Configurar o Active IQ Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Configurar o Active IQ Unified Manager . . . 1
- Saiba mais sobre como configurar o Active IQ Unified Manager . . . 1
- Saiba mais sobre a sequência de configuração no Active IQ Unified Manager . . . 1
- Acesse a interface web no Active IQ Unified Manager . . . 1
- Execute a configuração inicial da interface web do Active IQ Unified Manager . . . 2
- Adicionar clusters ao Active IQ Unified Manager . . . 4
- Configurar notificações . . . 6
  - Configure o Active IQ Unified Manager para enviar notificações de alerta . . . 6
  - Configure as definições de notificação de eventos no Active IQ Unified Manager . . . 7
  - Ative a autenticação remota no Active IQ Unified Manager . . . 8
  - Desative grupos aninhados na autenticação remota no Active IQ Unified Manager . . . 9
  - Configure os serviços de autenticação no Active IQ Unified Manager . . . 10
  - Adicionar servidores de autenticação ao Active IQ Unified Manager . . . 11
  - Teste a configuração dos servidores de autenticação no Active IQ Unified Manager . . . 12
  - Adicione alertas no Active IQ Unified Manager . . . 13
- Alterar a senha do usuário local no Active IQ Unified Manager . . . 15
- Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager . . . 15
- Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager . . . 16
- Alterar o nome do host do Unified Manager . . . 16
  - Alterar o nome do host da máquina virtual do Active IQ Unified Manager . . . 16
  - Gere um certificado de segurança HTTPS no Active IQ Unified Manager . . . 17
  - Reinicie a máquina virtual do Active IQ Unified Manager . . . 20
  - Altere o nome do host do Active IQ Unified Manager em sistemas Linux . . . 20
- Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager . . . 21

Configurar o Active IQ Unified Manager

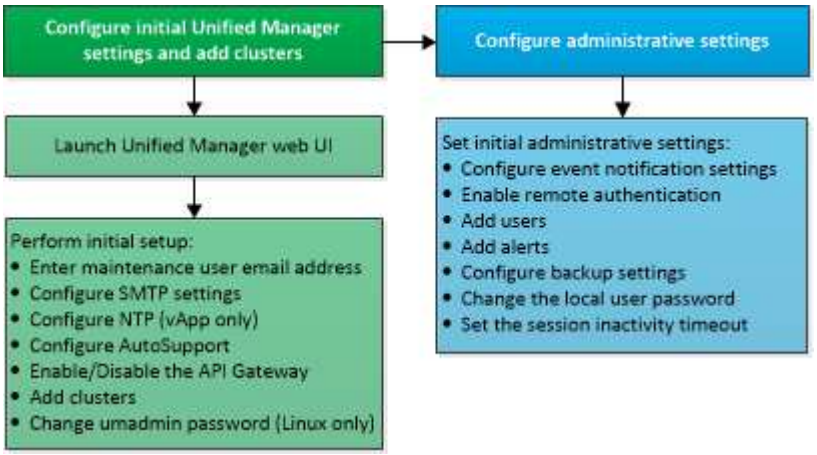
Saiba mais sobre como configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (anteriormente o OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface de usuário da web. Em seguida, você pode realizar tarefas de configuração adicionais, como adicionar clusters, configurar a 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 configurações recomendadas que podem ser úteis para configurar sua nova instância ou que é bom conhecer antes de iniciar o monitoramento regular dos seus sistemas ONTAP.

Saiba mais sobre a sequência de configuração no Active IQ Unified Manager

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



Acesse a interface web no Active IQ Unified Manager

Após instalar o Unified Manager, você poderá 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 está acessando a interface de usuário da web, você deve fazer login como o usuário de manutenção (ou o usuário umadmin para instalações do Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o domínio totalmente qualificado (FQDN) ou o 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 aceitar o risco para continuar acessando ou instalar um certificado digital assinado por uma Autoridade Certificadora (CA) para autenticação do servidor.

Passos

1. Inicie a interface web do Unified Manager no seu navegador usando a URL exibida no final da instalação. A URL é o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor Unified Manager.

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

2. Faça 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 de usuário da web em uma hora, seu acesso ao sistema será bloqueado, e você precisará entrar em contato com o administrador do sistema. Isso se aplica somente a usuários locais.

Execute a configuração inicial da interface web do Active IQ Unified Manager

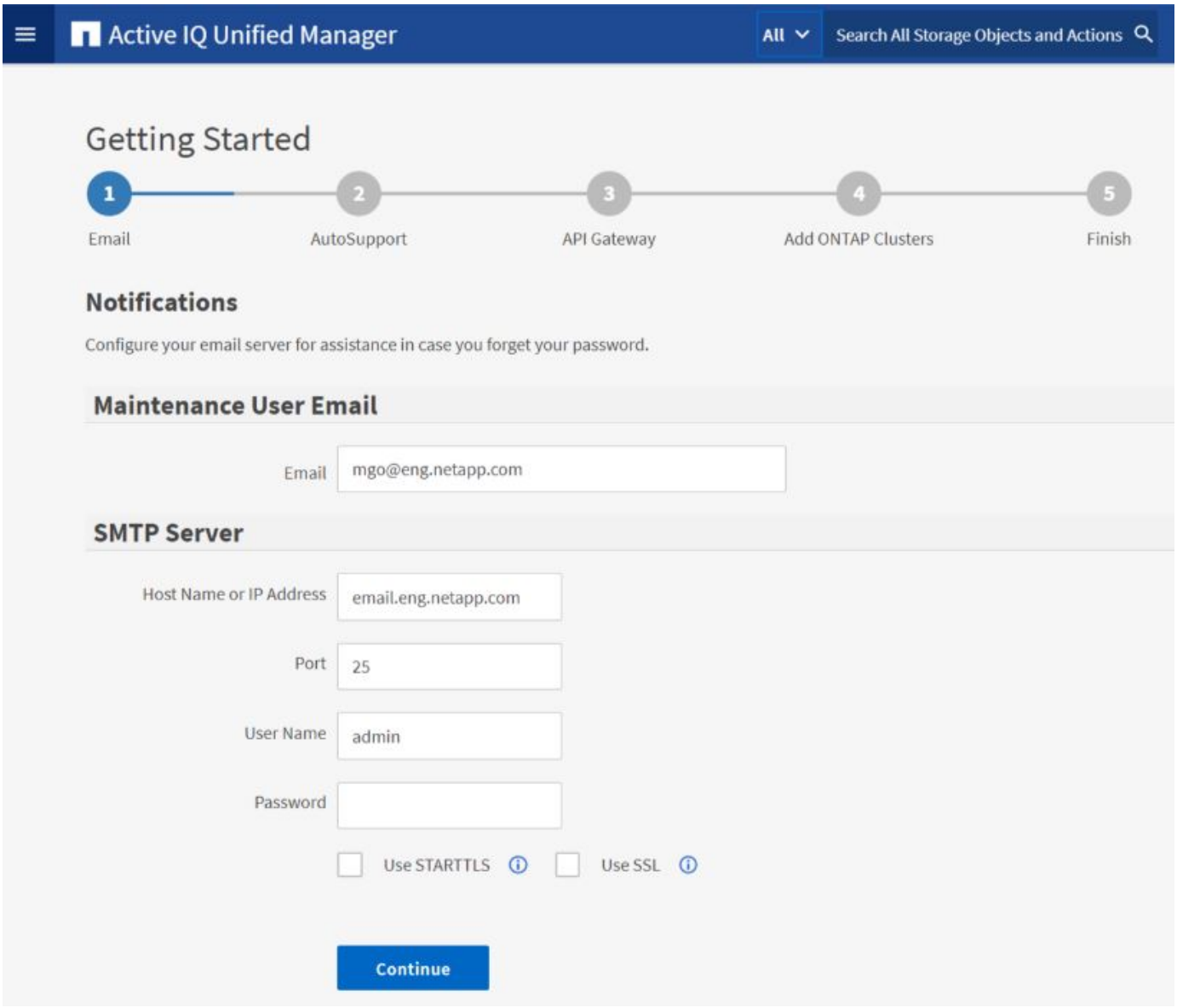
Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters do ONTAP.

Antes de começar

Você deve ter realizado as seguintes operações:

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

A página Active IQ Unified ManagerGetting Started aparece somente quando você acessa a interface web pela primeira vez. A página abaixo é de uma instalação no VMware.



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

Passos

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

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

2. Na página AutoSupport, clique em **Agree and Continue** 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 desativar 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 Gateway de API, selecione se deseja usar o recurso Gateway de API que permite ao Unified Manager gerenciar os clusters do ONTAP que você planeja monitorar usando as APIs REST do ONTAP. Em seguida, clique em **Continuar**.

   Você pode ativar ou desativar essa configuração posteriormente na interface da web em **Geral** > **Configurações de recursos** > **Gateway de API**. Para obter mais informações sobre as APIs, consulte "Primeiros passos com as 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 o nome de usuário e as credenciais de senha; o usuário deve ter a função “admin”.

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

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

A página de introdução é fechada e a página Dashboard do Unified Manager é exibida.

Adicionar clusters ao Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ao ONTAP Select e ao Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento do 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 do cluster deve ser a LIF de gerenciamento do cluster da máquina virtual de armazenamento administrativa (SVM). Se você usar uma LIF de gerenciamento de nó, 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*, *amqp*, *console* e *http*.

  - O número da porta para conectar-se ao cluster usando o protocolo HTTPS (normalmente a porta 443)

- Você possui os certificados necessários:

  Certificado SSL (HTTPS): este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS) autoassinado padrão é gerado com uma nova instalação do Unified Manager. NetApp recomenda que você o 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 como regenerar o certificado SSL, consulte "Gerando um certificado de segurança HTTPS".

  Certificado EMS: Este certificado pertence ao Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

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

  A autenticação baseada em certificado não é habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-la 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 pela interface de usuário da web, e a autenticação baseada em certificado é ativada automaticamente.
  - Você pode adicionar um cluster pela CLI do Unified Manager; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, precisará editar o cluster usando a interface do usuário do Unified Manager. Consulte "Comandos da CLI do Unified Manager suportados" para adicionar um cluster usando a CLI do Unified Manager.
  - Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurá-lo em outro servidor do Unified Manager em que o nome do host ou o endereço IP foi alterado, o monitoramento do cluster poderá falhar. Para evitar essa falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, consulte "Editando clusters".

  + **Certificados de cluster**: Este certificado pertence ao ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, caso o certificado já tenha expirado, você deve 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 do ONTAP na interface de usuário do System Manager".

- Você precisa ter espaço suficiente no servidor do Unified Manager. A adição de um cluster ao servidor não será possível se mais de 90% do espaço no diretório do banco de dados já estiver ocupado.

Para uma configuração do MetroCluster, você precisa adicionar os clusters local e remoto, e ambos devem estar configurados corretamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.

2. Na página de Configuração do Cluster, clique em **Adicionar**.
3. Na caixa de diálogo Add Cluster, especifique os valores necessários, como o nome do host ou o endereço IP do cluster, o nome de usuário, a senha e o número da porta.

   Você pode alterar o endereço IP de gerenciamento do cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP será 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 Authorize Host, clique em **View Certificate** para visualizar as informações do certificado do cluster.
6. Clique em **Yes**.

   Após salvar os detalhes do cluster, você poderá visualizar o certificado para a comunicação TLS mútua de um cluster.

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

Após todos os objetos de um novo cluster serem 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. Esse recurso fornece a você mais de duas semanas de informações de desempenho de um cluster imediatamente após sua adição. 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 muito da CPU, recomenda-se que você adicione novos clusters de forma escalonada para que as sondagens da 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 referentes ao período ausente.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os relógios dos 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 o NTP ou um serviço similar.

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado por uma Autoridade Certificadora (CA)"

Configurar notificações

Configure o Active IQ Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que alertem você sobre eventos em seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator.

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

Passos

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

   Se você quiser que as notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, será necessário configurar um servidor SMTP e fornecer um endereço de e-mail a partir do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, poderá 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, você deverá habilitar a autenticação remota.

3. "Adicionar servidores de autenticação".

   Você pode adicionar servidores de autenticação para que usuários remotos no 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 envio de notificações, adicionar os usuários que receberão as notificações, configurar as definições de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

Configure as definições de notificação de eventos no Active IQ Unified Manager

Você pode configurar o Unified Manager para enviar notificações de alerta quando um evento é gerado ou quando um evento é 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 traps SNMP.

Antes de começar

Você precisa ter as seguintes informações:

- Endereço de e-mail a partir do qual a notificação de alerta é enviada

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

- Nome do host do servidor SMTP, nome de usuário e senha para acessar o servidor

- Nome do host ou endereço IP do host de destino do trap que receberá o trap SNMP, juntamente com a versão SNMP, a porta de saída do trap, a comunidade e outros valores de configuração SNMP necessários

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

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

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

   Notas:

   - Se o campo "De" estiver preenchido automaticamente com o endereço "ActiveIQUnifiedManager@localhost.com", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.
   - Caso o nome do host do servidor SMTP não possa ser resolvido, você pode 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 é exibida após clicar no botão **Salvar**. Verifique os detalhes do certificado e aceite-o para salvar as configurações de notificação.

   Você pode clicar no botão **Exibir detalhes do certificado** para visualizar os detalhes do certificado. Se o certificado atual 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.

Ative a autenticação remota no Active IQ Unified Manager

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 storage e dados.

Antes de começar

Você precisa ter a função de Application Administrator.



O servidor do Unified Manager deve estar conectado diretamente ao servidor de autenticação. Você deve desativar quaisquer 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 via LDAP e LDAPS (Secure LDAP). O Unified Manager utiliza a porta 389 como padrão para comunicação não segura e a porta 636 como padrão para comunicação segura.

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

Passos

1. No painel de navegação à esquerda, 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 o tipo de autenticação…	Insira as seguintes informações…
Active Directory	• 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 de administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Open LDAP	• Nome diferenciado de bind (na notação LDAP apropriada) • Senha de vinculação • Nome diferenciado base

Se a autenticação de um usuário do Active Directory demorar muito ou expirar, o servidor de autenticação provavelmente está demorando muito para responder. Desativar o suporte a 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**.

Desative grupos aninhados na autenticação remota no Active IQ Unified Manager

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupos aninhados para que somente usuários individuais, e não membros de grupos, 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 precisa ter a função de Application Administrator.
- Desativar grupos aninhados só se aplica ao uso do Active Directory.

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa de seleção para **Disable Nested Group Lookup**.
3. Clique em **Salvar**.

Configure os serviços de autenticação no Active IQ Unified Manager

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de conceder 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 precisa ter a função de Application Administrator.

Passos

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

Se você selecionar…	Então faça isso…
Active Directory	a. Digite o nome do administrador e a senha. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.
O OpenLDAP	a. Insira o nome diferenciado de vinculação e a senha de vinculação. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

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

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

3. Clique em **Salvar**.

Adicionar servidores de autenticação ao Active IQ Unified Manager

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

Antes de começar

- As informações a seguir 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 precisa ter a função de Application Administrator.

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 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 à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Ative ou desative a opção **Use secure connection**:

Se você quiser…	Então faça isso…
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 o endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Authorize Host, clique em View Certificate. e. Na caixa de diálogo Exibir Certificado, verifique as informações do certificado e clique em **Fechar**. f. Na caixa de diálogo "Authorize Host", clique em **Yes**. Quando você ativa a opção **Use Secure Connection authentication**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa a porta 636 como porta padrão para comunicação segura e a porta 389 para comunicação não segura.
Desative-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, bem como os detalhes da porta. d. Clique em **Add**.

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

3. Realize um teste de autenticação para confirmar que você consegue autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação no Active IQ Unified Manager

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 nos seus servidores de autenticação e autenticando esse usuário ou grupo 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 remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa procurar o usuário remoto ou o grupo remoto nesses servidores e autenticá-los.
- Você precisa ter a função de Application Administrator.

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Clique em **Test Authentication**.
3. Na caixa de diálogo Test User, especifique o nome de usuário e a senha do usuário remoto ou o nome do grupo remoto e clique em **Test**.

   Se você estiver autenticando um grupo remoto, não deve inserir a senha.

Adicione alertas no Active IQ Unified Manager

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

Antes de começar

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

Além de criar um alerta na página de Configuração de Alertas, conforme descrito aqui, você pode criá-lo diretamente na página de detalhes do evento após receber um evento.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página Configuração de alertas, 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 que deseja incluir ou excluir do alerta.

   Você pode definir um filtro especificando uma cadeia de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na cadeia de texto que você especificar, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto que você especificar

diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão que você especificou, a regra de exclusão tem precedência sobre a regra de inclusão, e o alerta não é 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 os quais você deseja acionar um alerta.



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

6. Clique em **Ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, defina se um trap SNMP será enviado ao receptor de traps e atribua um script para executar 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, pois o endereço de e-mail modificado não estará mais vinculado ao 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 como adicionar um alerta

Este exemplo mostra como criar um alerta que atenda 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 “Test” e o usuário deve ser notificado a cada 15 minutos

Execute as etapas a seguir na caixa de diálogo Add Alert:

Passos

1. Clique em **Nome** e digite **HealthTest** no campo **Nome do alerta**.
2. Clique em **Resources** e, na guia Include, 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'>>** na área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
   c. Clique em **Excluir**, digite **xyz** no campo **Nome contém** e, em seguida, clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Severidade do evento.
4. Selecione **Todos os eventos críticos** na área Eventos correspondentes e mova-o para a área Eventos selecionados.
5. Clique em **Actions**, e digite **sample@domain.com** no campo Alert these users.

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 durante um período específico. Você deve determinar o horário a partir do qual a notificação do 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 no Active IQ Unified Manager

Você pode alterar a senha de login do seu usuário local para evitar possíveis riscos de segurança.

Antes de começar

Você precisa estar conectado como um usuário local.

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

Passos

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

   A opção **Change Password** não é exibida se você for um usuário remoto.

3. Na caixa de diálogo Change Password, insira 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.

Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager

Você pode especificar o valor de tempo limite de inatividade para o 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 precisa ter a função de Application Administrator.

Essa configuração afeta todas as sessões de usuários conectados.

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

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 isso…
Não defina um tempo limite para que a sessão nunca seja fechada automaticamente	No painel **Tempo limite de inatividade**, mova o botão deslizante para a esquerda (desativado) e clique em **Aplicar**.
Defina um número específico de minutos como o valor de tempo limite	No painel **Tempo limite de inatividade**, mova o botão deslizante para a direita (ativado), especifique o valor do tempo limite de inatividade em minutos e clique em **Aplicar**.

Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager

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. Por padrão, o tempo limite da sua sessão está definido para o valor máximo, que é de 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo se você estiver conectado e usando o Unified Manager.

Sobre esta tarefa

Você precisa ter a função de Application Administrator.

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

Passos

1. Faça login na CLI do Unified Manager digitando o `um cli login` comando. Use um nome de usuário e uma senha válidos para autenticação.
2. Digite o `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

Alterar o nome do host da máquina virtual do Active IQ 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 regenerar o certificado HTTPS.

Antes de começar

Para executar essas tarefas, você precisa estar conectado ao Unified Manager como usuário de manutenção ou ter a função de Application Administrator atribuída.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface do usuário da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você terá atribuído um nome ao 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 estiverem configurados corretamente, o nome do host "Unified Manager" será atribuído automaticamente e associado ao certificado de segurança.

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

Se você acessar a interface web usando o endereço IP em vez do nome do host, não precisará gerar um novo certificado caso altere 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 só entrará em vigor após a reinicialização da máquina virtual do Unified Manager.

Passos

1. Gere um certificado de segurança HTTPS

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

2. Reinicie a máquina virtual do Unified Manager

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

Gere um certificado de segurança HTTPS no Active IQ Unified Manager

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 para substituir o certificado existente.

Antes de começar

Você precisa ter a função de Application Administrator.

Pode haver vários motivos para regenerar o certificado, por exemplo, se você quiser valores melhores para o Nome distinto (DN), um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tiver expirado.

Se você não tiver acesso à interface web do Unified Manager, poderá regenerar o certificado HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar os certificados, você pode definir o tamanho da chave e a duração de validade da chave. Se você usar a opção `Reset Server Certificate` no console de manutenção, um novo certificado HTTPS será criado e será válido por 397 dias. Este certificado terá uma chave RSA de 2048 bits.

Passos

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

   A caixa de diálogo "Regenerate HTTPS Certificate" é exibida.

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

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

Se você quiser…	Faça isso…
Gere o certificado usando valores diferentes	Clique na opção **Atualizar os atributos do certificado atual**. 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 variam de um mínimo de 1 dia a um máximo de 36.500 dias. Embora seja permitido um período de validade de 36500 dias, recomenda-se que você utilize um período de validade de no máximo 397 dias ou 13 meses. Isso porque, se você selecionar um período de validade superior a 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA reconhecida, a validade do certificado assinado retornado a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção "Excluir informações de identificação local (ex.: localhost)" se quiser remover as informações de identificação local do campo Nomes Alternativos no certificado. Quando essa 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 ao visualizar o certificado HTTPS.

Reinicie a máquina virtual do Active IQ Unified Manager

Você pode reiniciar a máquina virtual a partir do 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 appliance virtual está ligado.

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

Você também pode reiniciar a máquina virtual a partir do vSphere usando a opção **Restart Guest**. Consulte a documentação da VMware para obter mais informações.

Passos

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

Altere o nome do host do Active IQ Unified Manager em sistemas Linux

Em algum momento, você poderá 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 os 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 raiz 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, então terá 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 pretender 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 prática recomendada é atualizar o certificado para que o nome do host no certificado corresponda ao nome real do host. O novo certificado só entrará em vigor depois que a máquina Linux for 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. Faça login como usuário raiz no sistema do Unified Manager que você deseja modificar.
2. Pare o software Unified Manager e o software MySQL associado digitando o seguinte comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Gere novamente 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 reiniciar o serviço, verifique se o novo nome do host consegue dar ping em si mesmo:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando deve retornar o mesmo endereço IP que você definiu 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
   ```

Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de storage (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 associação de políticas de QoS, mas, quando aplicada usando o Unified Manager, permite provisionar e gerenciar cargas de trabalho em todos os clusters que a sua instância do Unified Manager está monitorando.

Você precisa ter a função de Application Administrator.

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

Quando ativada, esta opção fornece vários novos itens na interface de 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 storage de desempenho	Disponível em **Configurações** > **Políticas** > **Eficiência de storage**
Painéis que descrevem o desempenho atual da sua carga de trabalho e as IOPS da sua carga de trabalho	Disponível no painel de controle

Consulte a ajuda online do produto para obter mais informações sobre essas páginas e sobre 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 storage baseado em políticas escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a esquerda.
Habilitar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a direita.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.