Configurar o Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Índice

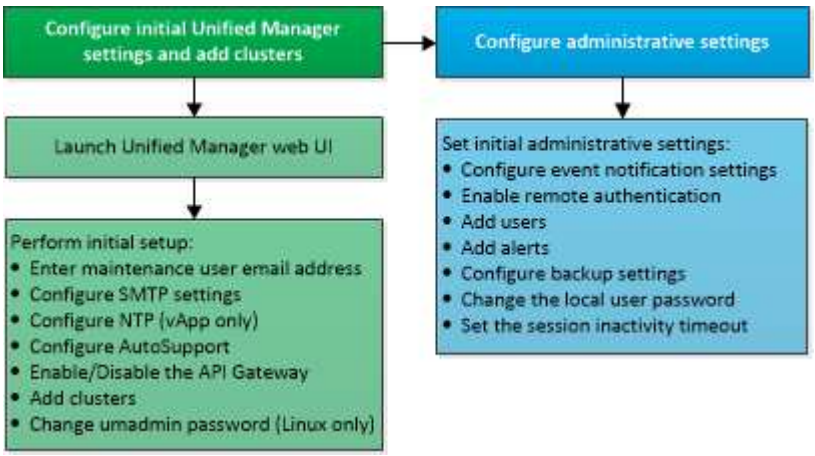
Configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (antigo OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface da web. Em seguida, você pode executar tarefas de configuração adicionais, como adicionar clusters, configurar autenticação remota, adicionar usuários e adicionar alertas.

Alguns dos procedimentos descritos neste manual são necessários para concluir a configuração inicial da sua instância do Unified Manager. Outros procedimentos são definições de configuração recomendadas que são úteis para configurar em sua nova instância ou que é bom saber antes de iniciar o monitoramento regular de seus sistemas ONTAP .

Visão geral da sequência de configuração

O fluxo de trabalho de configuração descreve as tarefas que você deve executar antes de poder usar o Unified Manager.



Acesse a interface da Web do Unified Manager

Depois de instalar o Unified Manager, você pode acessar a interface de usuário da Web para configurar o Unified Manager e começar a monitorar seus sistemas ONTAP .

Antes de começar

- Se esta for a primeira vez que você acessa a interface da web, você deve efetuar login como usuário de manutenção (ou usuário umadmin para instalações Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou endereço IP, sua configuração de rede precisa resolver esse nome curto para um FQDN válido.
- Se o servidor usar um certificado digital autoassinado, o navegador poderá exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela Autoridade de Certificação (CA) para autenticação do servidor.

Passos

1. Inicie a interface de usuário da Web do Unified Manager no seu navegador usando o URL exibido no final

da instalação. O URL é o endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor do Unified Manager.

O link está no seguinte formato: `https://URL`.

2. Efetue login na interface da Web do Unified Manager usando suas credenciais de usuário de manutenção.

> Se você fizer três tentativas consecutivas sem sucesso de login na interface da web em uma hora, seu acesso ao sistema será bloqueado e você precisará entrar em contato com o administrador do sistema. Isso é aplicável somente a usuários locais.

Execute a configuração inicial da interface da Web do Unified Manager

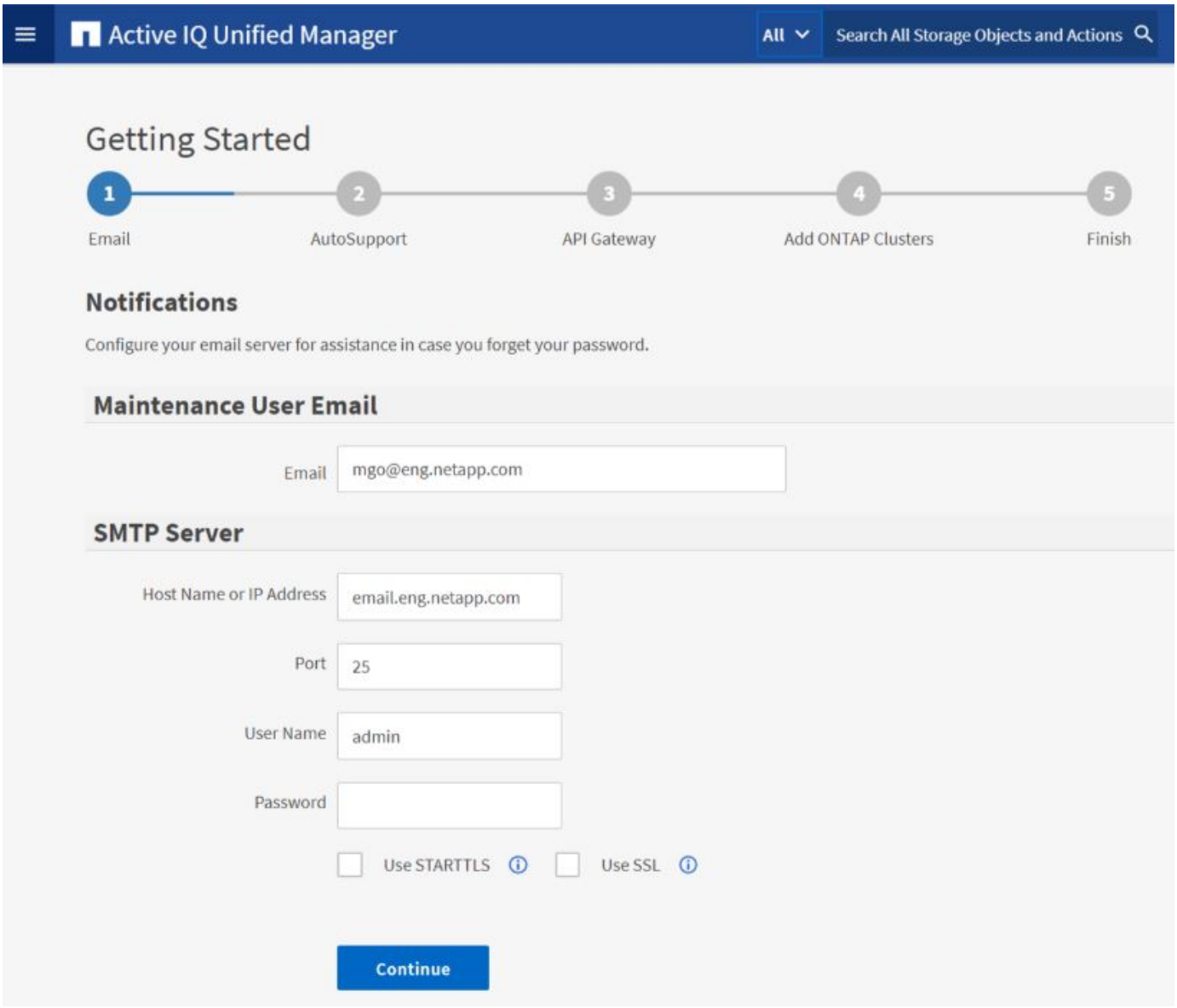
Para usar o Unified Manager, você deve primeiro configurar as opções de instalação inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters ONTAP .

Antes de começar

Você deve ter realizado as seguintes operações:

- Iniciou a interface de usuário da Web do Unified Manager usando o URL fornecido após a instalação
- Efetuou login usando o nome de usuário e a senha de manutenção (usuário umadmin para instalações Linux) criados durante a instalação

A página de introdução do Active IQ Unified Manager aparece somente quando você acessa a interface da Web pela primeira vez. A página abaixo é de uma instalação no VMware.



Se desejar alterar qualquer uma dessas opções posteriormente, você poderá selecionar sua escolha nas opções Gerais no painel de navegação esquerdo do Unified Manager. Observe que a configuração do NTP é somente para instalações do VMware e pode ser alterada posteriormente usando o console de manutenção do Unified Manager.

Passos

1. Na página Configuração inicial do Active IQ Unified Manager , insira o endereço de e-mail do usuário de manutenção, o nome do host do servidor SMTP e quaisquer opções SMTP adicionais, e o servidor NTP (somente instalações VMware). Em seguida, clique em **Continuar**.

   Se você selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado será exibida depois que você clicar no botão **Continuar**. Verifique os detalhes do certificado e aceite o certificado para continuar com as configurações iniciais da interface web.

2. Na página AutoSupport , clique em **Concordar e continuar** para habilitar o envio de mensagens de AutoSupport do Unified Manager para o NetAppActive IQ.

   Se você precisar designar um proxy para fornecer acesso à Internet para enviar conteúdo do AutoSupport , ou se quiser desabilitar o AutoSupport, use a opção **Geral** > * AutoSupport* na interface da web.

3. Em sistemas Red Hat, altere a senha do usuário umadmin da string padrão “admin” para uma string personalizada.
4. Na página Configurar API Gateway, selecione se deseja usar o recurso API Gateway que permite ao Unified Manager gerenciar os clusters ONTAP que você planeja monitorar usando APIs REST ONTAP . Em seguida, clique em **Continuar**.

   Você pode habilitar ou desabilitar essa configuração mais tarde na interface da web em **Geral** > **Configurações de recursos** > **Gateway de API**. Para obter mais informações sobre as APIs, consulte"Introdução às APIs REST do Active IQ Unified Manager" .

5. Adicione os clusters que você deseja que o Unified Manager gerencie e clique em **Avançar**. Para cada cluster que você planeja gerenciar, você deve ter o nome do host ou o endereço IP de gerenciamento do cluster (IPv4 ou IPv6), juntamente com as credenciais de nome de usuário e senha - o usuário deve ter a função “admin”.

   Esta etapa é opcional. Você pode adicionar clusters mais tarde na interface da web em **Gerenciamento de armazenamento** > **Configuração de cluster**.

6. Na página Resumo, verifique se todas as configurações estão corretas e clique em **Concluir**.

A página Introdução é fechada e a página Painel do Unified Manager é exibida.

Adicionar clusters

Você pode adicionar um cluster ao Active IQ Unified Manager para poder monitorá-lo. Isso inclui a capacidade de obter informações do cluster, como integridade, capacidade, desempenho e configuração do cluster, para que você possa localizar e resolver quaisquer problemas que possam ocorrer.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ONTAP Select e Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento de cluster

    O nome do host é o FQDN ou nome abreviado que o Unified Manager usa para se conectar ao cluster. O nome do host deve ser resolvido para o endereço IP de gerenciamento do cluster.

    O endereço IP de gerenciamento de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de armazenamento administrativo (SVM). Se você usar um LIF de gerenciamento de nós, a operação falhará.

  - O cluster deve estar executando o software ONTAP versão 9.1 ou superior.
  - Nome de usuário e senha do administrador do ONTAP

    Esta conta deve ter a função *admin* com acesso ao aplicativo definido como *ontapi*, *console* e *http*.

  - O número da porta para conectar ao cluster usando o protocolo HTTPS (normalmente porta 443)
  - Você possui os certificados necessários:

Certificado SSL (HTTPS): Este certificado é de propriedade do Unified Manager. Um certificado SSL autoassinado padrão (HTTPS) é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você atualize para um certificado assinado por CA para maior segurança. Se o certificado do servidor expirar, você deverá regenerá-lo e reiniciar o Unified Manager para que os serviços incorporem o novo certificado. Para obter mais informações sobre a regeneração do certificado SSL, consulte"Gerando um certificado de segurança HTTPS" .

Certificado EMS: Este certificado é de propriedade do Unified Manager. É usado durante a autenticação para notificações EMS recebidas do ONTAP.

Certificados para comunicação TLS mútua: usados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é habilitada para um cluster, com base na versão do ONTAP . Se o cluster que executa a versão do ONTAP for inferior à 9.5, a autenticação baseada em certificado não será habilitada.

A autenticação baseada em certificado não será habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-lo modificando e salvando os detalhes do cluster. Se o certificado expirar, você deverá regenerá-lo para incorporar o novo certificado. Para obter mais informações sobre como visualizar e regenerar o certificado, consulte"Editando clusters" .

- Você pode adicionar um cluster a partir da interface da web, e a autenticação baseada em certificado será ativada automaticamente.
- Você pode adicionar um cluster por meio do Unified Manager CLI; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, será necessário editar o cluster usando a interface do usuário do Unified Manager. Você pode ver"Comandos CLI do Unified Manager suportados" para adicionar um cluster usando o Unified Manager CLI.
- Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar em outro servidor do Unified Manager onde o nome do host ou endereço IP for alterado, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre a edição de detalhes do cluster, consulte"Editando clusters" .

+ **Certificados de cluster**: Este certificado é de propriedade da ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, se o certificado já tiver expirado, você deverá regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "Como renovar um certificado autoassinado ONTAP na interface de usuário do System Manager" .

- Você deve ter espaço adequado no servidor do Unified Manager. Você não poderá adicionar um cluster ao servidor quando mais de 90% do espaço no diretório do banco de dados já estiver consumido.

Para uma configuração do MetroCluster , você deve adicionar os clusters locais e remotos, e os clusters devem ser configurados corretamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.
2. Na página Configuração do cluster, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores necessários, como o nome do host ou endereço IP do cluster, nome de usuário, senha e número da porta.

Você pode alterar o endereço IP de gerenciamento de cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP é refletido na grade do cluster e na página de configuração do cluster após a conclusão do próximo ciclo de monitoramento.

4. Clique em **Enviar**.
5. Na caixa de diálogo Autorizar Host, clique em **Exibir Certificado** para visualizar as informações do certificado sobre o cluster.
6. Clique em **Sim**.

   Depois de salvar os detalhes do cluster, você pode ver o certificado para comunicação TLS mútua de um cluster.

   Se a autenticação baseada em certificado não estiver habilitada, o Unified Manager verificará o certificado somente quando o cluster for adicionado inicialmente. O Unified Manager não verifica o certificado para cada chamada de API para o ONTAP.

Depois que todos os objetos de um novo cluster são descobertos, o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Este recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ele ser adicionado. Após a conclusão do ciclo de coleta de continuidade de dados, os dados de desempenho do cluster em tempo real são coletados, por padrão, a cada cinco minutos.

Como a coleta de 15 dias de dados de desempenho exige muita CPU, é recomendável escalonar a adição de novos clusters para que as pesquisas de coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo. Além disso, se você reiniciar o Unified Manager durante o período de coleta de continuidade de dados, a coleta será interrompida e você verá lacunas nos gráficos de desempenho para o período ausente.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os relógios nos dois sistemas não estão sincronizados e se a data de início do certificado HTTPS do Unified Manager é posterior à data no cluster. Você deve garantir que os relógios estejam sincronizados usando NTP ou um serviço similar.

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado por uma CA"

Configurar o Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que o alertam sobre eventos no seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Após implantar o Unified Manager e concluir a configuração inicial, você deve considerar configurar seu ambiente para acionar alertas e gerar e-mails de notificação ou interceptações SNMP com base no

recebimento de eventos.

Passos

1. "Configurar as definições de notificação de eventos".

   Se você quiser que notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, você deve configurar um servidor SMTP e fornecer um endereço de e-mail do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, você pode selecionar essa opção e fornecer as informações necessárias.

2. "Habilitar autenticação remota".

   Se você quiser que usuários remotos do LDAP ou do Active Directory acessem a instância do Unified Manager e recebam notificações de alerta, será necessário habilitar a autenticação remota.

3. "Adicionar servidores de autenticação".

   Você pode adicionar servidores de autenticação para que usuários remotos dentro do servidor de autenticação possam acessar o Unified Manager.

4. "Adicionar usuários".

   Você pode adicionar vários tipos diferentes de usuários locais ou remotos e atribuir funções específicas. Ao criar um alerta, você atribui um usuário para receber as notificações de alerta.

5. "Adicionar alertas".

   Depois de adicionar o endereço de e-mail para enviar notificações, adicionar usuários para receber as notificações, configurar suas configurações de rede e configurar as opções SMTP e SNMP necessárias para seu ambiente, você poderá atribuir alertas.

Configurar as definições de notificação de eventos

Você pode configurar o Unified Manager para enviar notificações de alerta quando um evento for gerado ou quando um evento for atribuído a um usuário. Você pode configurar o servidor SMTP usado para enviar o alerta e definir vários mecanismos de notificação. Por exemplo, as notificações de alerta podem ser enviadas como e-mails ou interceptações SNMP.

Antes de começar

Você deve ter as seguintes informações:

- Endereço de e-mail de onde a notificação de alerta é enviada

  O endereço de e-mail aparece no campo “De” nas notificações de alerta enviadas. Se o e-mail não puder ser entregue por qualquer motivo, esse endereço de e-mail também será usado como destinatário de e-mails não entregues.

- Nome do host do servidor SMTP e o nome de usuário e senha para acessar o servidor
- Nome do host ou endereço IP do host de destino da armadilha que receberá a armadilha SNMP, juntamente com a versão SNMP, porta da armadilha de saída, comunidade e outros valores de configuração SNMP necessários

Para especificar vários destinos de interceptação, separe cada host com uma vírgula. Nesse caso, todas as outras configurações SNMP, como versão e porta de interceptação de saída, devem ser as mesmas para todos os hosts na lista.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Notificações**.
2. Na página Notificações, configure as configurações apropriadas.

   Notas:

   - Se o Endereço De estiver preenchido com o endereço "ActiveIQUnifiedManager@localhost.com", você deverá alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.
   - Se o nome do host do servidor SMTP não puder ser resolvido, você poderá especificar o endereço IP (IPv4 ou IPv6) do servidor SMTP em vez do nome do host.
3. Clique em **Salvar**.
4. Se você selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado será exibida depois que você clicar no botão **Salvar**. Verifique os detalhes do certificado e aceite o certificado para salvar as configurações de notificação.

   Você pode clicar no botão **Exibir detalhes do certificado** para visualizar os detalhes do certificado. Se o certificado existente estiver expirado, desmarque a caixa **Usar STARTTLS** ou **Usar SSL**, salve as configurações de notificação e marque novamente a caixa **Usar STARTTLS** ou **Usar SSL** para visualizar um novo certificado.

Habilitar autenticação remota

Você pode habilitar a autenticação remota para que o servidor do Unified Manager possa se comunicar com seus servidores de autenticação. Os usuários do servidor de autenticação podem acessar a interface gráfica do Unified Manager para gerenciar objetos de armazenamento e dados.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

O servidor do Unified Manager deve ser conectado diretamente ao servidor de autenticação. Você deve desabilitar todos os clientes LDAP locais, como SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Você pode habilitar a autenticação remota usando o Open LDAP ou o Active Directory. Se a autenticação remota estiver desabilitada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (LDAP seguro). O Unified Manager usa 389 como a porta padrão para comunicação não segura e 636 como a porta padrão para comunicação segura.

O certificado usado para autenticar usuários deve estar em conformidade com o formato X.509.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Ativar autenticação remota…**.
3. No campo Serviço de autenticação, selecione o tipo de serviço e configure o serviço de autenticação.

Para tipo de autenticação…	Insira as seguintes informações…
Diretório ativo	• Nome do administrador do servidor de autenticação em um dos seguintes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(usando a notação LDAP apropriada) • Senha do administrador • Nome distinto base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome distinto base

   Se a autenticação de um usuário do Active Directory demorar muito ou atingir o tempo limite, o servidor de autenticação provavelmente está demorando muito para responder. Desabilitar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação.

   Se você selecionar a opção Usar conexão segura para o servidor de autenticação, o Unified Manager se comunicará com o servidor de autenticação usando o protocolo Secure Sockets Layer (SSL).

4. **Opcional:** Adicione servidores de autenticação e teste a autenticação.
5. Clique em **Salvar**.

Desabilitar grupos aninhados da autenticação remota

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupo aninhada para que somente usuários individuais, e não membros do grupo, possam se autenticar remotamente no Unified Manager. Você pode desabilitar grupos aninhados quando quiser melhorar o tempo de resposta da autenticação do Active Directory.

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- A desabilitação de grupos aninhados só é aplicável ao usar o Active Directory.

Desabilitar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desabilitado e se um grupo remoto for adicionado ao Unified Manager, os usuários individuais deverão ser membros do grupo remoto para se autenticar no Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Clique em **Salvar**.

Configurar serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer a eles acesso ao Unified Manager. Você pode autenticar usuários usando serviços de autenticação predefinidos (como Active Directory ou OpenLDAP) ou configurando seu próprio mecanismo de autenticação.

Antes de começar

- Você deve ter habilitado a autenticação remota.
- Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Selecione um dos seguintes serviços de autenticação:

Se você selecionar…	Então faça isto…
Diretório ativo	a. Digite o nome e a senha do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Digite o nome distinto e a senha de vinculação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.

Se você selecionar…	Então faça isto…
Outros	a. Digite o nome distinto e a senha de vinculação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**. c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação. d. Insira o nome do usuário, a associação ao grupo, o grupo de usuários e os atributos do membro.

Se quiser modificar o serviço de autenticação, você deverá excluir todos os servidores de autenticação existentes e, em seguida, adicionar novos servidores de autenticação.

3. Clique em **Salvar**.

Adicionar servidores de autenticação

Você pode adicionar servidores de autenticação e habilitar a autenticação remota no servidor de gerenciamento para que usuários remotos dentro do servidor de autenticação possam acessar o Unified Manager.

Antes de começar

- As seguintes informações devem estar disponíveis:
  - Nome do host ou endereço IP do servidor de autenticação
  - Número da porta do servidor de autenticação
- Você deve ter habilitado a autenticação remota e configurado seu serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários ou grupos remotos no servidor de autenticação.
- Você deve ter a função de Administrador do Aplicativo.

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (HA) (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação do parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação estiver inacessível.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Habilite ou desabilite a opção **Usar conexão segura**:

Se você quiser…	Então faça isto…
Habilite-o	a. Selecione a opção **Usar conexão segura**. b. Na área Servidores de autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar servidor de autenticação, insira o nome de autenticação ou endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Autorizar Host, clique em Exibir Certificado. e. Na caixa de diálogo Exibir certificado, verifique as informações do certificado e clique em **Fechar**. f. Na caixa de diálogo Autorizar Host, clique em **Sim**. Quando você habilita a opção **Usar autenticação de conexão segura**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa 636 como porta padrão para comunicação segura e a porta número 389 para comunicação não segura.
Desabilite-o	a. Desmarque a opção **Usar conexão segura**. b. Na área Servidores de autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar servidor de autenticação, especifique o nome do host ou o endereço IP (IPv4 ou IPv6) do servidor e os detalhes da porta. d. Clique em **Adicionar**.

O servidor de autenticação que você adicionou é exibido na área Servidores.

3. Execute um teste de autenticação para confirmar se você pode autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação

Você pode validar a configuração dos seus servidores de autenticação para garantir que o servidor de gerenciamento consiga se comunicar com eles. Você pode validar a configuração pesquisando um usuário remoto ou grupo remoto em seus servidores de autenticação e autenticando-os usando as configurações definidas.

Antes de começar

- Você deve ter habilitado a autenticação remota e configurado seu serviço de autenticação para que o servidor do Unified Manager possa autenticar o usuário ou grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa procurar o usuário remoto ou grupo remoto nesses servidores e autenticá-los.
- Você deve ter a função de Administrador do Aplicativo.

Se o serviço de autenticação estiver definido como Active Directory e se você estiver validando a autenticação de usuários remotos que pertencem ao grupo principal do servidor de autenticação, as informações sobre o grupo principal não serão exibidas nos resultados da autenticação.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Clique em **Testar autenticação**.
3. Na caixa de diálogo Testar usuário, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Testar**.

   Se você estiver autenticando um grupo remoto, não deverá digitar a senha.

Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico for gerado. Você pode configurar alertas para um único recurso, para um grupo de recursos ou para eventos de um tipo de gravidade específico. Você pode especificar a frequência com que deseja ser notificado e associar um script ao alerta.

Antes de começar

- Você deve ter configurado as configurações de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de interceptação SNMP para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta, além dos nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se quiser que um script seja executado com base no evento, você deve adicionar o script ao Unified Manager usando a página Scripts.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode criar um alerta diretamente na página Detalhes do evento após receber um evento, além de criar um alerta na página Configuração de alerta, conforme descrito aqui.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de alerta**.
2. Na página Configuração de alerta, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar alerta, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **Recursos** e selecione os recursos a serem incluídos ou excluídos do alerta.

   Você pode definir um filtro especificando uma sequência de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na sequência de texto especificada, a lista de recursos

disponíveis exibe apenas aqueles que correspondem à regra de filtro. A sequência de texto que você especificar diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão especificadas, a regra de exclusão terá precedência sobre a regra de inclusão, e o alerta não será gerado para eventos relacionados ao recurso excluído.

5. Clique em **Eventos** e selecione os eventos com base no nome do evento ou no tipo de gravidade do evento para o qual você deseja acionar um alerta.

Para selecionar mais de um evento, pressione a tecla Ctrl enquanto faz suas seleções.

6. Clique em **Ações** e selecione os usuários que deseja notificar, escolha a frequência de notificação, escolha se uma armadilha SNMP será enviada ao receptor da armadilha e atribua um script a ser executado quando um alerta for gerado.

Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Nome aparecerá em branco porque o endereço de e-mail modificado não estará mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificar o endereço de e-mail do usuário selecionado na página Usuários, o endereço de e-mail modificado não será atualizado para o usuário selecionado.

Você também pode optar por notificar os usuários por meio de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de um alerta

Este exemplo mostra como criar um alerta que atende aos seguintes requisitos:

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujo nome contém “abc” e exclui todos os volumes cujo nome contém “xyz”
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script "Teste", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

Passos

1. Clique em **Nome** e insira **HealthTest** no campo **Nome do alerta**.
2. Clique em **Recursos** e, na guia Incluir, selecione **Volumes** na lista suspensa.
   a. Digite **abc** no campo **Nome contém** para exibir os volumes cujo nome contém “abc”.
   b. Selecione **+[All Volumes whose name contains 'abc'] +** da área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
   c. Clique em **Excluir** e insira **xyz** no campo **Nome contém** e depois clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Gravidade do Evento.
4. Selecione **Todos os Eventos Críticos** na área Eventos Correspondentes e mova-os para a área Eventos Selecionados.
5. Clique em **Ações** e insira **sample@domain.com** no campo Alertar estes usuários.

6. Selecione **Lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

   Você pode configurar um alerta para enviar notificações repetidamente aos destinatários por um período específico. Você deve determinar o horário a partir do qual a notificação de evento estará ativa para o alerta.

7. No menu Selecionar script para executar, selecione o script **Teste**.
8. Clique em **Salvar**.

Alterar a senha do usuário local

Você pode alterar sua senha de login de usuário local para evitar potenciais riscos de segurança.

Antes de começar

Você deve estar logado como usuário local.

As senhas do usuário de manutenção e dos usuários remotos não podem ser alteradas usando estas etapas. Para alterar a senha de um usuário remoto, entre em contato com o administrador de senhas. Para alterar a senha do usuário de manutenção, consulte"Usando o console de manutenção" .

Passos

1. Efetue login no Unified Manager.
2. Na barra de menu superior, clique no ícone do usuário e depois clique em **Alterar senha**.

   A opção **Alterar senha** não será exibida se você for um usuário remoto.

3. Na caixa de diálogo Alterar senha, digite a senha atual e a nova senha.
4. Clique em **Salvar**.

Se o Unified Manager estiver configurado em uma configuração de alta disponibilidade, você deverá alterar a senha no segundo nó da configuração. Ambas as instâncias devem ter a mesma senha.

Definir o tempo limite de inatividade da sessão

Você pode especificar o valor do tempo limite de inatividade do Unified Manager para que a sessão seja encerrada automaticamente após um determinado período de inatividade. Por padrão, o tempo limite é definido como 4.320 minutos (72 horas).

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Esta configuração afeta todas as sessões de usuários conectados.

Esta opção não estará disponível se você tiver habilitado a autenticação Security Assertion Markup Language (SAML).

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.

2. Na página **Configurações de recursos**, especifique o tempo limite de inatividade escolhendo uma das seguintes opções:

Se você quiser…	Então faça isto…
Não defina nenhum tempo limite para que a sessão nunca seja fechada automaticamente	No painel **Tempo limite de inatividade**, mova o botão deslizante para a esquerda (desligado) e clique em **Aplicar**.
Defina um número específico de minutos como valor de tempo limite	No painel **Tempo limite de inatividade**, mova o botão deslizante para a direita (ligado), especifique o valor do tempo limite de inatividade em minutos e clique em **Aplicar**.

Defina o tempo limite da sessão por meio da CLI

Você pode definir um valor máximo de tempo limite de sessão para o Unified Manager usando a CLI para que a sessão seja encerrada automaticamente após um determinado período de tempo. Por padrão, o tempo limite da sessão é definido para o valor máximo, que é 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo que você esteja conectado e usando ativamente o Unified Manager.

Sobre esta tarefa

Você deve ter a função de Administrador do Aplicativo.

A configuração de tempo limite de sessão afeta todas as sessões de usuários conectados.

Passos

1. Efetue login no Unified Manager CLI inserindo o `um cli login` comando. Use um nome de usuário e senha válidos para autenticação.
2. Entre no `um option set max.session.timeout.value=<in mins>` comando para modificar o valor do tempo limite da sessão.

Alterar o nome do host do Unified Manager

Em algum momento, você pode querer alterar o nome do host do sistema no qual instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado.

As etapas necessárias para alterar o nome do host são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat Linux ou em um servidor Microsoft Windows.

Alterar o nome do host do appliance virtual do Unified Manager

O host de rede recebe um nome quando o dispositivo virtual do Unified Manager é implantado pela primeira vez. Você pode alterar o nome do host após a implantação. Se você alterar o nome do host, também deverá gerar novamente o certificado HTTPS.

Antes de começar

Você deve estar conectado ao Unified Manager como usuário de manutenção ou ter a função de Administrador de Aplicativos atribuída a você para executar essas tarefas.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, você teria designado um nome para o host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do DNS. Se o DHCP ou o DNS não estiver configurado corretamente, o nome do host "Unified Manager" será automaticamente atribuído e associado ao certificado de segurança.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretende usar o novo nome do host para acessar a interface de usuário da Web do Unified Manager, será necessário gerar um novo certificado de segurança.

Se você acessar a interface da Web usando o endereço IP do servidor em vez do nome do host, não precisará gerar um novo certificado se alterar o nome do host. No entanto, a melhor prática é atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real.

Se você alterar o nome do host no Unified Manager, deverá atualizá-lo manualmente no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

O novo certificado não entrará em vigor até que a máquina virtual do Unified Manager seja reiniciada.

Passos

1. Gerar um certificado de segurança HTTPS

   Se quiser usar o novo nome de host para acessar a interface de usuário da Web do Unified Manager, você deverá gerar novamente o certificado HTTPS para associá-lo ao novo nome de host.

2. Reinicie a máquina virtual do Unified Manager

   Depois de regenerar o certificado HTTPS, você deve reiniciar a máquina virtual do Unified Manager.

Gerar um certificado de segurança HTTPS

Quando o Active IQ Unified Manager é instalado pela primeira vez, um certificado HTTPS padrão é instalado. Você pode gerar um novo certificado de segurança HTTPS que substitui o certificado existente.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Pode haver vários motivos para regenerar o certificado, como se você desejasse ter valores melhores para Nome Distinto (DN), se quisesse um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tivesse expirado.

Se você não tiver acesso à interface da Web do Unified Manager, poderá gerar novamente o certificado

HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar certificados, você pode definir o tamanho da chave e a duração da validade da chave. Se você usar o `Reset Server Certificate` opção do console de manutenção, então um novo certificado HTTPS é criado e é válido por 397 dias. Este certificado terá uma chave RSA de tamanho 2048 bits.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Regenerar certificado HTTPS**.

   A caixa de diálogo Regenerar certificado HTTPS é exibida.

3. Selecione uma das seguintes opções dependendo de como você deseja gerar o certificado:

Se você quiser…	Faça isso…
Regenerar o certificado com os valores atuais	Clique na opção **Regenerar usando atributos de certificado atuais**.

Se você quiser…	Faça isso…
Gerar o certificado usando valores diferentes	Clique na opção **Atualizar os atributos atuais do certificado**. Os campos Nome comum e Nomes alternativos usarão os valores do certificado existente se você não inserir novos valores. O “Nome comum” deve ser definido como o FQDN do host. Os outros campos não exigem valores, mas você pode inserir valores, por exemplo, para E-MAIL, EMPRESA, DEPARTAMENTO, Cidade, Estado e País, se quiser que esses valores sejam preenchidos no certificado. Você também pode selecionar entre o TAMANHO DA CHAVE disponível (o algoritmo da chave é “RSA”). e o PERÍODO DE VALIDADE. • Os valores permitidos para o tamanho da chave são `2048` , `3072` e `4096` . • Os períodos de validade são de no mínimo 1 dia e no máximo 36.500 dias. Embora seja permitido um período de validade de 36.500 dias, é recomendável usar um período de validade de no máximo 397 dias ou 13 meses. Porque se você selecionar um período de validade de mais de 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA conhecida, a validade do certificado assinado devolvido a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção “Excluir informações de identificação local (por exemplo, host local)” se quiser remover as informações de identificação local do campo Nomes alternativos no certificado. Quando esta caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

4. Clique em **Sim** para regenerar o certificado.
5. Reinicie o servidor do Unified Manager para que o novo certificado entre em vigor.
6. Verifique as novas informações do certificado visualizando o certificado HTTPS.

Reinicie a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual no console de manutenção do Unified Manager. Você deve reiniciar após gerar um novo certificado de segurança ou se houver um problema com a máquina virtual.

Antes de começar

O dispositivo virtual está ligado.

Você está conectado ao console de manutenção como usuário de manutenção.

Você também pode reiniciar a máquina virtual do vSphere usando a opção **Reiniciar Convidado**. Consulte a documentação do VMware para obter mais informações.

Passos

1. Acesse o console de manutenção.
2. Selecione **Configuração do sistema** > **Reinicializar máquina virtual**.

Alterar o nome do host do Unified Manager em sistemas Linux

Em algum momento, você pode querer alterar o nome do host da máquina Red Hat Enterprise Linux na qual instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado ao listar suas máquinas Linux.

Antes de começar

Você deve ter acesso de usuário root ao sistema Linux no qual o Unified Manager está instalado.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, você teria designado um nome para o host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do servidor DNS.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretende usar o novo nome do host para acessar a interface da Web do Unified Manager, será necessário gerar um novo certificado de segurança.

Se você acessar a interface da Web usando o endereço IP do servidor em vez do nome do host, não precisará gerar um novo certificado se alterar o nome do host. No entanto, a melhor prática é atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real. O novo certificado não entrará em vigor até que a máquina Linux seja reiniciada.

Se você alterar o nome do host no Unified Manager, deverá atualizá-lo manualmente no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

Passos

1. Efetue login como usuário root no sistema Unified Manager que você deseja modificar.
2. Pare o software Unified Manager e o software MySQL associado inserindo o seguinte comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Alterar o nome do host usando o Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Regenere o certificado HTTPS para o servidor:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Reinicie o serviço de rede:

   ```
   systemctl restart NetworkManager.service
   ```

6. Após o serviço ser reiniciado, verifique se o novo nome do host consegue fazer ping em si mesmo:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando deve retornar o mesmo endereço IP que foi definido anteriormente para o nome do host original.

7. Após concluir e verificar a alteração do nome do host, reinicie o Unified Manager digitando o seguinte comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Habilitar e desabilitar o gerenciamento de armazenamento baseado em políticas

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de armazenamento (volumes e LUNs) em seus clusters ONTAP e gerenciar essas cargas de trabalho com base nos níveis de serviço de desempenho atribuídos. Essa funcionalidade é semelhante à criação de cargas de trabalho no ONTAP System Manager e à anexação de políticas de QoS, mas quando aplicada usando o Unified Manager, você pode provisionar e gerenciar cargas de trabalho em todos os clusters que sua instância do Unified Manager está monitorando.

Você deve ter a função de Administrador do Aplicativo.

Esta opção é habilitada por padrão, mas você pode desabilitá-la se não quiser provisionar e gerenciar cargas de trabalho usando o Unified Manager.

Quando ativada, esta opção fornece muitos itens novos na interface do usuário:

Novo conteúdo	Localização
Uma página para provisionar novas cargas de trabalho	Disponível em **Tarefas comuns** > **Provisionamento**
Uma página para criar políticas de nível de serviço de desempenho	Disponível em **Configurações** > **Políticas** > **Níveis de serviço de desempenho**
Uma página para criar políticas de eficiência de armazenamento de desempenho	Disponível em **Configurações** > **Políticas** > **Eficiência de armazenamento**
Painéis que descrevem seu desempenho de carga de trabalho atual e IOPS de carga de trabalho	Disponível no Painel

Consulte a ajuda on-line do produto para obter mais informações sobre essas páginas e essa funcionalidade.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.
2. Na página **Configurações de recursos**, desative ou ative o gerenciamento de armazenamento baseado em políticas escolhendo uma das seguintes opções:

Se você quiser…	Então faça isto…
Desabilitar o gerenciamento de armazenamento baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a esquerda.
Habilitar gerenciamento de armazenamento baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a direita.

Informações sobre direitos autorais

Informações sobre marcas comerciais