Configurar notificações

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/task_configure_unified_manager_to_send_alert_notifications.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Configurar notificações . . . 1
- Configure o Active IQ Unified Manager para enviar notificações de alerta . . . 1
- Configure as definições de notificação de eventos no Active IQ Unified Manager . . . 1
- Ative a autenticação remota no Active IQ Unified Manager . . . 2
- Desative grupos aninhados na autenticação remota no Active IQ Unified Manager . . . 4
- Configure os serviços de autenticação no Active IQ Unified Manager . . . 4
- Adicionar servidores de autenticação ao Active IQ Unified Manager . . . 5
- Teste a configuração dos servidores de autenticação no Active IQ Unified Manager . . . 7
- Adicione alertas no Active IQ Unified Manager . . . 7
  - Exemplo de como adicionar um alerta . . . 9

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**.
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.

Se você quiser…	Então faça isso…
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**.

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.