórios sejam mais flexíveis e eficazes. Por exemplo, a lista Computador por relatório do tipo de sistema e do nome do sistema operacional tem os parâmetros do usuário definidos para o tipo de sistema e o nome do sistema operacional. Ao executar esse relatório, é possível especificar a combinação do tipo e do nome do sistema operacional que você deseja usar definindo os parâmetros apropriados. Sem parâmetros, os relatórios terão valores fixos definidos na consulta. Consulte “Para definir provedores de valores e parâmetros para um relatório personalizado” na página 460.
Buscas detalhadas	Uma busca detalhada no relatório é uma ação que será executada quando o usuário clicar em um item nos resultados do relatório. É possível adicionar buscas detalhadas para que um relatório permita que o usuário obtenha informações adicionais nos resultados do relatório. Para cada busca detalhada, você pode especificar a exibição em que a busca detalhada estará disponível e como o usuário acionará a busca detalhada. Você também pode especificar a ação que é executada e os parâmetros que são usados na ação. Você pode configurar vários detalhes para que um relatório execute ações diferentes em tipos diferentes de recursos. Consulte “Para configurar ações de busca detalhada para um relatório personalizado” na página 465.

Para criar e modificar relatórios personalizados do Notification Server

Os relatórios do Notification Server permitem exibir e gerenciar os dados de recursos. Estes relatórios apresentam informações sobre os computadores gerenciados e não gerenciados e sobre a configuração do Notification Server. Uma ampla gama de relatórios é fornecida com o Symantec Management Platform. Você também pode criar seus próprios relatórios personalizados para atender às necessidades de sua organização. Os relatórios do Notification Server recuperam dados do CMDB.

Os dados do relatório podem ser usados das seguintes maneiras:

- A fonte de dados para uma política de automação

- Uma Web part que exibe os dados atuais em uma página do portal
- Um relatório de recursos que permite ao usuário fazer uma busca detalhada sobre um recurso específico para exibir detalhes completos no Gerenciador de recursos
- Um relatório de tendências que mostra alterações de dados ao longo do tempo
- Vários relatórios de busca detalhada (por exemplo, relatórios de hierarquia) que permitem ao usuário fazer uma busca detalhada sobre dados de alto nível para exibir dados mais detalhados de baixo nível.

Para criar ou modificar um relatório personalizado, você precisa definir os componentes do relatório na página **Edição de relatório personalizado**.

Consulte [“Página de edição de relatório personalizado”](#) na página 527.

Consulte [“Componentes de um relatório personalizado do Notification Server”](#) na página 450.

Nota: Algumas políticas usam um relatório como uma fonte de dados e podem depender de alguns resultados ou parâmetros específicos. Quando você modificar um relatório, será preciso assegurar-se de que as mudanças não afetarão nenhuma política de automação.

Consulte [“Especificação da fonte de dados da política de automação”](#) na página 401.

Tabela 29-2 Processo para criar e modificar relatórios personalizados do Notification Server

Etapa	Ação	Descrição
Etapa 1	Crie um novo relatório ou selecione um relatório existente para modificá-lo.	Crie um novo relatório do zero ou duplique um relatório padrão fornecido com o Notification Server. Você pode modificar qualquer relatório personalizado que você tenha criado, mas não pode modificar os relatórios padrão. Consulte “Para criar um relatório personalizado do Notification Server” na página 455. Consulte “Para modificar um relatório personalizado existente do Notification Server” na página 456.

Etapa	Ação	Descrição
Etapa 2	Crie a consulta de relatório.	Você mesmo pode escrever a consulta SQL ou usar o Construtor de consultas para criar a consulta de relatório. O Criador de consulta é uma ferramenta simples que permite selecionar as tabelas e os campos que você quer usar. Consulte “Para definir uma consulta de recursos para um relatório personalizado” na página 457. Você pode gravar o código SQL do zero. Como alternativa, você pode copiar o SQL de outro filtro ou relatório e modificá-lo para satisfazer seus requisitos. Consulte “Para definir uma consulta SQL para um relatório personalizado” na página 459.
Etapa 3	Especifique os provedores de valor para os parâmetros.	Se a consulta de relatório incluir parâmetros, você poderá definir os provedores de valor correspondentes. O provedor de valor permite que o usuário defina o valor apropriado para o parâmetro da consulta ao executar o relatório. Consulte “Para definir provedores de valores e parâmetros para um relatório personalizado” na página 460.
Etapa 4	Crie as exibições de relatório.	Uma visão de relatório contém tipicamente um subconjunto dos resultados do relatório. Os resultados são apresentados de um modo que seja apropriado a uma função de usuário específico. Configurar várias exibições diferentes para um relatório permite personalizar os resultados para diferentes usuários. Consulte “Para criar ou modificar uma exibição em gráfico para um relatório personalizado” na página 462. Consulte “Para criar ou modificar uma exibição em grade para um relatório personalizado” na página 464.
Etapa 5	Criar as buscas detalhadas.	Uma busca detalhada no relatório será uma ação que será executada quando o usuário clicar em um item nos resultados do relatório. É possível configurar a busca detalhada para que um relatório permita que o usuário obtenha informações adicionais nos resultados do relatório. Consulte “Para configurar ações de busca detalhada para um relatório personalizado” na página 465.
Etapa 6	Especificar as propriedades do relatório.	Você pode escolher se os resultados do relatório são restritos ao escopo do usuário que o executa. Também pode escolher executar o relatório somente como uma captura de imagem. Para minimizar a carga no Notification Server, convém executar relatórios grandes ou de uso frequente como capturas de imagem. Consulte “Para especificar as propriedades de um relatório personalizado” na página 468.

Etapa	Ação	Descrição
Etapa 7	Salve o relatório.	Salve as mudanças feitas no novo relatório ou no relatório modificado. Consulte “Para criar um relatório personalizado do Notification Server” na página 455. Consulte “Para modificar um relatório personalizado existente do Notification Server” na página 456.

Para criar um relatório personalizado do Notification Server

Você pode criar seus próprios relatórios personalizados e configurá-los para satisfazer seus requisitos. Você pode criar um relatório novo do zero ou duplicar um relatório padrão fornecido com o Notification Server.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para criar um relatório personalizado do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta em que você quer adicionar o novo relatório e clique em **Novo(a) > Relatório**.

3 Clique em um dos seguintes itens:

Relatório do computador	A consulta de relatório é uma consulta de recursos e o modelo base seleciona todos os computadores. Você pode refinar a consulta para selecionar os computadores que deseja.
Relatório do usuário	A consulta de relatório é uma consulta de recursos e o modelo base seleciona todos os usuários. Você pode refinar a consulta para selecionar os usuários que deseja.
Relatório de recursos	A consulta de relatório é uma consulta de recursos e o modelo base seleciona todos os recursos (incluindo todos os computadores e todos os usuários). Você pode refinar a consulta para selecionar os recursos que deseja.
Relatório do SQL	A consulta de relatório é uma consulta SQL. Você pode gravar sua própria consulta SQL para extrair os dados que deseja do CMDb. Nenhum modelo é aplicado e não há nenhuma restrição sobre o que você pode gravar.

- 4 (Opcional) No painel direito, especifique o nome do relatório e a descrição.
- 5 Na página de edição de relatório personalizado, especifique os componentes e as propriedades do relatório nas guias apropriadas.

Consulte [“Página de edição de relatório personalizado”](#) na página 527.
Para obter mais informações, clique na página e pressione **F1**.
- 6 Para salvar as mudanças sem sair do modo de edição, clique em **Aplicar**.
- 7 Para visualizar as mudanças sem sair do modo de edição, clique em **Visualização**.
- 8 Para salvar as mudanças e sair do modo de edição, clique em **Salvar alterações**.

Para modificar um relatório personalizado existente do Notification Server

Você pode modificar seus próprios relatórios personalizados a qualquer momento. Você não pode modificar nenhum dos relatórios padrão que são fornecidos com o Notification Server. Se desejar modificar um relatório padrão, você pode clonar o relatório para criar uma cópia dele e então editar a cópia.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Pra modificar um relatório personalizado existente do Notification Server

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, clique no relatório que você quer modificar.
- 3 No painel direito, no canto direito, clique em **Editar**.
- 4 (Opcional) Modifique o nome e a descrição do relatório.
- 5 Na página **Edição de relatório personalizado**, faz as alterações nos componentes e propriedades do relatório nas guias apropriadas.

Consulte [“Página de edição de relatório personalizado”](#) na página 527.

Para obter mais informações, clique na página e pressione **F1**.

- 6 Para salvar as mudanças sem sair do modo de edição, clique em **Aplicar**.
- 7 Para visualizar as mudanças sem sair do modo de edição, clique em **Visualização**.
- 8 Para salvar as mudanças e sair do modo de edição, clique em **Salvar alterações**.

Para definir uma consulta de recursos para um relatório personalizado

Quando você criar ou modificar seu próprio relatório personalizado do Notification Server, poderá definir uma consulta de relatório. Para um relatório do computador, relatório do usuário ou relatório de recursos você precisa definir uma consulta de recursos.

Uma consulta de recursos é baseada nas tabelas que estão disponíveis no banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database). O Criador de consulta é uma ferramenta simples que fornece um modelo padrão e permite selecionar as tabelas e os campos que você deseja usar. Ele ajuda a definir a consulta para satisfazer a seus requisitos. Você não precisa de nenhum conhecimento em SQL para definir uma consulta de recursos. A consulta de recursos é convertida em SQL automaticamente e o SQL é executado no CMDB para extrair os recursos apropriados.

Quando você definir uma consulta de recursos para seu relatório personalizado, será possível converter uma consulta de recursos em uma consulta SQL

equivalente. Por exemplo, será possível usar o Criador de consulta para definir a estrutura de sua consulta, convertê-la ao SQL e modificar em seguida o SQL diretamente. Esse processo pode ser mais eficiente e mais rápido do que escrever a consulta inteira em SQL do zero.

Quando você cria um novo relatório do computador, do usuário ou de recursos, um modelo de consulta de recursos é adicionado ao relatório automaticamente. Quando você cria um novo filtro, o mesmo modelo de consulta de recursos é adicionado ao filtro quando você escolhe o modo de consulta do Criador de consulta. A consulta básica no modelo seleciona todos os computadores, usuários ou recursos que correspondem ao tipo de relatório. Você precisa modificar a consulta básica para selecionar os recursos apropriados.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para definir uma consulta de recursos para um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 Execute um destes procedimentos:
 - Para definir uma consulta de recursos para um relatório novo que você criar, no painel esquerdo, clique com o botão direito do mouse na pasta em que deseja adicionar o relatório novo. Clique em **Novo(a)** e, em seguida, em **Relatório do computador**, **Relatório do usuário** ou **Relatório de recursos**.
 - Para redefinir uma consulta de recursos para um relatório existente, no painel esquerdo, clique no relatório do computador, no relatório do usuário ou no relatório de recursos que deseja modificar. Em seguida, no painel direito, no canto superior direito, clique em **Editar**.
- 3 No painel direito, na guia **Fonte de dados**, especifique os detalhes da consulta. Consulte [“Página de edição do relatório personalizado: guia Fonte de dados”](#) na página 528.

Para obter mais informações, clique na página e pressione **F1**.

- 4 (Opcional) Para converter a consulta de recursos para a consulta SQL equivalente, clique em **Converter esta consulta em uma consulta SQL**.

Aviso: Converter uma consulta de recursos em uma consulta SQL é uma operação de sentido único. Você não pode converter a consulta SQL resultante de volta em uma consulta de recursos.

- 5 Clique em **Salvar alterações**.

Para definir uma consulta SQL para um relatório personalizado

Quando você criar ou modificar seu próprio relatório personalizado do Notification Server, poderá definir uma consulta de relatório. Para um relatório do computador, do usuário ou de recursos, você precisa definir uma consulta de recursos para o relatório. Para um relatório do SQL, você precisa definir uma consulta SQL.

É possível gravar uma consulta SQL para definir os recursos que você deseja incluir no relatório ou no filtro. Você pode gravar o código SQL do zero. Como alternativa, você pode copiar o SQL de outro filtro ou relatório e modificá-lo para satisfazer seus requisitos. Por exemplo, você pode criar uma consulta de recursos usando o Criador de consulta e copiar o SQL gerado da guia Consulta resolvida. Você também pode usar o Criador de consulta para definir a estrutura de sua consulta, convertê-la ao SQL e modificar em seguida o SQL diretamente.

Quando você cria um novo relatório do SQL, um modelo de consulta SQL é adicionado ao relatório automaticamente. Quando você cria um novo filtro, o mesmo modelo de consulta SQL é adicionado ao filtro quando você escolhe o modo de consulta SQL bruto. A consulta SQL básica seleciona todos os recursos disponíveis. Você precisa modificar a consulta básica para selecionar os recursos apropriados.

Você precisa do privilégio Editar SQL para criar ou modificar consultas SQL e ter boa compreensão sobre a estrutura da tabela do CMDB. Se você desejar aplicar um escopo aos resultados da consulta, será necessário incluir o código SQL apropriado na consulta.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para definir uma consulta SQL para um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 Execute um destes procedimentos:

- Para definir uma consulta SQL para um relatório novo que você criar, no painel esquerdo, clique com o botão direito do mouse na pasta em que deseja adicionar o relatório novo. Em seguida, clique em **Novo(a)** e em **Relatório do SQL**.
 - Para redefinir uma consulta SQL para um relatório existente, no painel esquerdo, clique no relatório do SQL que deseja modificar. Em seguida, no painel direito, no canto superior direito, clique em **Editar**.
- 3 No painel direito, na guia **Fonte de dados**, especifique os detalhes da consulta nas guias apropriadas.
- Consulte “[Página de edição do relatório personalizado: guia Fonte de dados](#)” na página 528.
- Para obter mais informações, clique na página e pressione **F1**.
- 4 Clique em **Salvar alterações**.

Para definir provedores de valores e parâmetros para um relatório personalizado

Se a consulta do relatório personalizado que você criar ou modificar incluir parâmetros, será possível definir os fornecedores apropriados de valor. O provedor de valor de um parâmetro permite que o usuário defina o valor apropriado para o parâmetro ao executar o relatório. Incluir parâmetros que podem ser definidos pelo usuário em uma consulta de relatório permite criar um único relatório flexível capaz de extrair diferentes conjuntos de resultados mudando os valores do parâmetro. A alternativa seria embutir no código os valores de parâmetro na consulta. Você precisaria então modificar a consulta cada vez em que desejar usar um valor de parâmetro diferente. Você também pode criar vários relatórios com um valor diferente definido em cada consulta.

O provedor de valor especifica como o valor de parâmetro é definido quando o usuário executa o relatório. Em muitos casos, o provedor de valor é um componente da interface do usuário que aceita um valor ou uma configuração do usuário. Por exemplo, você pode definir o provedor de valor de um parâmetro como uma lista suspensa com um conjunto de valores válidos entre os quais o usuário pode escolher. Como alternativa, você pode definir o provedor de valor como um campo de texto que aceite uma sequência de caracteres digitados pelo usuário. Em alguns casos, um parâmetro não exige um provedor de valor. O valor do parâmetro é definido automaticamente sem exigir ação do usuário.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte “[Para criar e modificar relatórios personalizados do Notification Server](#)” na página 452.

Para adicionar um parâmetro a um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja modificar.
- 3 Na página *Nome do relatório*, no canto direito superior, clique em **Editar**.
- 4 Na guia **Parâmetros do relatório**, faça o seguinte:

Para adicionar um parâmetro Clique em **Adicionar** e depois clique no parâmetro de consulta apropriado.

A lista suspensa contém todos os parâmetros definidos na consulta de relatório, mas que ainda não foram adicionados ao relatório.

Para adicionar um parâmetro do tipo avançado Clique em **Adicionar > Tipos avançados** e depois clique no tipo desejado.

- Para criar um novo parâmetro
- Clique em **Adicionar > Novo parâmetro**.
 - Na caixa de diálogo **Editar parâmetro**, em **Parâmetro**, especifique as configurações apropriadas do parâmetro.
 - No painel **Provedor de valor**, na lista suspensa **Nome**, selecione o tipo de provedor de valor desejado.
 - Em **Configuração**, especifique as configurações apropriadas do provedor de valor.
 - Clique em **OK**.

- Para modificar um parâmetro
- Clique no parâmetro que você quer modificar e depois clique no símbolo de **Editar**.
 - Na caixa de diálogo **Editar parâmetro**, em **Parâmetro**, especifique as configurações apropriadas do parâmetro.
 - No painel **Provedor de valor**, na lista suspensa **Nome**, selecione o tipo de provedor de valor desejado.
As opções que estão disponíveis dependem da configuração do tipo do parâmetro que você fez em **Parâmetro**.
 - Em **Configuração**, especifique as configurações apropriadas do provedor de valor.
Se você quiser exibir ou editar um outro parâmetro na lista, clique nos botões para cima e para baixo para exibir os detalhes do parâmetro apropriado.
 - Clique em **OK**.

5 Clique em **Salvar alterações**.

Para criar ou modificar uma exibição em gráfico para um relatório personalizado

Quando você criar ou modificar seu próprio relatório personalizado do Notification Server, poderá definir uma exibição de relatório. Uma exibição de relatório é a maneira específica como os resultados do relatório são exibidos. A configuração de várias exibições diferentes para um relatório permite personalizar os resultados para diferentes usuários. Uma exibição de gráfico permite exibir os resultados do relatório em formato de gráfico, como gráficos de barras, gráficos de linhas, gráfico de pizza e gráficos de área.

Nota: Um conjunto de ferramentas de terceiros fornece a funcionalidade que é usada em exibições de gráfico. Para descrições completas de componentes de gráficos, consulte a documentação que a [Dundas Data Visualization, Inc. \(Dundas.com\)](https://dundas.com) fornece.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte “[Para criar e modificar relatórios personalizados do Notification Server](#)” na página 452.

Para criar ou modificar uma exibição em gráfico para um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja modificar.
- 3 Na página *Nome do relatório*, clique em **Editar**.
- 4 Na guia **Exibições**, execute um destes procedimentos:
 - Para criar uma nova exibição em gráfico, clique em **Adicionar**.
 - Para modificar uma exibição existente em gráfico, na lista suspensa **Exibição**, selecione a exibição que deseja modificar.
- 5 (Opcional) Na caixa **Nome**, digite o nome da exibição do gráfico.
- 6 Na lista suspensa **Tipo**, clique em **Gráfico**.
- 7 Na lista suspensa **Tipo de gráfico**, clique no tipo de gráfico que você deseja usar.
- 8 Na lista suspensa **Estilo do gráfico**, clique no estilo que você deseja usar para processar o gráfico.

 O estilo do gráfico é um conjunto predefinido de cores que podem ser usadas para processar o gráfico.
- 9 Nas caixas **Tamanho**, especifique a altura e a largura do gráfico em pixels.
- 10 Na lista suspensa **Rótulos do gráfico**, selecione a opção apropriada:

Todos	Mostra os valores de dados reais e as porcentagens.
Valores	Mostra os valores de dados reais, como o número de itens de cada tipo.
Porcentagem	Mostra os dados como porcentagens, como a porcentagem dos itens de cada tipo.
Nenhum	Nenhum rótulo é mostrado.
Somente Eixo X	Mostra os valores de dados para o Eixo X somente. O Eixo Y não é rotulado.

- 11 Configure a exibição do gráfico especificando as configurações apropriadas nas seguintes guias:

Título	Permite especificar o texto do título do gráfico e o local em que ele aparece.
Legenda	Permite especificar a legenda do título do gráfico e o local em que ela aparece.
3D	Permite configurar o zoom em 3D. O zoom em 3D permite ampliar áreas selecionadas do gráfico em tamanho de janela cheia.
Eixo X	Permite escolher a coluna de resultados que será usada como o eixo X no gráfico, especificar o texto do título e configurar a aparência do eixo X.
Eixo Y	Permite escolher a coluna de resultados que será usada como o eixo Y no gráfico, especificar o texto do título e configurar a aparência do eixo Y.

Consulte [“Página de edição do relatório personalizado: guia Exibições para uma exibição de gráfico”](#) na página 540.

Para obter mais informações, clique na página e pressione **F1**.

- 12 Clique em **Salvar alterações**.

Para criar ou modificar uma exibição em grade para um relatório personalizado

Quando você criar ou modificar seu próprio relatório personalizado do Notification Server, será possível criar e modificar as exibições em grade que desejar em seus relatórios. Para cada exibição em grade, você pode selecionar as colunas de resultados para incluir e especificar como os resultados serão formatados.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para criar ou modificar uma exibição em grade para um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja modificar.
- 3 Na página *Nome do relatório*, no canto direito superior, clique em **Editar**.

4 Na guia **Exibições**, execute um destes procedimentos:

Para criar uma nova exibição Clique em **Adicionar**.
em grade

Para modificar uma exibição Na lista suspensa **Exibir**, selecione a exibição que
em grade existente deseja modificar.

5 (Opcional) Na caixa **Nome**, digite o nome da exibição.

6 Na lista suspensa **Tipo**, selecione **Grade**.

7 Na guia **Colunas ocultas**, especifique as colunas de dados para incluir na
exibição em grade do relatório personalizado.

Por padrão, a exibição em grade inclui todas as colunas nos resultados da
consulta. Você pode ocultar qualquer coluna de dados que você não deseja
exibir ao usuário.

8 Na guia **Formatação avançada**, configure um modelo de formatação que
aplique a marcação HTML às células ou linhas adequadas nos resultados do
relatório.

Por exemplo, em um relatório do espaço em disco do computador convém
destacar todos os computadores que têm menos que o mínimo especificado
de espaço livre restante. Você pode criar um modelo que formate as linhas
relevantes com um segundo plano amarelo brilhante e que use texto em negrito
na célula de espaço livre.

Consulte [“Página de edição do relatório personalizado: guia Exibições para
uma exibição em grade”](#) na página 543.

Para obter mais informações, clique na página e pressione **F1**.

9 (Opcional) Para visualizar a grade usando as configurações atuais, clique em
Visualizar.

10 Clique em **Salvar alterações**.

Para configurar ações de busca detalhada para um relatório personalizado

Quando você criar ou modificar seu próprio relatório personalizado do Notification
Server, poderá configurar uma busca detalhada no relatório. Uma busca detalhada
no relatório é uma ação que será executada quando o usuário clicar em um item
nos resultados do relatório. Convém configurar os detalhes para um relatório para
permitir que o usuário obtenha informações adicionais nos resultados do relatório.

Clicar duas vezes em um item abre a exibição apropriada, a qual pode ser outro relatório ou um URL (como o console do Gerenciador de recursos).

Você pode configurar vários detalhes para que um relatório execute ações diferentes em tipos diferentes de recursos.

Para cada busca detalhada, você pode especificar a exibição em que a busca detalhada estará disponível e como o usuário acionará a busca detalhada. Você também pode especificar a ação que é executada e os parâmetros que são usados na ação.

Você pode criar vários relatórios de detalhes, que são grupos de relatórios que são vinculados em uma estrutura hierárquica. Esta estrutura pode permitir que o usuário do relatório selecione um item em um conjunto de resultados e execute relatórios adicionais. Os relatórios detalhados podem apresentar informações mais abrangentes para um conjunto menor de recursos ou fornecer informações diferentes sobre o recurso, relatando em campos diferentes.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para definir ações de busca detalhada para um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja modificar.
- 3 Na página *Nome do relatório*, clique em **Editar**.
- 4 Na guia **Buscas detalhadas**, execute um destes procedimentos:

Para adicionar nova busca detalhada Clique em **Adicionar**.

Para modificar uma busca detalhada existente Na lista suspensa **Detalhes**, selecione a busca detalhada que deseja modificar.

- 5 Na caixa **Nome**, digite um nome apropriado para a busca detalhada.

6 Em **Associação da ação**, especifique as seguintes configurações:

Disponível em	Permite especificar a exibição de relatório apropriada.
Evento	Permite especificar o evento do usuário que é necessário para executar a busca detalhada.
Executa	Permite especificar a ação que a busca detalhada executa. Dependendo da ação que você selecionar, as opções em Configuração da ação serão alteradas.

7 Em **Configuração da ação**, especifique o seguinte:

Detalhes para relatório	Na lista suspensa Item do relatório , selecione o relatório que você quer que a ação de busca detalhada execute.
Mostrar menu contextual	Não se aplica.
Abrir URL em uma nova janela	Na caixa URL aberto , digite o URL do item que você deseja que seja aberto pela ação de busca detalhada e clique em Definir .
Abrir URL em uma nova janela para o NS remoto	Na caixa GUID do item do relatório remoto , digite o GUID do relatório remoto que você deseja que seja aberto pela ação de busca detalhada abrir e clique em Definir .

8 Em **Parâmetros de passagem**, configure os parâmetros que passam valores à ação de busca detalhada.

Adicione ou edite as seguintes opções do parâmetro:

Origem	A origem do valor do parâmetro: ■ Parâmetro nomeado ■ Primeiro valor selecionado ■ Linha selecionada ■ Seleção inteira
Informação do campo	O nome do campo de origem.
Parâmetro de destino	O nome do parâmetro.

Tipo de parâmetro de destino	O tipo de parâmetro. A lista suspensa contém todos os tipos de parâmetro disponíveis.

Você precisa adaptar as propriedades ou os valores do item selecionado aos parâmetros na ação de busca detalhada. Este processo garante que a ação apropriada seja executada. Por exemplo, se deseja que a ação de busca detalhada abra o Gerenciador de recursos, você pode passar o GUID de recursos apropriado como um parâmetro. Se deseja que a ação de busca detalhada execute um relatório, você pode passar os valores apropriados para a consulta de relatório.

9 Clique em **Salvar alterações**.

Para especificar as propriedades de um relatório personalizado

Quando você cria ou modifica seu próprio relatório personalizado do Notification Server, é possível restringir os resultados do relatório ao escopo do usuário que o executa. Por padrão, executar um relatório extrai o conjunto (sem escopo) completo de resultados do CMDB. O escopo dos resultados do relatório pode então ser determinado para assegurar que o usuário visualize somente os dados apropriados. Entretanto, você pode aplicar o escopo ao relatório de modo que somente os dados apropriados sejam extraídos do CMDB.

Também pode escolher executar o relatório somente como uma captura de imagem. Para minimizar a carga no Notification Server, convém executar relatórios grandes ou de uso frequente como capturas de imagem. Quando um usuário executa o relatório, os resultados são obtidos com base na captura de imagem mais recente e não executando a consulta de relatório no CMDB. Quando você define um relatório para executar somente como uma captura de imagem, você pode especificar a idade máxima da captura de imagem. Quando a captura de imagem atinge essa idade, a consulta de relatório é executada no CMDB para extrair o resultado mais recente definido e para atualizar a captura de imagem.

Esta tarefa é uma etapa do processo de criação e modificação de relatórios personalizados do Notification Server.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Para especificar as propriedades avançadas de um relatório personalizado

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, selecione o relatório que você deseja modificar.

3 Na página *Nome do relatório*, clique em **Editar**.

4 Na guia **Avançado**, execute um dos seguintes procedimentos:

Para promover informações de escopo para a fonte de dados

Selecione **Promover informações de escopo para a fonte de dados**.

Para executar o relatório somente como uma captura de imagem

1 Selecione **Sempre executar relatório como captura de imagem**.

2 Na caixa **Atualizar automaticamente a captura de imagem quando mais antiga que**, especifique a idade para atualizar a captura de imagem com os resultados de relatório mais recentes.

5 Clique em **Salvar alterações**.

Para exibir informações dos recursos

Este capítulo contém os tópicos a seguir:

- [Sobre recursos](#)
- [Exibição das informações da classe de dados dos recursos](#)
- [Exibição das informações do tipo de associação dos recursos](#)
- [Exibição das informações do tipo de recurso](#)

Sobre recursos

Recursos são os itens com que o Notification Server trabalha e sobre os quais armazena dados, como ativos, faturas, ordens de compra, projetos, contratos e usuários. Os dados sobre um recurso são adicionados ao banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database) usando um modelo chamado tipo de recurso. Cada recurso no CMDB tem um tipo de recurso que especifica as informações gravadas sobre o recurso. Por exemplo, o nome do recurso, descrição, modelo, número da etiqueta patrimonial, proprietário, departamento e assim por diante.

Quanto maior for a quantidade de recursos com que você trabalhar, mais você precisará agrupar recursos para fins de gerenciamento. Você pode usar exibições organizacionais, grupos organizacionais e filtros de recurso para ajudar a agrupar seus recursos.

Consulte [“Exibição das informações da classe de dados dos recursos”](#) na página 471.

Consulte [“Exibição das informações do tipo de associação dos recursos”](#) na página 471.

Consulte [“Exibição das informações do tipo de recurso”](#) na página 471.

Exibição das informações da classe de dados dos recursos

Você pode exibir as informações da classe de dados dos recursos. Uma classe de dados dos recursos define um ou mais campos, e as propriedades dos campos, que um recurso dessa classe pode ter.

Consulte [“Sobre recursos”](#) na página 470.

Para exibir as informações da classe de dados dos recursos

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda a pasta **Configurações > Notification Server > Configurações de classe de recursos e dados > Classes de dados e** selecione a classe de dados apropriada.

Exibição das informações do tipo de associação dos recursos

Você pode exibir as informações do tipo de associação dos recursos. Uma associação dos recursos é um link entre dois recursos, como entre um usuário e um computador. O usuário de um computador tem uma associação a esse computador e vice-versa.

Consulte [“Sobre recursos”](#) na página 470.

Para exibir informações sobre um tipo de associação de recurso

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda a pasta **Configurações > Notification Server > Configurações de classe de recursos e dados > Associações de recursos** e selecione o tipo de associação de recursos apropriado.

Exibição das informações do tipo de recurso

Você pode exibir as informações do tipo de recurso, como o tipo base e as associações que se aplicam ao tipo de recurso. Você também pode exibir as classes de dados incluídas no tipo de recurso.

Consulte “[Sobre recursos](#)” na página 470.

Para ver informações sobre um tipo de recurso

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda a pasta **Configurações > Notification Server > Configurações de classe de recursos e dados > Tipos de recursos** e selecione a classe de dados apropriada.
- 3 Na página **Informações do tipo de recurso**, na guia **Configuração**, exiba as seguintes informações do tipo de recursos:

Detalhes do tipo de recurso	Nome do tipo de recurso, descrição e o tipo base de recursos.

Tipos de associação	Associações de recursos que se aplicam ao tipo de recurso. Por padrão, somente são exibidos aqueles que são aplicados diretamente.

Para mostrar todas as associações de recursos, selecione **Mostrar tipos de associação herdadas**.

Classes de dados	As classes de dados incluídas no tipo de recurso. Por padrão, todas as classes de dados são exibidas.

Para mudar a exibição:

- 1 Clique em um dos seguintes itens:
 - Editável - mostrar as classes de dados que você pode editar.
 - Tudo - mostrar todas as classes de dados.
 - Esta seleção opera sobre as classes de dados disponíveis.
- 2 (Opcional) Para ocultar as classes de dados herdadas, desmarque **Mostrar classes de dados herdadas**.

Nenhuma mudança feita será mantida quando você deixar a página **Informações do tipo de recurso**. As configurações padrão serão restauradas na próxima vez em que você abrir a página.

Para gerenciar dados do CMDB com o Data Connector

- [Capítulo 31. Introdução ao Data Connector](#)
- [Capítulo 32. Para executar tarefas de gerenciamento de dados](#)

Introdução ao Data Connector

Este capítulo contém os tópicos a seguir:

- [Sobre o Data Connector](#)
- [Como o Data Connector funciona](#)
- [O que pode ser feito com o Data Connector](#)

Sobre o Data Connector

O Data Connector é um componente do Symantec Management Platform que permite transferir dados entre fontes de dados externas e o banco de dados de gerenciamento de configuração (CMDB). A capacidade de transferir dados permite aproveitar os dados que já existem no CMDB ou em outros aplicativos. As transferências de dados podem ser agendadas, assim as atualizações podem ser feitas de modo regular e automático para manter dados atuais. O Data Connector suporta muitos formatos de dados: OLEDB, ODBC, LDAP, XML e CSV.

O Data Connector permite também manipular os dados que já estão no CMDB. Esta capacidade permite facilmente normalizar e corrigir erros em seus dados. Por exemplo, é possível usar o Data Connector para normalizar nomes de empresas a fim de que os dados sejam consistentes.

Consulte [“Como o Data Connector funciona”](#) na página 474.

Como o Data Connector funciona

O Data Connector transfere dados usando definições da fonte de dados e regras de transferência de dados. Uma definição de fonte de dados especifica os

parâmetros para atuar com uma fonte de dados ou com um destinatário determinados (geralmente chamados de fonte de dados). Os parâmetros podem incluir o local e o nome da fonte de dados, o tipo de transferência de dados e as credenciais que são necessários para acessar a fonte de dados.

O Data Connector suporta os tipos de fontes de dados CSV, LDAP, ODBC, OLEDB e XML.

Uma regra de transferência de dados configura os detalhes de uma transferência de dados, tais como:

- Uma definição da fonte de dados que seja usada para a transferência
- O tipo de recurso que é envolvido na transferência
- Mapeamentos entre os campos que são envolvidos na transferência
- Se a transferência for uma importação ou uma exportação

Tipos diferentes de regras de transferência de dados estão disponíveis para tipos diferentes de transferência de dados:

Exportação de recursos em massa	Uma forma eficiente de exportar recursos em massa de um relatório ou de um destino de recurso para um arquivo XML de um evento do Notification Server (NSE). Você também pode usar este tipo de regra para exportar históricos de alteração de recursos.
Importação do filtro	Especifica a participação de um filtro do Symantec Management Platform pela importação da participação de um filtro de uma fonte de dados.
Importação do grupo organizacional	Especifica as participações de exibição organizacional e de grupo do Symantec Management Platform pela importação da participação da exibição organizacional ou de grupo de uma fonte de dados.
Exportação de relatório	Exporta dados de relatório para uma fonte de dados que tenha uma definição de fonte de dados que permita a exportação.
Transferência de dados dos recursos	Transfere (importações ou exportações) os dados dos recursos entre uma fonte de dados e o CMDB.

Para automatizar o processo de transferência de dados, é possível agendar que cada regra de transferência de dados seja executada em um horário específico. As regras de transferência de dados também podem ser executadas com as tarefas do Symantec Management Platform. Após as transferências de dados, é possível usar relatórios e arquivos de log predefinidos para ajudar a analisar os resultados das transferências de dados.

O Data Connector permite também manipular os dados que já estão no CMDB através das regras do CMDB. Estas regras permitem normalizar dados ou corrigir outros problemas de consistência com seus dados de CMDB. Para manipular o CMDB, você precisa do CMDB Solution.

Consulte [“Sobre o Data Connector”](#) na página 474.

Consulte [“O que pode ser feito com o Data Connector”](#) na página 476.

O que pode ser feito com o Data Connector

O Data Connector permite transferir dados entre o CMDB e uma fonte de dados e manipular dados dentro do CMDB.

Você pode executar as seguintes atividades de transferência de dados com o Data Connector:

- Transferir (importação e exportação) de dados dos recursos entre uma fonte de dados e o CMDB.
Consulte [“Para importar e exportar dados”](#) na página 477.
- Importar informações da participação do filtro, incluindo a adição ou remoção da participação dos recursos de um para mais filtros.
- Importar exibição organizacional e participações de grupo.
- Exportar um relatório.
- Exportar dados de recursos em massa.

O Data Connector permite também manipular dados dentro do CMDB. Por exemplo, é possível normalizar ou mudar um conjunto de dados dentro do CMDB. Para manipular os dados dentro do CMDB, é necessário ter a CMDB Solution.

Para executar tarefas de gerenciamento de dados

Este capítulo contém os tópicos a seguir:

- [Para importar e exportar dados](#)
- [Para criar uma classe de dados virtual](#)
- [Configuração das opções de limpeza de logs detalhados do Data Connector](#)

Para importar e exportar dados

Você precisa executar diversas etapas para transferir dados entre o banco de dados de gerenciamento de configuração (CMDB) e uma fonte de dados.

Tabela 32-1 Processo para importar e exportar dados

Etapa	Ação	Descrição
Etapa 1	Crie um arquivo de dados.	Primeiramente, você deve criar um arquivo de dados e preenchê-lo com valores. Você pode digitar os dados manualmente ou por meio de um processo externo. Quando você adicionar nomes de coluna como primeira linha no arquivo de dados, a regra de importação de dados permitirá fazer a correspondência das colunas às classes de dados do CMDB com mais facilidade. Você pode também pré-processar os dados na fonte de dados externa antes de importá-los no CMDB. Consulte “Sobre o pré-processamento de dados antes das importações de dados” na página 479.

Etapa	Ação	Descrição
Etapa 2	Crie uma fonte de dados.	Você define fontes de dados usando definições da fonte de dados. As definições da fonte de dados especificam os parâmetros que devem ser definidos para funcionar com a fonte de dados. Por exemplo, uma definição de fonte de dados pode especificar locais do banco de dados ou do arquivo, nomes do servidor e credenciais de acesso. Consulte “Criação de uma definição de fonte de dados” na página 479.
Etapa 3	Crie uma regra da transferência de dados.	A regra de transferência de dados permite configurar a transferência de dados. As regras de transferência de dados especificam os parâmetros da transferência de dados, como o agendamento da transferência de dados, o mapeamento da tabela de dados de entrada e saída e o sentido da transferência de dados. Consulte “Para criar uma regra de transferência de dados” na página 480.
Etapa 4	(Opcional) Crie uma chave de pesquisa de recursos.	Uma chave de pesquisa de recursos é um conjunto de colunas dr classes de dados usado para fazer a correspondência entre o CMDDB e a fonte de dados. Consulte “Para criar uma chave de pesquisa de recursos” na página 481.
Etapa 5	(Opcional) Execute a regra de transferência de dados como uma tarefa.	Você pode agendar uma tarefa para executar a regra da transferência de dados. Consulte “Execução de uma regra de transferência de dados como uma tarefa” na página 482.
Etapa 6	Verifique os resultados de uma transferência de dados.	Você pode usar relatórios predefinidos para verificar se as transferências de dados ocorreram com êxito. Consulte “Exibir resumos da transferência de dados” na página 483.
Etapa 7	(Opcional) Verifique a integridade das regras de transferência de dados.	Você pode verificar a integridade das regras de transferência de dados. Verificar a integridade garante que não há nenhum problema causado por mudanças à regra que possam impedir que uma transferência de dados seja concluída com êxito. Consulte “Verificação de integridade das regras de transferência de dados” na página 483.

Etapa	Ação	Descrição
Etapa 8	(Opcional) Gerencie os dados importados.	Você pode criar regras do CMDB que permitam limpar, normalizar ou fazer mudanças em massa nos dados do CMDB. Consulte “Para criar uma regra para editar dados do CMDB” na página 484. Consulte “Execução de uma regra de CMDB como uma tarefa” na página 485.

Sobre o pré-processamento de dados antes das importações de dados

Quando importar dados de uma fonte de dados externa no banco de dados de gerenciamento de configuração (CMDB), você poderá manipular os dados antes que os dados seja importados. Este pré-processamento de dados permite que você manipule os dados sem alterá-los na fonte de dados original.

Você grava uma função de pré-processamento dos dados usando a programação C#. A quantidade de pré-processamento que você pode fazer é apenas limitada pelo que você pode fazer com a programação C#. Uma função de pré-processamento de dados em C# toma uma tabela dos dados como um parâmetro de entrada. Você pode gravar o código C# para manipular a tabela dos dados e seu conteúdo. Uma tabela atualizada de dados é retornada como o valor de retorno do método. A tabela de dados que retorna contém os dados para a fonte de dados durante a importação.

Para entender melhor como o pré-processamento pode ser usado, considere o seguinte exemplo. Você tem uma fonte de dados OLEDB configurada para usar a “tabela A” do “banco de dados A”. Uma função de pré-processamento adiciona dinamicamente uma nova coluna à tabela. E preenche a nova coluna com os dados derivados das outras colunas na tabela.

Esta tarefa é uma etapa opcional do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Criação de uma definição de fonte de dados

Uma fonte de dados é uma fonte ou um destinatário de dados do CMDB. Por exemplo, um arquivo CSV ou um banco de dados de ODBC podem ser uma fonte de dados.

Você pode transferir dados entre os seguintes tipos de fonte de dados e o CMDB:

- CSV

- LDAP
- ODBC
- OLEDB
- XML
- Personalizar

Uma definição de fonte de dados especifica como acessar uma fonte de dados específica. A definição inclui o tipo de fonte de dados, o local, o nome da tabela e as informações de autenticação. Para transferências de dados em cada fonte de dados, você precisa de uma definição. Para tipos diferentes de fonte de dados, há tipos diferentes de definições de fontes de dados. Alguns tipos de definição de fonte de dados permitem a importação e a exportação dos dados do CMDB. Outros tipos apenas permitem a exportação ou a importação.

Você deve criar uma definição de fonte de dados para cada fonte de dados entre as quais deseja transferir dados.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para criar uma definição de fonte de dados

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Conector**.
- 3 Clique com o botão direito do mouse em **Fontes de dados** e em **Novo(a) > Fonte de dados**.
- 4 No painel direito, especifique os valores apropriados.
Para obter mais informações, clique na página e pressione **F1**.
- 5 (Opcional) Clique em **Testar fonte de dados** para testar o acesso à fonte de dados.
- 6 Clique em **Salvar alterações**.

Para criar uma regra de transferência de dados

Para transferir dados entre o banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database) e uma fonte de dados, você precisa especificar as opções da transferência de dados. Por exemplo, você deve especificar o seguinte:

- Que tipos de dados são transferidos

- Se os dados serão importados ou exportados para uma fonte de dados
- Quais dos dados são transferidos da fonte de dados
- Quando a transferência de dados ocorrer

Para especificar as opções de uma transferência de dados, você usa uma regra de transferência de dados. Diversos tipos de regras de transferência de dados estão disponíveis. O tipo utilizado dependerá do tipo de informações que você deseja transferir.

Antes que você use uma regra de transferência de dados em um ambiente de produção, recomendamos que você a teste. Use a opção **Testar regra** na página aplicável da regra de transferência de dados.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para criar uma regra de transferência de dados

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Conector**.
- 3 Clique com o botão direito do mouse em **Importar/exportar regras** e depois clique em **Novo(a) > > Regra de transferência de dados**.
- 4 No painel direito, especifique os mapeamentos da coluna e um agendamento para a regra.
 Para obter mais informações, clique na página e pressione **F1**.
- 5 Clique em **Salvar alterações**.

Para criar uma chave de pesquisa de recursos

Uma chave de pesquisa de recursos é um valor exclusivo para um tipo de recurso usado para fazer a correspondência dos recursos entre o banco de dados de gerenciamento de configuração (CMDB) e a fonte de dados

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para criar uma chave de pesquisa de recursos

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Conector**.
- 3 Clique com o botão direito do mouse em **Chaves de pesquisa de recursos** e clique em **Novo(a) > Chave de pesquisa de recursos**.
- 4 No painel direito, especifique as seguintes configurações:

Tipo do recurso de destino Tipo de recurso para o qual a chave de pesquisa foi especificada.

Selecionar uma classe de dados Permite selecionar a classe de dados que contém o valor que você quer usar como a chave de pesquisa.

Uso na chave Marque as caixas para especificar a chave de pesquisa.

- 5 Clique em **Salvar alterações**.

Execução de uma regra de transferência de dados como uma tarefa

Você pode executar uma regra de transferência de dados como uma tarefa. A execução de uma regra como uma tarefa permite que a regra seja executada com diversas outras tarefas incluídas em um único trabalho.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para executar uma regra de transferência de dados como uma tarefa

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você deseja que a tarefa seja adicionada e clique em **Novo(a) > Trabalho ou tarefa**.
- 3 No painel esquerdo da caixa de diálogo **Criar nova tarefa**, clique em **Tarefas de servidor > Executar regra de conector**.
- 4 No painel direito, especifique um nome para a tarefa e selecione uma regra de transferência de dados para que a tarefa seja executada.

- 5 Clique em **OK**.
- 6 No painel direito, especifique um agendamento para a execução da regra.
Consulte "[Para configurar um agendamento](#)" na página 123.
Consulte "[Execução de um trabalho ou uma tarefa](#)" na página 422.
Para obter mais informações, clique na página e pressione **F1**.

Exibir resumos da transferência de dados

Você pode exibir os resultados das transferências de dados, que podem incluir contagens dos recursos, contagens da linha, horas e data da transferência e fonte de dados, através dos relatórios predefinidos. Estes relatórios podem ser úteis para controle de transferências de dados.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte "[Para importar e exportar dados](#)" na página 477.

Para exibir resumos da transferência de dados

- 1 No Console de gerenciamento Symantec, no menu **Relatórios**, clique em **Todos os relatórios**.
- 2 No painel esquerdo, expanda **Relatórios > Gerenciamento do Notification Server > Conector** e clique no relatório que você quer exibir.

Verificação de integridade das regras de transferência de dados

Você pode verificar a integridade (funcionamento apropriado) de todas as regras de transferência de dados com as tarefas predefinidas. As tarefas de verificação de integridade testam cada regra. Elas equivalem a clicar na opção **Testar regra** associada com cada página de regra para cada regra.

Executar a verificação de integridade ajuda a avaliar se as regras e as definições da fonte de dados estão configuradas corretamente. Todos os erros durante os testes são relatados e podem ser exibidos do Status da tarefa para cada execução da tarefa de verificação da integridade.

As tarefas predefinidas, assim como outras tarefas, podem ser agendadas para serem executadas imediatamente, em um horário específico ou com regularidade.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte "[Para importar e exportar dados](#)" na página 477.

Para verificar a integridade das regras de transferência de dados

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, expanda **Trabalhos e tarefas do sistema > Notification Server > Conector**, e clique em **Tarefa Verificação de integridade de regras do conector** ou em **Tarefa Verificação de integridade das regras do CMDB**.
- 3 No painel direito, especifique um agendamento para executar a regra.
Consulte [“Para adicionar um agendamento a uma política, tarefa ou trabalho”](#) na página 425.
Consulte [“Para configurar um agendamento”](#) na página 123.
Para obter mais informações, clique na página e pressione **F1**.
- 4 Após a execução da tarefa, vá para a seção **Status da tarefa** para exibir a integridade de cada uma das regras de transferência de dados.

Para criar uma regra para editar dados do CMDB

As regras do CMDB são regras personalizadas criadas por usuários para gerenciar dados e tarefas. As regras de CMDB permitem manipular os dados que já estão no CMDB. Estas regras permitem normalizar dados ou corrigir outros problemas de consistência com seus dados de CMDB.

Você pode criar suas próprias regras de CMDB, tendo como objetivo um grupo de recursos baseado no tipo e nas propriedades, e depois fazer as mudanças. Para criar uma regra, é necessário definir os critérios para os recursos de destino, as mudanças que ocorrerão e o tipo de ação a ser tomada. Você pode testar as regras de CMDB personalizadas antes de executá-las em um ambiente de produção, criar agendamentos e notificar funcionários relevantes. As regras de CMDB também podem ser executadas usando tarefas e trabalhos.

Note que o uso de regras do CMDB exige o CMDB Solution.

Aviso: As regras do CMDB são poderosas e podem alterar quantidades vastas de dados. Para que você use uma regra personalizada do CMDB em um ambiente de produção, é altamente recomendado que você teste a regra usando a opção **Testar regra** na página **Regra do CMDB**.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para criar uma regra para editar dados do CMDB

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Conector**.
- 3 Clique com o botão direito do mouse em **Regras do CMDB** e clique em **Novo(a) > Regra do CMDB**.
- 4 No painel direito, especifique valores para a regra.
Para obter mais informações, clique na página e pressione **F1**.
- 5 Clique em **Salvar alterações**.

Execução de uma regra de CMDB como uma tarefa

Você pode executar uma regra de CMDB usando uma tarefa, que permite executar a regra junto com uma série de outras tarefas em um trabalho.

Consulte [“Para criar uma regra para editar dados do CMDB”](#) na página 484.

Nota: As tarefas definidas pelo usuário da Connector Solution 6.5 não são migradas automaticamente no produto atual. Você deve criar novamente estas tarefas de forma manual. Além disso, a capacidade para que uma tarefa suporte executar várias regras em uma ordem especificada foi movida para os trabalhos. Cada tarefa pode apenas executar uma única regra.

Esta tarefa é uma etapa do processo para importar e exportar dados.

Consulte [“Para importar e exportar dados”](#) na página 477.

Para executar uma regra do CMDB como uma tarefa

- 1 No Console de gerenciamento Symantec, no menu **Gerenciar**, clique em **Trabalhos e tarefas**.
- 2 No painel esquerdo, clique com o botão direito do mouse na pasta onde você deseja que a tarefa seja adicionada e clique em **Novo(a) > Trabalho ou tarefa**.
- 3 No painel esquerdo da caixa de diálogo **Criar nova tarefa**, clique em **Tarefas do servidor > Executar regra do CMDB**.
- 4 No painel direito, especifique um nome para a tarefa e selecione uma regra de CMDB para que a tarefa seja executada.

- 5 Clique em **OK**.
- 6 No painel direito, especifique um agendamento para executar a regra.
Consulte "[Para adicionar um agendamento a uma política, tarefa ou trabalho](#)" na página 425.
Consulte "[Para configurar um agendamento](#)" na página 123.

Para criar uma classe de dados virtual

As classes de dados virtuais permitem integrar dados de sistema de terceiros com o CMDB do Symantec Management Platform sem a necessidade de importar os dados para o CMDB.

Os dados externos que são mapeados para uma classe de dados virtuais aparecem como uma classe de dados normal dos recursos no CMDB. As classes de dados virtuais fornecem integração ininterrupta com os recursos de geração de relatórios do Symantec Management Platform. Você pode usar o construtor do relatório para criar os relatórios dos recursos baseados em classes de dados virtuais. O relatório consulta os dados diretamente da fonte de dados externa ao mesmo tempo que você executa o relatório.

Os servidores vinculados a estes sistemas devem inicialmente ser configurados em SQL Server antes de usar classes de dados virtuais. Consulte a documentação da Microsoft sobre os servidores vinculados ([http://msdn.microsoft.com/en-us/library/ms188279\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms188279(SQL.90).aspx)) para obter mais informações.

Você deve ter privilégios de "Gerenciar o Data Connector" para criar, editar ou excluir uma classe de dados virtuais. Para editar uma classe de dados virtuais, é necessário também ter a permissão de Gravação na classe de dados virtuais.

Para criar uma classe de dados virtuais editável

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Configurações de recursos e classes de dados**.
- 3 Clique com o botão direito do mouse em **Classe de dados** e, em seguida, em **Novo(a) > Classe de dados virtual**.
- 4 Clique em **Salvar alterações**.

Configuração das opções de limpeza de logs detalhados do Data Connector

Você pode configurar a limpeza de arquivos de log de regra. A limpeza é executada durante o agendamento padrão diário.

Para configurar as opções de limpeza de logs detalhados do Data Connector

- 1 No Console de gerenciamento Symantec, no menu **Configurações**, clique em **Todas as configurações**.
- 2 No painel esquerdo, expanda **Configurações > Notification Server > Conector** e clique em **Política de exclusão do conector**.
- 3 No painel direito, especifique as opções de apagamento do arquivo de log da regra.
- 4 Clique em **Salvar alterações**.

Privilégios e permissões de segurança

Este Apêndice contém os tópicos a seguir:

- [Categorias de privilégio de segurança](#)
- [Categorias de permissão de segurança](#)
- [Privilégios do perfil de conexão](#)
- [Privilégios de gerenciamento](#)
- [Privilégios do sistema](#)
- [Privilégios da credencial](#)
- [Privilégios do diretório de fluxo de trabalho](#)
- [Privilégios do Symantec Management Console](#)
- [Privilégios do Gerenciamento de software](#)
- [Privilégios do menu contextual](#)
- [Menu contextual - privilégios de exemplos de conector](#)
- [Menu de clique com o botão direito do mouse - Privilégios de hierarquia](#)
- [Menu de clique com o botão direito do mouse - Privilégios de ações](#)
- [Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos](#)
- [Permissões de gerenciamento de recursos](#)
- [Permissões do sistema](#)

- [Permissões do servidor de tarefas](#)
- [Permissões de relatório](#)
- [Permissões de políticas](#)
- [Permissões de pasta](#)
- [Permissões de filtros](#)
- [Permissões do perfil de conexão](#)
- [Permissões do Gerenciador de credenciais](#)

Categorias de privilégio de segurança

Um privilégio permite que o usuário execute uma ação específica no Symantec Management Platform ou em itens no Console de gerenciamento Symantec. Para executar uma ação em um item, a função do usuário deve ter a permissão necessária no item. Os privilégios que você pode atribuir a uma função de segurança são agrupados em categorias. Porém, quando você atribuir privilégios a uma função de segurança, precisará selecionar individualmente os privilégios apropriados.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-1 Categorias de privilégio de segurança

Categoria do privilégio	Descrição
Privilégios do perfil de conexão	Permite criar e modificar perfis de conexão. Consulte “Privilégios do perfil de conexão” na página 492.
Privilégios de gerenciamento	Permite criar itens de gerenciamento, como os filtros, destinos, relatórios e tarefas, no Symantec Management Platform. Consulte “Privilégios de gerenciamento” na página 493.
Privilégios do sistema	Permite executar atividades de gerenciamento, como configurar a segurança, gerenciar a hierarquia e a importação de arquivos XML, no Symantec Management Platform. Consulte “Privilégios do sistema” na página 494.
Privilégios da credencial	Permite usar o Gerenciador de credenciais para criar e modificar credenciais. Estas credenciais não são as mesmas credenciais internas e as do Windows associadas às contas do usuário. Nota: O Gerenciador de credenciais é um componente do Symantec Management Platform prolongado; assim, pode não ser instalado em seu ambiente. Consulte “Privilégios da credencial” na página 497.

Categoria do privilégio	Descrição
Privilégios do diretório de fluxo de trabalho	Permite publicar fluxos de trabalho do Workflow Designer no Notification Server como uma ação de tarefa ou item (uma opção no menu de clique com o botão direito do mouse). Consulte “Privilégios do diretório de fluxo de trabalho” na página 497.
Privilégios de console	Permite personalizar o Console de gerenciamento Symantec. Estes privilégios incluem a capacidade de editar o menu e de criar páginas do portal, Web parts e exibições. Consulte “Privilégios do Symantec Management Console” na página 498.
Privilégios de gerenciamento de software	Permite conceder capacidades específicas à função de usuário e permitir que o usuário execute tarefas específicas na exibição Software e na janela Catálogo de software. Estes privilégios também oferecem a capacidade de criar a Biblioteca de software e de criar e importar recursos de software. Consulte “Privilégios do Gerenciamento de software” na página 499.
Privilégios do Menu de clique com o botão direito do mouse	Permite executar ações gerais em itens do Console de gerenciamento Symantec. Quando você clica com o botão direito do mouse em um item, as opções relevantes a esse tipo de item ficam disponíveis no menu de clique com o botão direito do mouse. Estes privilégios incluem a capacidade de excluir um item, editar exibições, links da Web e links de itens, e também a capacidade de iniciar, interromper e agendar tarefas. Consulte “Privilégios do menu contextual” na página 501.
Menu de clique com o botão direito do mouse - Privilégios de amostras de conector	Exemplos de ações de clique com o botão direito do mouse que podem ser criadas pelo usuário. Consulte “Menu contextual - privilégios de exemplos de conector” na página 502.
Menu de clique com o botão direito do mouse - Privilégios de hierarquia	Permite gerenciar a replicação de hierarquia. Estes privilégios permitem incluir ou excluir itens específicos da replicação de hierarquia e replicar itens imediatamente. Consulte “Menu de clique com o botão direito do mouse - Privilégios de hierarquia” na página 503.
Menu de clique com o botão direito do mouse - Privilégios de ações	Permite executar as ações que são relevantes ao Software Management Framework. As soluções adicionais instaladas no Symantec Management Platform podem acrescentar mais privilégios a esta categoria. Consulte “Menu de clique com o botão direito do mouse - Privilégios de hierarquia” na página 503.

Categoria do privilégio	Descrição
Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos	Permite mudar o status de um ativo. Estes privilégios permitem definir o status de um recurso como Ativo ou Desativado. As soluções instaladas no Symantec Management Platform podem adicionar mais privilégios. Consulte “Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos” na página 505.

Categorias de permissão de segurança

As permissões em um item no Console de gerenciamento Symantec determinam o acesso que uma função de segurança tem a esse item. As permissões em itens são aplicadas às funções de segurança, não às contas do usuário. Por exemplo, a permissão Leitura em um item permite que o usuário exiba um item, e a permissão Gravar que o usuário o modifique.

Consulte [“Para atribuir permissões de segurança a pastas e itens”](#) na página 103.

As permissões são usadas com privilégios para determinar que ações uma função de segurança pode executar em um item. Por exemplo, para excluir um item, uma função de segurança deve ter o privilégio e a permissão Excluir nesse item específico. Ter somente o privilégio ou a permissão Excluir no item não é suficiente.

Você pode especificar as permissões que se aplicam a cada pasta ou item para cada função de segurança. As permissões que são aplicadas diretamente a uma pasta ou item (permissões não herdadas) são combinadas com as que são herdadas da pasta pai. As permissões combinadas determinam o acesso que a função de segurança tem a essa pasta ou item específicos.

Por padrão, os itens e as pastas filho herdam todas as permissões de uma pasta. Você pode modificar a herança de permissão para atender seus requisitos.

As categorias de permissão de segurança relacionam e descrevem as categorias que você pode definir para cada função.

Tabela A-2 Categorias de permissão de segurança

Categoria da permissão	Descrição
Gerenciamento de recursos	Estas permissões se aplicam aos recursos. Consulte “Permissões de gerenciamento de recursos” na página 506.

Categoria da permissão	Descrição
Sistema	Estas permissões se aplicam ao sistema, como a leitura, a gravação e a exclusão de itens. Consulte “Permissões do sistema” na página 506.
Task Server	Estas permissões se aplicam ao Task Server. Consulte “Permissões do servidor de tarefas” na página 507.
Relatório	Estas permissões se aplicam aos relatórios. Consulte “Permissões de relatório” na página 507.
Política	Estas permissões aplicam-se às políticas. Consulte “Permissões de políticas” na página 508.
Pasta	Estas permissões se aplicam às pastas. Consulte “Permissões de pasta” na página 508.
Filtro	Estas permissões se aplicam aos filtros. Consulte “Permissões de filtros” na página 508.
Perfil de conexão	Estas permissões permitem usar perfis de conexão. Consulte “Permissões do perfil de conexão” na página 509.
Gerenciador de credenciais	Estas permissões permitem usar o Gerenciador de credenciais. Consulte “Permissões do Gerenciador de credenciais” na página 509.

Privilégios do perfil de conexão

Os privilégios do perfil de conexão permitem criar e modificar perfis de conexão. Os perfis de conexão armazenam as informações necessárias à comunicação com computadores e outros dispositivos de rede usando protocolos padrão de monitoramento da rede. Estes protocolos incluem SNMP, WMI, WSMAN e muitos outros.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-3 Privilégios do perfil de conexão

Privilégio	Descrição
Criar perfil de conexão	Permite criar e modificar perfis de conexão.

Privilégios de gerenciamento

Os privilégios de gerenciamento permitem criar itens de gerenciamento, como os filtros, destinos, relatórios e tarefas, no Symantec Management Platform.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-4 Privilégios de gerenciamento

Privilégio	Descrição
Criar configurações do agente	Permite criar uma nova política de configurações direcionadas do agente ou duplicar uma existente. As configurações direcionadas do agente são os parâmetros gerais que controlam o Symantec Management Agent, incluindo como o agente se comunica com o Notification Server. Consulte “Para definir as configurações do agente de destino” na página 278.
Criar políticas de automação	Permite criar novas políticas de automação. Uma política de automação é dinâmica e especifica ações automatizadas a executar no computador do Notification Server. Ela é direcionada aos computadores adequados quando a política é ativada e executa todas as ações necessárias com base no estado atual de cada computador de destino. Consulte “Sobre as políticas de automação” na página 392.
Criar filtros	Permite criar novos filtros de recursos. Um filtro de recursos, geralmente conhecido como filtro, é uma definição dinâmica de um conjunto de recursos. Filtros são usados com grupos organizacionais para identificar os recursos (um destino de recursos) aos quais uma tarefa ou uma política se aplicam. Consulte “Sobre filtros de recursos” na página 354.
Criar trabalhos ou tarefas	Permite criar um novo trabalho ou tarefa, ou duplicar trabalhos e tarefas existentes. Os trabalhos podem conter várias tarefas, trabalhos e condições, o que lhe fornece grande flexibilidade para configurar a sequência de trabalhos necessária. Consulte “Para criar uma tarefa” na página 419. Consulte “Criação de trabalhos” na página 420.

Privilégio	Descrição
Criar janelas de manutenção	Permite criar uma nova política de janela de manutenção ou duplicar uma existente. Uma janela de manutenção é um horário e uma duração agendados nos quais as operações de manutenção podem ser executadas em um computador gerenciado. Uma política de janela de manutenção define uma ou mais janelas de manutenção.
Criar nova tarefa do cliente	Permite criar uma nova tarefa do cliente. As tarefas do cliente são distribuídas nos computadores gerenciados por um servidor de tarefas. Em seguida, o computador gerenciado executa a tarefa e informa o Notification Server. Consulte “Criação de trabalhos” na página 420.
Criar nova tarefa de servidor	Permite criar uma nova tarefa do servidor. As tarefas de servidor são executadas no Notification Server. Consulte “Criação de trabalhos” na página 420.
Criar grupos organizacionais	Permite criar novas exibições e grupos organizacionais. Uma exibição organizacional é um agrupamento hierárquico de recursos (como grupos organizacionais) que reflete uma exibição ou estrutura real de sua organização.
Criar relatórios	Permite duplicar um relatório novo ou clonar um existente. Consulte “Para criar e modificar relatórios personalizados do Notification Server” na página 452.
Criar destinos de recursos	Permite criar novos destinos de recursos. Um destino de recursos, geralmente conhecido como destino, é uma estrutura que permite aplicar tarefas e políticas a uma coleção dinâmica de recursos. Um destino consiste em ao menos uma exibição ou grupo organizacional e vários filtros. Os filtros refinam os recursos disponíveis para identificar aqueles que você quer. Consulte “Sobre destinos de recursos” na página 367.
Gerenciamento de tarefas de descoberta	Permite executar tarefas Descoberta de rede.

Privilégios do sistema

Os privilégios do sistema permitem executar atividades de gerenciamento, como configurar a segurança, gerenciar a hierarquia e a importação de arquivos XML, no Symantec Management Platform.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-5 Privilégios do sistema

Privilégio	Descrição
Alterar segurança	Permite mudar a configuração de segurança no Symantec Management Platform. Você pode criar funções de segurança, atribuir privilégios e contas do usuários a essas funções e atribuir permissões aos itens do gerenciamento para cada função. Consulte “Para configurar a segurança do Symantec Management Platform” na página 84.
Criar regras do CMDB	Permite criar regras do CMDB no Data Connector. Você usa o Data Connector para transferir dados entre o CMDB e uma fonte de dados e manipular dados dentro do CMDB. O Data Connector faz parte do Symantec Management Platform prolongado. Consulte “Sobre o Data Connector” na página 474.
Editar SQL diretamente	Permite criar ou modificar consultas SQL nos relatórios e nos filtros. Este privilégio também permite editar a consulta da fonte de dados e exibir os resultados da consulta de uma fonte de dados de uma Consulta SQL bruta para uma política de automação. Se um usuário for proficiente em SQL e familiarizado com o CMDB, este privilégio permitirá que ele escreva relatórios eficientes e muito específicos. Porém, também pode ser usado para impedir verificações de segurança. Por exemplo, um usuário pode gravar uma consulta que acesse os recursos que estão fora de seu escopo. Isto é, os recursos não são contidos nos grupos organizacionais que o usuário tem permissão para exibir. Aviso: Consultas SQL escritas incorretamente podem retornar resultados incorretos ou ser ineficientes, consumindo memória e tempo de CPU em excesso no computador do CMDB. Além disso, uma consulta SQL maliciosa pode excluir, modificar ou adicionar dados em qualquer lugar no CMDB. Consequentemente, este privilégio é muito sensível à segurança, sendo concedido por padrão somente à função Administradores Symantec. Se você permitir que os membros da função de segurança editem diretamente o SQL, será necessário usar as credenciais do aplicativo específicas para relatórios de modo que eles usem uma conta com acesso restrito ao CMDB Consulte “Para definir uma consulta SQL para um relatório personalizado” na página 459.

Privilégio	Descrição
Importar/exportar XML	Permite que você importe itens e recursos de arquivos XML especialmente estruturados e exporte itens e recursos para arquivos XML. Tome cuidado ao criar um item ou recurso no Symantec Management Platform importando as informações armazenadas em um arquivo XML. Criar um item dessa maneira ignora todas as verificações de segurança. Por exemplo, um usuário poderá criar um relatório importando seu XML mesmo quando o usuário não tiver os privilégios e as permissões necessários. Neste exemplo o usuário precisa do privilégio Criar relatórios e da permissão Criar filhos para a pasta na qual o relatório é armazenado. Esse privilégio é muito sensível à segurança. Por padrão, é concedido somente à função Administradores Symantec e não deve ser concedido a não administradores. Consulte “Para salvar elementos do console como arquivos XML” na página 61.
Gerenciar Data Connector	Permite gerenciar o Data Connector. O Data Connector faz parte do Symantec Management Platform prolongado. Você usa o Data Connector para transferir dados entre o CMDB e uma fonte de dados e manipular dados dentro do CMDB. Consulte “Sobre o Data Connector” na página 474.
Gerenciar replicação de hierarquia	Permite criar e executar regras de replicação de hierarquia. As regras de replicação de hierarquia especificam o que é replicado para o Notification Server pai e todos os Notification Servers filho. Este privilégio também permite acessar as regras de replicação autônomas. Consulte “Para configurar a replicação de hierarquia e as regras da replicação de hierarquia” na página 163.
Gerenciar hierarquia	Permite adicionar ou remover seu Notification Server de uma hierarquia. Você pode adicionar seu Notification Server a uma hierarquia como um filho de um Notification Server remoto existente ou como seu pai. Lembre-se de que seu Notification Server é aquele no qual você está conectado, que pode ser um logon remoto. Este privilégio é necessário nos dois Notification Servers para criar ou mudar um relacionamento hierárquico entre eles.
Obter propriedade	Permite tomar a posse de uma entidade de segurança. Este privilégio concede permissões completas na entidade ao novo proprietário. Por exemplo, seria necessário obter propriedade caso todas as permissões na entidade tenham sido removidas acidentalmente. Consulte “Para obter a propriedade de uma pasta ou item” na página 115.

Privilégio	Descrição
Exibir segurança	Permite exibir a configuração de segurança no Symantec Management Platform. Estas informações incluem detalhes das funções de segurança e das contas dos usuários, os privilégios e as permissões atribuídos a cada função.

Privilégios da credencial

Os privilégios da credencial permitem criar credenciais novas no Gerenciador de credenciais. O Gerenciador de credenciais fornece um local de armazenamento seguro para nomes de usuário e senhas. Os tipos de credenciais que o Gerenciador de credenciais armazena são definidos pelas soluções instaladas no Symantec Management Platform.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Quando uma credencial for criada, o acesso será concedido apenas ao criador. Se outros usuários precisarem executar uma operação de gerenciamento que exija uma credencial, você precisará atribuir este privilégio à função ou à conta do usuário apropriada que contenha a conta do usuário.

Tabela A-6 Privilégios da credencial

Privilégio	Descrição
Criar credencial	Permite criar e modificar credenciais no Gerenciador de credenciais.

Privilégios do diretório de fluxo de trabalho

Os privilégios do diretório de fluxo de trabalho permitem publicar fluxos de trabalho do Workflow Designer no Notification Server como uma ação de item ou tarefa (uma opção no menu contextual).

O Workflow Designer faz parte do Workflow Solution. Quando você instalar o Workflow Solution, será adicionada uma página ao Symantec Management Console que permite fazer o download e instalar o Workflow Designer. Ele não está incluído no Symantec Management Platform por padrão.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-7 Privilégios do diretório de fluxo de trabalho

Privilégio	Descrição
Registrar/cancelar registro de fluxos de trabalho	Permite publicar fluxos de trabalho do Workflow Designer no Notification Server como uma ação de tarefa ou item (uma opção no menu contextual). Para obter mais informações, consulte a documentação do Workflow Solution.

Privilégios do Symantec Management Console

Os privilégios do Symantec Management Console permitem personalizá-lo. Estes privilégios incluem a capacidade de editar o menu e de criar páginas do portal, Web parts e exibições.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-8 Privilégios do Symantec Management Console

Privilégio	Descrição
Criar páginas do portal	Permite criar novas páginas do portal. Uma página do portal é uma página do Symantec Management Console que pode ser personalizada para se adaptar às suas necessidades. Você pode usar uma página do portal para consolidar as informações importantes em uma única página de fácil exibição. Uma página do portal pode exibir o status do Symantec Management Platform e dos computadores gerenciados ou quaisquer outras informações que você queira disponibilizar. Por exemplo, você pode incluir páginas externas da Web, páginas da intranet, RSS feeds ou seus próprios aplicativos. É necessário ter a permissão Criar filhos na pasta em que você deseja criar a nova página do portal.
Criar Web parts	Permite criar novas Web parts. As Web parts são minipáginas da Web que você pode usar como componentes para páginas do portal. Uma Web part pode exibir um relatório ou o conteúdo de uma página da Web. É necessário ter a permissão Criar filhos na pasta em que você deseja criar a nova Web part. Consulte “Para criar e modificar Web parts” na página 60.

Privilégio	Descrição
Criar exibições	Permite criar novas exibições. Uma exibição é um layout em painel duplo com uma árvore de navegação no lado esquerdo e o conteúdo no lado direito. A árvore de navegação contém os links para os itens do Symantec Management Console e permite agrupar os itens de diferentes partes do console em uma estrutura apropriada. Um item pode aparecer várias vezes em uma exibição e em qualquer número de exibições diferentes. Uma exibição pode incluir pastas, links de itens e links da Web. Consulte “Sobre as exibições do console” na página 35.
Editar menu do Console	Permite personalizar os menus do Symantec Management Console. As opções de menu fornecidas com o Symantec Management Platform são somente leitura e não podem ser modificadas. É possível adicionar novos submenus e modificá-los conforme a necessidade. Você pode mover ou excluir qualquer item de menu, exceto aqueles que foram designados como somente leitura. Consulte “Para personalizar o menu do console” na página 52.

Privilégios do Gerenciamento de software

Cada privilégio do **Gerenciamento de software** concede capacidades específicas à função de usuário e permite que o usuário execute tarefas específicas na exibição **Software** e na janela **Catálogo de software** das exibições aprimoradas do console. Estes privilégios também oferecem a capacidade de criar a Biblioteca de software e de criar e importar recursos de software. Estes privilégios de **Gerenciamento de software** não são, por padrão, parte de nenhuma função de usuário. Você deve atribuir o privilégio relevante a uma função de usuário.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-9 Privilégios do Gerenciamento de software

Privilégio	Descrição
Criar produtos de software e Definir filtros de inventário de produtos de software	Este privilégio permite que o usuário use a pesquisa salva Software descoberto recentemente na exibição Software para encontrar softwares recém-descobertos. Este privilégio permite que o usuário use os painéis Software recém-descoberto/indefinido e Software não gerenciado, no Catálogo de software, para gerenciar o software. Para ter estas capacidades, você deve atribuir à função de usuário os privilégios Create software products e Definir produtos de software.

Privilégio	Descrição
Create software products	Este privilégio permite que o usuário utilize o botão Adicionar produto para abrir a caixa de diálogo Produto de software. Este privilégio permite também que o usuário insira dados na áreas Name, Company, Version e Category, da caixa de diálogo Produto de software para criar produtos de software. Se você não atribuir este privilégio à função de usuário, o usuário será incapaz de inserir a informações nas áreas Name, Company, Version e Category da caixa de diálogo Produto de software.
Define software product inventory filters	Este privilégio permite que o usuário use a guia Identificar inventário para definir filtros de inventário do produto de software.
Configure software usage tracking	Este privilégio permite que o usuário utilize o hiperlink Adicionar arquivos de programas e a guia Monitorar/rastrear uso para configurar o controle de uso do software.
Create software licenses	Este privilégio permite que o usuário utilize o botão Gerenciar licenças para criar licenças de software.
Gerenciar recursos de software	Permite criar, importar, editar e excluir recursos de software. Um recurso de software consiste nos metadados que descrevem uma instância específica de um produto de software. Um recurso de software fornece uma maneira comum de descrever o software de modo que todas as ações relacionadas ao software possam identificá-lo corretamente. Normalmente, é necessário fornecer privilégios de recursos de software às contas do usuário que distribuem e gerenciam software. As funções de segurança do Symantec Software Librarian e do Asset Manager têm este privilégio por padrão.
Gerenciar configurações da biblioteca de software	Permite criar e editar as Configurações da Biblioteca de software. A Biblioteca de software é o local físico do diretório dos arquivos de pacote associados ao software no Catálogo de software. Como a Biblioteca de software é um repositório das versões definitivas e autorizadas dos pacotes, é necessário restringir o acesso à biblioteca para manter sua integridade. As funções de segurança do Symantec Software Librarian e do Asset Manager têm este privilégio por padrão.

Privilégio	Descrição
Criar entregas de software	Permite criar entregas de software (tarefas de Entrega rápida ou de Entrega de pacotes e a política de Gerenciar entrega de software) para o recurso de software selecionado na lista de softwares disponíveis. Permite usar o recurso de arrastar e soltar para iniciar a entrega de software de qualquer lista de software. Este privilégio permite também que o usuário use a guia Delivery para criar entregas de software.

Privilégios do menu contextual

Os privilégios do menu contextual (também chamados de privilégios de ação de item) permitem executar ações gerais em itens no Symantec Management Console. Quando você clicar com o botão direito do mouse em um item, as opções relevantes a esse tipo de item ficarão disponíveis no menu contextual. Estes privilégios incluem a capacidade de excluir um item, editar exibições, links da Web e links de itens, e também a capacidade de iniciar, interromper e agendar tarefas.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-10 Privilégios do menu contextual

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Adicionar a grupo organizacional	Permite adicionar recursos a um grupo organizacional. Consulte “Para criar e configurar um grupo organizacional” na página 346.	Todos os recursos	Permissão de gravação no grupo organizacional.
Duplicar	Permite duplicar um item.	Todos os tipos de item	Permissão de duplicação no item.
Excluir	Permite excluir um item.	Todos os tipos de item	Permissão de exclusão no item.
Editar link do item	Permite modificar um link do item. Consulte “Sobre as exibições do console” na página 35.	Somente links do item.	Permissão de gravação no link do item.
Editar regra	Permite editar uma regra de inventário.	Apenas regras de inventário.	Permissão de gravação na regra de inventário.

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Editar exibição	Permite editar uma exibição. Consulte “Para criar e modificar exibições” na página 55.	Apenas exibições.	Permissão de gravação na exibição.
Editar link da Web	Permite modificar um link da Web. Consulte “Sobre as exibições do console” na página 35.	Apenas links da Web.	Permissão de gravação no link da Web.
Agendamento	Permite agendar uma política. Consulte “Especificação de um agendamento de política” na página 388.	Apenas políticas.	Permissão de gravação na política.
Agendar tarefa	Permite agendar uma tarefa. Você pode definir a tarefa para ser executada em um horário específico ou para ser repetida em intervalos regulares. Consulte “Para adicionar um agendamento a uma política, tarefa ou trabalho” na página 425.	Apenas tarefas.	Permissão de execução de tarefas na tarefa.
Gerenciador de função de segurança	Permite abrir o Gerenciador de função de segurança.	Todos os tipos de item	Permissão de gravação no item.
Iniciar tarefa	Permite iniciar uma tarefa imediatamente. Consulte “Execução de um trabalho ou uma tarefa” na página 422.	Apenas tarefas.	Permissão de execução de tarefas na tarefa.
Interromper tarefa	Permite interromper uma tarefa imediatamente.	Apenas tarefas.	Permissão de execução de tarefas na tarefa.

Menu contextual - privilégios de exemplos de conector

Os privilégios de exemplos de conector são exemplos de ações de clique com o botão direito do mouse que podem ser criadas pelo usuário.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-11 Menu contextual - privilégios de amostras de conector

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Fazer ping no computador	Permite fazer ping de TCP/IP em um computador.	Recursos de computador somente	Permissão de leitura no grupo organizacional que contém o computador.

Menu de clique com o botão direito do mouse - Privilégios de hierarquia

Os privilégios de hierarquia permitem gerenciar a replicação de hierarquia. Estes privilégios permitem incluir ou excluir itens específicos da replicação de hierarquia e replicar itens imediatamente.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-12 Menu de clique com o botão direito do mouse - Privilégios de hierarquia

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Desativar replicação	Permite impedir que um item participe da replicação de hierarquia. Todos os itens de configuração e gerenciamento, bem como as funções e os privilégios de segurança, são replicados por padrão. Esta opção estará disponível somente quando as regras personalizadas de replicação de hierarquia forem usadas. Consulte “Para configurar a replicação de hierarquia personalizada” na página 165.	Todos os tipos de item	Privilégio Gerenciar replicação de hierarquia, Gravar a permissão no item.
Replicar agora	Permite replicar os dados selecionados diretamente do Notification Server para todos os Notification Servers subordinados sem incluí-lo em uma regra de replicação. Esta operação é uma replicação única que ocorre imediatamente. Consulte “Para replicar manualmente dados selecionados” na página 168.	Todos os tipos de item	Privilégio Gerenciar replicação de hierarquia, Gravar a permissão no item.

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Ativar replicação	Permite consentir que um item participe da replicação de hierarquia. Todos os itens de configuração e gerenciamento, bem como as funções e os privilégios de segurança, são replicados por padrão. Esta opção estará disponível somente quando as regras personalizadas de replicação de hierarquia forem usadas. Consulte “Para configurar a replicação de hierarquia personalizada” na página 165.	Todos os tipos de item	Privilégio Gerenciar replicação de hierarquia, Gravar a permissão no item.

Menu de clique com o botão direito do mouse - Privilégios de ações

Os privilégios de ações permitem executar as ações relevantes para o Software Management Framework. As soluções adicionais instaladas no Symantec Management Platform podem acrescentar mais privilégios a esta categoria.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-13 Menu de clique com o botão direito do mouse - Privilégios de ações

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Atribuir tipo	Atribui um tipo a recurso de software não atribuído no Catálogo de software. Um recurso de software não atribuído não é categorizado como um release de software, uma atualização ou um service pack.	Somente recursos de software	
Criar filtro de software instalado	Cria filtros para encontrar computadores gerenciados pelo software instalado neles.	Somente recursos de software	
Exportação detalhada	Exporta um recurso de software e qualquer uma de suas informações de recurso associadas para um arquivo XML detalhado.	Somente recursos de software	

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Editar linha de comando	Abre a linha de comando selecionada para edição dentro da página de edição de recursos de software.	Somente recursos de software	
Editar pacote	Abre o pacote selecionado para edição dentro da página de edição de recursos de software.	Somente recursos de software	
Editar recurso de software	Abre o recurso de software selecionado para edição.	Somente recursos de software	
Importar pacote	Muda a fonte de um pacote para a Biblioteca de software de uma fonte diferente, como um diretório no servidor ou um caminho UNC.	Somente recursos de software	
Mesclar recursos de empresa	Mescla o recurso de empresa selecionado com outro recurso de empresa. Este privilégio é útil se você tem duas entradas para a mesma empresa que são escritas de forma um pouco diferente, como "Symantec" e "Symantec Corporation". Você pode selecionar os itens para mesclar e especificar o nome apropriado para usar.		
Resolver recursos de software duplicados	Quando dois recursos de software representarem o mesmo software, mas tiverem identificadores diferentes, esta caixa de diálogo permitirá que o usuário associe ambos os identificadores a um recurso de software.	Somente recursos de software	

Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos

Os privilégios da definição de status dos ativos permitem definir o status de um recurso como Ativo ou Desativado.

As soluções instaladas no Symantec Management Platform podem adicionar mais privilégios a esta categoria. Por exemplo, o Asset Management Solution adiciona três ou quatro privilégios aqui.

Consulte [“Categorias de privilégio de segurança”](#) na página 489.

Consulte [“Para atribuir privilégios a uma função de segurança”](#) na página 93.

Tabela A-14 Menu de clique com o botão direito do mouse - Privilégios da definição de status dos ativos

Privilégio	Descrição	Aplica-se a tipos de item	Requisitos adicionais
Ativos	Define o status dos recursos selecionados como ativo.	Recursos somente	Permissão de gravação no grupo organizacional que contém o recurso.
Desativado	Define o status dos recursos selecionados como desativado.	Recursos somente	Permissão de gravação no grupo organizacional que contém o recurso.

Permissões de gerenciamento de recursos

Essas permissões se aplicam aos recursos.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-15 Permissões de gerenciamento de recursos

Permissão	Descrição
Ler dados do recurso	Permite ler dados de recursos.
Ler associação de recursos	Permite ler dados de associação de recursos.
Gravar dados de recursos	Permite gravar dados de recursos.
Gravar associação de recursos	Permite gravar dados de associação de recursos.

Permissões do sistema

Estas permissões se aplicam ao sistema, como a leitura, a gravação e a exclusão de itens.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-16 Permissões do sistema

Permissão	Descrição
Controle total	Permite ter o controle total de um item que outro usuário possua. Consulte “Para obter a propriedade de uma pasta ou item” na página 115.
Excluir	Permite excluir itens
Gravar	Permite criar ou modificar itens.
Duplicar	Permite duplicar um item existente.
Ler	Permite abrir um item e visualizar o conteúdo do item.
Mudar permissões	Permite mudar permissões em itens.
Permissões de leitura	Permite ler as permissões para um item.

Permissões do servidor de tarefas

Estas permissões se aplicam ao servidor de tarefas.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-17 Permissões do servidor de tarefas

Permissão	Descrição
Criar nova tarefa	Permite criar tarefas novas.
Executar script	Permite executar um script.
Executar controle de energia	Permite executar tarefas de controle de energia.
Executar tarefa	Permite executar tarefas.
Executar estado do serviço de controle	Permite executar um estado do serviço de controle.

Permissões de relatório

Essas permissões se aplicam aos relatórios.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-18 Permissões de relatório

Permissão	Descrição
Executar relatórios	Permite executar um relatório.
Salvar relatórios	Permite salvar um relatório.

Permissões de políticas

Essas permissões aplicam-se às políticas.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-19 Permissões de políticas

Permissão	Descrição
Aplicar a destinos de recursos	Permite aplicar destinos de recursos às políticas.
Ativar política	Permite ativar ou desativar uma política.

Permissões de pasta

Essas permissões se aplicam às pastas.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-20 Permissões de pasta

Permissão	Descrição
Criar filhos	Permite adicionar itens e subpastas a uma pasta.

Permissões de filtros

Estas permissões se aplicam aos filtros.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-21 Permissões de filtros

Permissão	Descrição
Aplicar configurações do agente	Permite mudar uma política de configurações direcionadas do agente e aplicá-la a um destino de recursos.
Aplicar tarefas de entrega de software	Permite aplicar tarefas de entrega de software.

Permissões do perfil de conexão

Estas permissões permitem usar perfis de conexão. Os perfis de conexão armazenam as informações necessárias à comunicação com computadores e outros dispositivos de rede usando protocolos padrão de monitoramento da rede. Estes protocolos incluem SNMP, WMI, WSMAN e muitos outros.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Os perfis de conexão são associados aos dispositivos durante a descoberta de rede. Durante a descoberta, um perfil de conexão é selecionado para definir os protocolos e as credenciais que serão usados. Quando a descoberta for concluída, este perfil de conexão será associado a cada recurso descoberto. Quando forem necessárias informações, o perfil de conexão associado será usado para se conectar.

Tabela A-22 Permissões do perfil de conexão

Permissão	Descrição
Uso	Permite usar perfis de conexão.

Permissões do Gerenciador de credenciais

O Gerenciador de credenciais fornece um local de armazenamento seguro para nomes de usuário e senhas. Os tipos de credenciais que o Gerenciador de credenciais armazena são definidos pelas soluções instaladas no Symantec Management Platform. Estas permissões permitem usar o Gerenciador de credenciais.

Consulte [“Categorias de permissão de segurança”](#) na página 491.

Tabela A-23 Permissões do Gerenciador de credenciais

Permissão	Descrição
Uso	Permite usar o Gerenciador de credenciais.

Symantec Management Agent

Este Apêndice contém os tópicos a seguir:

- [Intervalos recomendados de atualização de dados do Symantec Management Agent](#)
- [Symantec Management Agent para comandos de solução de problemas de UNIX, Linux e Mac](#)

Intervalos recomendados de atualização de dados do Symantec Management Agent

O Symantec Management Agent envia regularmente dados do inventário básico e recebe dados de configuração do agente do Notification Server. Você pode configurar os intervalos para estas atualizações. Quanto mais computadores você gerenciar, menor será a frequência com que você deverá atualizar os dados para reduzir a carga no Notification Server.

Consulte [“Para definir as configurações do agente de destino”](#) na página 278.

Tabela B-1 Intervalos recomendados de atualização de dados do Symantec Management Agent

Número de computadores gerenciados	Inventário básico	Solicitação de configuração
0 - 499	30 minutos	15 minutos
500 - 1999	8 horas	4 horas
> 2000	24 horas	8 horas

O Notification Server inclui uma política de automação que envia automaticamente um e-mail quando os intervalos de atualização são inferiores aos valores recomendados. Esta política, a verificação de escalabilidade, evita a necessidade de verificar regularmente os intervalos de atualização à medida que computadores são adicionados ou removidos de sua rede. Você pode ativar ou desativar a política de verificação de escalabilidade conforme necessário e definir a agenda apropriada.

Consulte [“Gerenciamento de políticas de automação”](#) na página 394.

Symantec Management Agent para comandos de solução de problemas de UNIX, Linux e Mac

Você pode usar comandos para solucionar problemas. Você deve executá-los de dentro de uma janela de comando no sistema de destino. A menos que você especifique nomes de caminho completos, execute estes comandos do diretório local onde o binário reside. Os locais binários do caminho são especificados com cada comando.

Nota: O diretório de instalação do agente padrão para o Symantec Management Agent é `/opt/altiris/notification/nsagent`. Você pode modificá-lo no Console de gerenciamento Symantec, em **Configurações > Configurações da instalação > Configurações do agente**.

Consulte [“Para instalar o Symantec Management Agent para UNIX, Linux e Mac com instalação por envio manual”](#) na página 260.

Tabela B-2 Comandos do Symantec Management Agent

Finalidade	Comando de <code>/opt/altiris/notification/nsagent/bin</code>
Force uma atualização da política.	<code>aex-refreshpolicies</code>
Envie o inventário básico.	<code>aex-sendbasicinv</code>
Visualize tarefas disponíveis do pacote de software com a opção de executá-las manualmente.	<code>aex-swdapm</code>
Desinstale manualmente o agente.	<code>aex-uninstall</code>
Reinicie o agente.	<code>aex-helper agent restart</code>

O Client Task Agent pode exibir informações sobre todas as tarefas que forem atribuídas ao cliente UNIX/Linux. A seguinte tabela lista comandos úteis para o Client Task Agent.

Tabela B-3 Comandos do Client Task Agent

Finalidade	Execute este comando através de /opt/altiris/notification/ctagent/bin
Acessar a ajuda em um comando.	<code>aex-cta help</code>
Listar tarefas atuais e suas instâncias de execução.	<code>aex-cta list</code>
Listar as tarefas que são executadas no cliente e em seu GUIDs.	<code>aex-cta list --show-task-id</code>
Listar tarefas pendentes.	<code>aex-cta pending</code>
Atualizar configuração do agente.	<code>aex-cta refresh</code>
Forçar novo registro com o Task Server.	<code>aex-cta register</code>
Obter informações sobre o servidor de tarefas atualmente registrado.	<code>aex-cta ts</code>
Verificar se o agente está em execução.	<code>aex-helper check</code>
Recuperar uma lista das políticas de entrega gerenciada que são executadas.	<code>aex-cta list</code>
Recuperar uma lista das políticas da entrega gerenciada e das tarefas de entrega rápida que são executadas no cliente.	<code>aex-cta list --show-all-tasks</code>
Listar tarefas de instalação do plug-in.	<code>aex-smf list</code>

Finalidade	Execute este comando através de <code>/opt/altiris/notification/ctagent/bin</code>
Permitir o adiamento da execução da tarefa no cliente de acordo com as configurações da tarefa.	<code>aex-swd-defer</code>

Tabela B-4 Comandos de gerenciamento de software

Finalidade	Execute este comando através de <code>/opt/altiris/notification/smfagent/bin</code>
Exibir tarefas de gerenciamento de software e seu status.	<code>aex-smf list</code>

A seguinte tabela lista comandos `aex-helper`. O `aex-helper` é um utilitário do cliente para ajudar a solucionar problemas e acelerar as tarefas do administrador.

A sintaxe do utilitário é `aex-helper [command options]`

Tabela B-5 Comandos `Aex-helper`

Finalidade	Comando de <code>/opt/altiris/notification/nsagent/bin</code>
Registrar dependências entre soluções.	<code>adddep</code>
Executar várias tarefas com o agente UNIX.	<code>agent</code>
Mudar propriedades de serviços registrados de RC.	<code>changerc</code>
Verifique se o Symantec Management Agent para UNIX, Linux e Mac está em execução.	<code>check</code>
Limpar itens do registro de XML.	<code>clean</code>
Exibir ajuda no comando especificado.	<code>help</code>
Consultar o agente para várias informações.	<code>info</code>
Instalar e registrar scripts de RC.	<code>installrc</code>
Trabalhar com a estrutura do IPC do agente.	<code>ipc</code>
Criar scripts e links do wrapper para bibliotecas e executáveis.	<code>link</code>

Finalidade	Comando de <code>/opt/altiris/notification/nsagent/bin</code>
Listar objetos no registro do agente.	<code>list</code>
Consultar o agente para várias informações.	<code>query</code>
Iniciar, parar e listar serviços registrados de RC.	<code>rc</code>
Adicionar um objeto ao registro do agente.	<code>register</code>
Desinstalar soluções.	<code>uninstall</code>
Desinstalar scripts de RC.	<code>uninstallrc</code>
Remover scripts e links do wrapper para bibliotecas e executáveis.	<code>unlink</code>
Remover os objetos do registro do agente.	<code>unregister</code>
Fazer upgrade do plug-in do Symantec Management Agent	<code>upgrade</code>

Você pode também usar um arquivo de log do cliente para ajudar a solucionar problemas. Para solucionar problemas usando este arquivo de log, use os comandos na seguinte tabela.

Tabela B-6 Comandos do arquivo de log

Finalidade	Comando de <code>/opt/altiris/notification/nsagent/var</code>
Elevar o nível de registro em log para estado de depuração.	<code>aex-helper agent -s Configuration debug_level debug</code>
Desativar o limite de tamanho do log.	<code>aex-helper agent -s Configuration debug_file_size 0</code>
Retornar parâmetros ao padrão.	<code>aex-helper agent -s Configuration debug_level error</code> <code>aex-helper agent -s Configuration debug_file_size 1024</code>

Tópicos de referência do gerenciamento habilitado para nuvem

Este Apêndice contém os tópicos a seguir:

- [Ferramentas de linha de comando do Notification Server](#)
- [Configurações suportadas para servidores de pacotes em um ambiente misto](#)
- [Efeitos do gerenciamento habilitado para nuvem na funcionalidade do servidor de sites](#)
- [Scripts de gerenciamento de gateway da Internet](#)
- [Sobre o balanceamento de carga do gateway da Internet](#)
- [Parâmetros do pacote de instalação do agente habilitado para nuvem](#)
- [Parâmetros da linha de comando para a configuração de agente habilitado para nuvem](#)

Ferramentas de linha de comando do Notification Server

A seguinte tabela descreve as ferramentas de linha de comando disponíveis para você usar no Notification Server. Você pode usar estas ferramentas para manter seu ambiente de gerenciamento habilitado para nuvem.

Tabela C-1 Ferramentas de linha de comando do Notification Server

Nome executável	Descrição
AeXGenClientCert.exe	A ferramenta de geração de certificados do cliente permite criar os certificados do cliente de que você precisa. O certificado de autoridade de certificação (CA) do agente do Notification Server emite estes certificados. Consulte “Para gerar um certificado temporário do cliente” na página 330.
AeXGenSiteServerCert.exe	A ferramenta de geração de certificados do servidor permite criar os certificados do servidor de que você precisa. O certificado da CA do Notification Server emite estes certificados. Nota: Aplicar um certificado de servidor regenerado a um gateway da Internet afeta Symantec Management Agents existentes. Os agentes existentes não poderão se conectar ao gateway da Internet até que recebam detalhes atualizados da impressão digital do certificado do gateway. Consulte “Para gerar e aplicar o certificado de servidor de sites para acesso do agente habilitado para nuvem” na página 296.
AeXRevokeCertificate.exe	A ferramenta de revogação do certificado. Esta ferramenta permite revogar um certificado atualizando a lista de revogação do certificado (CRL). Consulte “Para revogar um certificado do gerenciamento habilitado para nuvem” na página 333.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Configurações suportadas para servidores de pacotes em um ambiente misto

O IT Management Suite suporta um ambiente misto onde alguns servidores de sites são internos e alguns são servidores de sites da internet. Em um ambiente misto, o Symantec Management Agent tenta primeiramente usar os servidores de pacotes internos. Se nenhum servidor de pacotes local estiver disponível, o agente será revertido para usar os servidores de pacotes de Internet que estão atrás de um gateway.

Tabela C-2 Configurações suportadas para servidores de pacotes em um ambiente misto

Configuração	Descrição
Defina alguns servidores de pacotes da Internet para cada site habilitado para nuvem.	Os servidores de pacotes da Internet devem publicar suas bases de código no formato HTTPS. Para esta configuração específica de site, é possível marcar todos os servidores de pacotes da Internet dentro do site como restritos. Esta configuração garante que os servidores de pacotes da Internet façam o download dos pacotes apenas de servidores de pacotes específicos da rede interna dentro de seu próprio site. Se um servidor de pacotes da Internet dentro do site fizer o download de um pacote pela Internet, o pacote ficará disponível a outros servidores de pacotes da Internet dentro desse site. Então os outros servidores de pacotes podem fazer o download do pacote do servidor de pacotes que está na mesma sub-rede, em vez de fazer o download do pacote através da Internet. Se nenhum servidor de pacotes interno for atribuído ao site, pelo menos um servidor de pacotes da Internet deverá estar disponível dentro do site. Esta configuração garante que pelo menos um servidor de pacotes possa obter os pacotes fora de seu site para a distribuição dentro de seu próprio site. Consulte “Para configurar um servidor de pacotes para publicar bases de código de pacotes HTTPS” na página 302.
Configure o Notification Server de modo a exigir SSL.	Esta configuração faz o Notification Server publicar bases de código HTTPS, o que permite aos agentes habilitados para nuvem e aos servidores de pacotes fazer o download dos pacotes do Notification Server. Porém, isso significa que todos os clientes (diretamente gerenciados) internos teriam também que se comunicar com o Notification Server usando HTTPS, o que pode não ser desejável. Consulte “Para configurar o Notification Server para usar o HTTPS” na página 290. Nota: O Notification Server não pode publicar bases de código HTTP e HTTPS ao mesmo tempo.

Efeitos do gerenciamento habilitado para nuvem na funcionalidade do servidor de sites

O gerenciamento habilitado para nuvem tem os seguintes efeitos na funcionalidade do servidor de pacotes e do servidor de tarefas:

Tabela C-3 Efeitos do gerenciamento habilitado para nuvem na funcionalidade do servidor de sites

Efeito	Descrição
Os servidores de pacotes na rede interna fornecem pacotes aos agentes e servidores de pacotes habilitados para nuvem usando apenas HTTPS.	Porém, os servidores de pacotes da rede interna ainda podem fazer o download de pacotes para os clientes da rede interna que usam UNC ou HTTP. De maneira semelhante, os servidores de pacotes desconectados no site local podem fornecer pacotes aos clientes habilitados para nuvem no mesmo site local usando qualquer protocolo.
O processo de seleção do servidor em servidores de pacotes e agentes habilitados para nuvem é diferente.	O processo de seleção de servidor em servidores de pacotes e agentes habilitados para nuvem é o seguinte: As fontes do servidor de pacotes que estão disponíveis para servidores de pacotes e agentes habilitados para nuvem tipicamente incluem servidores de pacotes locais e da rede interna. Por padrão, o agente escolhe na lista de servidores de pacotes locais. O agente usa os servidores de pacotes da rede interna apenas nos seguintes cenários: Todos os servidores de pacotes locais têm perfil de velocidade em 0 ou mais de sete erros serão gravados.
Atividades adicionais serão necessárias quando você excluir um servidor de pacotes.	Se você excluir um servidor de pacotes de um computador adicionado ao gateway da Internet, você deverá, por razões de segurança, excluir também o servidor de pacotes do gateway da Internet.
Um servidor de tarefas remoto não pode ser instalado em um computador-cliente com uma política de Configurações do gerenciamento habilitado para nuvem já aplicada a ele.	Contudo, a política de Configurações do gerenciamento habilitado para nuvem poderá ser aplicada ao computador-cliente depois que o servidor de tarefas estiver instalado.
Os servidores de tarefas não podem fornecer notificações ou entrega da tarefa em tempo real.	A pesquisa periódica é o modo suportado para executar tarefas em clientes habilitados para nuvem. Por padrão, o Symantec Management Agent procura tarefas a cada 30 minutos. Você deve mudar este período para agentes habilitados para nuvem modificando a configuração de Atualização da tarefa na política de Configurações do Task Agent . Você encontra esta página de política no Console de gerenciamento Symantec, em Configurações > Notification Server > Configurações de tarefas . Consulte "Alteração das configurações do Client Task Agent" na página 431.
O teste de velocidade para servidores da tarefa é substituído com a classificação aleatória.	O Client Task Agent escolhe aleatoriamente a lista de servidores de tarefas nas situações em que o ordenamento baseado em teste de velocidade seria usado. Observe que o agente apenas vai ignorar o teste de velocidade quando ele estiver no modo habilitado para nuvem.

Efeito	Descrição
Por padrão, os servidores de tarefas funcionam com agentes habilitados para nuvem e locais.	Os servidores de tarefas atribuídos a sites da Internet funcionam com os agentes localizados na intranet e com aqueles que são habilitado para nuvem. Para forçar os agentes habilitados para nuvem a comunicar-se com o servidor de tarefas selecionado, atribua manualmente aqueles agentes a um servidor de tarefas específico. Consulte “Para gerenciar agentes atribuídos manualmente” na página 134.

Scripts de gerenciamento de gateway da Internet

Para ajudar a gerenciar e manter seus gateways da Internet, vários scripts estão disponíveis no diretório de instalação do gateway da Internet do Symantec Management Platform.

Tabela C-4 Scripts de gerenciamento do gateway da Internet

Local e nome do script	Descrição
Apache\bin\GenerateCert.cmd	Gera novamente o certificado de servidor.
Apache\certs\client\UpdateCertHashes.cmd	Aplica um certificado de autoridade de certificação (CA) do Notification Server ao gateway da Internet.
Apache\certs\crl\UpdateCrlHashes.cmd	Aplica uma lista de revogação de certificados (CRL) ao gateway da Internet. Consulte “Para revogar um certificado do gerenciamento habilitado para nuvem” na página 333.
Apache\bin\StartService.cmd	Inicia o serviço de gateway da Internet.
Apache\bin\StopService.cmd	Interrompe o serviço de gateway da Internet.
Apache\bin\InstallService.cmd	Registra (ou registra novamente) o serviço de gateway da Internet nos Serviços do Windows.
Apache\bin\UninstallService.cmd	Cancela o registro do serviço de gateway da Internet dos Serviços do Windows.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem”](#) na página 328.

Sobre o balanceamento de carga do gateway da Internet

O gateway da Internet pode aceitar 3.000 conexões simultâneas e suportar de 1 a 60.000 endpoints. O número máximo de clientes que um gateway da Internet pode servir depende de seu ambiente. Por exemplo, uma política e intervalos mais curtos de solicitação da tarefa significam que o gateway recebe mais solicitações. Um número mais alto de solicitações reduz o número de clientes que o gateway pode suportar. Outra variável é o período de conexão que os agentes exigem. Na maioria dos casos, o agente se conecta apenas por um breve período. Porém, quando o agente fizer o download de pacotes ou gerar relatórios do inventário, uma conexão poderá durar um período muito mais longo.

No Symantec Management Platform, os gateways da Internet com problemas de conexão não são marcados como inválidos e não são ignorados. Em cada transferência, o Symantec Management Agent tenta todos os gateways de sua lista até que encontre um que funcione. Dependendo da natureza dos problemas que causam falhas do gateway, será possível que um gateway específico fique sobrecarregado. O sistema equilibra-se eventualmente corretamente sem nenhuma intervenção manual.

Os gateways da Internet não suportam nenhum balanceamento de carga manualmente configurável. Todo balanceamento de carga é feito automaticamente.

Um agente habilitado para nuvem executa o balanceamento de carga da seguinte forma:

- O Symantec Management Agent seleciona aleatoriamente um gateway da Internet na lista de gateways disponíveis especificados na política de **Configurações do gerenciamento habilitado para nuvem**. O agente usará o gateway selecionado até que a conexão falhe.
A seleção é sempre aleatória. Todos os gateways são considerados iguais e você não pode atribuir uma preferência ou uma ponderação a nenhum gateway específico.
- Quando o agente falhar ao se conectar através de seu gateway preferido, ele selecionará aleatoriamente outro gateway da lista. O agente usa esse gateway em todas as conexões até que ele também falhe.
- Periodicamente, duas vezes no intervalo da geração de relatórios do inventário básico, o agente redefine sua seleção aleatoriamente selecionando um gateway da lista de gateways disponíveis.

Este processo garante que se um gateway novo for adicionado ao sistema, logo haverá a redistribuição da carga de conexão automaticamente. A mesma

redistribuição automática ocorrerá se um gateway tiver um problema temporário e ficar off-line.

Consulte [“Para configurar o gerenciamento habilitado para nuvem”](#) na página 307.

Consulte [“Sobre a preparação do computador gateway da Internet”](#) na página 313.

Parâmetros do pacote de instalação do agente habilitado para nuvem

Você pode gerar um pacote de instalação do Symantec Management Agent pelo Console de gerenciamento Symantec. Você precisa gerar o pacote na instância do Symantec Management Platform que gerencia o agente instalado. O pacote de instalação gerado contém o instalador do Symantec Management Agent para a plataforma apropriada. O pacote contém também os certificados de que o cliente precisa para confiar no Notification Server.

Quando gerar um pacote de instalação do agente, você precisará especificar os parâmetros apropriados do pacote.

Tabela C-5 Parâmetros do pacote de instalação do Symantec Management Agent

Parâmetro	Descrição
Sistema operacional	O sistema operacional no computador-cliente. Nota: Apenas os clientes do Microsoft Windows são suportados no Symantec Management Platform 7.5.
Política	A lista suspensa contém todas as políticas de gerenciamento habilitado para nuvem que estão ativadas atualmente. Você precisa selecionar a política de Configurações do gerenciamento habilitado para nuvem que se aplica a este agente habilitado para nuvem. A política selecionada especifica os gateways da Internet disponíveis que o agente instalado pode usar. A lista de gateways disponíveis é incluída com o pacote de instalação do Symantec Management Agent. Consulte “Para configurar a política de Configurações do gerenciamento habilitado para nuvem” na página 320.

Parâmetro	Descrição
Grupo organizacional	O grupo organizacional ao qual o computador habilitado para nuvem pertence. Esta configuração é opcional. Se você selecionar um grupo organizacional, o agente recém-instalado será atribuído automaticamente ao grupo organizacional especificado quando o computador estiver sob gerenciamento. Você precisa usar um grupo organizacional criado por você. Não escolha nenhum dos grupos organizacionais padrão. Estes grupos são baseados em tipos de recursos e não são apropriados para computadores habilitados para nuvem. Por exemplo, um provedor de serviços gerenciado (MSP) pode ter vários clientes diferentes e gerenciar cada um usando um grupo organizacional específico por cliente. Esta configuração permite que cada computador recém-instalado seja atribuído automaticamente ao grupo organizacional apropriado.
Nome da instalação	Um nome simples para o pacote de instalação. Este nome é mostrado na linha de assunto do certificado do Symantec Management Agent que é anexado ao instalador. Este nome pode ser usado para diagnósticos e geração de relatórios. Para uma única instalação de computador, é possível usar o nome do computador ou do usuário primário. Para um pacote que seja instalado em vários computadores, é possível usar o identificador apropriado para o escritório ou o departamento.
Expiração	A data e a hora em que o pacote de instalação expira. O padrão é sete dias após a hora de criação. Você deve especificar uma data que seja pelo menos um dia após a data atual (de criação).
Automatizar distribuição de certificados	Define se o certificado permanente de um agente será emitido automaticamente. Se não for, então um administrador terá de gerenciar a distribuição do certificado e precisará autorizar cada solicitação da seção de relatórios do Notification Server.
Limite de registros de agentes	Define quantas vezes um certificado permanente pode ser emitido. O certificado é emitido com base no número de solicitações enviadas usando um certificado temporário ou do local.
Assinar usando	Você também tem a opção de adicionar uma assinatura ao pacote de instalação. Você pode escolher entre a assinatura com senha ou com impressão digital.

Parâmetros da linha de comando para a configuração de agente habilitado para nuvem

Você pode usar parâmetros da linha de comando para configurar o Symantec Management Agent para o gerenciamento habilitado para nuvem.

Nota: Depois de usar parâmetros da linha de comando, reinicie o Symantec Management Agent para que estas configurações tenham efeito.

Tabela C-6 Parâmetros da linha de comando de AeXNSAgent.exe

Parâmetro da linha de comando	Descrição
/gw=gatewayName,port,thumbprint	Especifica um gateway da Internet que o Symantec Management Agent pode usar. Consulte “Para forçar o Symantec Management Agent a usar um gateway da Internet especificado” na página 336.
/importcert=certificateFile.pfx	Adiciona um certificado especificado à configuração do Symantec Management Agent. Este comando coloca o certificado no armazenamento de certificados do serviço do Symantec Management Agent. Ele adiciona também a impressão digital do certificado ao registro. Consulte “Para instalar um certificado temporário em um computador gerenciado” na página 332.
/removecert	Remove o certificado atual da configuração do Symantec Management Agent. Este comando remove o certificado do agente do armazenamento de certificados do serviço do Symantec Management Agent. Remove também a impressão digital do certificado do registro. Consulte “Para instalar um certificado temporário em um computador gerenciado” na página 332.
/rootca=certificateFile.cer	Adiciona um certificado da autoridade de certificação raiz (CA). Este comando insere o certificado especificado no armazenamento de certificados de Autoridades de certificação raiz confiáveis. Consulte “Para aplicar uma autoridade de certificação raiz a um computador gerenciado” na página 292.
/cem=on	Ativa o gerenciamento habilitado para nuvem no Symantec Management Agent ativando a comunicação segura.
/cem=off	Desativa o gerenciamento habilitado para nuvem no Symantec Management Agent desativando a comunicação segura.
/clearcem	Limpa todas as configurações do gerenciamento habilitado para nuvem da configuração do Symantec Management Agent.

Consulte [“Solução de problemas e tarefas de manutenção do gerenciamento habilitado para nuvem ”](#) na página 328.

Configurações do relatório personalizado

Este Apêndice contém os tópicos a seguir:

- [Página de edição de relatório personalizado](#)
- [Página de edição do relatório personalizado: guia Fonte de dados](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Campos](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta parametrizada](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Capturas de imagem de dados](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida](#)
- [Página de edição do relatório personalizado: guia Fonte de dados : guia Resultados](#)
- [Página de edição do relatório personalizado: guia Exibições para uma exibição de gráfico](#)
- [Página de edição do relatório personalizado: guia Exibições para uma exibição em grade](#)

- [Caixa de diálogo Editar os campos fonte](#)
- [Caixa de diálogo Editar parâmetro](#)

Página de edição de relatório personalizado

A página **Edição de relatório personalizado** permite definir e editar os componentes e as propriedades do relatório personalizado do Notification Server que você criou ou modificou.

Consulte [“Componentes de um relatório personalizado do Notification Server”](#) na página 450.

Consulte [“Para criar e modificar relatórios personalizados do Notification Server”](#) na página 452.

Tabela D-1 Guias na página Edição de relatório personalizado

Guia	Descrição
Fonte de dados	Permite definir a consulta de relatório. Você mesmo pode escrever a consulta SQL ou usar o Criador de consulta para criar a consulta de relatório. Consulte “Para definir uma consulta de recursos para um relatório personalizado” na página 457. Consulte “Para definir uma consulta SQL para um relatório personalizado” na página 459. Consulte “Página de edição do relatório personalizado: guia Fonte de dados ” na página 528.
Exibições	Permite definir exibições de relatório. Uma exibição de relatório é a maneira específica como os resultados do relatório são exibidos. Consulte “Para criar ou modificar uma exibição em gráfico para um relatório personalizado” na página 462. Consulte “Para criar ou modificar uma exibição em grade para um relatório personalizado” na página 464. Consulte “Página de edição do relatório personalizado: guia Exibições para uma exibição de gráfico” na página 540. Consulte “Página de edição do relatório personalizado: guia Exibições para uma exibição em grade” na página 543.

Guia	Descrição
Parâmetros do relatório	Permite definir parâmetros de relatório e provedores de valor. Consulte “Para definir provedores de valores e parâmetros para um relatório personalizado” na página 460.
Detalhes	Permite configurar as ações de busca detalhada de um relatório. Consulte “Para configurar ações de busca detalhada para um relatório personalizado” na página 465.
Avançado	Permite especificar as propriedades de um relatório. Consulte “Para especificar as propriedades de um relatório personalizado” na página 468.

Página de edição do relatório personalizado: guia Fonte de dados

A guia **Fonte de dados** permite especificar os detalhes da consulta para um relatório personalizado do Notification Server que você cria ou modifica. A exibição da guia **Fonte de dados** depende do tipo de consulta de relatório que você define e pode conter as seguintes guias:

Para uma consulta de recursos Consulte [Tabela D-2](#)

Para uma consulta SQL Consulte [Tabela D-3](#)

Consulte [“Página de edição de relatório personalizado”](#) na página 527.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Se você estiver editando uma consulta de recursos, a guia **Fonte de dados** contém o botão **Converter esta consulta em uma consulta SQL**, que permite converter uma consulta de recursos em uma consulta SQL equivalente. Quando você converter uma consulta de recursos em uma consulta SQL, a exibição na guia **Fonte de dados** mudará automaticamente.

Tabela D-2 Guias em **Fonte de dados** para uma consulta de recursos

Guia	Descrição
Consulta	Permite criar uma consulta de recursos e definir a sintaxe da consulta de recursos. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta” na página 530.
Campos	Permite definir campos de origem para usar na consulta. Você pode selecionar a tabela de banco de dados (Origem) e coluna (Campo) que você deseja extrair do CMDB. Você pode especificar se cada campo de origem será mostrado nos resultados do relatório. Também é possível definir a ordem da coluna do campo de origem e enfileirar o agrupamento na grade dos resultados do relatório. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Campos” na página 533.
Parâmetros da consulta	Permite especificar os parâmetros que são usados na consulta. Estes são parâmetros internos para o uso do SQL. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta” na página 535.
Expressões do filtro	Permite configurar as instruções condicionais que são usadas para refinar mais os resultados da consulta. Cada instrução ou instrução agrupada pode ser considerada um filtro. Você precisa criar as instruções que deseja usar e agrupá-las de maneira apropriada. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro” na página 536.
Consulta resolvida	Permite exibir o código do SQL que é executado no CMDB para extrair os resultados do relatório. Este código inclui os valores padrão do teste para todos os parâmetros que o usuário especificar. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida” na página 538.
Resultados	Permite exibir os resultados da consulta. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Resultados” na página 539.

Tabela D-3 Guias em **Fonte de dados** para uma consulta SQL

Guia	Descrição
Consulta com parâmetros	Permite gravar o código SQL para a consulta. Este código pode incluir alguns parâmetros que usam valores especificados pelo usuário quando a consulta é executada no CMDB. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta parametrizada ” na página 534.
Parâmetros da consulta	Permite especificar os parâmetros que são usados na consulta. Estes são parâmetros internos para o uso do SQL. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta ” na página 535.
Capturas de imagem dos dados	Especifica os campos de GUID do escopo que são usados para o escopo dos dados carregados de uma captura de imagem de relatório. Os dados são exibidos como resultados do relatório e recebem escopo de acordo com as permissões de segurança do usuário. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Capturas de imagem de dados ” na página 536.
Consulta resolvida	Permite exibir o código do SQL que é executado no CMDB para extrair os resultados do relatório. Este código inclui os valores padrão do teste para todos os parâmetros que o usuário definir. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida ” na página 538.
Resultados	Permite exibir os resultados da consulta. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Resultados ” na página 539.

Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta

Quando você definir uma consulta de recursos para um relatório ou filtro personalizado, você precisará criar uma consulta de recursos na guia **Consulta**.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Para definir uma consulta de recursos para um filtro”](#) na página 359.

A guia **Consulta** permite criar uma consulta de recursos. O modelo padrão inclui uma consulta básica que seleciona todos os recursos. Você pode usar o Criador de consulta para refinar a consulta básica usando os blocos de construção fornecidos. Você não precisa entender ou gravar nenhum código SQL.

O painel esquerdo do Criador de consulta mostra a estrutura da consulta. O painel direito permite adicionar e modificar itens na estrutura da consulta. O Criador de consulta permite criar a consulta com base na estrutura de recursos (as classes, os tipos e as associações dos recursos) definida no CMDB. A consulta de recursos é convertida em código SQL em segundo plano. Você pode exibir o código SQL na guia **Consulta resolvida**.

Tabela D-4 Opções na guia **Consulta**

Opção	Descrição
Tipo de recurso	Permite mudar o tipo de recurso básico. Se você criou o relatório como Relatório do computador ou Relatório do usuário, o tipo básico de recurso será definido automaticamente como Computador ou Usuário .
Alias	O alias do tipo de recurso. O alias permite substituir um nome diferente pelo nome da tabela. Por exemplo, quando a mesma tabela é usada várias vezes em uniões.
Escopo determinado	Especifica se os resultados da consulta têm o escopo definido de acordo com a função do usuário que executa a consulta.
Usar campos e atributos da classe de dados	Permite adicionar campos à consulta. Você pode selecionar campos da classe de dados (como Resource.Name ou Resource.CreatedDate). Como alternativa, é possível selecionar campos de outras tabelas (por exemplo, o campo Domínio da tabela de Inv_AeX_AC_Identification). A guia Campos mostra os campos que estão definidos no conjunto de resultados da consulta e permite configurar a aparência na grade de resultados. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Campos” na página 533.

Opção	Descrição
Usar associações de tipo de recursos	Permite adicionar associações de recursos à consulta. Estas são associações predefinidas entre dois tipos de recursos do Notification Server (tal como a associação do usuário do computador que vincula um computador a um usuário). Você pode exibir a lista de associações disponíveis do tipo de recurso predefinido na pasta Configurações no painel esquerdo. Por exemplo, clique em Configurações > Notification Server > Configurações de classe de dados e recursos > Associações de recursos.
Criar uniões	Permite adicionar uniões à consulta. Uma união combina registros de duas tabelas diferentes do CMDB. A lista suspensa Uniões permite selecionar o tipo de união: ■ Cruzado Retorna o produto cartesiano dos conjuntos de registros das duas tabelas combinadas. ■ Externa completa Combina os resultados das uniões externas esquerda e direita. A tabela combinada contém todos os registros de ambas as tabelas e preenche valores NULOS para todas as correspondências ausentes de cada lado. ■ Interna Exige que cada registro nas duas tabelas combinadas tenha um registro correspondente. ■ Externa esquerda Uma união entre duas tabelas (A e B) de forma que a tabela combinada contenha sempre todos os registros da tabela "esquerda" (A), mesmo se a condição para união não encontrar um registro correspondente na tabela "direita" (B). ■ Externa direita O contrário da união externa esquerda. Cada registro da tabela "direita" (B) aparece na tabela combinada pelo menos uma vez. A lista suspensa seguinte permite selecionar a tabela de banco de dados que você quer usar. A lista suspensa Em permite selecionar a coluna que você quer unir.

Opção	Descrição
Incluir parâmetros	Abre a guia Parâmetros da consulta, que permite especificar os parâmetros que você deseja usar na consulta de recursos. Um parâmetro é uma variável incluída na consulta. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta” na página 535.
Adicionar expressões de filtro	Abre a guia Expressões do filtro. Consulte “Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro” na página 536.

Página de edição do relatório personalizado: guia Fonte de dados : guia Campos

Quando você definir uma consulta de recursos para um novo relatório personalizado, ou quando modificar uma consulta de recursos para um relatório personalizado existente, será possível especificar os campos de origem e os atributos de classe de dados que a consulta de recursos extrairá.

A guia **Campos** permite especificar os campos de origem e os atributos de classe de dados que a consulta de recursos extrairá. Campos são colunas de tabelas no CMDB (por exemplo, a coluna Domain da tabela **Inv_AeX_AC_Identification**). Classes de dados são classes de dados específicas do tipo de recurso que você selecionou (por exemplo, **Computer.Name**).

Você pode especificar se cada campo de origem será mostrado nos resultados do relatório. Também é possível definir a ordem da coluna do campo de origem e enfileirar o agrupamento na grade dos resultados do relatório.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Nota: Esta guia é usada para as consultas de relatório apenas. Não é relevante às consultas de filtros.

Consulte [“Caixa de diálogo Editar os campos fonte ”](#) na página 544.

Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta parametrizada

Quando você definir uma consulta SQL para um novo relatório ou filtro personalizado, será possível gravá-la para ser executada no CMD. Quando você modificar uma consulta SQL para um relatório ou filtro personalizado existente, será possível gravá-la para ser executada no CMD. A guia **Consulta parametrizada** permite salvar a consulta SQL que você deseja executar no CMD. Esta guia é basicamente uma caixa de texto de formato livre que permite gravar o código SQL ou colá-lo da Área de transferência. O painel Explorador de objetos permite selecionar campos de origem do CMD e inseri-lo na consulta. A inserção de campos de origem simplifica a gravação da consulta.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Você precisa do privilégio Editar SQL para criar ou modificar consultas SQL e ter boa compreensão sobre a estrutura da tabela do CMD. Se desejar aplicar o escopo aos resultados da consulta, você precisa incluir o código SQL apropriado na consulta.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Tabela D-5 Opções na guia **Consulta parametrizada**

Opção	Descrição
Caixa de texto	Permite digitar o texto da consulta SQL. Você pode digitar o SQL ou colá-lo da Área de transferência. Se quiser adicionar um campo de origem à sua consulta SQL, clique no código SQL no local onde você quer adicionar o objeto ou campo especificado e depois clique em Adicionar na linha Objeto ou Campo.
Objeto	Permite selecionar a tabela de banco de dados que você quer usar.
Campo	Permite selecionar a coluna da tabela que você quer usar.
Alias	Permite digitar os nomes de alias para a tabela de banco de dados e a coluna da tabela.

Página de edição do relatório personalizado: guia Fonte de dados : guia Parâmetros da consulta

Quando você definir uma consulta para um novo relatório ou filtro personalizado ou modificar uma consulta de um relatório ou filtro personalizado existente, poderá usar parâmetros da consulta. A guia **Parâmetros da consulta** permite especificar os parâmetros que você deseja usar na consulta do relatório ou do filtro. Um parâmetro é uma variável incluída na consulta. Os valores de parâmetro da consulta do filtro e do relatório podem ser definidos pelo sistema ou extraídos de outro relatório. Para consultas de relatório somente, um usuário pode definir os valores de parâmetro apropriados na página Relatório. Quando a consulta é executada, os valores de parâmetro especificados são usados no código SQL.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Consulte [“Para definir uma consulta de recursos para um filtro”](#) na página 359.

Consulte [“Para definir uma consulta SQL para um filtro”](#) na página 361.

O uso de parâmetros nas consultas permite criar uma consulta flexível. Você pode usar esse tipo de consulta para extrair resultados diferentes, inserindo os valores de parâmetro apropriados. Por exemplo, você pode criar uma consulta que inclua parâmetros para o tipo de sistema do computador e o nome do sistema operacional. Você pode executar esta consulta em qualquer combinação válida de tipo de sistema/nome do sistema operacional para extrair os resultados que você deseja. Como alternativa a usar parâmetros na consulta, é possível embutir em código os valores desses parâmetros. Assim, você modificaria a consulta cada vez que você desejasse usar uma combinação diferente de tipo de sistema/nome do sistema operacional. Você também pode criar várias consultas com uma combinação diferente de tipo de sistema/nome do sistema operacional definida em cada consulta.

Quando você cria um parâmetro na guia **Parâmetros da consulta**, a declaração apropriada do parâmetro é adicionada a uma consulta dos recursos automaticamente. Porém, se você gravar uma consulta SQL, precisará adicionar a declaração apropriada do parâmetro ao código da consulta manualmente.

Quando você inclui um parâmetro em uma consulta de relatório, você pode configurar o provedor de valor para o parâmetro. Você pode especificar o tipo de provedor de valor e os valores válidos para o parâmetro. Normalmente, o provedor de valor permite ao usuário definir o valor de parâmetro apropriado quando o relatório é executado. Você define o provedor de valor para um parâmetro na guia **Parâmetros do relatório**.

Consulte [“Para definir provedores de valores e parâmetros para um relatório personalizado”](#) na página 460.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Página de edição do relatório personalizado: guia Fonte de dados : guia Expressões do filtro

Quando você definir uma consulta para um novo relatório ou filtro personalizado, ou quando modificar uma consulta para um relatório ou filtro personalizado existente, será possível configurar expressões de filtro para refinar os resultados da consulta. A guia **Expressões do filtro** permite especificar regras para refinar os resultados da consulta. As regras são instruções condicionais que filtram os resultados brutos da consulta para selecionar os recursos que você deseja.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Página de edição do relatório personalizado: guia Fonte de dados : guia Capturas de imagem de dados

Esta informação é relevante às consultas de relatório apenas. A guia **Capturas de imagem de dados** não aparece nas consultas de filtros.

Você pode especificar os campos do escopo em uma consulta SQL para assegurar-se de que a captura de imagem do relatório feitas por você possam ter escopo correto quando outros usuários as acessarem. Os campos do escopo são os campos de GUID usados para o escopo dos dados que são extraídos de uma captura de imagem do relatório. Quando um usuário acessar uma captura de imagem do relatório, os dados serão carregados da captura de acordo com as permissões de segurança do usuário. Se não houver escopo de um campo, todos os itens relevantes serão carregados. Se um campo tiver escopo, apenas serão carregados os itens que possam ser lidos pelo usuário que exibir os dados.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Os campos do escopo que você configurar na guia **Capturas de imagem de dados** serão aplicados apenas para extração de dados das capturas de imagem de relatório. Eles não afetam a consulta SQL que extrai dados do CMDB para salvar

como capturas de imagem de relatório. Para o escopo de uma consulta SQL, você precisa incluir o código apropriado do SQL para extrair resultados de acordo com as permissões de segurança do usuário que executa a consulta

Nota: Se houver o escopo de uma consulta SQL, todas as capturas de imagem de relatório serão salvas com o escopo do usuário que executou a consulta. Se uma captura de imagem for projetada para ser compartilhada, certifique-se de que ela contenha todos os dados que podem ser relevantes a outros usuários. Você pode certificar-se de que tem todos os dados executando a consulta de relatório como um usuário que tenha o acesso aos recursos; por exemplo, um membro da função do administrador da Symantec. Você pode também usar Executar tarefa de relatório agendada para criar a captura de imagem apropriada: por padrão, a tarefa é executada no contexto do administrador; por isso, ela captura a imagem com um escopo global.

Por padrão, um relatório novo do SQL tem [_ItemGuid] configurado como um campo do escopo GUID. Este campo é usado para escopo dos resultados com uma união em uma função de escopo da seguinte forma:

```
INNER JOIN [fnGetTrusteeScopedResources] (@v1_TrusteeScope) AS [fnGTSR]
    ON ([vri2_Resource].[Guid] = [fnGTSR_3].[ResourceGuid])
```

Onde [vri2_Resource].[Guid] é o nome completo do campo com o alias [_ItemGuid].

Consulte “[Página de edição do relatório personalizado: guia Fonte de dados](#)” na página 528.

Tabela D-6 Opções na guia **Capturas de imagem de dados**

Opção	Descrição
Campos do escopo	Permite exibir todos os campos de GUID incluídos na consulta SQL. Você precisa especificar os campos de GUID usados para o escopo. Se você criar uma consulta SQL complexa que tenha várias uniões em recursos e vários aplicativos da função de escopo, será necessário adicionar todos os GUIDs de escopo apropriados à lista Campos de GUID do escopo.

Opção	Descrição
Consulta de capturas de imagem de dados	Permite exibir o código do SQL que é gerado quando a captura de imagem precisar ser salva ou carregada. Para salvar a consulta de relatório, verifique se o código SQL para carregamento dos dados da captura de imagem aplica corretamente o escopo aos resultados salvos. A consulta na caixa de texto será atualizada automaticamente sempre que você modificar os campos do escopo ou mudar a seleção na lista suspensa Modo da consulta de captura de imagem de dados. Se ela não for atualizada automaticamente, clique em Atualizar para atualizar o código do SQL exibido.
Modo da consulta de captura de imagem de dados	Permite selecionar o modo da consulta: ■ Criar tabela de dados de captura de imagem Exibe o código do SQL que cria a estrutura de tabela dos dados da captura de imagem. Esta estrutura não depende da configuração do escopo. ■ Salvar dados de captura de imagem Exibe o código do SQL que salva os dados de todos os campos na tabela de dados de captura de imagem. A configuração do escopo não afeta estes dados. ■ Carregar dados de captura de imagem Exibe o código do SQL que carrega os dados da tabela de dados de captura de imagem e determina o escopo de acordo com as permissões de segurança do usuário. O SQL usa os campos configurados do escopo e as participações de TrusteeScope do usuário para extrair os dados apropriados. Assim, estes dados são apresentados ao usuário como resultados do relatório. Os campos especificados de escopo fazem escopo desses dados.

Página de edição do relatório personalizado: guia Fonte de dados : guia Consulta resolvida

Você pode exibir a consulta resolvida de um relatório ou filtro personalizado que você criar ou modificar. A guia Consulta resolvida exibe o código SQL que é executado no CMDb. Todos os parâmetros especificados são definidos nos valores de teste apropriados.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Se exibir uma consulta de recursos, você poderá definir o modo de consulta da lista suspensa **Modo da consulta de recursos** :

Normal	Mostra a consulta resolvida padrão. A consulta resolvida padrão é gerada da consulta de recursos que você especificou no Criador de consulta, sem outras adições.
Criar tabela de dados de captura de imagem	Adiciona o código SQL à consulta que cria uma tabela de dados de captura de imagem para os resultados da consulta. A consulta modificada é mostrada.
Salvar dados da captura de imagem	Adiciona o código SQL à consulta que salva os resultados da consulta em uma tabela de dados de captura de imagem. A consulta modificada é mostrada.
Carregar dados da captura de imagem	Adiciona o código SQL à consulta que extrai os resultados da consulta de uma tabela de dados de captura de imagem em vez do CMDB. A consulta modificada é mostrada.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Página de edição do relatório personalizado: guia Fonte de dados : guia Resultados

Você pode exibir os resultados de uma consulta de relatório personalizado na guia **Resultados**. Quando você abre a guia Resultados, a consulta é executada automaticamente no CMDB e os resultados atuais são exibidos. Esse recurso permite verificar mudanças na consulta e testar configurações diferentes para os parâmetros da consulta.

Consulte [“Para definir uma consulta de recursos para um relatório personalizado”](#) na página 457.

Consulte [“Para definir uma consulta SQL para um relatório personalizado”](#) na página 459.

Consulte [“Página de edição do relatório personalizado: guia Fonte de dados ”](#) na página 528.

Página de edição do relatório personalizado: guia Exibições para uma exibição de gráfico

Na guia **Exibições** de uma exibição de gráfico, você pode especificar as configurações nas seguintes subguias:

Título	Permite especificar o texto do título do gráfico e o local em que ele aparece. Consulte Tabela D-7 na página 541.
Legenda	Permite especificar a legenda do título do gráfico e o local em que ela aparece. A legenda é o texto descritivo opcional mostrado no gráfico. Consulte Tabela D-8 na página 541.
3D	A configuração do zoom 3D permite ampliar áreas selecionadas do gráfico para o tamanho completo da janela. Por exemplo, talvez você queira detalhar um grande relatório que cubra um longo período de tempo: você pode exibir um curto período específico selecionando a parte relevante. Você pode definir cada eixo, ou ambos, como expansíveis. Consulte Tabela D-9 na página 541.
Eixo X	Permite escolher a coluna de resultados para usar como o eixo X no gráfico. A guia permite também especificar o texto do título e configurar a aparência do eixo X. Consulte Tabela D-10 na página 542.
Eixo Y	Permite escolher a coluna (ou colunas) de resultados para usar como o eixo Y no gráfico. A guia permite também especificar o texto do título e configurar a aparência do eixo Y. Para alguns tipos de gráfico, você pode reunir vários valores (várias colunas de resultados) no mesmo gráfico. Estes aparecem como várias linhas em um gráfico de linhas ou uma fileira de cores diferentes em uma barra, cada um codificado com cores e rotulados. Consulte Tabela D-11 na página 542.

Consulte [“Para criar ou modificar uma exibição em gráfico para um relatório personalizado”](#) na página 462.

Tabela D-7 Opções na guia **Título**

Opção	Descrição
Título	O título principal do gráfico. Se desejar criar um título de várias linhas, use caracteres ln para inserir as quebras de linha nos lugares apropriados. Nenhum padrão é definido; assim, o título padrão do gráfico é uma sequência de caracteres vazia.
Dica de ferramenta	O texto exibido na dica de ferramenta, que aparece quando o usuário passa o mouse sobre o título do gráfico. Nenhum padrão é definido.
Alinhado	Permite especificar o local e o alinhamento do texto relativo ao gráfico para o idioma do sistema (formato gravado).
Acoplamento	Permite especificar o local do título na página do gráfico.

Tabela D-8 Opções na guia **Legenda**

Opção	Descrição
Mostrar legenda	Selecione esta opção para mostrar a legenda.
Na área de plotagem	Selecione esta opção para mostrar a legenda dentro da área de plotagem. Se esta opção estiver desmarcada, a legenda aparece fora da área de plotagem.
Título	O texto da legenda. Nenhum padrão é definido; assim, a legenda padrão é uma sequência de caracteres vazia.
Estilo	Permite especificar o estilo da legenda.
Alinhado	Permite especificar o alinhamento do texto da legenda relativo ao gráfico.
Acoplamento	Permite especificar o local da legenda na página do gráfico.

Tabela D-9 Opções na guia **3D**

Opção	Descrição
Ativar 3D	Selecione esta opção para ativar o zoom 3D.
Zoom	Selecione estas opções para ativar o zoom nos eixos X e Y, respectivamente.

Opção	Descrição
Rotação	O ângulo da rotação sobre os eixos X e Y, respectivamente.

Tabela D-10 Opções na guia **Eixo X**

Opção	Descrição
Coluna principal	A coluna de dados para plotagem ao longo do eixo X. Selecione a opção apropriada na lista suspensa. As opções são as colunas de resultados especificadas no relatório.
Título	O texto do título do eixo X.
Visível	Selecione esta opção para exibir o eixo X.
Grades principais	Selecione esta opção para exibir as linhas de grade principais do eixo X.
Invertido	Selecione esta opção para processar o eixo X na ordem inversa.

Tabela D-11 Opções na guia **Eixo Y**

Opção	Descrição
Coluna principal	A coluna dos dados para plotagem no eixo Y. Selecione a opção apropriada na lista suspensa. As opções são as colunas de resultados especificadas no relatório.
Título	O texto do título do eixo Y.
Colunas empilhadas	As colunas da lista de que estão disponíveis para serem adicionadas ao gráfico. Selecione as colunas que você deseja adicionar. Esta opção aplica-se somente aos tipos de gráficos empilhados, como StackedColumn, StackedBar e StackedArea.
Visível	Selecione esta opção para exibir o eixo Y. Por padrão, esta opção está desativada; portanto, o eixo Y não é visível.
Grades principais	Selecione esta opção para exibir as linhas de grade principais do eixo Y. Por padrão, esta opção está desativada; portanto, as linhas de grade principais do eixo Y não são visíveis.

Opção	Descrição
Invertido	Selecione esta opção para processar o eixo Y na ordem inversa. Por padrão, esta opção está desativada.

Página de edição do relatório personalizado: guia Exibições para uma exibição em grade

A guia **Formatação avançada** permite configurar uma formatação avançada para a exibição em grade do relatório personalizado que você criar ou modificar.

O processo para configurar a formatação avançada inclui a criação de regras de formatação para as colunas de resultados apropriada. Para cada regra de formatação você precisa especificar a marcação HTML aplicada pela regra aos resultados. Se a regra de formatação é condicional em alguns valores de dados, você precisa especificar as condições apropriadas. Por exemplo, em um relatório do espaço em disco do computador, convém aplicar a regra de formatação apenas aos computadores que têm menos que o mínimo especificado de espaço livre restante. A regra seria condicional no valor de espaço livre, sendo inferior a uma quantidade especificada.

Consulte [“Para criar ou modificar uma exibição em grade para um relatório personalizado”](#) na página 464.

Tabela D-12 Opções na guia **Formatação avançada**

Opção	Descrição
Nome da regra	Permite especificar o nome da regra.
Tipo do formato	Permite especificar o tipo do formato do relatório.
Aplicado a	Permite especificar se a formatação HTML no modelo se aplica à linha inteira da grade ou apenas à coluna selecionada. Cada coluna de dados nos resultados do relatório é relacionada. Se os resultados do relatório incluem itens, a coluna ItemGUID também estará disponível. Esta coluna é ocultada em todas as exibições, mas é incluída nos resultados da consulta.

Opção	Descrição
Condicional	Você pode configurar instruções condicionais dentro das regras de formatação para fazer com que as regras sejam aplicadas somente a valores de dados específicos. Por exemplo, convém colocar em destaque na grade determinados valores de dados ou identificar todos os valores de dados ausentes. Se desejar definir as condições na regra de formatação, selecione Condicional. Em Condição, você pode definir condições para a regra de formatação: ■ Coluna Especifica a coluna à qual a condição se aplica. Cada coluna de dados nos resultados do relatório é relacionada. ■ Marcar Especifica o operador condicional. ■ Valor e Valor 2 Especifica o valor ou os valores que o operador usará para verificar a condição.
Formato	Permite configurar os campos apropriados do modelo da formatação: ■ Valor de origem Especifica a origem dos dados exibidos na célula formatada. O padrão é Valor aplicado, que vem a ser os dados que já estão na célula. Porém, você pode substituir esse valor por qualquer outro dado da mesma linha, selecionando a coluna apropriada. Cada coluna de dados nos resultados do relatório é relacionada. ■ Tipo de origem Especifica o tipo de valor da origem que será exibido.

Caixa de diálogo Editar os campos fonte

A caixa de diálogo **Editar os campos de origem** permite modificar as configurações DE cada campo de origem incluído em sua consulta de recursos.

Consulte “[Página de edição do relatório personalizado: guia Fonte de dados : guia Campos](#)” na página 533.

Tabela D-13 Configurações na caixa de diálogo de **Editar campos de origem**

Configuração	Descrição
Alias	O alias do campo. Convém especificar o alias do campo para fazer o SQL bruto (exibido na guia Consulta resolvida) mais legível e mais fácil de entender.
Selecionar	Especifica se o campo é incluído nos resultados da consulta. Por padrão, todos os campos são selecionados.
Visível	Especifica se o campo será exibido nos resultados do relatório que aparecem para o usuário. Por padrão, todos os campos são exibidos. Você pode usar esta opção para ocultar campos específicos do usuário. Por exemplo, talvez seja interessante que a consulta extraia algumas informações, tal como o GUID de um computador, que não sejam significativas para o usuário, mas que são úteis para outras finalidades. Os dados ainda são extraídos como parte dos resultados da consulta, e as políticas de automação podem usá-los.
Ordem de colunas	Especifica a ordem da coluna na grade de resultados do relatório. As colunas são numeradas da esquerda para a direita.
Direção da classificação	Permite especificar o sentido de classificação na grade de resultados do relatório.
Ordem de classificação	Especifica a ordem de classificação desta coluna na grade de resultados do relatório. A ordem da classificação é usada com a direção especificada. Quando você especificar campos de origem para uma consulta de recursos em um relatório ou em um filtro, a ordem de classificação será ajustada quando você mudar o sentido de classificação. Se você mudar a ordem de classificação de um campo para a mesma de outro campo, o campo que você alterar será colocado na ordem especificada. Os outros campos serão reorganizados de maneira apropriada. Para remover a classificação, redefina a ordem de classificação para N/A. O sentido da classificação é redefinido automaticamente como padrão, e a ordem de classificação dos outros campos é ajustada para preencher todas as lacunas.

Configuração	Descrição
Agregado	Permite especificar como agregar os valores nesta coluna na grade dos resultados do relatório.
Ordem do grupo	Especifica a ordem de classificação das linhas agregadas.
Determinando escopo	Especifica se o campo estará ou não no escopo dos resultados da consulta. Por padrão, todos os campos não estão no escopo. Se o campo não estiver no escopo, a consulta extrairá todos os itens relevantes. Se o campo estiver no escopo, a consulta extrairá somente os itens que o usuário que executa a consulta tiver permissão de ler. Nota: Os resultados da consulta que o usuário visualiza como resultados de um relatório ou associação de filtro são colocados no escopo sempre de acordo com a sua função. O escopo será aplicado automaticamente quando os resultados da consulta forem apresentados ao usuário. Mudar a configuração aqui não afeta o que o usuário pode ver.

Caixa de diálogo Editar parâmetro

A caixa de diálogo **Editar parâmetro** permite especificar as configurações do parâmetro para cada parâmetro do relatório personalizado. Em **Parâmetro**, você pode especificar as configurações gerais do parâmetro. Em **Provedor de valor**, você pode especificar as configurações específicas ao tipo de fornecedor do valor que você selecionou.

Consulte [“Para definir provedores de valores e parâmetros para um relatório personalizado”](#) na página 460.

Tabela D-14 Opções na caixa de diálogo **Editar parâmetro**

Opção	Descrição
Nome	Permite especificar o nome do parâmetro.
Parâmetro obrigatório	Permite especificar se o parâmetro será obrigatório no relatório.
Descrição	Permite especificar a descrição do parâmetro. Esta descrição é usada para identificar o parâmetro na lista suspensa Adicionar novo parâmetro.

Opção	Descrição
Tipo	Permite selecionar o tipo de parâmetro.
Ordem de exibição/avaliação	Permite especificar a ordem em que o parâmetro é exibido na página Relatório e a ordem em que o parâmetro é avaliado na consulta do relatório. A lista suspensa permite definir o valor da ordem entre 1 e 19.
Valor padrão	Permite especificar o valor padrão do parâmetro. Se o usuário não especificar um valor para o parâmetro quando o relatório for gerado, este valor será usado na consulta.
Valor do teste	Permite especificar o valor de teste do parâmetro. Este valor será usado quando você testar a consulta.
Provedor de valor	Permite especificar o fornecedor do valor do parâmetro. As configurações do provedor de valor especificam o tipo de controle da interface do usuário que é apresentado ao usuário. Para cada controle da interface do usuário, você pode definir as configurações relevantes, como a extensão do controle da interface do usuário, o texto do rótulo e o texto da dica de ferramenta. Os tipos de provedor de valor disponíveis dependem do tipo de parâmetro que é selecionado.

Campos passíveis de script para modificar regras de CMDB e de importação e exportação de recursos

Este Apêndice contém os tópicos a seguir:

- [Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDB](#)

Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDB

Quando você trabalhar com regras de importação e exportação de recursos para importar recursos ou regras de CMDB, você mapeará ou definirá valores para as colunas do tipo de recurso especificado no CMDB. Usar uma expressão é uma das opções para definir valores da coluna. Uma expressão permite gravar alguns scripts .NET.

A criação das expressões é documentada nos seguintes tópicos:

- Consulte [“Sintaxe de expressão”](#) na página 549.
- Consulte [“Operadores de expressão”](#) na página 550.
- Consulte [“Valores definidos pelo usuário”](#) na página 550.
- Consulte [“Operadores de sequências de caracteres”](#) na página 550.
- Consulte [“Caracteres curinga”](#) na página 551.

- Consulte [“Tipos agregados”](#) na página 551.
- Consulte [“Funções de expressão”](#) na página 551.

Sintaxe de expressão

Ao criar uma expressão para modificar as regras de importação e exportação de recursos ou as regras de CMDDB, use a propriedade **Nome da coluna** para consultar colunas. Por exemplo, se o **Nome da coluna** para uma coluna for "PreçoUnitário" e o outro, "Quantidade", a expressão será "PreçoUnitário* Quantidade".

Quando você criar uma expressão para um filtro, coloque strings com aspas simples. Por exemplo:

```
'Sobrenome = 'Alves'.'
```

Se você usar os seguintes caracteres especiais em um nome de coluna, eles deverão ser delimitados:

\n (linha nova)	\	*	[	"
\t (guia)	/	%	]	#
\r (retorno do carro)	=	&	'	-
~	>		+	)
(	<	^		

Se um nome de coluna contiver um dos caracteres na tabela anterior, o nome deverá ser colocado entre colchetes. Por exemplo, para usar uma coluna nomeada "NúmerodaColuna" em uma expressão, será necessário digitar:

```
[NúmerodaColuna]". Exemplo: Total * [NúmerodaColuna]
```

Se você estiver digitando uma data, será necessário usar o formato mês/dia/ano. Os formatos dia/mês/ano ou ano/mês/dia são inválidos.

Como os colchetes são caracteres especiais, será necessário usar uma barra ("\") para delimitá-los, se fizerem parte de um nome de coluna. Por exemplo, uma coluna nomeada "Coluna []" seria digitada:

```
"Total * [Coluna[\]]"
```

Apenas o segundo colchete deverá ser delimitado.

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDDB”](#) na página 548.

Operadores de expressão

A concatenação é suportada dentro das expressões usando operadores booleanos E, OU e NÃO. Você pode usar parênteses para agrupar cláusulas e forçar prioridade. O operador E tem prioridade sobre outros operadores. Exemplo: (Sobrenome = 'Silveira' OU Sobrenome = 'Alves') E Nome = 'João'

Quando você criar expressões de comparação, os seguintes operadores serão permitidos:

<	>	<=	>=	<>
=	EM	COMO		

Quando você criar expressões de comparação aritméticas, os seguintes operadores serão permitidos:

+	-	*	/	%
(adição)	(subtração)	(multiplicação)	(divisão)	(módulo)

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDDB”](#) na página 548.

Valores definidos pelo usuário

Os valores definidos pelo usuário podem ser usados dentro das expressões a serem comparadas com valores da coluna. Os valores de sequência de caracteres devem ser colocados dentro de aspas simples. Os valores de Data devem ser colocados dentro de sinais de sustenido (#). Os decimais e a notação científica são permitidos para valores numéricos. Exemplos: "Nome = 'João'"; "Preço <= 50,00"; "Data de nascimento < #1/31/ 82#".

Para as colunas que contêm valores de enumeração, ajuste o valor para um tipo de dados de número inteiro. Exemplo: "ColunadeEnumeração = 5"

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDDB”](#) na página 548.

Operadores de sequências de caracteres

Para concatenar uma string em uma expressão, use o caractere +.

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDDB”](#) na página 548.

Caracteres curinga

Ambos * e % podem ser usados nas expressões alternadamente para caracteres curinga em uma comparação de LIKE. Se a sequência de caracteres em uma cláusula de LIKE contém * ou %, esses caracteres devem ser delimitados entre colchetes ([]). Se um colchete estiver na cláusula, os caracteres de colchete devem ser delimitados entre colchetes. Exemplo: [[] ou []]. Um caractere curinga é permitido no início, no fim, ao final de um padrão ou em ambos. Exemplos: "Nomedoltem LIKE '*produto*'", "Nomedoltem LIKE '*produto'", "Nomedoltem LIKE 'produto*'", "Nomedoltem LIKE 'produto'".

Os caracteres curinga não são permitidos no meio de uma sequência de caracteres. Por exemplo, 'te*xto' não é permitido.

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDb”](#) na página 548.

Tipos agregados

Você pode usar os seguintes tipos agregados nas expressões:

Sum (soma)	Avg (média)	Min (Mínimo)	Max (Máximo)
Count (Total)	StDev (Desvio padrão estatístico)	Var (Variação estatística)	

Crie uma expressão agregada usando uma das funções listadas acima. Por exemplo, use Sum (preço) para criar um resumo de números em uma coluna chamada "Preço". Não há a funcionalidade para o grupo; portanto, todas as linhas exibem o mesmo valor na coluna. Se uma tabela não tiver nenhuma linha, as funções agregadas retornarão uma referência nula.

Consulte [“Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDb”](#) na página 548.

Consulte [“Função de conversão”](#) na página 552.

Funções de expressão

Você pode escolher entre as seguintes funções da expressão:

- Convert
Consulte [“Função de conversão”](#) na página 552.
- Len
Consulte [“Função Len”](#) na página 552.
- IsNull
Consulte [“Função IsNull”](#) na página 553.

- IIF
Consulte “[Função IIF](#)” na página 553.
- Trim
Consulte “[Função Trim](#)” na página 554.
- Substring
Consulte “[Função de subsequência de caracteres](#)” na página 554.

Consulte “[Campos passíveis de script para modificar regras de importação e exportação de recursos e de CMDDB](#)” na página 548.

Função de conversão

Converte uma expressão a um tipo especificado de .NET Framework.

Sintaxe: `Convert(expression, type)`

Tabela E-1 Argumentos da função de conversão

Argumento	Descrição
expressão	Especifica a expressão para converter.
tipo	Especifica o tipo de .NET Framework a que o valor é convertido.

Exemplo: `myDataColumn.Expression="Convert(total, 'System.Int32')"`

Todas as conversões são válidas, com as seguintes exceções:

- Booleano pode ser forçado a e do byte, SByte, Int16, Int32, Int64, UInt16, UInt32, UInt64, sequência de caracteres e ele próprio apenas.
- O caractere pode ser forçado a e de Int32, UInt32, sequência de caracteres e ele próprio apenas.
- Data e hora podem ser forçados a e de sequência de caracteres e elas próprias apenas.
- O TimeSpan pode ser forçado a e de sequência de caracteres e ele próprio apenas.

Consulte “[Funções de expressão](#)” na página 551.

Função Len

Obtém o comprimento de uma sequência de caracteres.

Sintaxe: `Len(expression)`

Tabela E-2 Argumentos da função Len

Argumento	Descrição
expressão	Especifica a sequência de caracteres a ser avaliada.

Exemplo: `myDataColumn.Expression="Len (ItemName) "`

Consulte “[Funções de expressão](#)” na página 551.

Função IsNull

Verifica uma expressão e retorna a expressão verificada ou um valor de substituição.

Sintaxe: `IsNull (expression, replacementvalue)`

Tabela E-3 Argumentos da função IsNull

Argumento	Descrição
expressão	Define a expressão a verificar.
replacementvalue	Define o valor para retornar se a expressão for uma referência nula (nada).

Exemplo: `myDataColumn.Expression="IsNull (price, -1) "`

Consulte “[Funções de expressão](#)” na página 551.

Função IIF

Obtém um de dois valores dependendo do resultado de uma expressão lógica.

Sintaxe: `IIF (expressão, parte_verdadeira, parte_falsa)`

Tabela E-4 Argumentos da função IIF

Argumento	Descrição
expressão	Define a expressão para avaliar.
parte_verdadeira	Define o valor para retornar se a expressão for verdadeira.
parte_falsa	Define o valor para retornar se a expressão for falsa.

Exemplo: `myDataColumn.Expression = "IIF(total>1000, 'expensive', 'dear')`

Consulte “[Funções de expressão](#)” na página 551.

Função Trim

Remove todos os caracteres à direita ou à esquerda, como \r,\n,\t, ' '

Sintaxe: Trim (expressão)

Tabela E-5 Argumentos da função Trim

Argumento	Descrição
expressão	Define a expressão para adaptar.

Consulte “Funções de expressão” na página 551.

Função de subsequência de caracteres

Obtém uma subsequência de caracteres de um comprimento especificado, iniciando em um ponto especificado na sequência de caracteres.

Sintaxe: Subsequência de caracteres (expressão, início, comprimento)

Tabela E-6 Argumentos da função da subsequência de caracteres

Argumento	Descrição
expressão	Define a sequência de caracteres de origem para a subsequência de caracteres.
Início	Especifica um número inteiro que define onde a subsequência de caracteres inicia.
Comprimento	Especifica o número inteiro que define o comprimento da subsequência de caracteres.

Exemplo: myDataColumn.Expression = "Substring(phone, 7, 8) "

Você pode redefinir a propriedade Expressão atribuindo-lhe um valor nulo ou uma sequência de caracteres vazia. Se um valor padrão for definido na coluna Expressão, a todas as linhas previamente preenchidas será atribuído o valor padrão depois que a propriedade Expressão for redefinida.

Consulte “Funções de expressão” na página 551.

Avisos legais de terceiros no Symantec™ Management Platform 7.5

Este Apêndice contém os tópicos a seguir:

- [Third-Party Legal Notices](#)
- [7-Zip](#)
- [Apache HTTP Server](#)
- [Apache Xerces C++](#)
- [Boost](#)
- [Bouncy Castle](#)
- [Curl](#)
- [glibc](#)
- [Libatomics_Ops](#)
- [LibXML2](#)
- [Makeself](#)
- [Microsoft Anti-Cross Site Scripting Library](#)
- [OpenPegasus](#)
- [OpenSSL 0.9.8u](#)
- [OpenSSL 0.9.8y](#)

- [OpenSSL 1.0.1e](#)
- [plists-cs](#)
- [SQLite](#)
- [Windows Template Library 'WTL' v8.0](#)
- [Zlib](#)

Third-Party Legal Notices

This Symantec product may contain third party software for which Symantec is required to provide attribution ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The license agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. This appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

7-Zip

7-Zip v9.20 [2010-11-18] for Windows

Copyright (c) 1999-2010 Igor Pavlov

All copyrights to original unRAR code are owned by Alexander Roshal

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache HTTP Server

Apache HTTP Server v2.2.22

Portions of this program contain components from the Apache Software Foundation. These components are made available under the Apache License 2.0, a copy of which is provided herein.

Apache License, Version 2.0

January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or

contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Apache Xerces C++

Apache Xerces C++ v3.0

Copyright © 2012 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Apache License, Version 2.0

January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the

copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of

the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Boost

Boost v1.42.0

Copyright Joe Coder 2004 - 2006.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND

NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Bouncy Castle

Bouncy Castle v1.5

The Legion Of The Bouncy Castle

Copyright (c) 2000 - 2010 The Legion Of The Bouncy Castle
(<http://www.bouncycastle.org>)

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Curl

Curl v7.24.0

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>. All rights reserved
COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

glibc

glibc i686 rpm v2.12-1.7

Free Software Foundation, a wide variety of years

Copyright (C) 1991 Regents of the University of California.

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Copyright (C) 1984, Sun Microsystems, Inc.

Copyright (C) 1991, 1990, 1989 Carnegie Mellon University

Copyright (c) 2000, Intel Corporation copyright (C) by Craig Metz, no year specified

The code may be accessed at: <http://rhn.redhat.com>

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License,

applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure

that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place

satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.

(It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED

BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and an idea of what it does.> Copyright (C)
<year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

Libatomics_Ops

Hewlett-Packard Development Company, L.P., Xerox Corporation, Silicon Graphics & Hewlett-Packard Company.

Copyright (c) 2003-2004 Hewlett-Packard Development Company, L.P.

Copyright (c) 1991-1994 by Xerox Corporation. All rights reserved.

Copyright (c) 1996-1999 by Silicon Graphics. All rights reserved.

Copyright (c) 1999-2003 by Hewlett-Packard Company. All rights reserved.

Our intent is to make it easy to use libatomic_ops, in both free and proprietary software. Hence most code that we expect to be linked into a client application is covered by an MIT-style license.

A few library routines are covered by the GNU General Public License. These are put into a separate library, libatomic_ops_gpl.a .

A parte de baixo nível da biblioteca é coberta em sua maior parte pela seguinte licença:

Copyright (c) ...

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A few files in the sysdeps directory were inherited in part from the Boehm-Demers-Weiser conservative garbage collector, and are covered by its license, which is similar in spirit:

Copyright (c) ...

THIS MATERIAL IS PROVIDED AS IS, WITH ABSOLUTELY NO WARRANTY EXPRESSED OR IMPLIED. ANY USE IS AT YOUR OWN RISK.

Permission is hereby granted to use or copy this program for any purpose, provided the above notices are retained on all copies. Permission to modify the code and to

distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

A few files are covered by the GNU General Public License. (See file "COPYING".) This applies only to test code, sample applications, and the libatomic_ops_gpl portion of the library. Thus libatomic_ops_gpl should generally not be linked into proprietary code. (This distinction was motivated by patent considerations.)

It is possible that the license of the GPL pieces may be changed for future versions to make them more consistent with the rest of the package. If you submit patches, and have strong preferences about licensing, please express them.

LibXML2

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Makeself

Makeself v2.1.5

(C) 1998-2008 by Stéphane Peter <megastep@megastep.org>

The source code for this component may be obtained from Symantec Corporation upon request.

The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary

way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the

sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does. Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ``show w'` and ``show c'`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program ``Gnomovision'` (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Microsoft Anti-Cross Site Scripting Library

Microsoft Anti-Cross Site Scripting Library v4.2.1

Copyright (c) 2010 Microsoft Corporation

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law. A "contribution" is the original software, or any additions or changes to the software. A "contributor" is any person that distributes its contribution under this license. "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide,

royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

OpenPegasus

OpenPegasus v2.7.0

Copyright (c) 2000, 2001, 2002 BMC Software; Hewlett-Packard Development

// Company, L.P.; IBM Corp.; The Open Group; Tivoli Systems.

// Copyright (c) 2003 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation, The Open Group.

// Copyright (c) 2004 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2005 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2006 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; Symantec Corporation; The Open Group.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL 0.9.8u

Eric Young & Tim Hudson Copyright (c) 1998-2011.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)'

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*=====

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

* This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 0.9.8y

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*=====

* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

* This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

- * The implementation was written so as to conform with Netscape SSL.
- * This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
- * Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
- * If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
- * This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
- * Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
 - * 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 - * 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 - * "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
 - * The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
 - * 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
 - * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 1.0.1e

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

/*=====

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

- * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- * 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- * 6. Redistributions of any form whatsoever must retain the following acknowledgment:
 - * "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
 - * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

- * This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

- /* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
- * All rights reserved.
- * This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
- * The implementation was written so as to conform with Netscape SSL.
- * This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
- * Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

- * If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
- * This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
- * Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
 - * 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 - * 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 - * "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
 - * The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
 - * 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
 - * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- * The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

plists-cs

plists-cs v1.3.zip - v1.30.0

Copyright (c) 2011 Chad Burggraf

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SQLite

SQLite v3.3.17

This component is in the public domain.

This software is placed in the public domain. It is provided "AS IS" without warranty or support of any kind.

Windows Template Library 'WTL' v8.0

Copyright © 2007 Microsoft Corporation. All rights reserved.

Microsoft Permissive License

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction” and “distribution” have the same meaning here as under U.S. copyright law.

“You” means the licensee of the software.

“Licensed patents” means any Microsoft patent claims which read directly on the software as distributed by Microsoft under this license.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce the software, prepare derivative works of the software and distribute the software or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free patent license under licensed patents to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the software or derivative works of the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you any rights to use Microsoft’s name, logo, or trademarks.

(B) Platform Limitation- The licenses granted in sections 2(A) & 2(B) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

(C) If you begin patent litigation against Microsoft over patents that you think may apply to the software (including a cross-claim or counterclaim in a lawsuit), your license to the software ends automatically.

(D) If you distribute copies of the software or derivative works, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute the software or derivative works in source code form you may do so only under this license (i.e., you must include a complete copy of this license with your distribution), and if you distribute the software or derivative works in compiled or object code form you may only do so under a license that complies with this license.

(F) The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Zlib

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

`zlib/libpng` License

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Índice

A

- AeXGenClientCert.exe
 - parâmetros da linha de comando 330
 - visão geral 516
- AeXGenSiteServerCert.exe
 - parâmetros da linha de comando 296
 - visão geral 516
- AeXNSAgent.exe
 - parâmetros da linha de comando 523
- AeXRevokeCertificate.exe
 - parâmetros da linha de comando 333
 - visão geral 516
- agenda
 - configuração 123
 - exibição do calendário de agenda do Notification Server 124
 - inclusão de várias agendas 123
 - instalação agendada do Symantec Management Agent 249
 - intervalo ativo de datas 123
 - janela de manutenção 119
 - política de agente 118
 - política do servidor 117
 - tarefa do agente 118
 - tarefa do servidor 117
 - usos no Notification Server 117
- agenda compartilhada
 - exibição do calendário de agenda interna 124
- agendamento
 - acionador 119
 - aplicação à política 388
 - atualizações da participação dos recursos 368
 - compartilhado 119
 - componentes 119
 - fuso horário 119
 - modificadores 119
 - período ativo 119
 - personalizado 119
- agendamento compartilhado
 - ativação 122
 - criação 122
 - exclusão 122
 - exibição de usuários do agendamento 122
 - modificação 122
- agendamento de atualização completa
 - configuração 368
- agendamento de atualização de política
 - configuração 368
- agendamento de atualização delta
 - configuração 368
- agendamentos compartilhados
 - sobre 122
- agente. *Consulte* Symantec Management Agent
- agente da solução
 - política de atualização 390
 - política de desinstalação 390
 - política de instalação 390
- agente habilitado na nuvem
 - instalar certificado temporário do cliente 332
- agente habilitado para nuvem
 - instalar no computador desconectado 324
 - parâmetros da linha de comando 523
 - remover o certificado do cliente 332
 - seleção de gateway da Internet, forçar 336
 - solucionar problemas 328
- agregado
 - tipos 551
- ajuda
 - acessar 49
 - contextual 31
- ajuda contextual 31
- ajuste automático
 - configurações de agente e tarefa 184
- apagar agora 79
- ARP 216
- arquivamento
 - dados da versão da tarefa 430
 - dados de tarefas 429
- arquivo CSV
 - como salvar resultados do relatório 446
- arquivo HTML
 - como salvar resultados do relatório 446

- arquivo XML
 - como salvar elementos do console 61
 - como salvar o menu do console 52
 - como salvar resultados do relatório 446
 - exportação de elementos do console 61
 - importação de submenu do console 52
 - importação do menu do console 52
 - restauração de elementos do console 61

- arquivos MIB
 - importação 233
- arranjo em sequência
 - tarefas 417

- arrastar e soltar
 - aplicar a política 379
 - executar trabalhos e tarefas 421
- assistente de descoberta de rede 212

- ativação
 - Task Server 410
- atualização de dados de resumo
 - relatórios da hierarquia 170
- atualizações de software
 - download do agendamento 187
 - instalação 187

- avaliação
 - licença 30

C

- campos passíveis de script
 - Substring 548
- captura de imagem
 - criação com os resultados do relatório 448
- captura de imagem de dados do relatório
 - apagar 79
- caractere curinga
 - caracteres 551
- certificado
 - aplicar ao computador gerenciado 292
 - exportar do Notification Server 292
- certificado de CEM
 - revogar 333
- certificado de servidor
 - aplicação ao servidor de sites 296
 - geração com AeXGenSiteServerCert.exe 296
- certificado do cliente
 - gerar com AeXGenClientCert.exe 330
- certificado do Notification Server
 - aplicar ao computador gerenciado 292
 - exportar do Notification Server 292

- chave de pesquisa de recursos
 - criar 481
- classe de dados
 - exibição dos dados de evento para 437
 - exibição dos dados de inventário para 436
 - virtual 486
- classe de dados virtual
 - criar 486
- classificação de dispositivos SNMP 210
- Client Task Agent
 - configurações 431
- CMDB
 - autenticação do SQL 76
 - autenticação do Windows 76
 - configuração 76
 - credenciais de acesso do banco de dados 76
 - credenciais do relatório público 76
 - histórico de dados de recursos 81
 - limpeza de dados antigos 79
 - nome do banco de dados 76
 - nome do servidor do banco de dados 76
 - sobre 76
 - tempo limite de comando 76
- computador
 - configuração da janela de manutenção 280
 - configuração das políticas do Symantec Management Agent 276
 - configurações de agente de destino 278
 - configurações globais de agentes 277
 - descoberta com a Identificação de recursos 192
 - descoberta com a importação do Microsoft Active Directory 199
 - desinstalação manual do Symantec Management Agent 274
 - envio do Symantec Management Agent 246
 - envio do Symantec Management Agent para UNIX, Linux e Mac 260
 - instalação agendada do Symantec Management Agent 249
 - instalação do Symantec Management Agent 238
 - instalação manual do Symantec Management Agent 240, 255
 - instalação pull do Symantec Management Agent 248
 - instalação pull do Symantec Management Agent para UNIX, Linux e Mac 264
 - intervalos de atualização de dados do Symantec Management Agent 511
 - janela de manutenção 280

- métodos para a descoberta 191
- pesquisar 38
- política de desinstalação do Symantec Management Agent 268
- política de upgrade do Symantec Management Agent 268
- pré-requisito para instalar o Symantec Management Agent 242
- procurar 44
- seleção para a instalação do Symantec Management Agent 246
- sobre a descoberta 191
- Symantec Management Agent 236
- computadores
 - descoberta 179
- comunicação de agente legado
 - ativar 67
 - desativar 67
- comunicação do agente legado
 - ativar 272
 - desativar 272
 - estados padrão 272
 - sobre 272
- confiança do agente
 - aceitar 243
 - bloquear 243
 - estabelecer 237
 - política de registro 243
 - revogar 251
 - sobre 237
- configuração
 - primeira instalação de solução 177
- configuração de HTTPS
 - em computador gerenciado 292
- configurações
 - Client Task Agent 431
 - configurar com o configurador do NS 75
 - Task Server 431
- configurações de agente de ajuste automático 181
- configurações de agente e tarefa
 - ajuste automático 184
 - otimização 184
- configurações de instalação
 - Symantec Management Agent para UNIX, Linux e Mac 259
- configurações do agente
 - ajuste automático 181
 - otimização 181
- configurações do agente do CEM
 - configurar 311
- configurações do ICMP
 - tarefa de identificação de rede 214
- configurações do protocolo
 - tarefa de identificação de rede 214
- Configurações do SNMP
 - tarefa de identificação de rede 214
- configurador do NS
 - sobre 75
- Configuration Management Database. *Consulte* CMDB
- console. *Consulte* console de gerenciamento Symantec
- console de gerenciamento Symantec
 - acesso 47
 - acesso local 47
 - acesso remoto 47
 - ajuda 49
 - componentes personalizáveis 51
 - documentação 49
 - home page 50
 - menu. *Consulte* menu do console
 - página do portal. *Consulte* página do portal
 - personalização 33
 - personalizar 51
 - sobre 33
 - Web part. *Consulte* Web part
- consulta de filtros
 - conversão de uma consulta de recursos em uma consulta SQL 457
 - criação de uma consulta de recursos 530
- consulta de recursos
 - adição de expressões do filtro à consulta 536
 - campos de origem
 - adição 533
 - edição 544
 - criação com o Criador de consulta 530
 - definição para o filtro 359
 - exibição da consulta resolvida 538
 - exibição dos resultados da consulta 539
 - fonte de dados para a política de automação 401
 - parâmetro da consulta
 - sobre 535
 - parâmetro do relatório
 - adição 460
 - adição de tipo avançado 460
 - configurações 546
 - criação 460

- modificação 460
 - parâmetro do relatório, definição 460
- consulta de relatório
 - adição de expressões do filtro à consulta 536
 - campos de origem
 - adição à consulta de recursos 533
 - edição 544
 - campos de origem da consulta SQL 534
 - consulta de recursos 457
 - consulta SQL 459
 - conversão de uma consulta de recursos em uma consulta SQL 457
 - criação de uma consulta de recursos 530
 - escopo da captura de imagem de dados 536
 - exibição da consulta resolvida 538
 - exibição dos resultados da consulta 539
 - gravação de uma consulta SQL 534
 - parâmetro da consulta
 - sobre 535
 - parâmetro do relatório
 - adição 460
 - adição de tipo avançado 460
 - configurações 546
 - criação 460
 - modificação 460
 - parâmetro do relatório, definição 460
 - sobre 457
- consulta do filtro
 - adição de expressões do filtro à consulta 536
 - campos de origem da consulta SQL 534
 - exibição da consulta resolvida 538
 - exibição dos resultados da consulta 539
 - gravação de uma consulta SQL 534
 - parâmetro da consulta
 - sobre 535
 - sobre 457
- consulta SQL
 - captura de imagem de dados 536
 - definição para o filtro 361
 - escopo das capturas de imagem de relatório 536
 - exibição da consulta resolvida 538
 - exibição dos resultados da consulta 539
 - fonte de dados para a política de automação 401
 - gravação 534
 - inserção de campos de origem 534
 - parâmetro da consulta
 - sobre 535
 - parâmetro do relatório
 - adição 460

- adição de tipo avançado 460
 - configurações 546
 - criação 460
 - modificação 460
- parâmetro do relatório, definição 460
- conta do usuário
 - atribuir às funções de segurança 102
 - configuração 94
 - configuração da herança de permissão nas pastas 104
 - configurações de bloqueio da senha 109
 - configurações de complexidade da senha 109
 - criação 94
 - desbloqueio de credenciais bloqueadas 113
 - detalhes gerais da conta 98
- contagem máxima do segmento
 - descoberta de rede 210
- credencial
 - criar 115
 - editar 115
- criação e execução de tarefas Descoberta de rede
 - ativação de Supervisores da Symantec 226
- criador de consulta
 - utilização para a consulta do filtro 359
- critérios de pesquisa personalizados
 - criar 38, 40

D

- dados
 - pré-processamento 479
- dados da versão da tarefa
 - limpar 430
- dados de evento do recurso
 - apagar 79
- dados de recurso
 - visualização 436
- dados de relatório legado
 - apagar 79
- dados de tarefas
 - limpeza 429
- dados do CMDDB
 - editar 484
- dados do computador
 - apagar 79
- dados do evento
 - visualização 437
- Data Connector
 - como funciona 474
 - recursos 476

- sobre 474
- usos 476
- DefaultAppPool
 - configurar 310
- definição da fonte de dados
 - criação 479
- definidos pelo usuário
 - valores 550
- descoberta
 - descoberta de rede 190
 - dispositivos de rede 208
 - importação do Active Directory 190
 - participação em domínio 190
 - recursos 190
- descoberta de computadores 179
- descoberta de dispositivos de rede 209
- descoberta de recursos
 - descoberta de rede 190
 - importação do Active Directory 190
 - participação em domínio 190
- Descoberta de rede 209
 - configurações 210
 - contagem máxima do segmento 210
 - métodos 216
- descoberta de rede 208, 212–213
 - assistente 209
 - configuração 210
 - configurações 210
 - delegação de tarefas 221, 224, 229, 231–232
 - delegação de tarefas de descoberta 231
 - processo 209
 - processo para delegar tarefas 221
 - relatórios 219
 - resultados 219
 - selecionar intervalo de rede 217
 - sobre 190
 - tarefa 213
- descoberta do dispositivo 208
- destino
 - agendamento de atualização 368
 - dependência em filtros 366
 - destino autogerado, como salvar 383
 - destino autogerado, sobre 367, 380
 - destino nomeado, como abrir 384
 - destino nomeado, como salvar 385
 - destino nomeado, seleção 387
 - destino nomeado, sobre 367, 380
 - especificação para a política 380
 - exclusão de itens 385

- grupos de destinos 387
- inclusão de itens 385
- modificação 382
- regras de filtragem 385
- seleção de computadores 383
- seleção de recursos 383
- seleção de usuários 383
- sobre 367
- destinos de recurso. *Consulte* destino
- diretiva
 - destino 367
- dispositivos de rede
 - delegação de tarefas de descoberta 221, 224, 226, 229, 232
 - permissão para que outros usuários façam descobertas 221
- dispositivos SNMP
 - classificar 220
- documentação 31
 - acessar 49

E

- Editor de agenda
 - uso 123
- editor de agendamento
 - como abrir 122
- entrada da tarefa
 - como receber 427
- entradas do registro do agente
 - apagar 79
- escopo do recurso
 - como 349
 - destinos 349
 - exibições organizacionais 349
 - filtros 349
 - sobre 349
- excluir
 - dados da versão da tarefa 430
- exclusão
 - dados de tarefas 429
- exibição computadores
 - sobre 35
- exibição das políticas
 - sobre 43
- exibição de gráfico, relatório
 - configurações do eixo X 540
 - configurações do eixo Y 540
 - legenda do gráfico 540
 - título do gráfico 540

- zoom 3D 540
- exibição de trabalhos e tarefas
 - sobre 43
- exibição do console
 - adição de componentes 57
 - adição de links da Web 57
 - adição de links do item 57
 - criação 55
 - modificação 55
 - sobre 35
 - substituição da árvore 35
- exibição do gráfico, relatório
 - criação 462
 - modificação 462
 - sobre 462
- exibição em grade, relatório
 - condições de formatação 543
 - criação 464
 - formatação avançada 543
 - modelo de formatação 543
 - modificação 464
 - sobre 464
- exibição organizacional
 - criação 344
 - exibição padrão 344
 - filtragem de grupos exibidos 344
 - modificação 344
 - sobre 344
 - uso na segurança dos recursos 341
- exibição Software
 - sobre 40
- exibições aprimoradas
 - aplicar a política 379
 - configurações 45
 - executar trabalhos e tarefas 421
- exibição computadores 35
- exibição software 40
 - sobre 35, 40
- exibições organizacionais
 - exibir dispositivos descobertos 219
- exportar dados 477
- expressão
 - operadores 550
 - sintaxe 549

F

- ferramenta de linha de comando
 - AeXGenClientCert.exe 516
 - AeXGenSiteServerCert.exe 516
- AeXRevokeCertificate.exe 516
- filtro
 - agendamento de atualizações de participação 368
 - atualização da participação 364
 - consulta 457
 - ver também* consulta do filtro
 - consulta de recursos 359
 - consulta SQL 361
 - criação de um filtro estático com os resultados do relatório 447
 - criar 357
 - dependências 366
 - exclusões 362
 - execução de ações em recursos 365
 - inclusões 362
 - menu contextual para membros 365
 - modificar 357
 - processo de criação 355
 - selecionar tipo de consulta 358
 - sobre 354
- filtro de recursos. *Consulte* filtro
- filtro estático
 - criação com os resultados do relatório 447
- fonte de dados
 - criação de uma definição 479
 - especificação para a política de automação 401
 - uso de um relatório para a política de automação 401
 - uso de uma consulta de recursos para a política de automação 401
 - uso de uma consulta SQL para a política de automação 401
 - uso de uma mensagem para a política de automação 401
- função
 - conversão 552
 - expressão 551
 - IIF 553
 - IsNull 553
 - Len 552
 - subsequência de caracteres 554
 - trim 554
- função de segurança
 - adição de membros 101
 - atribuição ao grupo organizacional 348
 - atribuição de permissões 103
 - atribuição de privilégios 93
 - atribuir como um membro de outras funções 102

- categorias de privilégio 489
- configuração da herança de permissão nas pastas 104
- definição das permissões personalizados no grupo organizacional 348
- obtenção de propriedade da pasta ou item 115
- padrão 106
- predefinidos 106
- privilégios da ação de gerenciamento de software 504
- privilégios da ação do clique com o botão direito do mouse 501
- privilégios da credencial 497
- privilégios de exemplos de conector 502
- privilégios de gerenciamento 493
- privilégios de hierarquia 503
- privilégios de item de status dos ativos 505
- privilégios de tarefas de item 501
- privilégios do diretório de fluxo de trabalho 497
- privilégios do perfil de conexão 492
- privilégios do sistema 494
- privilégios do Symantec Management Console 498
- replicação de hierarquia personalizada 165
- segurança dos recursos 341
- funções de segurança
 - configurar 88
 - criar 88
 - sobre 88

G

- gateway da Internet
 - aplicação da lista de revogação de certificados, script 520
 - aplicação do certificado do Notification Server, script 520
 - arquivos de configuração 307
 - arquivos de log 307
 - balanceamento de carga 521
 - cancelamento de registro do serviço do gateway da Internet, script 520
 - configuração do computador-host 313
 - configurar 307, 317
 - download do pacote de instalação 315
 - execução do pacote de instalação 315
 - fazer backup 337
 - forçar a seleção no agente habilitado para nuvem 336
 - gerenciamento 520
 - início do serviço do gateway da Internet, script 520
 - interrupção do serviço do gateway da Internet, script 520
 - porta 317
 - preparar 313
 - processo de instalação 307
 - regeneração do certificado de servidor, script 520
 - registro do serviço do gateway da Internet, script 520
 - restauração completa 337
 - restauração parcial 337
 - visão geral 307
- gerenciador de credenciais
 - sobre 115
- gerenciador de função de segurança
 - acessar 113
 - sobre 113
- Gerenciador de recursos
 - sobre 434
- gerenciador de recursos
 - acesso 435
 - adição de um recurso 437
 - como abrir através dos resultados do relatório 445
 - exibição de dados 436
 - exibição dos dados de evento 437
 - tarefas 438
- gerenciamento de patches
 - agendar 187
- gerenciamento de recursos. *Consulte* gerenciador de recursos
- gerenciamento de tarefas
 - sobre 407
- gerenciamento habilitado para nuvem
 - ambiente misto 517
 - atividades necessárias 287
 - configurar a política de Configurações do gerenciamento habilitado para nuvem 320
 - ferramentas da linha de comando 516
 - gateway da Internet 307
 - pacote de instalação do agente, geração 522
 - pacote de instalação do agente, parâmetros 522
 - parâmetros da linha de comando de AeXNSAgent.exe 523
 - preparar o ambiente 287
 - preparar servidores de sites 287
 - relatórios 339
 - revogar certificado 333

- servidores de pacotes 518
- servidores de sites 518
- servidores de tarefas 518
- sobre 284

- grupo organizacional
 - adição de computadores 346
 - adição de recursos 346
 - adição de um recurso a 437
 - adição de usuários 346
 - agendamento de atualização 368
 - atribuição de funções de segurança 348
 - configuração das permissões do gerenciamento de recursos 348
 - configuração das permissões do Task Server 348
 - configuração de permissões do sistema 348
 - definição das permissões de segurança personalizadas 348
 - edição de um grupo 346
 - execução de ações em membros 347
 - exibição de recursos 347
 - gerenciamento 347
 - sobre 346
 - uso na segurança dos recursos 341
- grupos e exibições organizacionais
 - criar 345
 - preencher 345

H

- hierarquia
 - ativação da replicação 157
 - como modificar relacionamentos hierárquicos 161
 - configurar 156
 - criação de relacionamentos hierárquicos 157, 161
 - executar políticas de automação 168
 - indicador de status de alerta 157
 - informações de status da tarefa 414
 - políticas de automação 168
 - processo de configuração 156
 - relatórios 169
 - remoção de um Notification Server 157
 - replicação. *Consulte* replicação de hierarquia
 - replicação manual de dados selecionados 168
 - requisitos 155
 - sobre 153
 - tarefas em execução 414
- hierarquia do Notification Server. *Consulte* hierarquia

- histórico de dados de recursos
 - como salvar no CMDB 81

I

- identidade do aplicativo
 - Notification Server 67
- identificação de recursos
 - descoberta de computadores com 192
 - sobre 190
- importação do Active Directory
 - agendamento de importações de recursos 204
 - agendamento de sincronização de diretório 205
 - associações de recursos, importação 198
 - descoberta de computadores 199
 - descoberta de recursos 190
 - executar manualmente importações de recursos 206
 - importações completas 204
 - importações de atualização 204
 - log de erros 197
 - processo de uso 199
 - regras de importação de recursos 201
 - relatórios 197
 - sobre 197
 - tipos de recursos suportados 201
- importar dados 477
- informações de status da tarefa
 - hierarquia 414
- instalação do agente 181
- instalação inicial
 - gerenciamento de patches 187
- instalação manual do Symantec Management Agent
 - selecionar computadores 246
- IT Management Suite 7.5
 - novos recursos 25
 - o que há de novo 25
- item
 - configuração de permissões 103
 - obtenção de propriedade 115
- item de menu
 - adição ao menu do console 52
 - exportação 52
 - importação 52

J

- janela Catálogo de software
 - sobre 42

janela de manutenção
 configuração da política 280
 exibição do calendário de agenda interna 124

L

licença
 avaliação 30
 soluções 30
 limpar
 dados da versão da tarefa 430
 limpeza
 dados de tarefas 429
 log detalhado
 limpeza 487

M

mensagem
 fonte de dados para a política de automação 401
 mensagens de status
 exibição no Visualizador de logs 72
 registro em log 72
 menu contextual
 adição de um URL 53
 adição de uma ação personalizada 53
 adição de uma linha de comando 53
 configuração de parâmetros de substituição 53
 utilização com membros do filtro 365
 menu do console
 adição de itens de menu 52
 adição de submenus 52
 importação de submenu de um arquivo XML 52
 personalização 52

N

notas de versão 31
 notificações de e-mail
 configuração 71
 Notification Server
 agendamentos 119
 ver também agendamento
 agendamentos compartilhados 122
 calendário de agenda interna 124
 configuração do servidor proxy 73
 configurações de processamento 67
 configurações do endereço de e-mail 71
 configurar com o configurador do NS 75
 configurar para o gerenciamento habilitado para
 nuvem 302

configurar para usar HTTPS 287, 290
 Configuration Management Database 76
 criação de relacionamentos hierárquicos 157,
 161
 exibição de mensagens de status 72
 exibição do arquivo de logs 72
 filtro. *Consulte* filtro
 funções 64
 hierarquia 153
 identidade do aplicativo 67
 políticas. *Consulte* política
 procedimento de configuração 66
 processamento do NSE 67
 ver também processamento do NSE
 registro em log da mensagem de status 72
 replicação 172
 serviços de site 127, 138
 ver também serviço de site
 servidor de pacotes 138
 ver também serviço do pacote
 servidor de sites. *Consulte* servidor de sites
 site. *Consulte* serviços
 sobre 64
 sub-rede. *Consulte* sub-rede
 tipos de configuração 65
 uso da agenda 117
 visão geral 28
 visão geral da configuração 65
 visão geral das configurações 66

O

operadores da pesquisa
 sobre 44
 otimização
 configurações de agente e tarefa 184
 otimizar configurações de agentes 181

P

pacote
 Symantec Management Agent 273
 pacote do Symantec Management Agent
 atualização de pontos de distribuição 273
 configuração 273
 pacote, software
 adição de um programa 374
 atualização de pontos de distribuição 371–372
 como ativar o acesso a partir do caminho do
 UNC 373

- configurações 371
- gerenciamento de programas 374
- remoção de um programa 374
- página de edição do relatório personalizado
 - guia Exibições 540, 543
- página do portal
 - criação 57
 - meu portal 57
 - modificação 57
 - página Início do Gerenciamento do Notification Server 50
 - sobre 57
- página Meu portal
 - sobre 49
- parâmetros
 - entrada 427
- parâmetros de entrada
 - como receber 427
- participação em domínio
 - descoberta de recursos 190
- pasta
 - configuração da herança de permissão 104
 - configuração de permissões 103
 - obtenção de propriedade 115
- pcAnywhere Solution
 - componentes do 29
 - recursos do 29
- perfil de conexão
 - criar 215
 - sobre 215
- período de bloqueio
 - exibição do calendário de agenda interna 124
- permissões
 - atribuição à função de segurança 103
 - categorias de permissões 491
 - como visualizar 113
 - filtros 508
 - gerenciamento de credenciais 509
 - gerenciamento de recursos 506
 - pastas 508
 - perfis de conexão 509
 - políticas 508
 - relatórios 507
 - servidor de tarefas 507
 - sistema 506
 - sobre 491
- personalização
 - menu do console 52
- pesquisa de software
 - executar 40
 - salvar 40
- pesquisa do computador
 - execução 38
 - salvar como filtro 38
- pesquisar de um computador 38, 44
- pesquisar um computador
 - configurações do campo de pesquisa 45
 - configurar limites 45
- pesquisar um software 40, 44
 - configurações do campo de pesquisa 45
 - configurar limites 45
- pesquisas salvas
 - gerenciar 40
- ping 216
- política
 - agendamento 388, 425
 - aplicar 379
 - baseado em usuário 377
 - configurações de agente de destino 278
 - configurações globais de agentes 277
 - dependência em filtros 366
 - desinstalação do agente 390
 - desinstalação do Symantec Management Agent 268
 - destino, especificação 380
 - exibição do calendário de agenda interna 124
 - exibição Políticas 379
 - gerenciamento 379
 - instalação do agente 390
 - política de automação agendada 397
 - política de automação baseada em mensagens 399
 - política de janela de manutenção 280
 - políticas de automação 392
 - ver também* política de automação
 - políticas de automação da hierarquia 168
 - sobre 377
 - sobre quando usar com tarefas e trabalhos 413
 - tipos 377
 - upgrade do agente 390
 - Upgrade do Symantec Management Agent 268
- política de automação
 - ação 393
 - acionador 393
 - ativação e desativação 394
 - baseada em mensagens, criação 399
 - baseada em mensagens, modificação 399

- como ativar a segurança 394
- como especificar a ação 402
- componentes 393
- configuração de regra de avaliação 397, 399
- criação de agenda 397
- criação de tarefa 405
- especificação da fonte de dados 401
- exclusão 394
- execução de ações em 394
- exibição do calendário de agenda interna 124
- fonte de dados 393
- gerenciamento 394
- hierarquia 168
- modificação de agenda 397
- modificação de tarefa 405
- regra de avaliação 393
- sobre 392
- teste 394
- política de Configurações do gerenciamento habilitado para nuvem
 - configurar 320
 - desativar 320
- política de configurações do gerenciamento habilitado para nuvem
 - ativar 320
- política de registro do agente
 - criar 243
- pontos de distribuição de pacotes
 - atualização 372
 - especificação de credenciais 74
- portal de trabalhos e tarefas
 - acesso 432
- pré-requisitos
 - instalação do Symantec Management Agent 242
 - instalação do Symantec Management Agent para UNIX, Linux e Mac 258
- primeira instalação
 - portal 177
- privilegio, segurança
 - ação de gerenciamento de software 504
 - ação do clique com o botão direito do mouse 501
 - ação específica da solução 504
 - atribuição à função de segurança 93
 - categorias 489
 - credencial 497
 - diretório de fluxo de trabalho 497
 - exemplos de conector 502
 - gerenciamento 493
 - hierarquia 503

- item de status dos ativos 505
- perfil de conexão 492
- replicação de hierarquia personalizada 165
- sistema 494
- Symantec Management Console 498
- processamento do NSE
 - ativação manual 67
 - configurações 67
- processamento do servidor
 - configurações 67
- propriedades
 - entrada 427
- propriedades de entrada
 - como receber 427

R

- recurso
 - adição a um grupo organizacional 437
- recursos
 - atualizações agendadas do filtro 368
 - atualizações da associação de filtro 364
 - exclusão do filtro 362
 - execução de ações em membros do filtro 365
 - exibição das informações da classe de dados 471
 - exibição das informações do tipo de associação dos recursos 471
 - exibição das informações do tipo de recurso 471
 - inclusão no filtro 362
 - segurança. *Consulte* segurança dos recursos
 - seleção com um filtro 354
 - sobre 470
- Recursos do Notification Server. *Consulte* recursos
- regra da exportação
 - criar 480
- regra de CMDB
 - executar como tarefa 485
- regra de importação
 - criar 480
- regra de transferência de dados
 - execução 482
 - verificação 483
- regras de replicação
 - replicação 175
 - replicação de hierarquia 163
- regras do CMDB
 - sobre 484
- relatório
 - como salvar como Web part 449

- como salvar resultados como um filtro
 - estático 447
- como salvar uma captura de imagem 448
- criação. *Consulte* relatório personalizado
- especificação de parâmetros do usuário 442
- execução de ações nos itens de resultado 445
- exibição de resultados 444
- exibição em grade, seleção 444
- exibição em gráfico, seleção 444
- expansão dos resultados 445
- extração de resultados 442
- fonte de dados para a política de automação 401
- gravando resultados em um arquivo 446
- impressão de resultados 445
- modificação. *Consulte* relatório personalizado
- personalização. *Consulte* relatório personalizado
- processo de uso 441
- relatórios da hierarquia 169
- seleção de captura de imagem 442
- sobre 440
- status da instalação do Symantec Management Agent 250
- relatório de recursos. *Consulte* relatório personalizado
- relatório do computador. *Consulte* relatório personalizado
- relatório do SQL. *Consulte* relatório personalizado
- relatório do usuário. *Consulte* relatório personalizado
- relatório personalizado
 - ação de busca detalhada, associação 465
 - ação de busca detalhada, especificação de 465
 - ação de busca detalhada, parâmetros 465
 - ação de busca detalhada, sobre 465
 - adição de expressões do filtro à consulta 536
 - campos de origem
 - adição à consulta de recursos 533
 - edição 544
 - campos de origem da consulta SQL 534
 - componentes 450
 - consulta 457
 - ver também* consulta de relatório
 - consulta de recursos 457
 - consulta SQL 459
 - conversão de uma consulta de recursos em uma consulta SQL 457
 - criação 455
 - criação de uma consulta de recursos 530
 - criar 452
 - editar 452
 - exibição da consulta resolvida 538
 - exibição do gráfico, sobre 462
 - ver também* exibição do gráfico, relatório
 - exibição dos resultados da consulta 539
 - exibição em grade, sobre 464
 - ver também* exibição em grade, relatório
 - expansão dos resultados 465
 - gravação de uma consulta SQL 534
 - modificar 456
 - parâmetro da consulta
 - sobre 535
 - parâmetro do relatório
 - adição 460
 - adição de tipo avançado 460
 - configurações 546
 - criação 460
 - modificação 460
 - parâmetro do relatório, definição 460
 - propriedades, especificar 468
 - sobre 452
- relatórios
 - gerenciamento habilitado para nuvem 339
- relatórios da hierarquia
 - atualização de dados de resumo 170
- replicação
 - ativação de regras de replicação 175
 - completa 172
 - configuração 175
 - criação de regras de replicação 175
 - diferencial 172
 - eventos 175
 - exclusão de regras de replicação 175
 - execução de regras de replicação 175
 - hierarquia. *Consulte* replicação de hierarquia
 - itens 175
 - recursos 175
 - regras de replicação 175
 - requisitos 174
 - segurança 175
 - sobre 172
- replicação de hierarquia
 - configuração 163
 - itens 163
 - objetos de segurança 163
 - recursos 163
 - regras de replicação 163
 - replicação completa 163
 - replicação diferencial 163
 - replicação manual de dados selecionados 168
 - replicação personalizada 165

substituição da agenda da replicação
diferencial 167
replicação do Notification Server. *Consulte* replicação

S

segurança

configuração 84
configurações de bloqueio da senha 109
configurações de complexidade da senha 109
desbloqueio de credenciais bloqueadas 113
funções padrão 106
funções predefinidas 106
gerenciar 108
recursos. *Consulte* segurança dos recursos
sobre 83

segurança dos recursos

configuração da segurança em grupo
organizacional 348
definição de permissões de segurança
personalizadas em um grupo
organizacional 348
exibições organizacionais 344
grupos organizacionais 346
processo de configuração 341
sobre 341

serviço de pacotes

definição como Sem limites 139
definição de configurações 139

serviço de site

definição de configurações 138

serviço de tarefas

definir configurações 139

Servidor de pacotes para Linux

detecção do Apache Web Server 143

servidor de pacotes para Linux 141

exemplos da configuração 147
plataformas suportadas 141
sobre 141
sobre a configuração do HTTPS e HTTP 146
sobre a integração do Apache Web Server 142
sobre configuração com o Apache Web
Server 145

servidor de sites

adição de serviços do site 131
atribuição manual ao site 133
criação 131
gerenciamento 131
modificação 131
remoção de serviços do site 131

remoção do site 131

status 131

servidor de tarefas

dimensionar 418

implementar 418

servidor proxy

configuração 73

servidores de pacotes

configurações 517

configurar para o gerenciamento habilitado para
nuvem 302

publicar bases de código HTTPS 302

servidores de sites

atribuir a um site 304

configurar para agentes habilitados para
nuvem 304

instalar certificado 296

sincronização de dados

execução manual da replicação de
hierarquia 167

hierarquia do Notification Server 153

replicação de hierarquia 163

replicação entre Notification Servers 172

requisitos de hierarquia 155

requisitos de replicação 174

site

atribuição de sub-rede 135

atribuição manual de agentes 134

atribuição manual do servidor de sites 133

configurar para agentes habilitados para
nuvem 304

criar 129

exclusão 129

gerenciar 129

manutenção de site 128

modificar 129

remoção de sub-rede 129

remoção do servidor de sites 129

serviços de site 127

servidor de pacotes sem limites 139

servidor de sites 128

site do agente IIS do CEM

configurações 311

site do IIS

configurar 310

software

pesquisar 40, 44

Software Management Framework

sobre 28

- solicitação de registro do agente
 - bloquear 251
 - permitir 251
- solucionar problemas 512
- solucionar problemas da linha de comando 512
- soluções
 - instalação 30
 - licença 30
- status do registro do agente
 - relatório 251
- string
 - operadores 550
- sub-rede
 - atribuição ao site 135
 - exclusão 135
 - gerenciamento 135
 - ressincronização 135
- Symantec Management Agent
 - atribuição manual a um site 134
 - configuração de políticas de agente 276
 - configuração de uma política de janela de manutenção 280
 - configurações de destino 278
 - configurações globais 277
 - configurações locais 278
 - desinstalação manual 274
 - desinstalar 268
 - envio aos computadores Windows 246
 - importar computadores do arquivo CSV 246
 - instalação 181
 - instalação agendada 249
 - instalação nos computadores Windows selecionados 246
 - instalação pull manual 248
 - instalar no computador desconectado, processo 324
 - intervalos de atualização dos dados 511
 - janela de manutenção 280
 - métodos de desinstalação 268
 - métodos de instalação 238
 - métodos de upgrade 266
 - pacote 273
 - ver também* pacote do Symantec Management Agent
 - parâmetros do pacote de instalação 522
 - política de atualização 390
 - política de desinstalação 268, 390
 - política de upgrade 268
 - pré-requisitos 242
 - processo de instalação manual 240, 255
 - redirecionar para usar HTTPS 287, 295
 - relatório de status da instalação 250
 - requisitos de instalação 242
 - selecionar computadores para a instalação 246
 - sobre 236
 - solução de problemas para o gerenciamento habilitado para nuvem 328
 - solucionar problemas 512
 - upgrade 266
- Symantec Management Agent para UNIX, Linux e Mac
 - arquivo do modelo .csv 256
 - criação do arquivo .csv para obter detalhes do computador 256
 - especificar configurações de instalação 259
 - instalação em computadores selecionados 260
 - instalação por envio para computadores 260
 - instalação pull manual 264
 - métodos de instalação 238
 - pacote 273
 - ver também* pacote do Symantec Management Agent
 - política de desinstalação 268
 - política de upgrade 268
 - pré-requisitos 258
 - processo de instalação manual 255
 - relatório de status da instalação 250
 - requisitos de instalação 258
 - sobre 236
 - tarefas de instalação simultâneas, definição 260
- Symantec Management Agent para Windows
 - importar computadores do arquivo CSV 246
 - selecionar computadores para a instalação 246
- Symantec Management Console
 - como salvar elementos como arquivos XML 61
 - como salvar o submenu como o arquivo XML 52
 - exibição. *Consulte* exibição do console
 - importação do menu do arquivo XML 52
- Symantec Management Platform
 - componentes 28
 - introdução 24
 - segurança 83–84, 108
 - sobre 24, 28
- Symantec Management Platform 7.5
 - novos recursos 25
 - o que há de novo 25

T

tarefa

- ação da política de automação 402
- agendamento 425
- arranjo em sequência 417
- como especificar parâmetros de entrada 402
- criação para política de automação 405
- criar 419
- dependência em filtros 366
- destino, especificação 380
- execução 422
- exibição do calendário de agenda interna 124
- modificação para a política de automação 405
- seleção para a política de automação 404
- sobre quando usar 413

tarefa de descoberta de rede

- criação 213
- local 213
- modificação 213

tarefa de identificação de rede

- configurações do protocolo 214
- perfil de conexão 214

tarefa Descoberta de rede

- criação 212
- local 212

tarefas Descoberta de rede

- ativação de criação de Supervisores da Symantec 226
- delegação 226

tarefas em execução

- hierarquia 414

Task Server

- ativação 410
- configurações 431

trabalho

- agendamento 425
- execução 422

trabalhos

- arranjo em sequência 417
- criação 420
- sobre quando usar 413

trabalhos e tarefas

- executar 421

transferência de dados

- configuração 477
- configurar 480
- resumos 483

U

usuários

- políticas baseadas em usuário 377

V

visualizador de logs

- como abrir 72

W

Web part

- adição à página do portal 57
- apresentação do URL 60
- apresentação dos resultados do relatório 60
- configuração de altura fixa 60
- criação 60
- criação com o relatório 449
- definição do tamanho padrão 60
- modificação 60
- sobre a utilização nas páginas do portal 57