Kaseya 2

Discovery

Guia do usuário

Version 7.0

Português

Setembro 17, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Conteúdo

Discovery Visão geral

Discovery (KDIS) detecta computadores e dispositivos em redes individuais ou domínios inteiros. Após serem detectados, os agentes podem ser instalados em qualquer computador ou dispositivo móvel. Se um dispositivo detectado não puder ser instalado com um agente, o dispositivo ainda poderá ser identificado utilizando SNMP. Dispositivos habilitados com SNMP podem ser, então, monitorados utilizando o módulo **Monitorar**. Auditorias de hardware de máquinas habilitadas com vPro também pode ser incluídas em varreduras de detecção. As máquinas habilitadas com vPro podem, então, ser gerenciadas utilizando o módulo **Desktop Management**. Uma página **Ativos** fornece uma visualização consolidada de todos os computadores e dispositivos gerenciados pelo VSA, independentemente do método de detecção.

A detecção por domínio permite a instalação de agentes em qualquer máquina conhecida para um domínio Active Directory. Além disso, a **Discovery** pode integrar logons do usuário do VSA e logons do Portal Access com logons do domínio. **Discovery** também pode criar registros de membros com base nos contatos no domínio. As alterações no domínio são sincronizadas com o **Discovery** de forma programada e não exigem um agente VSA no controlador do domínio do DA. **Discovery** utiliza o protocolo LDAP padrão do setor para se comunicar com os domínios Active Directory de modo seguro.

Discovery LAN Watch:

- detecta computadores e dispositivos em redes individuais.
- Implementa agentes em máquinas sem agente detectadas.
- Identifica dispositivos SNMP e máquinas vPro.
- Permite que um dispositivo seja "promovido" para um **ativo** *(página 6)* gerenciado.

Discovery Domain Watch:

- Detecta domínios AD automaticamente que podem ser sincronizados com o VSA.
- Cria automaticamente uma hierarquia de segurança do VSA modelada conforme uma hierarquia existente do domínio.
- Mantém automaticamente o VSA sincronizado com todas as alterações do domínio.
- Cria automaticamente registros de integrantes e usuários do VSA no VSA com base na criação de usuários e contatos nos domínios.
- Preenche automaticamente o usuário de domínio e informações de contato nos tickets do **Service Desk**.
- Implementa automaticamente agentes para os computadores de domínio. Os agentes são colocados automaticamente no grupo de máquinas apropriado relativo à hierarquia do domínio.
- Redefine uma senha de domínio ou habilita/desabilita um usuário de domínio a partir do VSA.

Nota: Consulte DiscoveryRequisitos de sistema.

Funções	Descrição
Visão geral	Exibe o fluxo de trabalho da detecção de computadores e dispositivos por rede e por domínio.
LAN Watch por verificação *(página 18)*	Detecta dispositivos na mesma LAN como uma máquina de "verificação" selecionada.
LAN Watch por rede *(página 8)*	Detecta computadores e dispositivos por LAN.
Dispositivos detectados - Visualização em grade *(página 19)*	Exibe computadores e dispositivos detectados em formato de tabela.

Dispositivos detectados - Visualização lado a lado *(página 21)*	Exibe computadores e dispositivos detectados em formato lado a lado.
Domain Watch *(página 45)*	Configura a integração do Discovery com os domínios Active Directory.
Computadores *(página 58)*	Gerencia contas de ID de máquinas criadas, com base nas políticas aplicadas dos computadores do Discovery, para todos os domínios monitorados pelas verificações do Discovery.
Contatos *(página 60)*	Gerencia registros de integrantes criados, com base nas políticas aplicadas de contato do Discovery, para todos os domínios monitorados pelas verificações do Discovery.
Usuários e Usuários do portal *(página 62)*	Gerencia usuários do VSA e candidatos do Portal Access criados, com base nas políticas de grupo aplicadas do Discovery, para todos os domínios monitorados pelas verificações do Discovery.
Visualizar ativos	Fornece uma visão consolidada de todos os "ativos" gerenciados pelo VSA.
Configurações *(página 67)*	Define opções e valores padrão que se aplicam ao módulo inteiro do Discovery.
Registro de auditoria *(página 68)*	Exibe um log de atividades do módulo Discovery.

Discovery Requisitos do módulo

servidor da Kaseya

- O módulo Discovery 7.0 requer o VSA 7.0.

Serviços de diretório

- Directory Services 1.2 é um conjunto de recursos que pode ser licenciado e habilitado separadamente. O conjunto de recursos fornece uma funcionalidade avançada no módulo do Discovery.

Verificação de rede

- É possível usar qualquer sistema operacional Windows, Apple ou Linux compatível com o Kaseya. Consulte **Requisitos de agentes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/reqs/index.asp#home.htm)*.

Verificação do domínio

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Nota: Consulte **Requisitos gerais do sistema** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/reqs/index.asp#home.htm)*.

Capítulo 1

LAN Watch

Neste capítulo

Como começar a usar o LAN Watch

As páginas **LAN Watch por rede** e **LAN Watch por verificação** detectam computadores e dispositivos em LANs. Qualquer máquina do agente em uma LAN pode ser selecionada como a máquina de "verificação" para aquela LAN. A varredura de uma LAN utilizando uma máquina de verificação detecta qualquer dispositivo ou máquina com um endereço IP. Dispositivos detectados podem ser estações de trabalho e servidores sem agentes, Dispositivos SNMP e máquinas habilitadas com vPro. Os dispositivos detectados são exibidos nas seguintes páginas:

- **Dispositivos detectados - Visualização em grade** *(página 19)*
- **Dispositivos detectados - Visualização lado a lado** *(página 21)*

Como as LANs são identificadas

Uma LAN é detectada se um único computador naquela LAN estiver instalado com um agente. As LAN detectadas são identificadas consecutivamente como `LAN1`, `LAN2`, `LAN3`, etc. O nome atribuído a uma LAN pode ser alterado para reconhecimento mais fácil. Cada LAN é distinguida por uma combinação única dos seguintes dois itens:

- O intervalo de IP interno mostrado na coluna **Intervalo de varredura**, e
- o endereço IP externo mostrado na coluna **Gateway**.

O intervalo de IP interno mostrado na coluna **Intervalo de varredura** é expresso como o endereço IP inicial seguido pelo número de bits - por exemplo, `/24` — representando a parte da rede do endereço IP.

Como utilizar LAN Watch por rede

1. Selecione a linha de uma LAN detectada no painel superior.
2. Selecione **Novo** ou **Editar** para definir as propriedades da varredura. Esta inclui a máquina para servir como uma máquina de verificação. Máquinas de agente Linux, Mac e Windows podem todas servir como máquinas de verificação.
3. Opcionalmente, implemente agentes para computadores detectados por política, utilizando a guia **Política de implementação de agentes** no painel inferior.
4. Opcionalmente, crie alertas para tipos de computadores e dispositivos detectados recentemente utilizando a guia **Perfis de alertas** no painel inferior.
5. Opcionalmente, defina as políticas de ativos para computadores e dispositivos detectados, utilizando a página **Promoção de ativos**.
6. Agende uma varredura uma vez ou em uma base recorrente utilizando o botão **Agendar varredura**, ou execute uma varredura imediatamente utilizando o botão **Fazer varredura agora**.

- Opcionalmente, busque dispositivos SNMP e máquinas habilitadas com vPro utilizando a caixa de diálogo Agendar varredura.
- Uma varredura pode ser atribuída a diversas LANs ao mesmo tempo. Cada LAN executará as políticas atribuídas para aquela LAN utilizando as guias no painel inferior.

Como utilizar LAN Watch por verificação

1. Selecione uma ou mais IDs de máquina.

   Nota: Máquinas com Windows XP não são recomendadas como máquinas de verificação. NMAP é mais confiável com sistemas operacionais Windows posteriores.

2. Agende uma varredura uma vez ou em uma base recorrente utilizando o botão **Agendar varredura**, ou execute uma varredura imediatamente utilizando o botão **Fazer varredura agora**.
   - Opcionalmente, busque dispositivos SNMP e máquinas habilitadas com vPro utilizando a caixa de diálogo **Agendar varredura**.
   - Uma varredura pode ser atribuída a diversas IDs de máquina.

Intervalos LAN duplicados

Ocasionalmente, duas LANs são listadas na página **LAN Watch por rede** com o mesmo intervalo de endereço IP ou sobrepondo intervalos de endereços IP. Esta condição é geralmente causada por um dispositivo, roteador ou DHCP com uma máscara de sub-rede mal configurada. Quando isto acontece, o

- Discovery gera um alerta do sistema que é exibido na página Monitor > Resumo de alarmes.
- Executar varreduras do **Discovery** em LANs sobrepostas parecerá que move máquinas para frente e para trás entre cada LAN enquanto elas são detectadas novamente.

Para evitar este comportamento, os administradores da rede podem:

- Reconfigurar os dispositivos nas redes deles para corrigir a condição, ou
- Configurar o **Discovery** para "ignorar" uma das redes.

Guia Políticas de implementação de agentes

A guia **Políticas de implementação de agentes** da página **LAN Watch por rede** define as políticas para implementação de agentes em computadores detectados em uma rede selecionada. Para cada tipo de sistema operacional — para Windows, Mac e Linux — configure o seguinte:

- **Instalar agentes automaticamente para máquinas <do tipo de SO>** : marque para habilitar.
- **Pacote padrão**: para cada tipo de SO, selecione um pacote de instalação do agente apropriado do SO.
- **Agente implementador designado**: uma máquina do agente na mesma rede usada para implementar o agente.
- **Nome de usuário/Senha/Confirmar senha**: insira uma credencial do administrador que habilita a instalação remota de um agente.

As políticas que você configurar também servem como padrões ao implementar um agente *manualmente* utilizando:

- **Dispositivos detectados - Visualização em grade** *(página 19)*
- **Dispositivos detectados - Visualização lado a lado** *(página 21)*
- **Resultados de varredura** *(página 15)*

Requerimento de tipo de SO correspondente

Qualquer tipo de SO de computador que pode dar suporte a um agente pode ser usado para fazer a varredura de uma rede: Windows, Mac ou Linux. Se um agente é implementado, o **Discovery** automaticamente é alterado, se necessário, para uma máquina do tipo de SO correspondente na mesma LAN. Já que cada tipo de SO somente pode implementar agentes em máquinas de destino

que correspondem a seu próprio tipo de SO, você deve instalar manualmente, ao menos, um agente de cada tipo de SO — Windows, Mac e Linux — em uma LAN para implementar agentes automaticamente para todos os três tipos de sistemas operacionais.

Credencial do administrador

A credencial especificada deve ter direitos de administrador na máquina remota selecionada.

- **Se a máquina de destino estiver em um domínio**, a credencial do administrador deverá usar o formato `domain\administrator` ou `administrator@domain`.
- **Se a máquina de destino não estiver em um domínio**, a credencial do administrador poderá requerer o formato `local\administrator` ou `<hostname>\administrator`.
- **Se a máquina de destino for uma máquina Linux**, o nome de usuário `root` sozinho — sem um nome de host ou domínio — deverá ser usado.

Guia Perfis de alerta

A guia **Perfis de alerta** da **LAN Watch por rede** define as políticas de alerta do **Discovery** para uma LAN selecionada e um tipo de dispositivo: computador, móvel, rede e firewall.

> **Nota:** A caixa de seleção **Alertas ativos** na caixa de diálogo **Editar** habilita e desabilita alertas do **Discovery** configurados nesta guia para uma rede selecionada.

Guia Promoção de ativos

A guia **Promoção de ativos** da página **LAN Watch por rede** configura a promoção automática de dispositivos a ativos quando os dispositivos são detectados.

Quando um agente não pode ser instalado em um dispositivo detectado, o dispositivo pode ser "promovido" para um ativo gerenciado. Por exemplo, um roteador ou uma impressora ainda pode exigir monitoramento, mesmo que não seja possível instalar um agente na máquina.

Todos os ativos gerenciados devem ser atribuídos a um grupo de máquinas e organização. **As regras de escopo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4578.htm)* e os recursos de **filtragem de visualização** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#214.htm)* dentro do VSA dependem desta atribuição.

Um dispositivo detectado pode ser promovido ou rebaixado manualmente na página **LAN Watch por rede** *(página 8)* ou **LAN Watch por verificação** *(página 18)* ao alternar o ícone /.

Resultados de varredura

A janela **Resultados da varredura** exibe os resultados da varredura mais recente para uma rede. A mesma janela é exibida ao clicar no ícone em duas páginas diferentes.

- Clique no ícone para uma rede na página **LAN Watch por rede** *(página 8)*.
- Clique no ícone para uma máquina do agente na página **LAN Watch por verificação** *(página 18)*.

> **Nota:** Pode haver um atraso na exibição desta página se uma varredura de rede estiver em andamento.

A janela **Resultados da varredura** tem duas guias.

- Guia Resumo
- Guia Dispositivos

Dispositivos detectados

A página **Dispositivos detectados - Visualização em grade** mostra os computadores e dispositivos detectados utilizando **LAN Watch por verificação** *(página 18)* e **LAN Watch por rede** *(página 8)*. Utilize esta página para instalar os agentes em dispositivos móveis e computadores detectados. Você também pode tornar dispositivos detectados em um ativo gerenciado, mesmo que eles não possam

ser instalados com o agente.

A página **Dispositivos detectados - Visualização lado a lado** mostra os computadores e dispositivos detectados utilizando **LAN Watch por rede** *(página 8)* e **LAN Watch por verificação** *(página 18)*. Os resultados da varredura são *cumulativos* de todas as máquinas de verificação. Um registro não é removido até que você o exclua.

Formato de visualização lado a lado

A visualização lado a lado exibe cada dispositivo em seu próprio bloco. Um bloco pode incluir os seguintes ícones:

 - Clique para exibir dados de varredura NMAP.

 - Somente é exibido caso um agente esteja instalado. Passe o mouse sobre este ícone para exibir a janela **Visualização rápida** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#9339.htm)*. Clique para executar o **Live Connect** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4796.htm)*.

 /  - Alternar este ícone manualmente **promove ou rebaixa um dispositivo sem agente para um ativo** *(página 15)*.

 - Somente é exibido caso um agente esteja instalado. O número de tickets criados para este computador. Clique para exibir os tickets em uma tabela de tickets.

 - Somente é exibido caso um agente esteja instalado. O número de alarmes criados para este dispositivo ou computador. Clique para exibir a página **Resumo de alarmes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4112.htm)* para este dispositivo.

 - Somente é exibido se um agente é atribuído a um conjunto de monitores ou se um dispositivo SNMP é atribuído a um conjunto SNMP. Clique para exibir o dashlet **Status da máquina** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2803.htm)* ou o dashlet **Status do dispositivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2817.htm)*.

 - Passar o mouse sobre um bloco exibe um ícone de lápis. Você pode editar o nome de uma máquina ou dispositivo detectado.

Visualizar ativos

A página Auditoria > **Visualizar ativos** é preenchida por varreduras de redes e domínios do **Discovery**. A página **Visualizar ativos** fornece uma visão consolidada de todos os "ativos" gerenciados pelo VSA. Os tipos de ativos incluem:

- **Máquinas e dispositivos móveis gerenciados pelo cliente**: computadores e dispositivos móveis que têm um agente instalado neles são sempre considerados ativos gerenciados e são exibidos nesta página enquanto o agente estiver instalado neles.
- **Dispositivos promovidos a um ativo**: Quando um agente não pode ser instalado em um dispositivo detectado, o dispositivo ainda pode ser "promovido" para um ativo gerenciado e ser exibido nesta página. Por exemplo, um roteador ou uma impressora ainda pode exigir monitoramento, mesmo que não seja possível instalar um agente na máquina. Há diversos tipos diferentes de dispositivos sem agente que podem ser gerenciados pelo VSA: roteadores, alternadores, impressoras, firewalls, etc. O botão **Criar ativo** em Discovery > **Dispositivos detectados - Visualização em grade** *(página 19)* permite que você "promova" um dispositivo para um ativo. Quando você faz isso, o dispositivo começa a ser exibido nesta página. Você pode "rebaixar" um ativo utilizando **Rebaixar ativo para dispositivo** nesta página. Quando você faz isso, o ativo é removido desta página.

todos os ativos gerenciados são atribuídos a um grupo de máquinas e organização. **As regras de escopo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4578.htm)* e os recursos de **filtragem de visualização** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#214.htm)* dentro do VSA dependem desta atribuição.

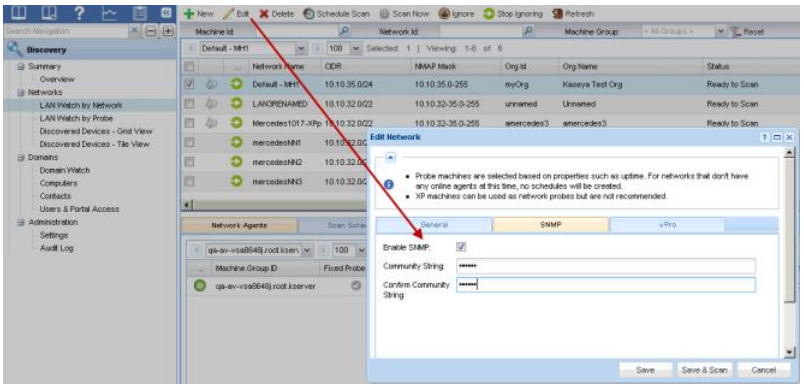
- Diversas credenciais podem ser definidas para cada ativo. Para ativos do agente, uma das credenciais pode ser designada uma credencial do agente e ser usada, opcionalmente, pelo **Policy Management** como uma credencial do agente.

- **Service Desk** Como opção, é possível associar tickets com ativos listados nessa página.

LAN Watch and SNMP

LAN Watch by Network or **LAN Watch by Probe** in the **Discovery** module uses an existing VSA **agent** *(página 69)* on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran.

The LAN Watch discovery machine issues the SNMP requests to the SNMP devices it discovers on the same LAN. So you must run LAN Watch *first* to have access to SNMP-enabled devices using the VSA.



To include SNMP devices in the discovery scan performed by LAN Watch:

1. Select a machine ID on the same LAN as the SNMP devices you want to discover.
2. Check the **Enable SNMP** checkbox.
3. Enter a `community name` in the **Read Community Name** and **Confirm** fields.

   A community name is a credential for gaining access to an SNMP-enabled device. The default "read" community name is typically `public`, in all lower case, but each device may be configured differently. You may have to identify or reset the community name on the device directly if you're not sure what community name to use.
4. Click the **Schedule and Scan** button at the bottom of the **Edit Network** dialog. This will start the scan immediately.
5. Review discovered SNMP-enabled devices using the Monitor > Assign SNMP page.

LAN Watch e vPro

A guia Auditoria > Visualizar ativos > **vPro** exibe informações de hardware sobre máquinas habilitadas para vPro detectadas ao permitir uma varredura com o vPro com o uso do diálogo **Editar rede** *(página 10)* e, em seguida, com a execução do **LAN Watch** *(página 18)*. Essas informações estão disponíveis apenas se a credencial vPro de uma máquina for especificada pelo **LAN Watch**.

Os tipos de informações de hardware retornadas pela máquina vPro incluem:

- Status de entrada do agente, se a máquina vPro tiver um agente instalado.
- Informações do computador
- Informações do ativo d alpaca mãe
- Informações da BIOS
- Informações do processador
- Informações da RAM
- Informações da unidade de disco rígido

Nota: O módulo do **Desktop Policy** fornece **recursos de gerenciamento do vPro** *(http://help.kaseya.com/webhelp/PTB/KDPM-Online-Help.asp?10070.htm).*

LAN Watch por rede

Discovery > Redes > LAN Watch por rede

As páginas **LAN Watch por rede** e **LAN Watch por verificação** detectam computadores e dispositivos em LANs. Qualquer máquina do agente em uma LAN pode ser selecionada como a máquina de "verificação" para aquela LAN. A varredura de uma LAN utilizando uma máquina de verificação detecta qualquer dispositivo ou máquina com um endereço IP. Dispositivos detectados podem ser estações de trabalho e servidores sem agentes, Dispositivos SNMP e máquinas habilitadas com vPro. Os dispositivos detectados são exibidos nas seguintes páginas:

- **Dispositivos detectados - Visualização em grade** *(página 19)*
- **Dispositivos detectados - Visualização lado a lado** *(página 21)*

Como as LANs são identificadas

Uma LAN é detectada se um único computador naquela LAN estiver instalado com um agente. As LAN detectadas são identificadas consecutivamente como `LAN1`, `LAN2`, `LAN3`, etc. O nome atribuído a uma LAN pode ser alterado para reconhecimento mais fácil. Cada LAN é distinguida por uma combinação única dos seguintes dois itens:

- O intervalo de IP interno mostrado na coluna **Intervalo de varredura**, e
- o endereço IP externo mostrado na coluna **Gateway**.

O intervalo de IP interno mostrado na coluna **Intervalo de varredura** é expresso como o endereço IP inicial seguido pelo número de bits - por exemplo, `/24` — representando a parte da rede do endereço IP.

Intervalos LAN duplicados

Ocasionalmente, duas LANs são listadas na página **LAN Watch por rede** com o mesmo intervalo de endereço IP ou sobrepondo intervalos de endereços IP. Esta condição é geralmente causada por um dispositivo, roteador ou DHCP com uma máscara de sub-rede mal configurada. Quando isto acontece, o

- Discovery gera um alerta do sistema que é exibido na página Monitor > Resumo de alarmes.
- Executar varreduras do **Discovery** em LANs sobrepostas parecerá que move máquinas para frente e para trás entre cada LAN enquanto elas são detectadas novamente.

Para evitar este comportamento, os administradores da rede podem:

- Reconfigurar os dispositivos nas redes deles para corrigir a condição, ou
- Configurar o **Discovery** para "ignorar" uma das redes.

Como utilizar LAN Watch por rede

1. Selecione a linha de uma LAN detectada no painel superior.
2. Selecione **Novo** ou **Editar** para definir as propriedades da varredura. Esta inclui a máquina para servir como uma máquina de verificação. Máquinas de agente Linux, Mac e Windows podem todas servir como máquinas de verificação.
3. Opcionalmente, implemente agentes para computadores detectados por política, utilizando a guia **Política de implementação de agentes** no painel inferior.
4. Opcionalmente, crie alertas para tipos de computadores e dispositivos detectados recentemente utilizando a guia **Perfis de alertas** no painel inferior.
5. Opcionalmente, defina as políticas de ativos para computadores e dispositivos detectados, utilizando a página **Promoção de ativos**.
6. Agende uma varredura uma vez ou em uma base recorrente utilizando o botão **Agendar varredura**, ou execute uma varredura imediatamente utilizando o botão **Fazer varredura agora**.
   - Opcionalmente, busque dispositivos SNMP e máquinas habilitadas com vPro utilizando a caixa de diálogo Agendar varredura.

- Uma varredura pode ser atribuída a diversas LANs ao mesmo tempo. Cada LAN executará as políticas atribuídas para aquela LAN utilizando as guias no painel inferior.

Ações

- **Novo**: adiciona manualmente uma nova rede. Exibe as mesmas propriedades que **Editar rede** *(página 10)*.
- **Editar**: exibe **Editar rede** *(página 10)*. Configura as opções de varredura utilizadas por **Fazer varredura agora**. As mesmas configurações servem como as configurações padrão exibidas pela caixa de diálogo **Agendar varredura**.
- **Excluir**: exclui uma rede. Utilize esta opção para remover uma rede que não tem mais agentes gerenciados.
- **Agendar varredura**: exibe a caixa de diálogo **Caixa de diálogo Agendar varredura** *(página 11)*. Agenda uma varredura LAN Watch, de maneira recorrente, para uma rede selecionada.
- **Fazer varredura agora**: executa uma LAN Watch imediatamente em uma rede selecionada utilizando as opções de varredura definidas pela **caixa de diálogo Editar**.
- **Ignorar**: evita que seja feita a varredura de uma rede.
- **Deixar de ignorar**: reabilita a varredura de uma rede que foi ignorada anteriormente.
- **Atualizar**: atualiza a página.

Colunas de tabelas do painel superior

- **Resultados da varredura** -  : clique neste ícone para exibir os **resultados da varredura mais recente e os resultados acumulados de todas as varreduras anteriores** *(página 15)*.
- **Ignorar rede**
  -  - A rede pronta para receber a varredura.
  -  - A rede é ignorada da varredura.
- **Nome da rede**: o nome amigável atribuído pelo VSA para identificar uma rede.
- **Gateway**: o endereço IP do gateway da conexão.
- **Faixa de varredura**: a faixa interna de IP, expressa como o endereço inicial do IP seguida pelo número de bits, por exemplo, `/24`, representando a parte da rede do endereço IP.
- **Máscara de sub-rede**: determina o número de endereços IP em uma sub-rede.
- **ID da Org**: o único identificador de uma **organização** *(página 70)* no VSA.
- **Nome da Org**: o nome amigável do VSA da organização.
- **Status** - O status de uma varredura. Uma varredura progride através dos seguintes status. Estes status são exibidos em Procedimentos pendentes e **Histórico de procedimentos**. Se a varredura não falha, o status retorna para `ReadyToScan` quando a varredura é concluída.
  - 0 - `ReadyToScan`: varredura ainda não iniciada.
  - 1 - `Installing`
  - 2 - `PerformingQuickScan`
  - 3 - `CompletedQuickScan`
  - 4 - `PerformingDeepScan`
  - 5 - `DNSScan`
  - 6 - `Failed`
- **Progresso da varredura**: exibe uma barra de progresso para uma varredura profunda.
- **Próxima varredura**: a data/hora em que uma próxima varredura está agenda.
- **Última varredura**: a data/hora da última execução de uma varredura.
- **Dispositivos varridos**: uma contagem dos dispositivos detectados neste rede.
- **Ativos**: uma contagem do número de dispositivos marcados como Ver ativos gerenciados.
- **Agentes**: o número de máquinas e dispositivos instalados com agentes na LAN.
- **Alertas ativos**: se marcado, os alertas estão ativos nesta rede.

- **Prefixo de rede**: o número de bits usados para especificar a parte da rede de um endereço IP.
- **Contagem máximo de endereços**: o número máximo de endereços IP especificados por uma rede.

Guias do painel inferior

- **Guia Agentes da rede** *(página 12)*
- **Guia Agendamentos de varredura** *(página 13)*
- **Guia Implementação do agente** *(página 13)*
- **Guia Perfis de alertas** *(página 14)*
- **Guia Promoção de ativos** *(página 15)*

Editar rede

Discovery > Redes > LAN Watch por rede *(página 8)* > Novo ou editar

A caixa de diálogo **Editar** configura opções de varredura utilizadas por **Fazer varredura agora**. As mesmas configurações servem como as configurações padrão exibidas pela caixa de diálogo **Agendar varredura**.

Guia Geral

- **Nome da rede**: o nome amigável atribuído pelo VSA para identificar uma rede.
- **Verificação**: a máquina do agente a ser usada para fazer a varredura com esta rede. Máquinas de agente Linux, Mac e Windows podem todas servir como máquinas de verificação.

  > **Nota:** Máquinas com Windows XP não são recomendadas como máquinas de verificação. NMPA funciona muito melhor com sistemas operacionais mais novos.

- **Intervalo de IP**: especifica o intervalo de endereços IP a incluir em uma varredura. Por padrão, todo o intervalo da varredura configurado para uma rede é especificado. Exemplo: 192.168.32-35.0-255. Somente intervalos individuais de IP são compatíveis.
- **Exclusões de IP**: especifica um intervalo de endereços IP a serem excluídos da varredura. Intervalos múltiplos de IP separados por vírgulas são compatíveis. Exemplo: 192.168.32-35.0-255, 10.10.14-15.0-255. Por padrão, este campo fica em branco.
- **Organização**: atribua uma organização a uma rede. Após as organizações serem atribuídas a todas as suas redes, a tabela de redes pode ser classificada e filtrada por organização. *Esta atribuição não tem efeito nos dispositivos detectados atribuídos da organização quando eles são promovidos a um ativo (página 15).*
- **Alertas ativos**: se marcado, os alertas configurados na guia **Guia Perfis de alertas** *(página 14)* estão ativos. Se em branco, os alertas não são gerados para dispositivos detectados nesta rede.
- Armazene as informações do contato para uma rede selecionada utilizando os seguintes campos.
  - **Telefone primário**
  - **Fax central**
  - **E-mail primário**
  - **País**
  - **Rua**
  - **Cidade**
  - **Estado**
  - **Compactar**
- **Dias para manutenção de dispositivos ocultos**: insira o número de dias para suprimir alertas para novos dispositivos. Isso impede a criação de alertas para dispositivos que estiverem conectados à rede temporariamente.

Guia SNMP

Após o **Discovery** ter realizado uma varredura habilitada com SNMP utilizando um nome válido da comunidade, você pode:

- Identificar, classificar e filtrar dispositivos habilitados para SNMP na página **Dispositivos detectados - Visualização em grade** *(página 19)* utilizando a coluna **SNMP ativo**.
- Comece monitorando dispositivos habilitados para SNMP ao atribuir conjuntos SNMP utilizando Monitor > **Atribuir SNMP** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2190.htm)*.

Opções

- **Habilitar SNMP**: se marcado, faz a varredura dos dispositivos SNMP dentro do **Intervalo de IP da varredura** especificado.
- **Nome de comunidade de leitura/Confirmar sequência da comunidade**: LAN Watch somente pode identificar dispositivos SNMP que compartilham o mesmo valor de *leitura* da Comunidade SNMP como a máquina gerenciada executando o LAN Watch. Os nomes da comunidade *diferenciam maiúsculas de minúsculas*. Normalmente, o valor padrão do nome da comunidade de leitura é `public`, mas pode ser redefinido por um administrador como `Public`, `PUBLIC` etc.

Guia vPro

Após o **Discovery** ter realizado uma varredura habilitada para vPro utilizando uma credencial válida vPro em uma rede, você pode:

- Identificar, classificar e filtrar dispositivos habilitados para vPro na página **Dispositivos detectados - Visualização em grade** *(página 19)* utilizando a coluna **Máquina vPro**.
- Exibir atributos de hardware para máquinas habilitadas para vPro utilizando o botão **Visualizar** na página **Dispositivos detectados - Visualização em grade** *(página 19)*.
- Exibir atributos de hardware para máquinas habilitadas para vPro classificadas como ativos utilizando a guia vPro na página **Ativos**.
- Listar máquinas vPro na página Gerenciamento de desktops > vPro > **Gerenciamento vPro** *(http://help.kaseya.com/webhelp/PTB/KDPM/7000000/index.asp#10070.htm)* se a caixa de seleção **Mostrar ativos detectados** estiver selecionada. Nesta mesma página, estas máquinas vPro sem agente podem ser ligadas, sob demanda ou por agendamento, e desligadas sob demanda.

Uma máquina não precisa ser uma máquina vPro para detectar máquinas vPro utilizando o **Discovery**.

Nota: A configuração vPro é um pré-requisito para utilizar este recurso. Consulte a documentação mais recente da Intel para obter informações sobre como configurar o vPro. No momento em que este documento está sendo escrito, o link a seguir leva para a documentação da Intel:
http://communities.intel.com/community/openportit/vproexpert
(http://communities.intel.com/community/openportit/vproexpert).

Opções

- **Habilitar vPro**: somente Windows. Se marcado, a varredura vPro está habilitada para esta rede.
- **Nome de usuário/Senha/Confirmar senha**: insira as credenciais apropriadas vPro para retornar detalhes do ativo de hardware sobre máquinas vPro detectadas durante a varredura. Normalmente, as mesmas credenciais são definidas para todas as máquinas vPro na mesma LAN.

Caixa de diálogo Agendar varredura

Discovery > Redes > LAN Watch por rede *(página 8)* > Agendar varredura

A caixa de diálogo **Agendar varredura** agenda uma varredura de LAN Watch, em uma base recorrente, para uma rede selecionada.

> Nota: Configure os parâmetros SNMP e vPro utilizando **Editar rede** *(página 10)*.

Guia Agendamento de varredura

- **Recorrência**: agenda uma varredura periodicamente. Cada tipo de recorrência (Uma vez, Horária, Diariamente, Semanalmente, Mensalmente) exibe opções adicionais apropriadas ao respectivo tipo. A programação periódica inclui definir as datas inicial e final para a recorrência.
- **O agendameto se baseará no fuso horário do agente (e não no fuso horário do servidor)**: se selecionado, o conjunto de configurações de hora na caixa de diálogo Agendador faz referência ao horário local na máquina do agente para determinar quando executar esta tarefa. Se em branco, as definições de hora indicam a hora do servidor, com base na opção de hora do servidor selecionada em Sistema > Preferências. Padrões da página Sistema > Configurações padrão.
- **Ignorar se não estiver conectado** - Se estiver selecionada e a máquina estiver desconectada, ignora e executa o próximo período e hora programados. Se estiver em branco e a máquina desconecta, executa a tarefa assim que a máquina estiver conectada novamente.
- **Alimentação está off-line** - somente Windows. Se selecionado, inicia a máquina se off-line. Requer o Wake-On-LAN ou vPro ou outro sistema gerenciado na mesma LAN.

Verificar parâmetros

- **Agente de verificação**: atribui a máquina do agente usada para fazer a varredura da rede. Esta atribuição sobrepõe a configuração padrão na guia **Guia Agentes da rede** *(página 12)*, mas somente para esta varredura agendada.
- **Intervalo de IP**: especifica o intervalo de endereços IP a incluir em uma varredura. Por padrão, todo o intervalo da varredura configurado para uma rede é especificado. Exemplo: 192.168.32-35.0-255. Somente intervalos individuais de IP são compatíveis.
- **Exclusões de IP**: especifica um intervalo de endereços IP a serem excluídos da varredura. Intervalos múltiplos de IP separados por vírgulas são compatíveis. Exemplo: 192.168.32-35.0-255, 10.10.14-15.0-255. Por padrão, este campo fica em branco.
- **Endereços de e-mail**: atribui o endereço de e-mail usado para alertas do **Discovery**. Esta atribuição sobrepõe a configuração padrão na guia **Guia Perfis de alertas** *(página 14)*, mas somente para esta varredura agendada.

Guia Agentes da rede

Discovery > Redes > LAN Watch por rede > Guia Agentes de rede

A guia **Agentes de rede** exibe as máquinas do agente detectadas em uma rede. Somente máquinas do agente na mesma rede da rede selecionada são exibidas nesta tabela.

Colunas de tabela

- **(Status da entrada)**): Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **ID Machine.Group ID**: Nome de **ID de máquina/ID de grupo/ID de organização** *(página 71)* exclusivo para uma máquina no VSA.

- **Status** - O status de uma varredura. Uma varredura progride através dos seguintes status. Estes status são exibidos em Procedimentos pendentes e **Histórico de procedimentos**. Se a varredura não falha, o status retorna para `ReadyToScan` quando a varredura é concluída.
  - 0 - `ReadyToScan`: varredura ainda não iniciada.
  - 1 - `Installing`
  - 2 - `PerformingQuickScan`
  - 3 - `CompletedQuickScan`
  - 4 - `PerformingDeepScan`
  - 5 - `DNSScan`
  - 6 - `Failed`
- **Nome DNS**: o nome de domínio totalmente qualificado usado para identificar um computador ou dispositivo na rede.
- **Última entrada**: a última vez que este agente do computador entrou no VSA.
- **Verificação preferida**: se marcado, o **Discovery** tenta usar este computador para a varredura primeiro se o agente estiver ativo no momento em que a varredura ocorrer. Se o agente para este computador está inativo no momento em que a varredura é executada, outra máquina do agente na mesma LAN é selecionada aleatoriamente para executar a varredura.

Guia Agendamentos de varredura

Discovery > Redes > LAN Watch por rede > Guia Agendamentos de varredura

A guia **Agendamento de varreduras** mantém os agendamentos recorrentes de varredura para uma rede selecionada.

Ações

- **Editar**: adiciona ou edita um **agendamento de varredura** *(página 11)* selecionado para uma rede selecionada.
- **Excluir**: exclui um agendamento de varredura selecionado.

Colunas de tabela

- **Tipo**: o período de tempo recorrente: `Hourly`, `Daily`, `Weekly`, `Monthly`.
- **Próxima varredura**: a data/hora em que uma próxima varredura está agenda.
- **Faixa de varredura**: o intervalo de endereços IP a ser incluído em uma varredura.
- **Excluir faixa**: o intervalo de endereços IP a ser excluído da varredura.
- **E-mail de alerta**: se não estiver em branco, o endereço de e-mail utilizado para alertas do **Discovery** para esta varredura agendada. Se em branco, a configuração padrão na guia **Guia Perfis de alertas** *(página 14)* é utilizada.

Guia Implementação do agente

Discovery > Redes > LAN Watch por rede > Guia Implementação do agente

Guia Políticas de implementação de agentes

A guia **Políticas de implementação de agentes** da página **LAN Watch por rede** define as políticas para implementação de agentes em computadores detectados em uma rede selecionada. Para cada tipo de sistema operacional — para Windows, Mac e Linux — configure o seguinte:

- **Instalar agentes automaticamente para máquinas <do tipo de SO>** : marque para habilitar.
- **Pacote padrão**: para cada tipo de SO, selecione um pacote de instalação do agente apropriado do SO.
- **Agente implementador designado**: uma máquina do agente na mesma rede usada para implementar o agente.

- **Nome de usuário/Senha/Confirmar senha**: insira uma credencial do administrador que habilita a instalação remota de um agente.

As políticas que você configurar também servem como padrões ao implementar um agente *manualmente* utilizando:

- **Dispositivos detectados - Visualização em grade** *(página 19)*
- **Dispositivos detectados - Visualização lado a lado** *(página 21)*
- **Resultados de varredura** *(página 15)*

Requerimento de tipo de SO correspondente

Qualquer tipo de SO de computador que pode dar suporte a um agente pode ser usado para fazer a varredura de uma rede: Windows, Mac ou Linux. Se um agente é implementado, o **Discovery** automaticamente é alterado, se necessário, para uma máquina do tipo de SO correspondente na mesma LAN. Já que cada tipo de SO somente pode implementar agentes em máquinas de destino que correspondem a seu próprio tipo de SO, você deve instalar manualmente, ao menos, um agente de cada tipo de SO — Windows, Mac e Linux — em uma LAN para implementar agentes automaticamente para todos os três tipos de sistemas operacionais.

Credencial do administrador

A credencial especificada deve ter direitos de administrador na máquina remota selecionada.

- **Se a máquina de destino estiver em um domínio**, a credencial do administrador deverá usar o formato `domain\administrator` ou `administrator@domain`.
- **Se a máquina de destino não estiver em um domínio**, a credencial do administrador poderá requerer o formato `local\administrator` ou `<hostname>\administrator`.
- **Se a máquina de destino for uma máquina Linux**, o nome de usuário `root` sozinho — sem um nome de host ou domínio — deverá ser usado.

Solução de problemas

- Consulte Falhas e problemas de instalação para problemas e falhas gerais de instalação do agente.
- Consulte a **base de conhecimento** *(https://helpdesk.kaseya.com/entries/34435416)* da Kaseya para ver solução de problemas e falhas específicas para implementar agentes utilizando o **Discovery**.

Guia Perfis de alertas

Discovery > Redes > LAN Watch por rede > Guia Perfis de alerta

Guia Perfis de alerta

A guia **Perfis de alerta** da **LAN Watch por rede** define as políticas de alerta do **Discovery** para uma LAN selecionada e um tipo de dispositivo: computador, móvel, rede e firewall.

> **Nota:** A caixa de seleção **Alertas ativos** na caixa de diálogo **Editar** habilita e desabilita alertas do **Discovery** configurados nesta guia para uma rede selecionada.

Ações

- **Configurar**: edita as configurações do perfil de alerta da rede e da verificação exibidas nesta guia.

Perfil

- **Rede**: o nome da LAN que está sendo configurada.
- **Tipo de dispositivo**: o tipo dos alertas do dispositivo que estão sendo configurados: por exemplo, computador, aparelho móvel, rede, firewall.
- **Novo dispositivo**: se um novo dispositivo é detectado para o tipo de dispositivo selecionado:

  - **Alarme**: se marcado, crie um alarme.
  - **Ticket**: se marcado, crie um ticket.
  - **E-mail**: se marcado, notifique os destinatários de e-mail nos **Endereços de e-mail**.
  - **Agente**: executa um procedimento do agente selecionado na máquina especificada do agente. Se o dispositivo detectado é um computador, deixe em branco para executar o procedimento do agente no computador detectado.
  - **Procedimento**: especifique o procedimento do agente a ser executado.
- **Novo IP dispositivo**: se o endereço IP associado a um endereço MAC existente mudar:
  - **Alarme**: se marcado, crie um alarme.
  - **Ticket**: se marcado, crie um ticket.
  - **E-mail**: se marcado, notifique os destinatários de e-mail nos **Endereços de e-mail**.
- **Endereço de e-mail**: especifica um ou mais endereços de e-mail, delimitados por vírgula.

Guia Promoção de ativos

Discovery > Redes > LAN Watch por rede > Guia Promoção de ativos

Guia Promoção de ativos

A guia **Promoção de ativos** da página **LAN Watch por rede** configura a promoção automática de dispositivos a ativos quando os dispositivos são detectados.

Quando um agente não pode ser instalado em um dispositivo detectado, o dispositivo pode ser "promovido" para um ativo gerenciado. Por exemplo, um roteador ou uma impressora ainda pode exigir monitoramento, mesmo que não seja possível instalar um agente na máquina.

Todos os ativos gerenciados devem ser atribuídos a um grupo de máquinas e organização. **As regras de escopo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4578.htm)* e os recursos de **filtragem de visualização** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#214.htm)* dentro do VSA dependem desta atribuição.

Um dispositivo detectado pode ser promovido ou rebaixado manualmente na página **LAN Watch por rede** *(página 8)* ou **LAN Watch por verificação** *(página 18)* ao alternar o ícone /.

- **Regra de promoção automática de ativos**: especifica quais ativos detectados, aqueles que não podem ser instalados com um agente, devem ser promovidos automaticamente a um ativo gerenciado.
  - **Todos**
  - **Nenhum**
  - **Faixa endereço IP**
- **Grupo padrão**: seleciona o grupo de máquinas e organizações a serem atribuídas para dispositivos detectados para um ativo gerenciado.
  - **Grupo selecionado**: seleciona um grupo de máquinas e organizações fixo.
  - **Usar verificação**: utiliza o grupo de máquinas e organizações da máquina de verificação. Este é o padrão.
  - **Raiz padrão**: utiliza o grupo de máquinas padrão da organização associada com esta LAN.

Resultados de varredura

Discovery > Redes > LAN Watch por rede > ícone
Discovery > Redes > LAN Watch por verificação > ícone

Resultados de varredura

A janela **Resultados da varredura** exibe os resultados da varredura mais recente para uma rede. A mesma janela é exibida ao clicar no ícone em duas páginas diferentes.

- Clique no ícone para uma rede na página **LAN Watch por rede** *(página 8)*.
- Clique no ícone para uma máquina do agente na página **LAN Watch por verificação** *(página 18)*.

Nota: Pode haver um atraso na exibição desta página se uma varredura de rede estiver em andamento.

A janela **Resultados da varredura** tem duas guias.

- Guia Resumo
- Guia Dispositivos

Guia Resumo

Ações

- **Implementar agentes**: implementa um agente em todos os computadores sem agentes encontrados no *painel inferior*.

(Painel superior)

O *painel superior* desta guia mostra contagens para a *varredura mais recente em uma rede.*

- **Dispositivos AIL encontrados**: o número total de dispositivos encontrados pela varredura.
- **Classificados**: o número total de dispositivos que foram classificados.
- **Computadores não gerenciados**: o número total de dispositivos que não são ativos. Este pode incluir máquinas e dispositivos móveis e dispositivos promovidos a ativos.

Os endereços IP usados por esta rede são listados no canto superior direito.

(Painel inferior)

O *painel inferior* desta guia mostra contagens para *cada tipo de dispositivo encontrado por todas as varreduras em uma rede*. Ao clicar na contagem de qualquer tipo de dispositivo, todos os membros daquela contagem são exibidos na guia **Dispositivos** em formato lado a lado. Consulte

- **Computadores**: por sistema operacional.
- **Móvel**: por tipo de dispositivo.
- **Rede**: por tipo de dispositivo.
- **Impressora**
- **Sem Classificação**
- **Servidor virtual**: por tipo de servidor virtual.

(Informações da verificação)

- **Nome da rede**: o nome amigável atribuído pelo VSA para identificar uma rede.
- **IP da verificação**: endereço IP da máquina de verificação.
- **Máscara de sub-rede**: máscara de sub-rede da máquina de verificação.
- **Gateway padrão**: gateway padrão da máquina de verificação.
- **Servidor DNS**: servidor DNS para a máquina de verificação.
- **Servidor Wins**: servidor WINS para a máquina de verificação.

Guia Dispositivos

Cada bloco nesta guia exibe um resumo de informações sobre um dispositivo. Um bloco pode incluir os seguintes ícones:

- Clique para exibir dados de varredura NMAP.

- Somente é exibido caso um agente esteja instalado. Passe o mouse sobre este ícone para exibir a janela **Visualização rápida** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#9339.htm)*.

Clique para executar o **Live Connect** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4796.htm)*.

 - Somente é exibido caso um agente esteja instalado. O número de alarmes criados para este dispositivo ou computador. Clique para exibir a página **Resumo de alarmes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4112.htm)* para este dispositivo.

 - Somente é exibido se um agente é atribuído a um conjunto de monitores ou se um dispositivo SNMP é atribuído a um conjunto SNMP. Clique para exibir o dashlet **Status da máquina** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2803.htm)* ou o dashlet **Status do dispositivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2817.htm)*.

 - Passar o mouse sobre um bloco exibe um ícone de lápis. Você pode editar o nome de uma máquina ou dispositivo detectado.

Ações

- **Implementar agentes**: implementa um agente para todos os computadores nesta guia que não têm um agente instalado. A filtragem limita o agente implementado nos blocos mostrados.

Configurações de filtros de dispositivos

- **Dispositivo**: filtra a exibição dos dispositivos por ID do dispositivo. Insira o *início* de uma sequência para encontrar todas as IDs de dispositivos que correspondam àquela sequência. Inclua um asterisco no início de uma sequência para encontrar todos os dispositivos que correspondam àquela sequência em qualquer lugar na ID do dispositivo. Por exemplo, inserir a sequência `*ABC` corresponde a todas IDs de dispositivos que incluem ABC em qualquer lugar na sua ID do dispositivo.
- **Tipo**: filtra a exibição por tipo de dispositivo:
  - `Computer`
  - `Mobile`
  - `Network`
  - `Power`
  - `Printer`
  - `Unclassified`
  - `Virtual Server`
- **Redefinir**: limpa o filtro dos dispositivos.
- **(Seletor de dados)**: quando se seleciona mais linhas de dados do que podem ser exibidas em uma única página, clique nos botões  e  para exibir a página anterior e seguinte.
- **(Linhas por página)**: Selecione o número de linhas exibidas por página.
- **Classificar por**: ordena a exibição de dados por:
  - `Name`
  - `IP Address`
  - `Device Type`
- **Ativos**: se marcado, exibe Visualizar ativos.
- **Não gerenciados**: se marcado, exibe os dispositivos sem um agente.
  - Se tanto **Ativos** quanto **Não gerenciados** estiverem *em branco*, somente os blocos de *agentes* serão exibidos.
  - Se tanto **Ativos** quanto **Não gerenciados** estiverem *selecionados*, *todos os dispositivos detectados* serão exibidos.
  - Se **Ativos** estiver em branco e **Não gerenciados** estiver selecionado, então, somente *não-ativos* será exibidos.
  - Se **Ativos** estiver selecionado e **Não gerenciados** estiver em branco, então, somente *ativos* serão exibidos.

LAN Watch por verificação

Discovery > Redes > LAN Watch por verificação

A página **LAN Watch por verificação** detecta dispositivos na mesma LAN como uma máquina de *verificação*. Estes dispositivos podem ser estações de trabalho e servidores sem agentes, Dispositivos SNMP e máquinas vPro. Os dispositivos detectados são exibidos nas seguintes páginas:

- **Dispositivos detectados - Visualização em grade** *(página 19)*
- **Dispositivos detectados - Visualização lado a lado** *(página 21)*

Como utilizar LAN Watch por verificação

1. Selecione uma ou mais IDs de máquina.

   Nota: Máquinas com Windows XP não são recomendadas como máquinas de verificação. NMAP é mais confiável com sistemas operacionais Windows posteriores.

2. Agende uma varredura uma vez ou em uma base recorrente utilizando o botão **Agendar varredura**, ou execute uma varredura imediatamente utilizando o botão **Fazer varredura agora**.
   - Opcionalmente, busque dispositivos SNMP e máquinas habilitadas com vPro utilizando a caixa de diálogo **Agendar varredura**.
   - Uma varredura pode ser atribuída a diversas IDs de máquina.

Ações

- **Editar**: exibe **Editar rede** *(página 10)*. Configura as opções de varredura utilizadas por **Fazer varredura agora**. As mesmas configurações servem como as configurações padrão exibidas pela caixa de diálogo **Agendar varredura**.
- **Agendar varredura**: exibe a caixa de diálogo **Caixa de diálogo Agendar varredura** *(página 11)*. Agenda uma varredura LAN Watch, de maneira recorrente, para uma rede selecionada.
- **Fazer varredura agora**: executa LAN Watch imediatamente na rede à qual a máquina do agente selecionado pertence, utilizando as opções de varredura definidas em **Editar rede** *(página 10)* da página **LAN Watch por rede**.
- **Ignorar**: evita que seja feita a varredura de uma rede.
- **Deixar de ignorar**: reabilita a varredura de uma rede que foi ignorada anteriormente.
- **Atualizar**: atualiza a página.

Colunas de tabelas

- **(Status da entrada)**): Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- : clique neste ícone para exibir os **resultados da varredura mais recente e os resultados acumulados de todas as varreduras anteriores** *(página 15)*.
- **Detecção de rede**
  - - A rede pronta para receber a varredura.

 - A rede é ignorada da varredura.

- **ID Machine.Group ID**: Nome de **ID de máquina/ID de grupo/ID de organização** *(página 71)* exclusivo para uma máquina no VSA.
- **Endereço IP**: o endereço IP da máquina de verificação.
- **Endereço MAC**: o endereço MAC da máquina de verificação.
- **Gateway padrão**: o gateway padrão da máquina de verificação.
- **Nome da rede**: o nome amigável atribuído pelo VSA para identificar uma rede.
- **Status da varredura**: O status de uma varredura. Uma varredura progride através dos seguintes status. Estes status são exibidos em Procedimentos pendentes e **Histórico de procedimentos**. Se a varredura não falha, o status retorna para `ReadyToScan` quando a varredura é concluída.
  - 0 - `ReadyToScan`: varredura ainda não iniciada.
  - 1 - `Installing`
  - 2 - `PerformingQuickScan`
  - 3 - `CompletedQuickScan`
  - 4 - `PerformingDeepScan`
  - 5 - `DNSScan`
  - 6 - `Failed`
- **Faixa de varredura**: o intervalo de endereços IP analisado pela ID da máquina selecionada quando LAN Watch é executado.
- **Próxima varredura**: a data/hora em que uma próxima varredura está agenda.
- **Última varredura**: a data/hora da última execução de uma varredura.
- **SNMP Ativa**: se marcado, o dispositivo tem funcionalidade SNMP, embora ela possa não estar habilitada.

Dispositivos detectados - Visualização em grade

Discovery > Redes > Dispositivos detectados - Visualização em grade

A página **Dispositivos detectados - Visualização em grade** mostra os computadores e dispositivos detectados utilizando **LAN Watch por verificação** *(página 18)* e **LAN Watch por rede** *(página 8)*. Utilize esta página para instalar os agentes em dispositivos móveis e computadores detectados. Você também pode tornar dispositivos detectados em um ativo gerenciado, mesmo que eles não possam ser instalados com o agente.

Os resultados são mostrados em formato de tabela. Essa tabela é compatível com **colunas selecionáveis, classificação de coluna, filtragem de coluna e larguras de colunas flexíveis** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#6875.htm)*.

Ações

- **Visualizar** : exibe uma janela pop-up de informações coletadas sobre um dispositivo selecionado. Visualizações diferentes, baseadas no tipo de verificação usada para coletar as informações, podem ser selecionadas usando a lista suspensa **Tipo de verificação**
  - `NMAP Probe` - O método padrão de detecção de um dispositivo na rede, utilizando o módulo do **Discovery**.
  - `Machine Audit` - A auditoria realizada na máquina instalada com um agente.
  - `vPro` - O inventário de atributos de hardware retornado por uma auditoria vPro. Uma máquina vPro deve ser habilitada, e uma varredura deve incluir uma credencial vPro para retornar atributos de hardware vPro de uma máquina. Consulte **Editar rede** *(página 10)* e a guia vPro para mais informações.

  - `Merge View` - Mescla todos os métodos de coleta de dados em uma visualização consolidada. A visualização padrão.
- **Implementar agente**: instala um agente em uma máquina detectada selecionada. Consulte os **pré-requisitos de implementação de agente** *(página 13)*.
- **Excluir**: exclui a linha de um dispositivo ou máquina detectada. Por exemplo, um dispositivo móvel pode se "encontrado" em uma rede durante uma varredura, mas somente residir lá de modo temporário. Ele continuará a ser listado nas páginas **Dispositivos detectados** até que a linha seja excluída.
- **Ignorar**: evita que uma máquina ou dispositivo detectado seja incluído em varreduras subsequentes. Você pode remover o status ignorado ao excluir a linha. Na próxima vez que for realizada uma varredura da rede, ele será detectado novamente como um novo dispositivo.
- **Mesclar**: mescla duas ou mais linhas selecionadas que referenciam a mesma máquina ou dispositivo. Alguns dispositivos e máquinas têm múltiplos endereços IP. Clique em **Mesclar** para exibir uma caixa de diálogo. Selecione a linha que você deseja manter, então, clique em **Mesclar** dentro da caixa de diálogo para completar a mescla e remover as linhas duplicadas.
- **Renomear dispositivo**: renomeia um computador ou dispositivo detectado dentro do VSA.
- **Criar ativo**: designa manualmente um dispositivo sem um agente como um ativo gerenciado. Todos os computadores e dispositivos móveis com agentes instalados neles são, necessariamente, ativos gerenciados. Um dispositivo incapaz de dar suporte a um agente, tal como um roteador ou uma impressora, pode necessitar de monitoramento e, portanto, ser designado como um ativo gerenciado. Todos os dispositivos e computadores gerenciados são exibidos na página Visualizar ativos.
- **Alterar tipo**: altera um dispositivo ou computador para outro tipo de dispositivo. Isto pode ser necessário para implementar um agente com sucesso em um computador que foi digitado incorretamente.

Colunas de tabela

- **(Elegível para implementar agente)**: se marcado, este dispositivo pode instalar um agente.
- **(Status do dispositivo)**
  -  - Somente é exibido caso um agente esteja instalado. Passe o mouse sobre este ícone para exibir a janela **Visualização rápida** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#9339.htm)*. Clique para executar o **Live Connect** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4796.htm)*.
  -  /  : se habilitado, este dispositivo sem agente foi **promovido para um ativo** *(página 15)*.
- **Nome do dispositivo**: um único nome da ID da organização/ID do grupo/ID da máquina para um dispositivo ou máquina no VSA.
- **Nome detectado**: o nome do computador ou dispositivo atribuído pelo seu próprio sistema operacional ou hardware.
- **Endereço IP**: o endereço IP do dispositivo ou máquina detectada.
- **Endereço MAC**: o endereço MAC do dispositivo ou máquina detectada.
- **Tipo de dispositivo**: o tipo de dispositivo ou máquina.
- **Visto pela última vez**: a última vez que este dispositivo ou esta máquina foi detectada pelo LAN Watch.
- **Nome da rede**: o nome amigável atribuído pelo VSA para identificar uma rede.

  > **Nota:** A frase `Unscanned Network` é exibida neste campo para máquina que já são "conhecidas" no VSA por terem um agente instalado, mas que ainda não foram incluídas em uma varredura do **Discovery**.

- **Resultados da varredura NMAP**: clique no ícone nesta coluna para exibir dados de varreduras NMAP para este dispositivo.

- **Verificação primária**: a verificação primária que detectou este dispositivo ou esta máquina por último.
- **Tipo de verificação**: o tipo de verificação usada para detectar este dispositivo.
- **SO**: o sistema operacional do dispositivo ou da máquina detectada.
- **Precisão do SO**: a precisão provável de identificar o sistema operacional corretamente.
- **Fabricante**: o fabricante do dispositivo.
- **SNMP Ativa**: se marcado, o dispositivo tem funcionalidade SNMP, embora ela possa não estar habilitada.
- **Agente do computador**: se marcado, um agente já está instalado nesta máquina.
- **Agente móvel**: se marcado, este dispositivo é um dispositivo móvel.
- **Ativo**: se marcado, este dispositivo já está sendo gerenciado e é exibido na página Visualizar ativos.
- **Ignorar**: se marcado, não continua a fazer a varredura deste dispositivo.
- **Tentativa de implementação**: a hora/data em que uma implementação do agente foi tentada.
- **Status da implementação**: o status da implementação do agente. Revise mensagens de erro utilizando esta coluna. Consulte os **pré-requisitos de implementação de agente** *(página 13)*.
- **Máquina vPro**: se marcado, a máquina é uma máquina habilitada para vPro. Consulte **Editar rede** *(página 10)* para obter mais informações sobre máquinas habilitadas para vPro.

Dispositivos detectados - Visualização lado a lado

Discovery > Redes > Dispositivos detectados - Visualização lado a lado

A página **Dispositivos detectados - Visualização lado a lado** mostra os computadores e dispositivos detectados utilizando **LAN Watch por rede** *(página 8)* e **LAN Watch por verificação** *(página 18)*. Os resultados da varredura são *cumulativos* de todas as máquinas de verificação. Um registro não é removido até que você o exclua.

Formato de visualização lado a lado

A visualização lado a lado exibe cada dispositivo em seu próprio bloco. Um bloco pode incluir os seguintes ícones:

-  - Clique para exibir dados de varredura NMAP.
-  - Somente é exibido caso um agente esteja instalado. Passe o mouse sobre este ícone para exibir a janela **Visualização rápida** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#9339.htm)*. Clique para executar o **Live Connect** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4796.htm)*.
-  /  - Alternar este ícone manualmente **promove ou rebaixa um dispositivo sem agente para um ativo** *(página 15)*.
-  - Somente é exibido caso um agente esteja instalado. O número de tickets criados para este computador. Clique para exibir os tickets em uma tabela de tickets.
-  - Somente é exibido caso um agente esteja instalado. O número de alarmes criados para este dispositivo ou computador. Clique para exibir a página **Resumo de alarmes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4112.htm)* para este dispositivo.
-  - Somente é exibido se um agente é atribuído a um conjunto de monitores ou se um dispositivo SNMP é atribuído a um conjunto SNMP. Clique para exibir o dashlet **Status da máquina** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2803.htm)* ou o dashlet **Status do dispositivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2817.htm)*.
- - Passar o mouse sobre um bloco exibe um ícone de lápis. Você pode editar o nome de uma máquina ou dispositivo detectado.

Ações

- **Implementar agentes**: implementa um agente para todos os computadores nesta guia que não têm um agente instalado. A filtragem limita o agente implementado nos blocos mostrados.
- **Implementar agente por endereço**: implementa agentes para endereços IP4 que não foram detectados.
  - **Agente de**: uma máquina do agente na mesma rede usada para implementar o agente.
  - **Tipo de SO**: implementação para Windows, Mac ou Linux.
  - **Endereço**: um endereço IP4. Delimite múltiplos endereços IP com vírgulas.
  - **Nome de usuário/Senha**: um nome de usuário e senha de nível de administrador. Para credenciais de domínio, utilize o formato `domain\username`.

Configurações de filtros de dispositivos

- **Dispositivo**: filtra a exibição dos dispositivos por ID do dispositivo. Insira o *início* de uma sequência para encontrar todas as IDs de dispositivos que correspondam àquela sequência. Inclua um asterisco no início de uma sequência para encontrar todos os dispositivos que correspondam àquela sequência em qualquer lugar na ID do dispositivo. Por exemplo, inserir a sequência `*ABC` corresponde a todas IDs de dispositivos que incluem ABC em qualquer lugar na sua ID do dispositivo.
- **Tipo**: filtra a exibição por tipo de dispositivo:
  - `Computer`
  - `Mobile`
  - `Network`
  - `Power`
  - `Printer`
  - `Unclassified`
  - `Virtual Server`
- **Rede**: o nome e o intervalo de IP de uma rede selecionada.
- **Redefinir**: limpa o filtro dos dispositivos.
- **(Seletor de dados)**: quando se seleciona mais linhas de dados do que podem ser exibidas em uma única página, clique nos botões  e  para exibir a página anterior e seguinte.
- **(Linhas por página)**: selecione o número de linhas exibidas por página.
- **Classificar por**: ordena a exibição de dados por:
  - `Name`
  - `IP Address`
  - `Device Type`
- **Ativo**: se marcado, exibe os **Ativos** *(página 6)*.
- **Não gerenciados**: se marcado, exibe os dispositivos sem um agente.
  - Se tanto **Ativos** quanto **Não gerenciados** estiverem *em branco*, somente os blocos de *agentes* serão exibidos.
  - Se tanto **Ativos** quanto **Não gerenciados** estiverem *selecionados*, *todos os dispositivos detectados* serão exibidos.
  - Se **Ativos** estiver em branco e **Não gerenciados** estiver selecionado, então, somente *não-ativos* será exibidos.
  - Se **Ativos** estiver selecionado e **Não gerenciados** estiver em branco, então, somente *ativos* serão exibidos.

Capítulo 2

Domain Watch

Neste capítulo

Como começar a usar o Domain Watch

Discovery no servidor da Kaseya utiliza um agente de verificação em um computador do domínio para se comunicar com o domínio Active Directory (AD). Quando conectado, a verificação leva os dados de domínio coletados de volta para o servidor da Kaseya.

- Os agentes são implementados nas máquinas do domínio utilizando um objeto de política do grupo para fazer download do pacote de instalação do agente.
- VSA os usuários podem utilizar a credencial de domínio deles para fazer logon no VSA.
- Os usuários do Portal Access podem usar as suas credenciais de domínio para fazer logon remotamente em suas máquinas.
- O protocolo de aplicativos utilizado para se comunicar com o servidor de domínio é o Lightweight Directory Access Protocol (LLDAP).
- Consulte **Contêiner/UO** *(página 72)* para mais informações sobre "unidades organizacionais".

Os seguintes tópicos fornecem o procedimento detalhado para configurar o **Discovery**.

- **Pré-requisitos da página de domínios** *(página 35)*
- **Como configurar a implementação da verificação** *(página 36)*
- **Como configurar a implementação do agente** *(página 37)*
- **Como configurar políticas do contêiner/UO** *(página 38)*
- **Como configurar políticas do computador** *(página 39)*
- **Como configurar políticas de contato** *(página 39)*
- **Como configurar políticas de grupo** *(página 40)*
- **Como configurar políticas de usuário** *(página 42)*
- **Como configurar políticas de alerta** *(página 43)*
- **Como configurar status e agendamento** *(página 43)*

Estes tópicos adicionais fornecem uma visão geral dos conceitos do **Discovery**.

Como gerenciar um modelo de segurança sincronizado

Um dos benefícios da sincronização do VSA com o domínio é que a hierarquia de pastas e itens do domínio — domínios, unidades organizacionais/contêineres, computadores grupos, usuários e contatos — é "detectada" automaticamente para criar e manter um modelo de segurança similar no VSA: organizações, grupos de máquinas, máquinas, usuários, escopos, funções e integrantes. Os provedores de serviços não precisam inserir os mesmos dados uma segunda vez no VSA. Por exemplo, os dados do usuário, tais como e-mail, telefone e outras informações de contato, somente precisam ser atualizados no domínio para atualizar os campos correspondentes no VSA.

O modelo de segurança criado no VSA pela integração do **Discovery** com o domínio Active Directory resulta no seguinte mapeamento de objetos.

Directory Sync - Kaseya Structure reflects AD Structure

Active Directory Object	Maps To	Kaseya Object
Domains	→	Organizations
OUs/ Containers	→	Machine Groups & Departments
Users	→	Users & Related Staff Members
Contacts	→	Staff Members
Computers	→	Agents
Groups	→	Roles & Scopes

Como gerenciar domínios múltiplos

O **Discovery** fornece acesso consolidado por todo o VSA até os computadores, usuários e contatos do domínio gerenciado do **Discovery**, independentemente de estes domínios terem um relação de "confiança" entre eles. Por exemplo, o **Discovery** pode fornecer uma visualização consolidada dos domínios de uma companhia principal e uma companhia subsidiária.

Cada domínio gerenciado do **Discovery** é associado a uma organização única dentro do VSA.

- Um escopo correspondendo ao nome da organização é criado. Se você quiser, pode adicionar diversas organizações ao mesmo escopo. Isso permite que o usuário do VSA use um escopo individual para ter visibilidade de todos os grupos de máquinas em diversas organizações.
- O filtro ID de máquinas/ID de grupos permite que você filtre a exibição de máquinas por propriedade de máquina, grupo de máquinas ou organização.

Como gerenciar o Portal Access remoto

Discovery define as políticas que permitem o usuário utilizar suas credenciais de domínio para fazer logon remotamente em suas máquinas utilizando o Portal Access. O acesso remoto utilizando o Portal Access pode ser feito de dentro ou fora do firewall da companhia. Por exemplo, o usuário do Portal Access pode desejar acessar seu computador do escritório em sua casa.

Licenciamento

Discovery domínios são licenciados separadamente das licenças do agente. **Discovery** as contas de licença do domínio são exibidas na guia **Licenças** da página Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm)*.

Um domínio gerenciado do **Discovery** é um domínio anexado a uma organização. Um domínio é anexado a uma organização quando *ativado* utilizando a guia Domínios > Domain Watch > **Implementação de verificação** *(página 46)*. Um domínio gerenciado pode estar em um dos seguintes estados de licença:

- **Sem licença**: o **Discovery** está instalado e visível no VSA, mas nenhum domínio está licenciado.
- **Licenciado**: um número suficiente de licenças existe para os domínios sendo gerenciados.
- **Excedido**: outro domínio não pode ser instalado pois o número máximo de domínios foi instalado.
- **Expirado**: o **Discovery** foi desabilitado pois a licença do módulo inteiro expirou.

O conjunto de recursos do Directory Services

Directory Services 1.2 é um **conjunto de recursos** *(página 69)*, licenciado separadamente, que fornece funcionalidades avançadas no módulo **Discovery**.

Políticas de domínio	As políticas de domínio podem ser especificadas para diversas máquinas e usuários por: • OU/contentores • Grupos
Ativação/desativação de Sincronização incremental	Fornece detecção e sincronização incrementais de dados do controlador de domínio. Sem o Directory Services 1.2 somente detecção e sincronização completas é compatível. Os botões Ativação e Desativação são exibidos na página Domain Watch > Implementação da verificação, Como habilitar e desabilitar a detecção e sincronização incrementais.
Acesso automático ao portal	Cria acesso ao portal automaticamente para uma máquina, com base na última pessoa que se conectou à máquina.
Contatos	Detecta e sincroniza contatos do domínio e registros de pessoal do VSA. Um contato de domínio contém informações similares a um usuário de domínio, mas um contato não tem privilégios de logon ao domínio. Directory Services 1.2 permite que você configure políticas que criem registros de membros da equipe do VSA para contatos recém detectados em um domínio e mantenha os dois registros sincronizados entre si. Criar um registro dos membros utilizando uma política do Directory Services também cria uma hierarquia dos departamentos que reflete a hierarquia do contêiner/UP no domínio.
Usuários	• Habilita e desabilita logons no domínio a partir do módulo Directory Services. • Redefine as senhas do domínio. • Desbloqueia as contas do domínio.
Alertas	Fornece alertas para computadores novos ou alterados, contatos, UO/contêineres, domínios, grupos, organizações ou usuários.

Como definir políticas do Discovery

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Discovery as políticas podem ser definidas para três tipos de objetos do domínio:

Como definir políticas do Discovery para computadores

As seguintes políticas de *computador* do **Discovery** podem ser definidas por UO/contêiner ou computador individual. A definição de uma política por computador tem precedência sobre a definição de uma política por UO/contêiner.

- Implementação automática de agentes em máquinas recentemente detectadas.
- Implementação manual de agentes em máquinas selecionadas.
- Implementação do agente no sistema que hospeda o domínio Active Directory.
- Designando todas as máquinas ou máquinas selecionadas como **candidatos ao portal** *(página 29)*.

Criar uma conta de ID da máquina utilizando uma política do **Discovery** também cria uma hierarquia do grupo de máquinas para a nova conta da ID máquina que reflete a hierarquia do contêiner/UO no domínio.

Discovery as políticas do computador são definidas utilizando a guia Domínios > Domain Watch > Políticas > **OU/Containers** *(página 49)* ou guia **Computadores** *(página 51)*.

Como definir políticas para computadores

As seguintes políticas de *contato* do **Discovery** podem ser definidas para cada contêiner/UO no domínio.

- Criação automática de registros dos integrantes do VSA para todos os contatos de domínios recentemente detectados.
- Criação manual de registros dos integrantes do VSA para todos os contatos do domínio selecionado em um contêiner/UO.

Criar um registro dos membros utilizando uma política do **Discovery** também cria uma hierarquia dos departamentos que reflete a hierarquia do contêiner/UP no domínio.

Discovery as políticas de contato são definidas utilizando a guia Domínios > Domain Watch > Políticas > **OU/Containers** *(página 49)*.

Como definir políticas do Discovery para usuários

Discovery pode criar usuários do VSA e usuários do Portal Access com base nos usuários do domínio. Isto significa que os administradores de TI podem fornecer aos seus usuários a mesma credencial para aqueles aplicativos e gerenciar a autenticação e autorização de uma localização individual, utilizando o domínio Active Directory.

As seguintes políticas de *usuário* do **Discovery** podem ser definidas por grupo (usuário) ou por usuário individual.

1. `Do Not Include Users` - Não criar logons de usuário do VSA ou logons de Portal Access para usuários do domínio listados nesse grupo de usuários.
2. `Create Staff Members` : cria um registro do membro da equipe. É possível atribuir a estes usuários acesso Portal Access a uma máquina *manualmente*.
3. `Create Staff and make Auto Portal Candidates` : designa usuários de domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
4. `Create VSA Users` - Cria logons do usuário do VSA para usuários do domínio listados neste grupo.

Discovery as políticas do usuário são definidas utilizando a guia Domínios > Domain Watch >

Políticas > **Grupos** *(página 52)* ou a guia **Usuários** *(página 54)*.

Como aplicar políticas do Discovery

Quando todas as políticas do **Discovery** são definidas, as configurações são aplicadas. Alguns minutos depois, novos computadores do VSA, contatos, usuários do VSA e usuários do Portal Access são exibidos nas suas respectivas páginas do **Discovery**, na seguinte página do **Discovery**, dependendo das políticas do **Discovery** que foram aplicadas.

- **Computadores** *(página 58)*
- **Contatos** *(página 60)*
- **Usuários e Usuários do portal** *(página 62)*

Reveja os seguintes tópicos especializados para assegurar que você entende como estes novos registros do VSA são criados e quais tarefas de configuração adicionais podem ser necessárias para cada tipo de registro do VSA criado utilizando o **Discovery**.

- **Como os agentes são instalados utilizando o Discovery** *(página 27)*
- **Como as contas de ID de máquinas são criadas no Discovery** *(página 28)*
- **Como as máquinas que se movem no domínio são refletidas no Discovery** *(página 29)*
- **Como habilitar o Portal Access remoto no Discovery** *(página 29)*
- **Como habilitar/desabilitar contas dos usuários de domínio ou redefinir senhas de usuários de domínio** *(página 30)*
- **Como fazer alterações nos logons dos usuários gerenciados do Discovery** *(página 31)*
- **Formatos compatíveis de logon no domínio** *(página 31)*

Como os agentes são instalados utilizando o Discovery

Todos os agentes instalados nas máquinas de domínio utilizando o **Discovery** são instalados utilizando um único pacote de instalação do agente especificado para cada domínio.

Já que diferentes tipos de máquinas podem necessitar diferentes configurações do agente, a Kaseya recomenda especificar um pacote de instalação do agente "genérico" para instalações de agentes do **Discovery**. Altere as configurações do agente após a instalação, conforme apropriado, para cada tipo de máquina. As configurações do agente podem ser alteradas manualmente utilizando modelos de ID de máquinas e Agente > Copiar configurações ao importar as configurações do agente utilizando Agente > Importar/Exportar.O

Discovery usa dois métodos para instalar os agentes.

Método 1 - Instalação de agentes utilizando Kconnect

Se aplica tanto a instalações de rede quanto de domínios.

Este método é bem-sucedido na maioria das vezes e instala o agente imediatamente sem necessitar a reinicialização da máquina. É a mesma tecnologia utilizada pelo **LAN Watch por rede** *(página 8)* para instalar um agente remotamente. O pacote de instalação do agente é obtido por download do servidor da Kaseya para o computador de verificação do agente. O computador de verificação do agente executa um utilitário da Kaseya chamado `Kconnect.exe`. A máquina de verificação do agente usa sua credencial do domínio Active Directory para transferir o arquivo para o computador de destino e instalar o agente.

Método 2 - Instalação do agente utilizando GPO Script

Se aplica somente a instalações do domínio. Tanto o método 1 quanto o método 2 são iniciados ao mesmo tempo para uma instalação de domínio. Se uma instalação utilizando um método já tiver sido bem-sucedida, qualquer tentativa subsequente de instalar um agente será cancelada.

Este método não ocorre até que o computador de destino é reiniciado. Uma única cópia do pacote de instalação do agente para cada domínio é armazenada no sistema que hospeda o domínio Active

Directory. Um Objeto de Política de Grupo (GPO) é criado para o domínio no Active Directory. Quando um agente é implementado utilizando o **Discovery**, o GPO é atribuído para aquela máquina do domínio no Active Directory. Se um agente ainda não foi instalado na máquina do domínio, o GPO aciona uma instalação do agente na próxima vez que a máquina do domínio for reiniciada. *Se o agente é excluído da máquina do domínio, o método GPO de instalação do agente assegura que o agente seja reinstalado.*

Como atualizar o pacote de instalação no controlador de domínio

A cópia do pacote de instalação do agente no sistema que hospeda o domínio Active Directory *não* é automaticamente atualizada quando o pacote de instalação do agente é alterado. Para esta versão, atualize o pacote de instalação do agente manualmente:

1. Em Active Directory, localize Recursos > Gerenciamento da política de grupo > <floresta> > Domínios<domínio> > pasta **Objetos de política de grupo**.
2. Clique com o botão direito no objeto de política de grupo **ADAgentDeployGPO** e selecione a opção **Editar...** para abrir a caixa de diálogo **Editor de gerenciamento da política de grupo**.
3. Localize Configurações do computador > Políticas > Configurações do Windows > pasta Scripts.
4. Clique com o botão direito no script **Inicialização** e selecione a opção **Propriedades** para abrir a caixa de diálogo **Propriedades de inicialização**.
5. Selecione o script **InstallAgent.vbs** e clique no botão **Mostrar arquivos...** para exibir a janela do Windows Explorer.
6. Um arquivo `KcsSetup<number>.exe` é exibido na pasta do arquivo selecionado com um único número adicionado ao final do nome do arquivo. Por exemplo: `KcsSetup35475311.exe`.
7. Renomeie o antigo arquivo `KcsSetup<number>.exe` e o substitua pelo seu `KcsSetup.exe` atualizado.

> **Nota:** Certifique-se de renomear o arquivo `KcsSetup.exe` para o nome do arquivo exato `KcsSetup<number>.exe` que foi utilizado antes, incluindo o número único que era utilizado previamente.

As novas instalações do agente utilizando o método GPO serão agora instaladas utilizando as configurações do agente no novo pacote de instalação do agente.

> **Nota:** Ao instalar um agente na máquina de domínio do Windows XP utilizando o método GPO, as instalações podem falhar se a **Política do domínio do Centro de segurança estiver desabilitada** *(http://technet.microsoft.com/en-us/library/cc725578(WS.10).aspx)*.

Como as contas de ID de máquinas são criadas no Discovery

A criação e o agrupamento de **contas de ID de máquinas** *(página 71)* utilizando o **Discovery** depende de como as máquinas estão organizadas no domínio e se as contas de ID de máquinas já existem no VSA.

- Uma organização individual é especificada para cada domínio no **Discovery**. A organização selecionada determina a organização atribuída para as *contas da ID de máquinas recém-criadas* quando instaladas utilizando o **Discovery**.
- A hierarquia apropriada dos grupos de máquinas para uma nova conta da ID de máquinas é criada, se a hierarquia do grupo de máquinas ainda não existir, correspondendo a localização da máquina na hierarquia da UO no domínio.
- Contas de IDs de máquinas recém-criadas são inicialmente exibidas como contas modelo de ID da máquina "vazia" - identificadas com um ícone de entrada, que significa que não há agente correspondente para esta conta da ID da máquina.
- Se nenhum *agente* existir na máquina do domínio, um novo agente será instalado após a reinicialização do computador utilizando a conta da ID de máquinas recém-criada.

- Se um agente já existe em uma máquina gerenciada em um grupo de máquinas diferente, então o **Discovery** cria uma conta **modelo da ID da máquina** *(página 71)* vazia, identificada com um ícone de entrada, e nenhum agente faz entrada. A nova conta modelo da ID da máquina exibe uma **ID da organização/ID do grupo/ID da máquina** *(página 71)* com base no nome canônico do computador no domínio Active Directory. *Você pode mesclar estas contas duplicadas.* A conta do agente ativa existente adota o nome da nova conta modelo da ID da máquina, então, a nova conta modelo da ID da máquina é excluída. Nenhum dado é perdido pela mescla, e a conta da ID da máquina agora combina seu local na hierarquia do domínio.
- Selecione uma linha **Há duplicatas** na página Discovery > **Computadores** *(página 58)* e, em seguida, clique no botão **Sincronizar máquinas**.

> **Aviso:** Utilize o método **Sincronizar máquinas** para mesclar duplicatas em vez de mesclar contas utilizando a página Agente > Renomear.

Como as máquinas que se movem no domínio são refletidas no Discovery

Quando uma máquina é *movida* para uma nova UO no domínio, o efeito que ela tem no **Discovery** depende das políticas selecionadas utilizando Discovery > Domínios > Domain Watch > Políticas > **OU/Containers** *(página 49)* ou **Computadores** *(página 51)*. **Discovery** o monitoramento de uma máquina-membro no domínio depende se sua política está configurada como "incluída" ou "excluída", tanto no local de origem da UO quanto no local de destino da UO.

Assumindo que a caixa de seleção `Include New Computers` esteja marcada no local de destino:

- **De incluída para incluída**: a hierarquia da conta da ID de máquina é alterada para corresponder ao novo local na hierarquia do domínio.
- **De incluída para excluída**: a hierarquia da conta da ID de máquina não é alterada. O VSA deve mover a ID de máquina manualmente utilizando Agente > Alterar grupo.
- **De excluída para incluída**: uma nova hierarquia da conta da ID de máquina "vazia" é criada, correspondendo o novo local na hierarquia do domínio. O usuário do VSA pode escolher mesclar a antiga conta da ID de máquina com a conta da ID de máquina recém-criada utilizando o botão Domínios > Computadores > **Sincronizar máquinas**.
- **De excluída para excluída**: nenhuma alteração é feita no VSA.

Como habilitar o Portal Access remoto no Discovery

O Portal Access permite que o usuário final de uma máquina gerenciada faça logon remotamente naquela máquina. Somente um usuário final de uma máquina pode ter Portal Access àquela máquina por vez. O usuário final deve ter feito logon previamente na máquina localmente ao menos uma vez. O **Discovery** é compatível com atribuições do Portal Access tanto manuais quanto automáticas. Para obter mais informações consulte:

- **Como gerenciar o Portal Access remoto** *(página 24)*

Atribuição automática ao Portal Access

Quando um usuário de domínio entra em uma máquina do domínio, *a máquina do domínio e o usuário de domínio* devem ser designados como **candidatos do portal** do **Discovery**para permitir que o usuário seja *atribuído automaticamente* como usuário do **Portal Access** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#438.htm)* daquela máquina.

Atribuição automática ao Portal Access

Discovery também pode atribuir e remover manualmente Portal Access para usuários de domínio, independentemente de o usuário de domínio ou o computador dr domínio for um candidato ao portal ou não.

Nota: Um usuário de domínio pode ser usuário do VSA ou usuário do Portal Access, mas não de ambos. Quando um logon de usuário do VSA é criado para um usuário de domínio, aquele usuário não será mais elegível para ser usuário do Portal Access de nenhuma máquina.

Como utilizar o Portal Access Discovery

O Portal Access gerenciado do **Discovery** fornece o seguinte comportamento único não disponível fora do **Discovery**.

- Quando um usuário candidato ao portal entra em uma máquina candidata ao portal — e essa máquina candidata ao portal ainda não está atribuída a um usuário do Portal Access — ele ou ela é automaticamente atribuído(a) como usuário do Portal Access daquela máquina.
- A guia **Alterar perfil** do Portal Access é preenchida automaticamente com o *nome*, *e-mail* e *número do telefone* do usuário atualmente conectado no candidato do Portal Access. Os campos do remetente de novos tickets do **Service Desk** são preenchidos com as informações de contato armazenadas na guia **Alterar perfil**. Isto significa que os usuários do Portal Access não precisam reinserir as mesmas informações de contato cada vez que criam um novo ticket do **Service Desk**.

  Nota: Independentemente das informações do remetente registradas em um ticket, o atual usuário do Portal Access vê todos os tickets relacionados àquela máquina.

- Se a conexão com o servidor do Active Directory for perdida, evitando a autenticação do domínio, os usuários ainda poderão utilizar seu logon do Portal Access para se conectar remotamente à máquina do Portal Access atribuída por último a eles.
- Todas as máquinas podem se designadas candidatos do portal utilizando a caixa de seleção **Atribuir automaticamente Portal Access para candidatos do portal** na caixa de diálogo Política de computadores na guia **OU/Containers** *(página 49)*.
- Qualquer usuário de domínio que ainda não é um usuário VSA — sendo um candidato ao portal ou não — pode ser atribuído manualmente como usuário do Portal Access de um computador de domínio, utilizando o botão **Atribuir usuário do portal** na página **Computadores** *(página 58)*.

  Nota: *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.

- Qualquer usuário de domínio — sendo um candidato do portal ou não — pode ser removido manualmente como usuário do Portal Access de um computador a qualquer momento, utilizando o botão **Remover usuário do portal** na página **Computadores** *(página 58)*.

Como habilitar/desabilitar contas dos usuários de domínio ou redefinir senhas de usuários de domínio

Nota: A habilitação e desabilitação de logons do domínio, a redefinição de senhas do domínio e o desbloqueio das contas do domínio estão disponíveis somente se o conjunto de recursos do **Directory Services** estiver habilitado.

Quando a página Usuários e Acesso ao portal do **Discovery** > é usada para habilitar ou desabilitar uma conta do usuário de domínio ou redefinir a senha do usuário de domínio, a sincronização ocorre imediatamente somente para aquele registro do usuário de domínio. Dados detalhados do domínio são detectados somente para aquele usuário de domínio.

- Um usuário desabilitado de domínio não será mais capaz de fazer logon usando a credencial de logon, nem de fazer logon no VSA utilizando sua credencial de domínio.

- As alterações da senha são efetivadas na próxima vez que o usuário de domínio fizer logon, tanto no domínio quanto no VSA utilizando sua credencial de domínio.

Nota: A habilitação ou desabilitação de contas do usuário de domínio ou a redefinição da senha do usuário de domínio *no Active Directory* não atualizará o VSA até que uma sincronização de tempo de leitura ocorra.

Nota: Não faça alterações na senha de um usuário gerenciado do **Discovery** nem habilite/desabilite aquele usuário utilizando a página Sistema > **Usuário** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4576.htm)* ou Sistema > Alterar logon. Estas alterações *somente ocorrem no VSA* e somente têm um efeito temporário sobre aquele usuário. Eventualmente, a sincronização irá redefinir a senha do VSA do usuário e habilitar/desabilitar o usuário do VSA como especificado no Active Directory.

Como fazer alterações nos logons dos usuários gerenciados do Discovery

Você pode desejar fazer alterações para o logon criado do usuário do VSA ou de candidatos ao Portal Access após aplicar as políticas do **Discovery**. Você deve saber que:

- Os usuários do VSA e os usuários do Portal Access criados pelo **Discovery** nunca são removidos automaticamente pelo **Discovery**.
- Os agentes instalados pelo **Discovery** nunca são desinstalados pelo **Discovery**.

A exclusão de usuários do VSA e usuários do Portal Access, e a desinstalação dos agentes devem sempre ser feitas manualmente, fora do **Discovery**.

Nota: Um usuário de domínio pode ser associado a *apenas* um logon de usuário do VSA *ou* a um logon do Portal Access, *mas não ambos a ao mesmo tempo.*

Como remover acesso de logon do usuário do VSA somente

- Somente exclua o logon de usuário do VSA.

Como remover o acesso do usuário ao portal somente

- Utilize o botão Remover usuários do Portal na página Usuário e Portal Access.

Promoção de um candidato ao Portal Access para um usuário do VSA

- Utilize o botão Remover usuários do Portal na página Usuário e Portal Access.
- Modifique as políticas do **Discovery** para que, ao menos, um grupo ao qual o usuário de domínio pertence esteja configurado como `Create VSA User`. O usuário do <VSA será criado quando a política de usuário do **Discovery** for aplicada.

Rebaixamento de um usuário do VSA para usuário do Portal Access

- Somente exclua o logon de usuário do VSA.
- Modifique as políticas do **Discovery** para que, ao menos, um grupo ao qual o usuário de domínio pertence esteja configurado como `Create Staff and make Auto Portal Candidate` e nenhum grupo ao qual o usuário de domínio pertence esteja configurado como `Create VSA user`. O candidato ao Portal Access será criado quando a política do usuário do **Discovery** for aplicada.

Formatos compatíveis de logon no domínio

Os seguintes formatos de logon de domínio são compatíveis usando o**Discovery**, tanto para usuários do VSA quanto usuários do Portal Access.

Formato	Campo	Logons do nome completo do domínio DNS*	Logons do nome de domínio pré-Windows 2000**
Barra invertida do domínio	Nome do usuário	*ITservices.acme.com\william*	*ITservices\william*
	Senha	********	********
	Domínio		
Barra do domínio	Nome do usuário	*ITservices.acme.com/william*	*ITservices/william*
	Senha	********	********
	Domínio		
Domínio separado	Nome do usuário	*william*	*william*
	Senha	********	********
	Domínio	*ITservices.acme.com*	*ITservices*
Domínio de estilo de e-mail	Nome do usuário	*william@ITservices.acme.com*	*william@ITservices*
	Senha	********	
	Domínio		

** O nome completo do domínio DNS também é conhecido como sufixo UPN.*

*** O nome do domínio pré-Windows 2000 também é conhecido como Nome do domínio NetBIOS.*

Sincronização

A sincronização se refere à atualização do **Discovery** com dados detectados de um domínio Active Directory. Os seguintes eventos do **Discovery** acionam a sincronização entre o **Discovery** e um domínio.

- Visualizações
- Ativação/Sincronização incremental
- Aplicar alterações
- Sincronização completa

> **Nota:** Uma sincronização também ocorre para um usuário especificado quando da **Habilitação/Desabilitação de contas dos usuários de domínio ou da Redefinição da senha do usuário de domínio** *(página 30)*.

Visualizações

Quando a verificação do **Discovery** está instalada, a primeira tarefa que a verificação realiza é uma **visualização**. Uma visualização atualiza o **Discovery** com:

- Dados resumidos do domínio para todas as pastas e itens.

Já que está é a primeira vez que os dados são "detectados" de um domínio, somente são necessários os dados resumidos do domínio.

- Pastas são objetos do domínio que contêm outros objetos. Isso pode se referir a unidades organizacionais ou contêineres e grupos, sendo que grupos significa grupos de usuários.
- Os itens podem se referir a computadores, usuários e contatos.

Ativação/Sincronização incremental

> **Nota:** A sincronização incremental está somente disponível se o **Conjunto de recursos dos Serviços de diretório** *(página 25)* estiver disponível.

Após a verificação ser instalada, e normalmente antes das políticas do **Discovery** serem configuradas, uma verificação do **Discovery** é ativada. **A ativação** habilita a sincronização incremental entre um domínio Active Directory e o computador da verificação. Uma verificação ativada aguarda um período fixo, chamado de **intervalo de sincronização**, antes de atualizar o VSA com estas alterações. Por padrão, este intervalo de sincronização é de 60 minutos. Se o valor padrão é utilizado, estas alterações do domínio podem não ser refletidas no VSA até 60 minutos após as alterações serem feitas.

Inicialmente, nenhuma política do **Discovery** está configurada, logo, nenhuma pasta ou item está "incluído", o que exigiria uma detecção de dados detalhada. Neste caso, uma sincronização incremental detecta dados resumidos de um domínio que é similar a uma visualização, exceto que a detecção de dados é limitada a *alterações* no domínio.

Posteriormente, quando as políticas do **Discovery** tiverem sido configuradas e os itens e pastas selecionadas estiverem "incluídos", a sincronização exigirá tanto dados detalhados quanto resumidos. Novamente, a detecção de dados é limitada a *alterações* no domínio.

A sincronização incremental fornece uma atualização de *todas as alterações* para:

- Dados resumidos do domínio para todas as pastas e itens, "incluídos" ou "excluídos".
- Dados detalhados do domínio para todas as pastas e itens "incluídos". Computadores e contatos podem ser "incluídos" individualmente. Usuários sempre são "incluídos" por grupo.

Alterações de domínio utilizando intervalo de sincronização incremental

A maioria das alterações de domínio é armazenada pela verificação até que o intervalo de sincronização tenha decorrido, sendo, em seguida, carregada no **Discovery**. O padrão é 60 minutos. Estes tipos de alterações de domínio incluem:

- Usuário adicionado, movido ou excluído
- Computador adicionado, movido ou excluído
- Alterações de contato ou de usuário, tais como nome, endereço, número de telefone, endereço de e-mail
- Reorganização da hierarquia da UO do domínio

Alterações do domínio passadas imediatamente

Algumas alterações importantes de domínio precisam ser carregadas pela verificação imediatamente. Estas incluem:

- Alterações de senha
- Desabilitação de uma conta do usuário

Aplicar alterações

A sincronização também ocorre quando da **aplicação de políticas do KDIS** *(página 27)*, e é equivalente a uma sincronização *completa*. Isto assegura que as políticas aplicadas afetem *todos* os computadores **incluídos** *(página 72)* de domínio, usuários e contatos que podem existir naquele momento, independentemente de qualquer sincronização que possa ter ocorrido anteriormente.

Sincronização completa

A verificação do **Discovery** acumula *alterações* do domínio em tempo real. Se a conexão entre a

verificação do **Discovery** e um domínio é perdida por um período, a verificação não tem como recuperar aquelas alterações. Para assegurar que as alterações do domínio não sejam perdidas para sempre, defina os **alertas de verificação** *(página 34)* e agende uma *sincronização* **completa** *(página 32)* de modo recorrente. *Se um alerta de verificação for acionado, considere executar uma sincronização completa imediatamente.*

Uma sincronização completa fornece ao **Discovery** uma atualização completa dos dados de domínio, incluindo:

- Dados resumidos do domínio para todas as pastas e itens, "incluídos" ou "excluídos".
- Dados detalhados do domínio para todas as pastas e itens "incluídos". Computadores e contatos podem ser "incluídos" individualmente. Usuários sempre são "incluídos" por grupo.

Normalmente, uma sincronização completa ocorre com menos frequência do que uma sincronização incremental. Uma vez por dia ou uma vez por semana, por exemplo, deve ser suficiente.

Ativação/Desativação

Os botões Ativação e **Desativação** são exibidos na guia Domain Watch > **Implementação de verificação**, mas somente se o **Conjunto de recursos do Directory Services** *(página 25)* estiver instalado.

- **Ativação**: permite a detecção e a sincronização incrementais dos dados do controlador de domínio. A ativação de uma verificação em um computador de domínio *desativa* qualquer outra verificação naquele mesmo domínio, sem perda de dados.

  Nota: *A ativação não é necessária para executar uma sincronização completa na guia Domain Watch >* **Agendamento e status** *(página 57).*

- **Desativação**: desabilita atualizações da sincronização incremental do domínio. Se a ativação ocorrer novamente mais tarde, um "intervalo de alterações" pode existir nos dados coletados pela verificação, necessitando o agendamento de uma sincronização completa para a correção.

Como desinstalar a verificação e remover a Org

Você associa uma organização a um domínio quando a verificação é instalada. Após a instalação, a associação com a organização não pode ser alterada sem a desinstalação da verificação e remoção da mesma. Isto evita a criação de registros de usuários, equipes e computadores duplicados em diversas organizações.

A desinstalação e remoção da organização limpa todos os registros para aquele domínio nas páginas **Computadores** *(página 58)*, **Contatos** *(página 60)* e **Usuários & Usuários do Portal** *(página 62)* porque estes registros não são mais conhecidos como membros do domínio pela associação da org. Os verdadeiros registros do VSA não são excluídos.

Alertas de verificação e alertas de domínio

Nota: Alertas são somente disponíveis se o **Conjunto de recursos dos Serviços de diretório** *(página 25)* estiver habilitado.

Alertas de verificação

Alertas de aviso de verificação e alertas de falha fornecem alertas e notificações de e-mail para

qualquer problema em relação à comunicação da verificação com o servidor do Active Directory. Alertas de verificação podem incluir:

- O servidor do Active Directory fica off-line.
- A credencial de domínio usada pelo **Discovery** não é mais válida.
- A verificação não pode se comunicar com o controlador de domínio.

Aviso: *A verificação do* **Discovery** *acumula* ***alterações*** *do domínio em tempo real. Se a conexão entre a verificação do* **Discovery** *e um domínio é perdida por um período, a verificação não tem como recuperar aquelas alterações. Para assegurar que as alterações do domínio não sejam perdidas para sempre, defina os* **alertas de verificação** *(página 34) e agende uma* ***sincronização completa*** *(página 32) de modo recorrente. Se um alerta de verificação for acionado, considere executar uma sincronização completa imediatamente.*

Alertas de domínio

Os alertas de domínio fornecem notificações de e-mail, ticket e alarme para a criação, alteração ou exclusão dos tipos de objetos selecionados no domínio. Os tipos de objetos de domínio podem incluir:

- Computador
- Contato
- Contêiner
- Domínio
- Grupo
- Unidade organizacional
- Usuário

Como configurar a Página de domínios do Discovery

Os seguintes tópicos fornecem um procedimento detalhado para a configuração da página Discovery > **Domain Watch** *(página 45)*.

- **Pré-requisitos da configuração** *(página 35)*
- **Como configurar a implementação da verificação** *(página 36)*
- **Como configurar a implementação do agente** *(página 37)*
- **Como configurar políticas do contêiner/UO** *(página 38)*
- **Como configurar políticas do computador** *(página 39)*
- **Como configurar políticas de contato** *(página 39)*
- **Como configurar políticas de grupo** *(página 40)*
- **Como configurar políticas de usuário** *(página 42)*
- **Como configurar perfis de alerta** *(página 43)*
- **Como configurar status e agendamento** *(página 43)*

Pré-requisitos da configuração

1. identifique as credenciais do administrador do domínio para o domínio Active Directory que você planeja integrar ao VSA. O **Discovery** necessita de uma credencial do domínio autorizada para realizar os seguintes tipos de atualizações:
   - Criação de um GPO para o propósito de armazenar pacotes de instalação Kaseya
   - Redefinição de senha
   - Habilitação ou desabilitação de uma conta do usuário

> **Nota:** Uma credencial do administrador do domínio fornece a autorização necessária, mas você pode, se quiser, limitar o **Discovery** apenas aos privilégios listados acima.

2. Instale um agente do VSA em uma máquina que é membro do domínio Active Directory que você deseja integrar ao VSA. Você não verá um domínio no painel superior da página **Domain Watch** *(página 45)* até que, ao menos, um computador de domínio tenha um agente instalado nele.

Como configurar a implementação da verificação

> **Nota:** Nenhuma guia é exibida a menos que uma linha do domínio no painel superior seja selecionada. Ao menos um agente deve ser instalado em um computador de domínio para ver aquela linha do domínio exibida no painel superior.

1. Clique na guia Discovery > Domínios > Domain Watch > **Implementação da verificação** *(página 46)* .
2. Selecione a linha do **Nome de domínio** no painel superior que você deseja configurar.
   - O **Status da verificação** exibe `Un-installed`.
   - As máquinas que são membros deste domínio e que têm agentes Kaseya instalados nelas serão exibidas agora no painel inferior.
   - Inicialmente, você somente pode ver um único computador do domínio com o agente Kaseya instalado exibido no painel inferior. Conforme os agentes são instalados automaticamente em outros computadores do domínio utilizando políticas do **Discovery**, todos estes computadores do domínio são exibidos no painel inferior.
3. Selecione uma das máquinas no painel inferior.
   - Clique no botão **Instalar** habilitado no painel inferior.
4. A primeira solicitação da caixa de diálogo **Instalar** é que você insira uma credencial. **Discovery** necessita de uma credencial do domínio autorizada para realizar os seguintes tipos de atualizações:
   - Criação de um GPO para o propósito de armazenar pacotes de instalação Kaseya
   - Redefinição de senha
   - Habilitação ou desabilitação de uma conta do usuário

   > **Nota:** Uma credencial do administrador do domínio fornece a autorização necessária, mas você pode, se quiser, limitar o **Discovery** apenas aos privilégios listados acima.
5. Clique no botão **Verificar e configurar credenciais**.
   - Se a credencial for válida, a caixa de diálogo exibe um segundo botão **Instalar**.
6. Opcionalmente, filtre a varredura realizada pela máquina de verificação utilizando **Filtrar sequência**. Útil para grandes domínios. Utilize notação distinguida do nome. Por exemplo, `CN=Users,DC=myDomain,DC=com`
7. A caixa de diálogo **Instalar** solicita que você especifique uma organização **única** do VSA para cada domínio integrado ao **Discovery**.
   - Quando agentes são instalados nas máquinas para este domínio, as contas da ID da máquina criadas no VSA se tornam membros desta organização.
   - Quando os registros do usuário ou dos membros da equipe são criados no VSA para este domínio, eles são associados à organização que você seleciona.
   - Após a instalação, a associação com a organização não pode ser alterada sem a **Como desinstalar a verificação e remover a Org** *(página 34)*. Isto evita a criação de registros de usuários, equipes e computadores duplicados em diversas organizações.
8. Clique no botão **Instalar** na caixa de diálogo. A caixa de diálogo se fecha. Os componentes da verificação do

- **Discovery** são instalados na máquina do agente.
- Após a instalação, o agente de verificação automaticamente começa a "coletar" uma **visualização** de todos os *itens e pastas* no domínio em relação à hierarquia de UO/contêiner, computadores, contatos, grupos e usuários. Nenhuma informação detalhada é necessária. A visualização preenche as guias **Políticas** com estes dados resumidos.
- O **Status da verificação** exibe `Previewing` enquanto a detecção dos dados é feita. Isso pode levar alguns minutos. Utilize o botão **Atualizar** para atualizar a página. A atualização da página não é feita automaticamente.
- Quando a visualização é concluída, o ícone **Status da verificação** exibe `Installed`.

> **Nota: Os botões Ativação e Desativação** somente são exibidos se o **Conjunto de recursos do Directory Services** *(página 25)* estiver instalado.

9. Selecione novamente a linha do agente da verificação. Clique no botão **Ativar** no painel inferior. A caixa de diálogo **Ativar verificação** se abre.
   - Neste momento, você pode inserir uma credencial diferente para a verificação daquela inserida para a instalação. Normalmente, a mesma credencial é utilizada.

     > **Nota:** Se uma verificação já tiver sido instalada e ativada uma vez, o campo **Organização do VSA** poderá ser desabilitado. Clique no botão **Desinstalar e excluir Org**. Então, clique no botão **Ativar** para habilitar a lista e escolher uma org. diferente. Consulte **Ativação/Desativação** *(página 34)* para questões a se considerar antes de *desativar* uma verificação.

   - Configure um **intervalo de sincronização incremental** *(página 32)* para a sincronização de dados entre o domínio e o **Discovery**. O padrão é 60 minutos. Esta opção somente está disponível se **O conjunto de recursos do Directory Services** *(página 25)* estiver disponível.
   - Clique no botão **Ativar** para fechar esta caixa de diálogo e ativar a verificação. Isto deve levar apenas um minuto ou dois. Utilize o botão **Atualizar** para atualizar a página. A atualização da página não é feita automaticamente.
   - O **Status da verificação** exibe `Activated`.

     > **Nota:** A ativação é recomendada imediatamente após a instalação da verificação, mesmo antes que você configure políticas adicionais do **Discovery**. Isto assegura que todas as alterações no domínio sejam monitoradas enquanto você continua com sua configuração.

Como configurar a implementação do agente

1. Clique na guia **Discovery** > Domínios > Domain Watch > **Implementação do agente** *(página 48)* .
2. Clique no botão **Editar**. Configure o seguinte:
   - **Instalar agentes automaticamente quando o computador é detectado**: **deixe esta caixa de seleção em branco se você já ativou a verificação pela primeira vez. Aguarde até que as políticas sejam aplicadas, então retorne a esta guia e marque esta caixa de seleção.** Quando as políticas são aplicadas, os agentes são instalados automaticamente nos computadores que são membros daquelas políticas. *Os computadores devem ser reiniciados para completar a instalação dos agentes Kaseya.*

     > **Nota:** A Kaseya recomenda deixar esta caixa de seleção em *branco* até que todas as **Políticas** *(página 49)* sejam configuradas para um domínio pela primeira vez.

   - **Permitir que agentes sejam instalados no servidor do Directory**: deixe esta caixa de seleção em branco. Se marcada, os agentes também serão instalados no sistema que hospeda o domínio Active Directory.
   - **Pacote padrão**: selecione um pacote de instalação de agentes com base em Windows para utilizar com o domínio selecionado.

> **Nota: Domain Watch** não é compatível com a instalação de agentes em máquinas Linux e Apple. Os agentes devem ser instalados em máquinas Linux e Apple de domínio fora do **Domain Watch**. Consulte **Como os agentes são instalados utilizando o Discovery** *(página 27)*.

3. Clique no botão **Salvar** para fechar esta caixa de diálogo.

Como configurar políticas do contêiner/UO

> **Nota:** A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

1. Clique em Discovery > Domínios > Domain Watch > Políticas > **OU/Containers** *(página 49)*.
   - Utilize esta guia para especificar em quais máquinas do domínio você quer que o agente Kaseya seja instalado.
   - Cada **UO/contêiner** *(página 72)* nesta guia está identificado pelo seu nome canônico. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
   - Colunas adicionais mostram contagens para os computadores e contatos selecionados e disponíveis em cada UO/contêiner.
2. Selecione um UO/contêiner que mostra uma contagem para um ou mais computadores.

   > **Nota:** Ordene esta guia ao clicar na opção **Classificar descendente** no cabeçalho da coluna **Total de computadores**. Isso assegura que qualquer contêiner/UO com contagens de computadores maiores do que zero sejam listados primeiro.

3. Selecione o botão **Políticas de computadores**.
   - A caixa de diálogo lista todos os computadores disponíveis do contêiner/UO que você pode *incluir* (página 72) nas políticas selecionadas.
   - Inserir uma caixa de seleção próxima a um computador nesta caixa de diálogo significa que você deseja instalar um agente naquele computador de domínio.
     - ✓ Se a caixa de seleção **Instalar automaticamente agentes quando o computador é detectado** na guia **Implementação do agente** *(página 48)* estiver marcada, os agentes serão instalados automaticamente nos computadores selecionados do contêiner/UO logo após os computadores de domínio serem reiniciados. Se esta mesma caixa de seleção não for marcada, você deverá implementar os agentes manualmente ao selecionar a conta **modelo da ID da máquina** *(página 71)* criada para um computador de domínio na página **Computadores** *(página 58)*, e, em seguida, clicar no botão **Implementar agente** na mesma página. O computador de domínio ainda precisa ser reiniciado para completar a instalação do agente.
   - Opcionalmente, marcar **Atribuir automaticamente acesso ao portal para candidatos do portal** significa que você quer designar estes computadores como **máquinas candidatas ao portal** *(página 29)*.
   - Opcionalmente, marcar a caixa de seleção **Incluir novos computadores** significa que você quer *incluir* novos computadores adicionados a este contêiner/UO. Eles serão atribuídos à mesma política do **Discovery** que você configurou anteriormente para os computadores selecionados neste contêiner/UO.
4. Marque um ou mais computadores nesta lista e clique em **Salvar**.
   - A caixa de diálogo se fecha e a contagem na coluna **Computadores selecionados** é atualizada com o número de máquinas incluídas na política de computadores que você recém configurou.

- O **Status da verificação** exibe Activated e o **Status dos contatos/computadores** exibe Modified pois as alterações na política recém feitas ainda não foram aplicadas.

Nota: Você não precisa **Aplicar alterações** até que todas as guias **Políticas** tiverem sido configuradas. Clicar no botão **Aplicar alterações** em qualquer guia aplica as alterações da política do **Discovery** para todas as guias ao mesmo tempo.

Como configurar políticas de contato

Nota: A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

1. Clique na guia Discovery > Domínios > Domain Watch > **OU/Containers** *(página 49)*.
   - Utilize esta guia para especificar em quais contatos do domínio você deseja criar um registro de equipe no VSA. Um **contato** de domínio contém informações de contato similares às informações definidas para um usuário, mas um contato não tem privilégios de logon no domínio.
   - Cada UO/contêiner nesta guia está identificado pelo seu nome canônico. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
   - Colunas adicionais mostram contagens para os computadores e contatos selecionados e disponíveis em cada UO/contêiner.
2. Selecione um UO/contêiner que mostra uma contagem para um ou mais contatos.

   Nota: Ordene esta guia ao clicar na opção **Classificar descendente** no cabeçalho da coluna **Total de contatos**. Isso assegura que qualquer contêiner/UO com contagens de contatos maiores do que zero sejam listados primeiro.
3. Selecione o botão **Política de contatos**.
   - A caixa de diálogo lista todos os contatos disponíveis do contêiner/UO que você pode *incluir* (página 72) nas políticas selecionadas.
   - Inserir uma caixa de seleção próximo a um contato nesta caixa de diálogo significa que você deseja criar um registro de equipe do VSA para aquele contato do domínio.
   - Opcionalmente, marcar a caixa de seleção **Incluir novos contatos** significa que você quer *incluir* novos contatos adicionados a este contêiner/UO. VSA Registros de equipe do VSA serão criados para estes novos contatos à medida que são detectados.
4. Marque um ou mais contatos nesta lista e clique em **Salvar**.
   - A caixa de diálogo se fecha e a contagem na coluna **Contatos selecionados** é atualizada com o número de contatos incluídos na política de contatos que você recém configurou.
   - O **Status da verificação** exibe Activated e o **Status dos contatos/computadores** exibe Modified pois as alterações na política recém feitas ainda não foram aplicadas.

     Nota: Você não precisa **Aplicar alterações** até que todas as guias **Políticas** tiverem sido configuradas. Clicar no botão **Aplicar alterações** em qualquer guia aplica as alterações da política do **Discovery** para todas as guias ao mesmo tempo.

Como configurar políticas do computador

1. Clique em Discovery > Domínios > Domain Watch > **Computadores** *(página 51)*.

- Utilize esta guia para selecionar os computadores *individuais* do domínio nos quais você deseja instalar o agente Kaseya. Esta guia tem precedência sobre o conjunto de políticas na guia **UO/Contêineres**.
- Cada computador nesta guia é identificado pelo seu nome canônico. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.

2. Selecione o botão **Políticas de computadores**.
   - Configure a política do computador para a máquina selecionada como `Include` ou `Do Not Include`.
   - Opcionalmente, configure a lista suspensa **Substituir grupo de computadores**. Isto especifica o grupo de máquinas a utilizar quando um agente é instalado neste computador.
3. Clique em **Salvar**.
   - O **Status da verificação** exibe `Activated` e o **Status da política** exibe `Modified` pois as alterações na política recém feitas ainda não foram aplicadas.

> **Nota:** Você não precisa **Aplicar alterações** até que todas as guias **Políticas** tiverem sido configuradas. Clicar no botão **Aplicar alterações** em qualquer guia aplica as alterações da política do **Discovery** para todas as guias ao mesmo tempo.

Como configurar políticas de grupo

> **Nota:** A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

1. Clique na guia Discovery > Domínios > Domain Watch > Políticas > **Grupos** *(página 52)*. As políticas de usuário do
   - **Discovery** permitem que os usuários façam logon no VSA ou no **Portal Access** *(página 29)* utilizando suas credenciais de domínio.
   - Cada credencial de domínio pode ser aplicada a *somente um* dos dois tipos de logons do VSA:
     - ✓ **VSA Logons do usuário do VSA**: estes logons são usados pelos administradores do VSA.
     - ✓ **Logons do Portal Access**: estes logons são usados pelos usuários da máquina que desejam acessar suas próprias máquinas de modo remoto.
   - Grupos de usuários são simplesmente chamados de "grupos" em um domínio Active Directory. Cada grupo nesta guia é identificado pelo seu nome canônico. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
   - Uma coluna adicional mostra uma contagem do número de usuários em cada grupo.
2. Selecione um grupo que mostra uma contagem para um ou mais usuários.
   - O mesmo membro pode ser um membro de diversos grupos em um domínio Active Directory.

> **Nota:** Ordene esta guia ao clicar na opção **Classificar descendente** no cabeçalho da coluna **Total de usuários**. Isso assegura que qualquer grupo com contagens de usuários maiores do que zero que ainda não tiveram políticas atribuídas sejam listadas perto do topo da guia.

3. Selecione o botão **Configurar política de grupos**.
   - A caixa de diálogo **Política de grupos** é exibida, listando os **Usuários membros** neste grupo.
4. Selecione uma **Política do grupo de membros.**

- É possível atribuir a cada grupo de usuários no **Discovery** uma das três diferentes políticas de logon do VSA. Estas políticas são aplicadas a todos os usuários que pertencem ao grupo. Elas não podem ser aplicadas a usuários individuais dentro de um grupo.
  - ✓ `Do Not Include Users` - Não criar logons de usuário do VSA ou logons de Portal Access para usuários do domínio listados nesse grupo de usuários.
  - ✓ `Create Staff Members` : cria um registro do membro da equipe. É possível atribuir a estes usuários acesso Portal Access a uma máquina *manualmente*.

    > **Nota:** *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.

  - ✓ `Create Staff and make Auto Portal Candidates` : designa usuários de domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
  - ✓ `Create VSA Users` - Cria logons do usuário do VSA para usuários do domínio listados neste grupo de usuários.
- *Já que cada usuário de domínio pode pertencer a diversos grupos de usuários de domínio, atribui-se a um usuário de domínio a* **a política de logon do VSA mais alta**, *atribuída a qualquer grupo de usuários do qual o usuário de domínio é membro.*
  - ✓ `Create VSA Users` superam em hierarquia a `Create Staff and make Auto Portal Candidates`
  - ✓ `Create Staff and make Auto Portal Candidates` superam em hierarquia a `Create Staff Members`
  - ✓ `Create Staff Members` superam em hierarquia a `Do Not Include Users`

5. Se `Create VSA Users` for selecionado:
   - **Pesquisa de função**: selecione a função que estes usuários utilizarão.
   - **Pesquisa de escopo**: selecione o escopo que estes usuários utilizarão.
   - Se *um escopo com o mesmo nome da organização* ainda não existe, um + é exibido no lado da lista suspensa **Pesquisa de escopo** da caixa de diálogo **Política do usuário**. Clicar no ícone + permite que você crie um novo escopo que tem o mesmo nome da organização associada ao domínio. Após o escopo ser criado, o + não é mais exibido ao lado da lista suspensa **Pesquisa de escopo**, e o texto no topo da caixa de diálogo indica que o escopo padrão já existe.
   - Se o mesmo usuário é atribuído a diversos grupos, e diferentes funções e escopos são atribuídos a cada grupo, então, quando o usuário entrar no VSA, estas funções e escopos estarão disponíveis no seletor de funções/escopo no canto superior direito da janela do VSA.

     > **Nota:** As atribuições de funções/escopo utilizando a guia **Grupos** e a guia **Usuários** podem ser modificadas e reaplicadas diversas vezes. Alterações sucessivas farão com que as funções e os escopos se *acumulem, em vez de serem substituídos*. O **Discovery** nunca remove registros no VSA.

6. Clique em **Salvar** para fechar esta caixa de diálogo.
   - A caixa de diálogo se fecha e a política que você selecionou é exibida na coluna **Política de usuários**.
7. Se você já configurou as políticas do **Discovery** para computadores e contatos, clique no botão **Aplicar alterações**.

> **Nota:** Você não precisa **Aplicar alterações** até que todas as guias **Políticas** tiverem sido configuradas. Clicar no botão **Aplicar alterações** em qualquer guia aplica as alterações da política do **Discovery** para todas as guias ao mesmo tempo.
>
> **Nota:** Consulte **Formatos compatíveis de logon no domínio** *(página 31)*.

Como configurar políticas de usuário

1. Clique na guia Discovery > Domínios > Domain Watch > Políticas > **Usuários** *(página 52)*. As políticas de usuário do
   - **Discovery** permitem que os usuários façam logon no VSA ou no **Portal Access** *(página 29)* utilizando suas credenciais de domínio.
   - Cada credencial de domínio pode ser aplicada a *somente um* dos dois tipos de logons do VSA:
     - ✓ **VSA Logons do usuário do VSA**: estes logons são usados pelos administradores do VSA.
     - ✓ **Logons do Portal Access**: estes logons são usados pelos usuários da máquina que desejam acessar suas próprias máquinas de modo remoto.
   - Grupos de usuários são simplesmente chamados de "grupos" em um domínio Active Directory. Cada grupo nesta guia é identificado pelo seu nome canônico. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
   - Uma coluna adicional mostra uma contagem do número de usuários em cada grupo.
2. Selecione um usuário.
3. Selecione o botão **Configurar políticas de usuários**.
   - A caixa de diálogo **Política de usuários** é exibida.
4. Selecione uma **Política de usuário do membro.**
   - É possível atribuir a cada usuário de domínio no **Discovery** uma das três diferentes políticas de logon do VSA.
     - ✓ `Do Not Include Users` - Não criar logons de usuário do VSA ou logons de Portal Access para usuários do domínio listados nesse grupo de usuários.
     - ✓ `Create Staff Members` : cria um registro do membro da equipe. É possível atribuir a estes usuários acesso Portal Access a uma máquina *manualmente*.

       > **Nota:** *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.

     - ✓ `Create Staff and make Auto Portal Candidates` : designa usuários de domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
     - ✓ `Create VSA Users` - Cria logons do usuário do VSA para usuários do domínio listados neste grupo de usuários.
5. Se `Create VSA Users` for selecionado:
   - **Pesquisa de função**: selecione a função que estes usuários utilizarão.
   - **Pesquisa de escopo**: selecione o escopo que estes usuários utilizarão.
   - Se *um escopo com o mesmo nome da organização* ainda não existe, um + é exibido no lado da lista suspensa **Pesquisa de escopo** da caixa de diálogo **Política do usuário**. Clicar no

ícone + permite que você crie um novo escopo que tem o mesmo nome da organização associada ao domínio. Após o escopo ser criado, o + não é mais exibido ao lado da lista suspensa **Pesquisa de escopo**, e o texto no topo da caixa de diálogo indica que o escopo padrão já existe.

- Se o mesmo usuário é atribuído a diversos grupos, e diferentes funções e escopos são atribuídos a cada grupo, então, quando o usuário entrar no VSA, estas funções e escopos estarão disponíveis no seletor de funções/escopo no canto superior direito da janela do VSA.

> **Nota:** As atribuições de funções/escopo utilizando a guia **Grupos** e a guia **Usuários** podem ser modificadas e reaplicadas diversas vezes. Alterações sucessivas farão com que as funções e os escopos se *acumulem, em vez de serem substituídos*. O **Discovery** nunca remove registros no VSA.

6. Clique em **Salvar** para fechar esta caixa de diálogo.
   - A caixa de diálogo se fecha e a política que você selecionou é exibida na coluna **Política de usuários**.
7. Se você já definiu as políticas para outras guias, clique no botão **Aplicar alterações**.

> **Nota:** Você não precisa **Aplicar alterações** até que todas as guias **Políticas** tiverem sido configuradas. Clicar no botão **Aplicar alterações** em qualquer guia aplica as alterações da política do **Discovery** para todas as guias ao mesmo tempo.
>
> **Nota:** Consulte **Formatos compatíveis de logon no domínio** *(página 31)*.

Como configurar perfis de alerta

> **Nota:** A guia **Perfis de alerta** somente é exibida se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado.

1. Clique na guia Discovery > Domínios > Domain Watch > **Perfis de alerta** *(página 56)*.
2. Habilite todos os alertas de verificação.

> **Aviso:** A verificação do **Discovery** acumula *alterações* do domínio em tempo real. Se a conexão entre a verificação do **Discovery** e um domínio é perdida por um período, a verificação não tem como recuperar aquelas alterações. Para assegurar que as alterações do domínio não sejam perdidas para sempre, defina os **alertas de verificação** *(página 34)* e agende uma *sincronização* **completa** *(página 32)* de modo recorrente. *Se um alerta de verificação for acionado, considere executar uma sincronização completa imediatamente.*

3. Habilite os alertas de domínio selecionados.
   - Se os agentes são implementados automaticamente utilizando a caixa de seleção **Instalar automaticamente agentes quando o computador é detectado** em **Implementação do agente** *(página 48)*, você não precisa ser notificado sobre a detecção de novos computadores. Se os agentes não são instalados automaticamente, *você precisa ser notificado* sobre computadores detectados recentemente.
   - Habilite a notificação por e-mail e alarmes para a criação e exclusão de unidades organizacionais, contêineres, grupos e usuários. Você pode, então, rever as políticas do **Discovery** após a criação ou exclusão de um destes objetos.

Como configurar status e agendamento

1. Clique na guia Discovery > Domínios > Domain Watch > **Agendamento e Status** *(página 57)*.

2. Habilite a sincronização completa em base semanal.

> **Aviso:** A verificação do **Discovery** acumula *alterações* do domínio em tempo real. Se a conexão entre a verificação do **Discovery** e um domínio é perdida por um período, a verificação não tem como recuperar aquelas alterações. Para assegurar que as alterações do domínio não sejam perdidas para sempre, defina os **alertas de verificação** *(página 34)* e agende uma *sincronização* **completa** *(página 32)* de modo recorrente. *Se um alerta de verificação for acionado, considere executar uma sincronização completa imediatamente.*

Como remover um domínio do gerenciamento do Discovery

Se você deseja remover um domínio do gerenciamento do **Discovery**, considere a exclusão dos seguintes tipos de registros gerados por domínios do VSA:

- Opcionalmente, exclua qualquer registro de modelo da ID da máquina gerado pelo domínio utilizando Agente > **Excluir** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#541.htm)*. Estes geralmente são identificados como pertencentes à organização associada ao domínio no **Discovery**.
- Opcionalmente, exclua os usuários do VSA gerados pelo domínio, utilizando Sistema > **Usuários** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4576.htm)*. Cada nome de usuário do VSA gerado pelo domínio é prefixado com o nome do domínio, utilizando o seguinte formato: `domain/username`.
- Opcionalmente, exclua os logons de usuário do Portal Access gerados pelo domínio, utilizando a página Agente> **Portal Access** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#438.htm)*.
- Opcionalmente, exclua a organização associada ao domínio utilizando Sistema > Orgs/Grupos/Depts/Pessoal> **Gerenciar** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4017.htm)*.
  - Uma organização não pode ser excluída se as contas da ID da máquina são membros daquela organização.
  - Para contas da ID da máquina que você deseja manter, utilize Agente > **Alterar grupo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#545.htm)* para mover as contas da ID da máquina para um grupo de máquinas em outra organização.
  - Para contas da ID da máquina que você não deseja manter, utilize Agente > **Excluir** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#541.htm)* para desinstalar os agentes e excluir as contas da ID da máquina.
- Se você escolher manter a organização associada com o domínio, opcionalmente, exclua os registros do pessoal criados para contas do domínio na organização, utilizando a guia Sistema > Orgs/Grupos/Depts/Pessoal> Gerenciar > **Pessoal** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#7018.htm)*.
- É possível que um escopo dedicado tenha sido criado utilizando a guia Discovery > Domínio> **Políticas de usuários** *(página 52)*. Inicialmente, atribui-se a este escopo dedicado o mesmo nome da organização associada com o domínio. Opcionalmente, exclua este escopo dedicado.

Como desinstalar Discovery

> **Nota:** Antes de desinstalar o módulo do **Discovery**, reveja o tópico **Como remover um domínio do gerenciamento do Discovery** *(página 44)*.

1. Desative e remova a organização.
2. Desinstale a verificação do agente.
3. Desinstale o módulo **Discovery** do servidor da Kaseya.

Domain Watch

Discovery > Domínios > Domain Watch

A página **Domain Watch** configura a integração do **Discovery** com domínios Active Directory. Os recursos de configuração incluem:

- Instalação das verificações do **Discovery** que monitoram um domínio.
- Ativação e agendamento da sincronização de dados entre o **Discovery** e o domínio.
- Aplicação das políticas do **Discovery** para:
  - A implementação dos agentes.
  - A criação de usuários do VSA, usuários do Portal Access e registros de pessoal.
- Configuração de alertas do **Discovery**.
- Exibição do status de configuração do **Discovery**.

As informações sobre um domínio selecionado no painel superior da página **Domain Watch** são organizadas nas seguintes guias no painel inferior. *Configure um domínio selecionado na classificação da guia apresentada, da esquerda para a direita.*

1. **Implementação da verificação** *(página 46)*
2. **Política de implementação de agentes** *(página 48)*
3. **OU/Containers** *(página 49)*
4. **Políticas de usuário** *(página 52)*
5. **Políticas de alertas** *(página 56)*
6. **Programação e status** *(página 57)*

Painel superior

Ações

- **Atualizar**: atualiza a página inteira.

Cabeçalhos de coluna

- **Nome do domínio**: o nome do domínio Active Directory.
- Guid do domínio:
- **ID da Org**: o único identificador de uma **organização** *(página 70)* no VSA.
- **Nome da Org**: o nome amigável do VSA da organização.
- **Verificar status**
  - - Desinstalada: uma verificação não está instalada para este domínio.
  - - Processando: a verificação executando uma solicitação do usuário.
  - - Instalada: a verificação está instalada e a detecção de informações foi completada.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** não foram modificadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas e aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram

modificadas, mas ainda não foram aplicadas por, ao menos, três intervalos de sincronização. O administrador do **Discovery** pode ter esquecido de aplicar as políticas modificadas.

- Atenção ou off-line: a verificação encontrou um problema que pode requerer atenção do usuário. Pelo fato de que o status de atenção da verificação pode ser corrigido automaticamente, o status de atenção não corresponde necessariamente a uma alerta de aviso ou alerta de erro. Se off-line, a máquina do domínio fica indisponível. As páginas do **Discovery** não são atualizadas automaticamente. Clique no botão **Atualizar** para assegurar que o **Status da verificação** mais recente seja exibido.

Nota:

- **Computadores/Contatos/Status das políticas de usuários**: as políticas para ambas as guias pode estar em um dos três estados.
  - Original: as políticas do **Discovery** ainda não foram configuradas.
  - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.
  - Aplicada: as políticas do **Discovery** foram aplicadas.
- **Última entrada do agente da verificação**: a data/hora mais recente que o agente da verificação entrou.
- **Última resposta da verificação**:
- **Última mensagem de status**:

Implementação da verificação

Discovery > Domínios > Domain Watch > Guia Implementação da verificação

A guia **Implementação da verificação** configura o agente da verificação para um domínio selecionado. Todos os computadores de domínio com um agente Kaseya instalado são exibidos no painel inferior.

Discovery se comunica com um domínio Active Directory utilizando um **agente da verificação**. A verificação usa o protocolo LDAP padrão do setor para se comunicar de modo seguro com o domínio. Cada agente da verificação deve ser um membro do domínio que ele monitora. A implementação da verificação instala a funcionalidade extra que um agente necessita para agir como uma verificação.

Inicialmente, você somente pode ver um único computador do domínio com o agente Kaseya instalado exibido no painel inferior. Conforme os agentes são instalados automaticamente em outros computadores do domínio utilizando políticas do **Discovery**, todos estes computadores do domínio são exibidos no painel inferior.

Para obter mais informações consulte:

- **Como configurar a implementação da verificação** *(página 36)*.

Painel inferior

Campos do cabeçalho

- **Verificar status**
  - Desinstalada: uma verificação não está instalada para este domínio.
  - Processando: a verificação executando uma solicitação do usuário.
  - Instalada: a verificação está instalada e a detecção de informações foi completada.
  - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** não foram modificadas.
  - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas.
  - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas e aplicadas.
  - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas por, ao menos, três intervalos de

sincronização. O administrador do **Discovery** pode ter esquecido de aplicar as políticas modificadas.

- Atenção ou off-line: a verificação encontrou um problema que pode requerer atenção do usuário. Pelo fato de que o status de atenção da verificação pode ser corrigido automaticamente, o status de atenção não corresponde necessariamente a uma alerta de aviso ou alerta de erro. Se off-line, a máquina do domínio fica indisponível. As páginas do

> **Nota:** **Discovery** não são atualizadas automaticamente. Clique no botão **Atualizar** para assegurar que o **Status da verificação** mais recente seja exibido.

- **Nome do domínio**: o nome do domínio Active Directory.
- **Nome do usuário administrador**: o nome do administrador da credencial usada para se conectar ao domínio Active Directory.

Ações

- **Instalar**: instala a verificação. Após a instalação, a associação com a organização não pode ser alterada sem a desativação da verificação e remoção da mesma. Isto evita a criação de registros de usuários, equipes e computadores duplicados em diversas organizações.
  - **Nome do domínio**: a máquina da verificação é um membro deste domínio.
  - **Nome de usuário do administrador**: a máquina da verificação usa este nome de usuário do administrador para acessar o controlador de domínio.
  - **Senha do administrador/Confirmar senha**: a senha do administrador.
  - **Filtrar sequência**: filtra a varredura realizada pela máquina de verificação. Útil para grandes domínios. Utilize notação distinguida do nome. Por exemplo, `CN=Users,DC=myDomain,DC=com`
  - **Organização VSA**: a organização do VSA associada com o domínio selecionado.
- **Desinstalar**: desinstala a verificação.

> **Nota:** Antes de desinstalar o módulo **Discovery** do VSA, certifique-se de desativar e remover a organização e logo desinstale o agente da verificação.

Os botões Ativação e **Desativação** somente são exibidos se o **Conjunto de recursos do Directory Services** *(página 25)* estiver instalado.

- **Ativar**: permite a detecção e a sincronização incrementais dos dados do controlador de domínio. A ativação de uma verificação em um computador de domínio *desativa* qualquer outra verificação naquele mesmo domínio, sem perda de dados.

> **Nota:** A ativação não é necessária para executar uma sincronização completa na guia Domain Watch > **Agendamento e status** *(página 57)*.

- **Desativar**: desabilita atualizações da sincronização incremental do domínio. Se a ativação ocorrer novamente mais tarde, um "intervalo de alterações" pode existir nos dados coletados pela verificação, necessitando o agendamento de uma sincronização completa para a correção.
- **Desinstalar e remover org.**: desinstala a verificação e remove a organização. Isto pode ser necessário se a organização errada foi inicialmente selecionada para o domínio. Consulte **Como desinstalar a verificação e remover a Org** *(página 34)* para questões a se considerar antes de *desinstalar* uma verificação.

Cabeçalhos de coluna

- **Nome do domínio**: o nome do domínio Active Directory.
- **ID Machine.Group**: o ID.groupID.orgID da máquina no VSA.
- **Nome do computador DNS**: o nome de domínio totalmente qualificado do computador.
- **Nome do computador**: o nome do host local do computador.

- **Guid do agente**: Um identificador exclusivo para uma conta de ID de grupo/ID de máquina e seu agente correspondente.
- **Endereço IP**: o endereço IP do computador.
- **GUID do domínio**: o GUID único identificando este domínio no **Discovery**.
- **Tipos de host**: `Domain Server` ou `Domain Member`.
- **Status**: o status da verificação da máquina.
- **Última entrada do agente**: a última vez que o agente entrou nesta máquina.
- **Organização**: a **organização** *(página 70)* do VSA da qual este computador é membro.

Implementação do Agent

Discovery > Domínios > Domain Watch > Guia Implementação do agente

A guia **Implementação do agente** configura as políticas de implementação do agente para um domínio selecionado.

Para obter mais informações consulte:

- **Como configurar a implementação do agente** *(página 37)*.

Campos do cabeçalho

- **Verificar status**
  - - Desinstalada: uma verificação não está instalada para este domínio.
  - - Processando: a verificação executando uma solicitação do usuário.
  - - Instalada: a verificação está instalada e a detecção de informações foi completada.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** não foram modificadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas e aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas por, ao menos, três intervalos de sincronização. O administrador do **Discovery** pode ter esquecido de aplicar as políticas modificadas.
  - - Atenção ou off-line: a verificação encontrou um problema que pode requerer atenção do usuário. Pelo fato de que o status de atenção da verificação pode ser corrigido automaticamente, o status de atenção não corresponde necessariamente a uma alerta de aviso ou alerta de erro. Se off-line, a máquina do domínio fica indisponível. As páginas do

> **Nota:** **Discovery** não são atualizadas automaticamente. Clique no botão **Atualizar** para assegurar que o **Status da verificação** mais recente seja exibido.

Ações

- **Editar**: edita as políticas de implementação do agente.
  - **Instalar automaticamente agentes quando o computador é detectado**: selecione esta caixa de verificação. Quando as políticas são aplicadas, os agentes são instalados automaticamente nos computadores que são membros daquelas políticas. *Os computadores devem ser reiniciados para completar a instalação dos agentes Kaseya.*

> **Nota:** *A* Kaseya recomenda deixar esta caixa de seleção em *branco* até que todas as **Políticas** *(página 49)* sejam configuradas para um domínio pela primeira vez.

- **Permitir que agentes sejam instalados no servidor do Directory**: deixe esta caixa de seleção em branco. Se marcada, os agentes também serão instalados no sistema que hospeda o domínio Active Directory.
- **Pacote padrão**: selecione um pacote de instalação de agentes com base em Windows para utilizar com o domínio selecionado.

> **Nota: Domain Watch** não é compatível com a instalação de agentes em máquinas Linux e Apple. Os agentes devem ser instalados em máquinas Linux e Apple de domínio fora do **Domain Watch**. Consulte **Como os agentes são instalados utilizando o Discovery** *(página 27)*.

Políticas

Discovery > Domínios > Domain Watch > Guia Políticas

> **Nota:** A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

Nesta seção

OU/Containers

Discovery > Domínios > Domain Watch > Políticas > Guia UO/Contêineres

> **Nota:** A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

A guia **UO/Contêineres** configura as políticas do **Discovery** por UO ou contêiner de domínio tanto para computadores quanto para contatos.

Tópicos relacionados:

- **Como configurar políticas do contêiner/UO** *(página 38)*
- **Como configurar políticas de contato** *(página 39)*
- **Como definir políticas do Discovery para contatos** *(página 26)*

Como configurar políticas por computador individual

Você pode configurar as políticas por computador individual utilizando a guia **Computadores** *(página 51)*. As políticas configuradas por computador têm precedência sobre políticas configuradas por UO/Contêiner.

Incluído e excluído

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Campos do cabeçalho

- **Status da política**

 - Original: as políticas do **Discovery** ainda não foram configuradas.

 - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.

 - Aplicada: as políticas do **Discovery** foram aplicadas.

- **Última sincronização completa**: data/hora da última sincronização completa para este domínio.
- **Última sincronização incremental**: data/hora da última sincronização incremental de todas as alterações pendentes para este domínio.

Ações

- **Política de computadores**: configura a política de computadores do **Discovery** para computadores *incluídos* em um contêiner/UO.
  - **Incluir novos computadores**: se marcado, a política atribuída a este contêiner/UO é aplicada para os computadores recentemente detectados.
  - **Atribuir automaticamente acesso ao portal para candidatos ao portal**: se marcado, estes computadores são atribuídos automaticamente para serem máquinas **candidatas ao Portal Access** *(página 29)*.
  - **Sobreposição do grupo da máquina do computador**: especifica o grupo da máquina a atribuir quando um agente é instalado. `Use Directory Default` especifica o grupo padrão da máquina para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.
- **Política de contatos**: configura a política de contatos do **Discovery** para contatos incluídos em um contêiner/UO.
  - **Incluir novos contatos**: se marcado, a política atribuída a este contêiner/UO é aplicada para os contatos recentemente detectados.
- **Aplicar alterações**: aplica as alterações das políticas pendentes do **Discovery** em todas as guias **Políticas**.

Cabeçalhos de coluna

- **Tipo**

   - Domínio

   - Contêiner

   - Unidade organizacional
- **Unidade Organizacional/Contêiner**: o nome canônico de um contêiner ou unidade organizacional no domínio Active Directory. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Incluir novos computadores**: se marcado, a política atribuída a este contêiner/UO é aplicada para os computadores recentemente detectados.
- **Computadores selecionados**: representa o número de máquinas que estão *incluídas* neste contêiner/UO. Inicialmente, este número é zero.
- **Total de computadores**: representa o número total de máquinas que são membros deste contêiner/UO.
- **Sobreposição do grupo de máquinas**: especifica o grupo de máquinas a atribuir quando um agente é instalado. `Use Directory Default` especifica o grupo padrão da máquina para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.
- **Computadores com acesso automático ao Portal**: se marcado, estes computadores são atribuídos automaticamente como máquinas **candidatas ao Portal Access** *(página 29)*.
- **Incluir novos contatos**: se marcado, a política atribuída a este contêiner/UO é aplicada para os contatos recentemente detectados.

- **Contatos selecionados**: o número de contatos que estão *incluídos* neste contêiner/UO. Inicialmente, este número é zero.
- **Total de contatos**: o número total de contatos que são membros deste contêiner/UO.

Computadores

Discovery > Domínios > Domain Watch > Políticas > Guia Computadores

A guia **Computadores** configura as políticas do **Discovery** por computador individual.

Para obter mais informações consulte:

- **Como configurar políticas do computador** *(página 39)*
- **Como definir políticas do Discovery para computadores** *(página 26)*

Como configurar políticas por UO/contêiner

Você pode configurar políticas para computadores e contatos por *UO/Contêiner* utilizando a guia **OU/Containers** *(página 49)*. As políticas configuradas por computador têm precedência sobre políticas configuradas por UO/Contêiner.

> **Nota:** A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

Incluído e excluído

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Campos do cabeçalho

- **Status da política**
  -  - Original: as políticas do **Discovery** ainda não foram configuradas.
  -  - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.
  -  - Aplicada: as políticas do **Discovery** foram aplicadas.
- **Última sincronização completa**: data/hora da última sincronização completa para este domínio.
- **Última sincronização incremental**: data/hora da última sincronização incremental de todas as alterações pendentes para este domínio.

Ações

- **Configurar política de computadores**: configura a política de computadores do **Discovery** para computadores incluídos em um contêiner/UO.
  - **Política do computador**: `Include` ou `Do Not Include`
  - **Sobreposição do grupo da máquina do computador**: especifica o grupo da máquina a atribuir quando um agente é instalado. `Use Default` especifica o grupo padrão da máquina para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.
- **Aplicar alterações**: aplica as alterações das políticas pendentes do **Discovery** em todas as guias **Políticas**.

Cabeçalhos de coluna

- **Tipo**

 - Domínio

 - Contêiner

 - Unidade organizacional

- **Unidade Organizacional/Contêiner**: o nome canônico de um contêiner ou unidade organizacional no domínio Active Directory. A Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Nome do computador**: o nome canônico do computador em um domínio Active Directory.
- **Incluída**: se marcado, esta máquina pode ser instalada com um agente utilizando o **Discovery**.
- **Sobreposição do grupo de máquinas**: especifica o grupo de máquinas a atribuir quando um agente é instalado. `Use Default` especifica o grupo padrão da máquina para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.

Grupos

Discovery > Domínios > Domain Watch > Políticas > Guia Grupos

Nota: *A guia* **UO/Contêineres** *e a guia* **Grupos** *são exibidas se o* **conjunto de recursos do Directory Services** *(página 25) estiver habilitado. As políticas para contatos são configuradas utilizando a guia* **UO/Contêineres**.

A guia **Grupos** configura as políticas do **Discovery** por grupos (de usuários) para um domínio selecionado.

Para obter mais informações consulte:

- **Como configurar políticas de grupo** *(página 40)*
- **Como gerenciar o Portal Access remoto** *(página 24)*
- **Como habilitar o Portal Access no Discovery** *(página 29)*
- **Como habilitar/desabilitar contas dos usuários de domínio ou redefinir senhas de usuários de domínio** *(página 30)*
- **Como fazer alterações nos logons dos usuários gerenciados do Discovery** *(página 31)*
- **Formatos compatíveis de logon no domínio** *(página 31)*

Como configurar políticas por usuário individual

Você pode configurar as políticas por usuário individual utilizando a guia **Usuários** *(página 54)*.

Incluído e excluído

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Campos do cabeçalho

- **Status da política**

   - Original: as políticas do **Discovery** ainda não foram configuradas.

   - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.

   - Aplicada: as políticas do **Discovery** foram aplicadas.
- **Última sincronização completa**: data/hora da última sincronização completa para este domínio.
- **Última sincronização incremental**: data/hora da última sincronização incremental de todas as alterações pendentes para este domínio.

Ações

- **Configurar política do grupo**: *inclui* usuários selecionados como usuários do VSA *ou* candidatos ao Portal Access. Quando este diálogo se abre, a lista suspensa **Política de usuário do membro** fornece as seguintes opções:
  - `Do Not Include Users` - Não criar logons de usuário do VSA ou logons de Portal Access para usuários do domínio listados nesse grupo de usuários.
  - `Create Staff Members` : cria um registro do membro da equipe. É possível atribuir a estes usuários acesso Portal Access a uma máquina *manualmente*.

    Nota: *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.
  - `Create Staff and make Auto Portal Candidates` : designa usuários de domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
  - `Create VSA Users` - Cria logons do usuário do VSA para usuários do domínio listados neste grupo de usuários.
    - ✓ Pesquisa de função
    - ✓ Pesquisa de escopo
  - Se *um escopo com o mesmo nome da organização* ainda não existe, um + é exibido no lado da lista suspensa **Pesquisa de escopo** da caixa de diálogo **Política do usuário**. Clicar no ícone + permite que você crie um novo escopo que tem o mesmo nome da organização associada ao domínio. Após o escopo ser criado, o + não é mais exibido ao lado da lista suspensa **Pesquisa de escopo**, e o texto no topo da caixa de diálogo indica que o escopo padrão já existe.
  - Se o mesmo usuário é atribuído a diversos grupos, e diferentes funções e escopos são atribuídos a cada grupo, então, quando o usuário entrar no VSA, estas funções e escopos estarão disponíveis no seletor de funções/escopo no canto superior direito da janela do VSA.

    Nota: *As atribuições de funções/escopo utilizando a guia* **Grupos** *e a guia* **Usuários** *podem ser modificadas e reaplicadas diversas vezes. Alterações sucessivas farão com que as funções e os escopos se acumulem, em vez de serem substituídos.* O **Discovery** nunca remove registros no VSA.
  - **Sobreposição do departamento do usuário**: especifica o departamento a ser atribuído a um usuário criado recentemente. Utilizar Padrão do diretório especifica o departamento padrão para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.
- **Aplicar alterações**: aplica as alterações das políticas pendentes do **Discovery** em todas as guias **Políticas**.

Cabeçalhos de coluna

- **Tipo** - - Grupo
- **Nome do grupo**: Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Política de usuários**
  - `Do Not Include Users` - Não criar logons de usuário do VSA ou logons de Portal Access para usuários do domínio listados nesse grupo de usuários.
  - `Create Staff Members` : cria um registro do membro da equipe.

- `Create Staff and make Auto Portal Candidates` : designa usuários de domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
- `Create VSA Users` - Cria logons do usuário do VSA para usuários do domínio listados neste grupo de usuários.

- **Total de usuários**: o número total de usuários neste grupo.
  - **Política da função**: a função do VSA a ser atribuída a usuários do VSA recém-criados se a **Política de usuários** for `Create VSA Users`.
  - **Política do escopo**: o escopo do VSA a ser atribuído a usuários do VSA recém-criados se a **Política de usuários** for `Create VSA Users`.
- **Sobreposição do departamento**: especifica o departamento a ser atribuído a um usuário recém-criado. Utilizar Padrão do diretório especifica o departamento padrão para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.

Usuários

Discovery > Domínios > Domain Watch > Políticas > Guia Usuários

A guia **Usuários** configura as políticas do **Discovery** por usuário individual.

Tópicos relacionados:

- **Como definir políticas do Discovery para usuários** *(página 26)*
- **Como configurar políticas de usuário** *(página 42)*

Como configurar políticas por grupo (usuário)

Você pode configurar políticas para usuários por grupo (de usuários) utilizando a guia **Grupos** *(página 52)*.

Nota: A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**.

Incluído e excluído

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Campos do cabeçalho

- **Status da política**
  - - Original: as políticas do **Discovery** ainda não foram configuradas.
  - - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.
  - - Aplicada: as políticas do **Discovery** foram aplicadas.
- **Última sincronização completa**: data/hora da última sincronização completa para este domínio.
- **Última sincronização incremental**: data/hora da última sincronização incremental de todas as alterações pendentes para este domínio.

Ações

- **Configurar política de usuários**: *inclui* o usuário selecionado como usuário do VSA *ou* candidato ao Portal Access. Quando este diálogo se abre, a lista suspensa **Política de usuário do membro** fornece as seguintes opções:

- `Do Not Include Users` : não cria um logon de usuário do VSA ou logon ao Portal Access para este usuário do domínio.
- `Create Staff Members` : cria um registro do membro da equipe. É possível atribuir a este usuário acesso Portal Access a uma máquina *manualmente*.

  Nota: *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.

- `Create Staff and make Auto Portal Candidates` : designa um usuário do domínio neste grupo de usuários como candidatos ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
- `Create VSA Users` : cria um logon de usuário do VSA para o usuário de domínio selecionado.
  - ✓ Pesquisa de função
  - ✓ Pesquisa de escopo
- **Sobreposição do departamento do usuário**: especifica o departamento a ser atribuído a um usuário criado recentemente. Utilizar Padrão do diretório especifica o departamento padrão para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.

- **Aplicar alterações**: aplica as alterações de políticas do **Discovery** tanto para a guia **Políticas > Computadores** quanto para a guia **Políticas do usuário**.

Cabeçalhos de coluna

- **Nome do usuário**: Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Política**
  - `Do Not Include Users` : não cria um logon de usuário do VSA ou logon ao Portal Access para este usuário do domínio.
  - `Create Staff Members` : cria um registro do membro da equipe.
  - `Create Staff and make Auto Portal Candidates` : designa este usuário de domínio como candidato ao Portal Access. Consulte **Como criar candidatos ao Portal Access** *(página 29)* para mais informações.
  - `Create VSA Users` : cria um logon de usuário do VSA para este usuário de domínio.
- **Membros do grupos**: os grupos dos quais este usuário é membro.
  - **Política da função**: a função do VSA a ser atribuída ao usuário recém-criado do VSA se a **Política** for `Create VSA Users`.
  - **Política do escopo**: o escopo do VSA a ser atribuído ao usuário recém-criado do VSA se a **Política** for `Create VSA Users`.
- **Sobreposição do departamento**: especifica o departamento a ser atribuído a um usuário recém-criado. `Use Directory Default` : especifica o departamento padrão para a organização associada com o domínio utilizando a guia **Implementação da verificação** *(página 46)*.

Alertando os perfis

Discovery > Domínios > Domain Watch > Guia Políticas de alerta

> **Nota:** A guia **Perfis de alerta** somente é exibida se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado.

A guia **Perfis de alerta** configura as políticas de alerta do **Discovery** para um domínio selecionado.

Para obter mais informações consulte:

- **Alertas de verificação e alertas de domínio** *(página 34)*
- **Como configurar políticas de alerta** *(página 43)*

Ações

- **Configurar**: edita as configurações da política de alerta do domínio e da verificação exibidas nesta guia.

Verificar política de alertas

Exibe as configurações da política de alerta da *verificação* habilitadas/desabilitadas.

- Alarme de advertência
- Alarme de falha
- Ticket de advertência
- Ticket de falha
- E-mail de advertência
- E-mail de falha
- Endereços de e-mail (para advertência)
- Endereços de e-mail (para falha)

Política de alertas do domínio

Exibe as configurações da política de alerta do *domínio* habilitadas/desabilitadas.

- Tipo/Tipo de objeto
  -  - Computador
  -  - Contato
  -  - Contêiner
  -  - Domínio
  -  - Grupo
  -  - Unidade organizacional
  -  - Usuário
- Alarme em criação
- Alarme em alteração
- Alarme em eliminação
- Ticket em criação
- Ticket em alteração
- Ticket em exclusão
- Enviar e-mail em caso de criação
- Enviar e-mail em caso de alteração
- Enviar e-mail em caso de exclusão
- Endereços de e-mail

Programação e status

Discovery > Domínios > Domain Watch > Guia Agendamento e status

A guia **Agendamento e status** agenda sincronizações completas para um domínio selecionado. Ela também exibe o status de sincronizações completas e incrementais.

Para obter mais informações consulte:

- **Sincronização** *(página 32)*

Ações

- **Agendar sincronização completa**:agenda uma sincronização completa uma vez ou periodicamente. Cada tipo de recorrência (Uma vez, Minutos, Por hora, Diariamente, Semanalmente, Mensalmente, Anualmente) exibe opções adicionais apropriadas para cada tipo de recorrência. A programação periódica inclui definir as datas inicial e final para a recorrência. As opções são:
  - **Janela de distribuição** - Reprograma a tarefa para uma hora selecionada aleatoriamente, dentro do número de períodos especificado, para dividir o tráfego de rede e cargas do servidor. Por exemplo, se um horário agendado para a tarefa for às 3 horas da manhã e a janela de distribuição for de 1 hora, então, o agendamento da tarefa será alterado para executar em um tempo aleatório entre 3 horas e 4 horas da manhã.
  - **Ignorar se não estiver conectado** - Se estiver selecionada e a máquina estiver desconectada, ignora e executa o próximo período e hora programados. Se estiver em branco e a máquina desconecta, executa a tarefa assim que a máquina estiver conectada novamente.
  - **Alimentação está off-line** - somente Windows. Se selecionado, inicia a máquina se off-line. Requer o Wake-On-LAN ou vPro ou outro sistema gerenciado na mesma LAN.
  - **Excluir o seguinte intervalo de tempo**: **se aplica apenas à janela de distribuição.** Caso esteja marcado, especifica um intervalo de tempo para excluir o agendamento de uma tarefa na janela de distribuição. A especificação de intervalo de tempo fora da janela de distribuição é ignorada pelo agendador.
- **Cancelar sincronização completa**: cancela o agendamento da sincronização completa.

Campos do cabeçalho

- **Verificar status**
  - - Desinstalada: uma verificação não está instalada para este domínio.
  - - Processando: a verificação executando uma solicitação do usuário.
  - - Instalada: a verificação está instalada e a detecção de informações foi completada.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** não foram modificadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas e aplicadas.
  - - Ativada: a verificação está monitorando o domínio. As políticas do **Discovery** foram modificadas, mas ainda não foram aplicadas por, ao menos, três intervalos de sincronização. O administrador do **Discovery** pode ter esquecido de aplicar as políticas modificadas.
  - - Atenção ou off-line: a verificação encontrou um problema que pode requerer atenção do usuário. Pelo fato de que o status de atenção da verificação pode ser corrigido automaticamente, o status de atenção não corresponde necessariamente a uma alerta de aviso ou alerta de erro. Se off-line, a máquina do domínio fica indisponível. As páginas do

> **Nota:** **Discovery** não são atualizadas automaticamente. Clique no botão **Atualizar** para assegurar que o **Status da verificação** mais recente seja exibido.

- **Status de computadores/status** e **Status de políticas do usuário**
  -  - Original: as políticas do **Discovery** ainda não foram configuradas.
  -  - Modificada: as políticas do **Discovery** já foram configuradas, mas não foram aplicadas. Após clicar no botão **Aplicar alterações**, este ícone permanece inalterado até que a coleta seja completada.
  -  - Aplicada: as políticas do **Discovery** foram aplicadas.

Informações gerais

- **Nome do domínio**: o nome do domínio Active Directory.
- **Incr. Sincr. Intervalo (minutos)**: o intervalo da sincronização incremental para este domínio. O intervalo da sincronização é configurado quando uma verificação é ativada utilizando a guia **Implementação da verificação** *(página 46)*. Esta opção somente está disponível se **O conjunto de recursos do Directory Services** *(página 25)* estiver disponível.
- **Nome do usuário administrador**: o nome do administrador da credencial usada para se conectar ao domínio Active Directory.

Histórico de sincronização

- **Entrada recente do agente**: a entrada mais recente de algum agente no domínio.
- **Entrada ativa do agente**: data/hora em que o agente da verificação deste domínio se conectou pela última vez.
- **Última solicitação de verificação**: data/hora em que uma solicitação de sincronização foi enviada para a verificação deste domínio.
- **Última execução de script** : data/hora que um script foi executado pela última vez para este domínio.
- **Última visualização completa**: data/hora em que uma sincronização de visualização foi executada pela última vez para este domínio. Uma visualização somente é realizada quando uma verificação se encontra instalada.
- **Última sincronização completa**: data/hora da última sincronização completa para este domínio.
- **Última sincronização incremental**: data/hora da última sincronização incremental de todas as alterações pendentes para este domínio.
- **Status do último script**: status do último script do **Discovery** executado para este domínio. Por exemplo, `Then/Else Success`ou `Then/Else failure in step N`.

Sincronização agendada

- **Período da sincronização completa**: o padrão agendado da sincronização completa para este domínio. Pode ser uma vez ou recorrente.
- **Próxima sincronização completa**: a próxima sincronização completa agendada para este domínio.

Computadores

Discovery > Domínios > Computadores

A página **Computadores** lista as contas de **ID da organização/ID do grupo/ID da máquina** *(página 71)* criadas utilizando as políticas do computador do **Discovery** aplicadas, por todos os domínios monitorados pelas verificações do **Discovery**.

Contas de IDs de máquinas recém-criadas são inicialmente exibidas como contas modelo de ID da máquina "vazia" - identificadas com um ícone de entrada, que significa que não há agente correspondente para esta conta da ID da máquina.

As alterações feitas para computadores **incluídos** *(página 72)* atualizam suas contas de ID de máquinas do VSA correspondentes na próxima sincronização.

Para obter mais informações consulte:

- **Como os agentes são instalados utilizando o Discovery** *(página 27)*

- **Como as contas de ID de máquinas são criadas no Discovery** *(página 28)*
- **Como as máquinas que se movem no domínio são refletidas no Discovery** *(página 29)*

Painel superior

Ações

- **Implementar agente**: se um agente ainda não foi implementado para uma conta da ID da máquina criada, você pode implementar o agente manualmente utilizando esta página.
- **Sincronizar máquinas**: Se um agente já existe em uma máquina gerenciada em um grupo de máquinas diferente, então o **Discovery** cria uma conta **modelo da ID da máquina** *(página 71)* vazia, identificada com um ícone de entrada, e nenhum agente faz entrada. A nova conta modelo da ID da máquina exibe uma **ID da organização/ID do grupo/ID da máquina** *(página 71)* com base no nome canônico do computador no domínio Active Directory. *Você pode mesclar estas contas duplicadas.* A conta do agente ativa existente adota o nome da nova conta modelo da ID da máquina, então, a nova conta modelo da ID da máquina é excluída. Nenhum dado é perdido pela mescla, e a conta da ID da máquina agora combina seu local na hierarquia do domínio.
- **Atualizar**: atualiza a página.

Cabeçalhos de coluna

- **ID Machine.Group ID**: Nome de **ID de máquina/ID de grupo/ID de organização** *(página 71)* exclusivo para uma máquina no VSA.
- **Domínio**: o nome do domínio Active Directory.
- **Há duplicidade**: se marcado, uma conta da ID da máquina do VSA existe para este computador do domínio.
- **Duplicar ID do grupo de máquinas**: o nome de uma ID do grupo de máquinas duplicada para esta mesma máquina.
- **Agente implementado**: se selecionado, um agente foi implementado neste computador.
- **Instalar pacote**: o agente instala o pacote selecionado para este domínio do computador. O pacote de instalação do agente para um domínio é especificado utilizando a página **Implementação do agente** *(página 48)*.
- **SO**: o sistema operacional do computador.
- **Acesso automático ao Portal**: um usuário de domínio é automaticamente atribuído como o usuário do **Portal Access** *(página 29)* da máquina de domínio se o **Acesso automático ao Portal** está habilitado *tanto* ao usuário de domínio quanto ao computador de domínio.
- **Nome canônico**: Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Data da implementação**: a data/hora em que uma implementação do agente foi tentada.
- **Status da implementação**: o status da implementação do agente. Revise mensagens de erro utilizando esta coluna.

Painel inferior

O painel inferior exibe informações detalhadas sobre a linha selecionada no painel superior.

Configurações do agente VSA

- **ID da máquina**: Nome de **ID de máquina/ID de grupo/ID de organização** *(página 71)* exclusivo para uma máquina no VSA.
- **Pacote de implementação do agente**: o pacote de instalação do agente selecionado para este domínio do computador.

Status

- **Sistema operacional**: o sistema operacional do computador.
- **Última reinicialização**: a data/hora da última reinicialização do computador.
- **Criado no AD**: a data/hora em que o computador foi adicionado ao domínio Active Directory.
- **Última modificação no AD**: a data/hora em que o registro do computador foi modificado pela última vez no domínio Active Directory.
- **Última ID de usuário conectada**: a ID do usuário do último logon no computador.
- **Nome do último usuário conectado**: o nome do usuário do último logon no computador.

Detalhes do servidor de diretório

Descreve informações detalhadas sobre o computador no domínio.

- **Nome do computador**: o nome do computador.
- **Nome do domínio**: o nome do domínio Active Directory.
- **Nome canônico**: Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Nome distinguido**: Um **nome distinguido** fornece as mesmas informações de um nome canônico, formatado como uma série de atributos, sequenciados em ordem inversa ao nome canônico. NC = Nome comum ou contêiner. UO = Unidade organizacional. CD = Componente do domínio.
- **Nome do Host DNS**: o nome do domínio totalmente qualificado do computador.
- **Tipo de CD**: `Domain Server` ou `Domain Member`.
- **Site**: o nome do local geográfico, abrangendo uma ou mais sub-redes. Uma rede de área local (LAN).
- **Descrição**: uma descrição de uma linha do computador.
- **Local**: o site/a sub-rede do computador. Usado para localizar impressoras e outros recursos próximos.
- **Grupo primário**: um usuário ou computador está associado a um **grupo primário** para conformidade POSIX, com base em UNIX. Para computadores do domínio Active Directory, o grupo primário padrão é `Domain Computers`.

Contatos

Discovery > Domínio > Contatos

Nota: As políticas para contatos são configuradas utilizando a guia **UO/Contêineres**. A guia **UO/Contêineres** e a guia **Grupos** são exibidas se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado.

A página **Contatos** lista os registros de pessoal criados utilizando as políticas de contato do **Discovery** aplicadas, para todos os domínios monitorados por verificações do **Discovery**.

As alterações feitas nos contatos **incluídos** *(página 72)* do domínio atualizam seus registros de pessoal do VSA correspondentes na próxima sincronização.

Painel superior

Ações

- **Atualizar**: atualiza a página.

Cabeçalhos de coluna

- **Contato**: o nome canônico para o contato do domínio. A Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Pessoal**: o nome completo do registro de pessoal criado no VSA.
- **Org. VSA**: a organização do VSA do registro de pessoal.
- **Depart. VSA**: o departamento do VSA do registro de pessoal.
- **E-mail**: o e-mail do registro de pessoal.
- **Número de telefone**: o número de telefone do registro de pessoal.
- **Número de celular**: o número do telefone celular do registro de pessoal.

Painel inferior

O painel inferior exibe informações detalhadas detectadas a partir do domínio sobre um contato selecionado no painel superior.

Geral

- **Nome**: o nome do contato.
- **Sobrenome**: o sobrenome do contato.
- **Nome de exibição**: o nome completo do contato.
- **Descrição**: uma descrição do contato.
- **Escritório**: o local do escritório do contato.
- **Número de telefone**: o número de telefone principal do contato.
- **E-mail**: o e-mail do contato.

Endereço

O endereço do contato.

- **Rua**
- **Caixa postal**
- **Cidade**
- **Estado/Província**
- **CEP/Código postal**
- **País/Região**

Telefones

Os números de telefone e avisos do contato.

- **Principal**
- **Pager**
- **Celular**
- **Fax**
- **Telefone IP**
- **Notas**

Conta

- **Nome comum**: o nome comum do contato.
- **Nome canônico**: o nome canônico do contato. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou

grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.

- **Nome do domínio**: o nome do domínio Active Directory.
- **Nome distinguido**: Um **nome distinguido** fornece as mesmas informações de um nome canônico, formatado como uma série de atributos, sequenciados em ordem inversa ao nome canônico. NC = Nome comum ou contêiner. UO = Unidade organizacional. CD = Componente do domínio.
- **Descrição**: uma descrição do contato.
- **Criado no AD**: a data/hora em que o registro do contato foi criado no domínio Active Directory.
- **Última modificação no AD**: a data/hora em que o registro do contato foi modificado pela última vez no domínio Active Directory.

Empresa

- **Cargo**: o título do cargo do contato.
- **Departamento**: o departamento do qual o contato é membro.
- **Empresa**: a empresa da qual o contato é membro.
- **Gerente**: o gerente do contato.
- **Subordinados**: os usuários ou contatos que se reportaram a este contato.

Usuários e Usuários do portal

Discovery > Domínios > Usuários e Portal Access

Usuários e Portal Access lista os usuários do VSA e candidatos ao Portal Access criados utilizando as políticas aplicadas do grupo do **Discovery**, para todos os domínios monitorados por verificações do **Discovery**.

As alterações feitas nos grupos de domínio (usuário) **incluídos** *(página 72)* atualizam seus registros de candidatos ao Portal Access e usuários do VSA correspondentes na próxima sincronização.

Para obter mais informações consulte:

- **Como definir políticas do Discovery para usuários** *(página 26)*
- **Como habilitar o Portal Access no Discovery** *(página 29)*
- **Como habilitar/desabilitar contas dos usuários de domínio ou redefinir senhas de usuários de domínio** *(página 30)*
- **Como fazer alterações nos logons dos usuários gerenciados do Discovery** *(página 31)*
- **Formatos compatíveis de logon no domínio** *(página 31)*

Painel superior

Ações

- **Desabilitar conta**: desabilita a conta do usuário de domínio imediatamente. Afeta os logons do VSA e logons do Portal Access utilizando o mesmo logon no domínio. Esta opção é somente exibida se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado.
- **Habilitar conta**: habilita uma conta do usuário de domínio imediatamente. Afeta os logons do VSA e logons do Portal Access utilizando o mesmo logon no domínio. Esta opção é somente exibida se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado.
- **Redefinir senha**: redefine uma senha do usuário de domínio. Em vigor no próximo logon. Afeta os logons do VSA e logons do Portal Access utilizando o mesmo logon no domínio. Esta opção é somente exibida se o **conjunto de recursos do Directory Services** *(página 25)* estiver habilitado. As opções são:
  - **Desbloquear conta**: se selecionado, desbloqueia uma conta bloqueada do usuário de domínio.

  - **Forçar alteração de senha**: se selecionado, força o usuário de domínio a alterar a senha redefinida na próxima vez que o usuário entrar no domínio.
- **Atribuir usuário ao portal**: atribui manualmente Portal Access a um computador de domínio *para* um usuário de domínio.
- **Remover usuários do portal**: remove manualmente o Portal Access a um computador de domínio *de* um usuário de domínio.
- **Atualizar**: atualiza a página.

Cabeçalhos de coluna

- **Nome do domínio**: o nome do domínio Active Directory.
- **Usuário de domínio**: o nome de domínio totalmente qualificado do usuário.
- **Nome do usuário**: o nome do usuário de domínio.
- **Nome de usuário de logon**: o nome de usuário do VSA, se este também for um logon de usuário do VSA.
- **Habilitado**: se selecionado, o usuário está habilitado no domínio.
- **Org. VSA**: a **organização** *(página 70)* do VSA da qual este usuário é membro.
- **Depart. VSA** : o departamento do VSA do qual este usuário é membro.
- **Supervisor**: o supervisor do VSA para este membro da equipe.
- **Expira**: a data em que esta conta expira.
- **VSA**: se selecionado, o usuário do VSA pode fazer logon no VSA utilizando a sua credencial de domínio.
- **Portal**: se selecionado, este usuário do domínio é atribuído como usuário do Portal Access da máquina de domínio listada na coluna **Atribuição ao Portal**. Se desmarcado, o usuário não está atribuído a nenhum computador de domínio como usuário do Portal Access.
- **Acesso automático ao Portal**: um usuário de domínio é automaticamente atribuído como o usuário do **Portal Access** *(página 29)* da máquina de domínio se o **Acesso automático ao Portal** está habilitado *tanto* ao usuário de domínio quanto ao computador de domínio.
- **Atribuição do portal**
  - `None (will be assigned upon login to an 'Auto Portal' computer)` : o acesso automático ao Portal está habilitado para este usuário.
  - `None (assign using the 'Assign Portal User' button)` - O acesso automático ao Portal não está habilitado para este usuário, mas pode ser atribuído manualmente para ser o usuário do Portal Access de uma máquina.

    > **Nota:** *O usuário somente pode ser atribuído manualmente como usuário do Portal Access de uma máquina — utilizando a página* **Usuários e Usuários do portal** *(página 62) — se tiver sido a última pessoa conectada naquela máquina.* A lista de máquinas elegíveis é exibida no campo **Última pessoa conectada nas máquinas** no painel inferior desta mesma página.

  - `<machineID>` : o computador do domínio atualmente atribuído a este usuário de domínio com Portal Access para aquela máquina.
  - `VSA User` : o usuário é um usuário do VSA e não pode ser atribuído como um usuário do Portal Access de uma máquina.
- **E-mail**: o e-mail do usuário de domínio.
- **Telefone**: o telefone do usuário de domínio.
- **Cidade**: a cidade do usuário de domínio.
- **País**: o país do usuário de domínio.
- **Política de usuários**: a política atribuída a este usuário.

Painel inferior

O painel inferior exibe informações detalhadas detectadas a partir do domínio sobre um usuário selecionado no painel superior.

Detalhes do usuário

Geral

- **Nome**: o nome do usuário.
- **Sobrenome**: o sobrenome do usuário.
- **Nome de exibição**: o nome completo do usuário.
- **Escritório**: a localização do escritório do usuário.
- **Número do telefone**: o número do telefone principal do usuário.
- **E-mail**: o e-mail do usuário.
- **Visualizar todos os tickets**: se essa opção for marcada, o usuário do VSA associado com este membro da equipe poderá visualizar todos os tickets do **Service Desk** em seu escopo, assim como os tickets associados com este registro específico de membro da equipe. Se essa opção for deixada em branco, este usuário do VSA poderá visualizar somente tickets do **Service Desk** associados com este registro específico de membro da equipe.
- **Aprovar todos os registros de tempo**: se essa opção for marcada, esse membro da equipe poderá aprovar qualquer registro de tempo. Isso garante que todos os registros de tempo possam ser aprovados em tempo hábil caso outros aprovadores estejam temporariamente indisponíveis.
- **Padrão de aprovação do registro de tempo**: Especifica o padrão de aprovação necessário para aprovar os registros de tempo desse membro da equipe. Os padrões de aprovação determinam se o supervisor do membro da equipe, ou o supervisor do supervisor, ou ambos, precisa aprovar o registro de tempo do membro da equipe.
- **Logon no VSA**: se `Yes`, o VSA pode fazer logon no VSA utilizando a sua credencial de domínio.
- **Funções do VSA**: as funções do VSA atribuídas ao usuário do VSA.
- **Escopos do VSA**: os escopos do VSA atribuídos ao usuário do VSA.

Endereço

O endereço do usuário.

- **Rua**
- **Caixa postal**
- **Cidade**
- **Estado/Província**
- **CEP/Código postal**
- **País/Região**

Telefones

Os números de telefone e avisos do usuário.

- **Principal**
- **Pager**
- **Celular**
- **Fax**
- **Telefone IP**
- **Notas**

Últimas máquinas acessadas

- **Última entrada (Máquinas)**: o computador de domínio no qual o usuário de domínio entrou pela última vez. O Portal Access para uma máquina de domínio somente pode ser atribuído à última máquina à qual um usuário do domínio acessou.

Conta

- **Nome de logon do usuário**: o nome do logon do usuário de domínio.
- **Conta expira**: a data de expiração da conta do domínio.
- **Nome comum**: o nome comum do usuário no domínio.
- **Nome canônico**: o nome canônico do usuário. Um **nome canônico** fornece a *hierarquia completa de contêiner/UOs* utilizada para localizar pastas e itens, tais como computadores, contatos ou grupos, em um domínio, similar em formato ao nome do caminho completo de um arquivo em um diretório de disco.
- **Nome do domínio**: o nome do domínio Active Directory.
- **Nome distinguido**: Um **nome distinguido** fornece as mesmas informações de um nome canônico, formatado como uma série de atributos, sequenciados em ordem inversa ao nome canônico. NC = Nome comum ou contêiner. UO = Unidade organizacional. CD = Componente do domínio.
- **Última alteração de senha**: a data da última alteração de senha.
- **Último logon**: a data/hora em que o usuário se conectou pela última vez.
- **Último logoff**: a data/hora na qual o usuário se desconectou pela última vez.
- **Criado no AD**: a data/hora em que o registro do usuário foi criado no domínio Active Directory.
- **Última modificação no AD**: a data/hora em que o registro do usuário foi modificado pela última vez no domínio Active Directory.

Empresa

- **Título**: o título do cargo do usuário.
- **Departamento do domínio**: o departamento do qual o usuário é membro.
- **Departamento do VSA**: o departamento do qual o registro de pessoal do VSA é membro.
- **Empresa do domínio**: a empresa da qual o usuário é membro.
- **Supervisor**: o usuário ou contato ao qual este usuário se reporta. Chamado de `Manager` no domínio e `Supervisor` no VSA.
- **ID da Org. do VSA**: o identificador do VSA da **organização** *(página 70)*.
- **Nome da Org. do VSA**: o nome amigável do VSA da organização.
- **Descrição**: uma descrição da conta do usuário de domínio.
- **Subordinados**: os contatos de domínio ou usuários de domínio que se reportam a este usuário de domínio.

Guia Portal Access

Detalhes adicionais são exibidos na guia **Portal Access** se o usuário é um **candidato ao Portal Access** *(página 29)*.

Configurações de portal VSA

Estas configurações são as mesmas daquelas mostradas na página Agente > **Portal Access** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#438.htm)*.

- **Portal Access habilitado**: se `Yes`, o usuário de domínio tem um logon remoto ao Portal Access atribuído para uma máquina gerenciada do VSA.
- **ID do usuário**: a ID do usuário do Portal Access.
- **Nome de contato**: o nome do usuário do Portal Access.
- **E-mail de contato**: o nome do usuário do Portal Access.
- **Telefone de contato**: o telefone do usuário do Portal Access.

> **Nota:** A guia **Alterar perfil** do Portal Access é preenchida automaticamente com o *nome, e-mail* e *número do telefone* do usuário atualmente conectado no candidato do Portal Access. Os campos do remetente de novos tickets do **Service Desk** são preenchidos com as informações de contato armazenadas na guia **Alterar perfil**. Isto significa que os usuários do Portal Access não precisam reinserir as mesmas informações de contato cada vez que criam um novo ticket do **Service Desk**.

- **Preferência de idioma**: a preferência de idioma dos usuários do portal.
- **Função da máquina**: a **função da máquina** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#4827.htm)* atribuída à máquina do Portal Access.
- **Mostrar notas como dica**: se marcado, as notas de Agente > **Editar perfil** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#256.htm)* são incluídas como parte da dica que é exibida sempre que o cursor passar sobre um ícone de status de verificação da ID da máquina.
- **Atribuir automaticamente tickets de e-mails recebidos**: se `Yes`, atribui-se automaticamente um ticket para esta ID da máquina se o leitor de e-mail do ticket receber um e-mail do mesmo endereço de e-mail como o e-mail de contato. Se aplica quando novos e-mails chegam no leitor de e-mail de tickets que não são mapeados para nenhum dos mapeamentos de e-mail.

> **Nota:** : se diversas IDs de máquinas tem o mesmo contato de e-mail, então, somente uma ID de máquina pode ter esta caixa de verificação selecionada.

- **Atribuição ao portal**: a máquina à qual o usuário do Portal Access está atribuído.
- **Último acesso à máquina**: a data/hora que o usuário do Portal Access acessou a máquina pela última vez.

Administrador de máquina VSA

- **E-mail do admin.**: o endereço de e-mail que fornece suporte de administrador a esta máquina gerenciada. Configure utilizando a página Agente > **Editar perfil** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#256.htm)*.

Gerente do computador do servidor de diretório+

- **Gerente**: o usuário de domínio ao qual este usuário de domínio se reporta. Chamado de `Manager` no domínio Active Directory e `Supervisor` no VSA.
- **Escritório**: a localização do escritório do usuário.
- O endereço do usuário:
  - **Rua**
  - **Cidade**
  - **Estado/Província**
  - **País/Região**
- **Número de telefone** : o número de telefone do usuário.
- **Nº de fax** : o número de fax do usuário.

Capítulo 3

Administração

Neste capítulo

Configurações

Discovery > Administração > Configurações

A página **Configurações** configura as opções e os valores padrões para todo o módulo do **Discovery**.

Configuração do Discovery

- **Permitir detecção automática da rede**: se marcado, as redes são detectadas e criadas com base em, ao menos, um agente instalado em cada rede.
- **Intervalo, em minutos, para a detecção da rede**: se **Permitir detecção automática da rede** estiver selecionado, o número de minutos entre as detecções de rede.
- **Usar somente agentes on-line na detecção de rede**: se marcado, somente agentes on-line são usados para detectar redes.
- **Ignorar redes que começam com 192,168...** : se marcado, a varredura de redes privadas iniciando com 192.168 não é feita.
- **Ignorar redes que começam com 172...** : se marcado, a varredura de redes privadas iniciando com 172 não é feita.
- **Ignorar redes que começam com 10...** : se marcado, a varredura de redes privadas iniciando com 10 não é feita.
- **Ignorar redes que tenham máscara de sub-rede de 255.255.255.255**: se marcado, a varredura de redes de um único nó não é feita porque somente um dispositivo pode existir na rede e ele deve pertencer à máquina do agente que está realizando a varredura.

Alarmes padrão

Configura valores padrões, marcado ou não marcado, para a **Guia Perfis de alertas** *(página 14)*.

- **Alertar sobre novo dispositivo**
- **Ticket em novo dispositivo**
- **Enviar e-mail em caso de novo dispositivo**
- **Alterar alarme em IP**
- **Ticket em alteração de IP**
- **Enviar e-mail em caso de alteração de IP**

Ações

- **Editar**: edita as configurações.

Registro de auditoria

Discovery > Administração > Log de auditoria

A página **Log de auditoria** exibe um log das atividades do módulo **Discovery** por:

- **ID do evento**
- **Data do evento**
- **Admin**
- **Nome do evento**
- **Mensagem**

Se as informações tiverem sido alteradas ou removidas inesperadamente, verifique essa página para determinar quais eventos e administradores podem estar envolvidos.

Essa tabela é compatível com **colunas selecionáveis, classificação de coluna, filtragem de coluna e larguras de colunas flexíveis** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#6875.htm)*.

KDS - Atividade do domínio

Centro de informações > Emissão de relatórios > Relatórios > KDS - Atividade do domínio

- É exibido somente se o módulo complementar do Discovery estiver instalado.

A definição do relatório da **Atividade do domínio** gera um relatório das alterações de configuração do domínio visíveis para **Discovery**.

Configure o relatório usando estes parâmetros:

Seleção de tempo

Filtrar por intervalo de datas.

- **Iniciar DateTime**
- **DateTime final**

Atividade

Filtrar por tipo de objeto e tipo de ações realizadas nestes objetos.

- **Tipos de objetos**: `Computer`, `Contact`, `Container`, `Domain`, `Group`, `Organization Unit`, `User`
- **Tipos de ações**: `Created`, `Updated`, `Deleted`

Glossário

Acesso ao portal

O Acesso ao portal é uma sessão do Conectar ao-vivo iniciada pelo usuário da máquina. O usuário da máquina exibe a página **Acesso ao portal** ao clicar no ícone do agente  na bandeja do sistema de uma máquina gerenciada. O **Portal Access** contém opções de usuário de máquina, como alterar as informações de contato do usuário, criar ou rastrear tickets de problemas, conversar com usuários do VSA ou controlar remotamente a sua própria máquina a partir de outra máquina. Os logons ao **Portal Access** são definidos usando Agente > Portal Access. A lista de funções que o usuário vê durante uma sessão do **Portal Access** é determinada pela página Sistema > Funções da máquina. É possível personalizar as sessões do **Portal Access** usando a página Sistema > Personalizar > Live Connect. Ambos os instaladores dos plug-ins **Live Connect** e **Portal Access** podem ser pré-instalados com o uso da página Agente > Atualizar agente.

Agent de verificação

Discovery se comunica com um domínio Active Directory utilizando um **agente da verificação**. A verificação usa o protocolo LDAP padrão do setor para se comunicar de modo seguro com o domínio. Cada agente da verificação deve ser um membro do domínio que ele monitora. A implementação da verificação instala a funcionalidade extra que um agente necessita para agir como uma verificação.

Agentes

O VSA gerencia máquinas ao instalar um cliente de software denominado **agente** em uma máquina gerenciada. O agente é um serviço do sistema que não requer que o usuário esteja conectado para funcionar e não requer reinicialização para ser instalado. O agente é configurável e pode ficar totalmente invisível ao usuário. A única finalidade do agente é executar as tarefas solicitadas pelo usuário do VSA. Após a instalação:

- Um ícone do agente, por exemplo o  ícone do agente, é exibido na bandeja do sistema da máquina gerenciada. Os ícones dos agentes podem ser imagens personalizadas e podem ser totalmente removidos.
- A cada agente instalado é atribuída uma **ID de máquina/grupo/organização exclusiva do VSA** *(página 71)*. As IDs das máquinas podem ser criadas automaticamente durante a instalação do agente ou individualmente antes da respectiva instalação.
- Cada agente instalado usa uma das licenças disponíveis adquiridas pelo provedor de serviços.
- Os agentes são geralmente instalados por meio de pacotes criados usando Agente > Implementar agentes no VSA.
- Vários agentes podem ser instalados na mesma máquina, cada um apontando para um servidor diferente.
- Um ícone de verificação é exibido ao lado de cada ID de máquina no VSA, mostrando o status geral da máquina gerenciada. Por exemplo,  o ícone de verificação indica que um agente está on-line e que o usuário está conectado no momento.
- Clicar em um ícone de entrada exibe uma interface de máquina única da máquina gerenciada denominada Live Connect. O **Live Connect** oferece acesso instantâneo a dados e ferramentas abrangentes necessários para trabalhar nessa máquina.
- Passar o cursor do mouse sobre o ícone de entrada exibe de forma imediata uma janela de Visualização rápida do agente. É possível iniciar um procedimento de agente, visualizar logs ou iniciar o **Live Connect** de qualquer janela de visualização rápida do agente.

Conjunto de recursos

Um conjunto de recursos fornece funcionalidade avançada e especializada, que geralmente está oculta no módulo básico. O módulo básico deve ser instalado e os recursos licenciados separadamente para exibição das opções do conjunto de recursos.

Contato

Um **contato** de domínio contém informações de contato similares às informações definidas para um usuário, mas um contato não tem privilégios de logon no domínio.

Emp

O VSA oferece suporte a três tipos diferentes de relações comerciais:

- **Organizações**: oferece suporte a grupos de máquinas e gerencia máquinas usando agentes.
- **Clientes**: oferece suporte à cobrança de clientes usando o **Service Billing**.
- **Fornecedores**: oferece suporte à aquisição de materiais usando o **Service Billing**.

A tabela `Org` é uma tabela de suporte compartilhada por *organizações*, *clientes* e *fornecedores*. Cada registro na tabela `Org` é identificado por uma `orgID` exclusiva. A tabela `Org` contém informações básicas que você geralmente precisaria para manter qualquer tipo de relação comercial: endereço de correspondência, número de telefone principal, número DUNS, receita anual, etc. Como a tabela `Org` é compartilhada, você pode facilmente converter:

- Um cliente em uma organização ou fornecedor.
- Um fornecedor em uma organização ou cliente.
- Uma organização em um cliente ou fornecedor.

Nota: `myOrg` é a organização do provedor de serviços usando o VSA.

Funções da máquina

A página **Funções da máquina** cria e exclui funções da máquina. As funções da máquina determinam o que os *usuários da máquina* visualizam quando usam o Portal Access, uma versão do Live Connect, de uma máquina com um agente. A janela **Acesso ao portal** é exibida quando um *usuário de máquina clica duas vezes no ícone do agente na bandeja do sistema na sua máquina gerenciada.*

Nota: A página **Funções do usuário** determina o que os *usuários do VSA* visualizam quando usam o **Live Connect** do VSA.

Na página **Funções da máquina**, é possível selecionar:

- Membros: atribuir ou remover máquinas de uma função da máquina.
- Direitos de acesso: selecionar os direitos de acesso para uma função da máquina. Os direitos de acesso determinam as funções que um *usuário da máquina* pode acessar.
- Tipos de função: atribuir ou remover tipos de função de uma função da máquina. Atualmente, há somente um tipo de função de máquina fornecido e nenhum direito de acesso é restrito.

Grupos de máquinas

As máquinas são sempre definidas por **grupo de máquinas** e os grupos de máquinas são sempre definidos por organização. É possível definir hierarquias de múltiplos níveis de grupos de máquinas ao identificar um grupo de máquinas principal para um grupo de máquinas. Também é possível mover um grupo de máquinas e todas as suas máquinas associadas para um grupo de máquinas principal diferente dentro da mesma empresa.

Há duplicidade

Se um agente já existe em uma máquina gerenciada em um grupo de máquinas diferente, então o **Discovery** cria uma conta **modelo da ID da máquina** *(página 71)* vazia, identificada com um ícone de entrada, e nenhum agente faz entrada. A nova conta modelo da ID da máquina exibe uma **ID da organização/ID do grupo/ID da máquina** *(página 71)* com base no nome canônico do computador no domínio Active Directory. *Você pode mesclar estas contas duplicadas.* A conta do agente ativa existente adota o nome da nova conta modelo da ID da máquina, então, a nova conta modelo da ID da máquina é excluída. Nenhum dado é perdido pela mescla, e a conta da ID da máquina agora combina seu local na hierarquia do domínio.

ID de máquina/ID de grupo/ID de organização

Cada **agente** *(página 69)* instalado em uma máquina gerenciada recebe uma **ID de máquina/ ID de grupo / ID de organização exclusiva**. Todas as IDs de máquinas pertencem a uma ID de grupo de máquinas e, como opção, a uma ID de subgrupo. Todas as IDs de grupos pertencem a uma ID de organização. Uma organização, normalmente, representa uma única conta de cliente. Se uma organização for pequena, ela poderá ter apenas um grupo de máquinas que contenha todas as IDs de máquinas da organização. Uma organização maior pode ter muitos grupos e subgrupos de máquinas, normalmente organizados por local ou rede. Por exemplo, o identificador completo de um agente instalado em uma máquina gerenciada poderia ser definido como `jsmith.sales.chicago.acme`. Nesse caso `sales` é uma ID de subgrupo dentro da ID de grupo `chicago` dentro da ID de organização intitulada `acme`. Em alguns lugares no VSA, essa hierarquia é exibida em ordem inversa. Cada ID de organização tem uma única ID de grupo de máquinas padrão intitulada `root`. IDs de grupo e IDs de subgrupo são criadas usando a página Sistema > Orgs/Grupo/Deptos/Membros > Gerenciar > Grupos de máquinas.

IDs de máquina versus agentes

Ao discutir agentes, é útil distinguir entre a **ID de máquina / ID de grupo / ID de organização** *(página 71)* e o **agente** *(página 69)*. A ID de máquina/ID de grupo/ID de organização é o **nome da conta** para uma máquina gerenciada no banco de dados do VSA. O agente é o software do cliente sendo executado na máquina gerenciada. Um relacionamento de um para um existe entre o agente em uma máquina gerenciada e seu nome de conta no VSA. As tarefas atribuídas a uma ID de máquina pelos usuários do VSA direcionam as ações do agente na máquina gerenciada.

Máquina gerenciada

Uma máquina monitorada com um **agente** *(página 69)* instalado e conta de **ID de máquina/ID de grupo** *(página 71)* ativa no servidor da Kaseya. Cada máquina gerenciada utiliza até uma licença de agente.

Modelo de ID de máquina

Um modelo de ID| de máquina é *um registro de ID de máquina sem um agente*. Como um agente nunca entra em uma conta de modelo de ID de máquina, ele não é contado, em relação à sua contagem total de licenças. Você pode criar quantos modelos de IDs de máquinas desejar, sem custo adicional. Quando um pacote de instalação de agente é criado, as configurações do pacote são normalmente copiadas de um modelo de ID de máquina selecionado. Modelos de IDs de máquinas são normalmente criados e configurados para certos tipos de máquinas. Exemplos de tipos de máquinas incluem desktops, Autotocad, QuickBooks, servidores de pequenas empresas, servidores Exchange, servidores SQL etc. **Um pacote de instalação correspondente pode ser criado, com base em cada modelo de ID de máquina definido.**

- Crie modelos de IDs de máquinas usando Agente > Criar.
- Importe um modelo de ID de máquina usando Agente > Importar/Exportar.
- Baseie um pacote de instalação de agente em um modelo de ID de máquina usando Agente > Implementar agentes.
- Copie as configurações *selecionadas* de modelos de IDs de máquinas para contas de IDs de máquinas existentes usando Agente > Copiar configurações.
- Identifique o número total de contas de modelos de IDs de máquinas no seu VSA usando Sistema > Estatísticas.
- Configure as definições do modelo de ID de máquina usando as funções padrão do VSA, da mesma maneira que você configuraria uma conta de ID de máquina com um agente.
- Modelos separados de ID de máquina são recomendados para máquinas Windows, Apple e Linux. Alternativamente, você pode criar um pacote que seleciona automaticamente o SO apropriado e copiar as configurações de um modelo que inclua um procedimento de agente que usa etapas específicas do SO.

Nome distinguido

Um **nome distinguido** fornece as mesmas informações de um nome canônico, formatado como uma

série de atributos, sequenciados em ordem inversa ao nome canônico. NC = Nome comum ou contêiner. UO = Unidade organizacional. CD = Componente do domínio.

OU/contentores

Uma **unidade organizacional** (UO) é um objeto do contêiner dentro do Active Directory. Um contêiner/UO é usado para organizar usuários, grupos, computadores e outras unidades organizacionais. Uma unidade organizacional não pode conter objetos de outros domínios.

Pastas e itens incluídos/excluídos do domínio

Após a instalação de uma verificação, o **Discovery** é configurado ao definir pastas e itens selecionados do domínio como **incluídos** ou **excluídos**. As políticas do **Discovery** fornecem automação de TI, tal como a instalação de agentes ou criação de usuários; somente a pastas e itens *incluídos*. O **Discovery** somente detecta informações detalhadas para pastas e itens *incluídos*, minimizando a quantidade de dados necessários para manter a sincronização com o domínio.

Índice

P

R

S

U

V