



Configurando o Unified Manager para enviar notificações de alerta

Active IQ Unified Manager 9.7

NetApp
October 22, 2024

Índice

- Configurando o Unified Manager para enviar notificações de alerta 1
 - Antes de começar 1
 - Sobre esta tarefa 1
 - Passos 1
 - Configurar definições de notificação de eventos 2
 - Ativar autenticação remota 2
 - Desativando grupos aninhados da autenticação remota 4
 - Adicionando servidores de autenticação 4
 - Testando a configuração dos servidores de autenticação 6
 - Adicionando usuários 6
 - Adicionar alertas 7

Configurando 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

Tem de ter a função Administrador de aplicações.

Sobre esta tarefa

Depois de implantar o Unified Manager e concluir a configuração inicial, você deve considerar a configuração do ambiente para acionar alertas e gerar e-mails de notificação ou traps 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, configure um servidor SMTP e forneça um endereço de e-mail a partir 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. ["Ativar autenticação remota"](#)

Se você quiser que os usuários remotos LDAP ou ative Directory acessem a instância do Unified Manager e recebam notificações de alerta, habilite 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 utilizadores"](#)

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 notificações, configurar as configurações de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

Configurar definições de notificação de eventos

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 que é usado para enviar o alerta, e você pode definir vários mecanismos de notificação - por exemplo, notificações de alerta podem ser enviadas como e-mails ou traps SNMP.

Antes de começar

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

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

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Passos

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



****If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.**

**** If the host name of the SMTP server cannot be resolved, you can specify the IP address (IPv4 or IPv6) of the SMTP server instead of the host name.**

Ativar 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 e dados de storage.

Antes de começar

Tem de ter a função Administrador de aplicações.



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).

Sobre esta tarefa

Você pode ativar a autenticação remota usando LDAP aberto ou Active Directory. Se a autenticação remota estiver desativada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (Secure LDAP). O Unified Manager usa o 389 como a porta padrão para comunicação não segura e o 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 **Authentication Service** (Serviço de autenticação), selecione o tipo de serviço e configure o serviço de autenticação.

Para tipo de autenticação...	Digite as seguintes informações...
Ative Directory	<ul style="list-style-type: none">• Nome do administrador do servidor de autenticação em um dos seguintes formatos:<ul style="list-style-type: none">◦ domainname\username◦ username@domainname◦ Bind Distinguished Name (Usando a notação LDAP apropriada)• Senha do administrador• Nome diferenciado base (usando a notação LDAP apropriada)
Abra o LDAP	<ul style="list-style-type: none">• Vincular nome distinto (na notação LDAP apropriada)• Vincular senha• Nome diferenciado da base

Se a autenticação de um usuário do Active Directory demorar muito tempo ou tempo limite, o servidor de autenticação provavelmente levará muito tempo para responder. Desativar 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 SSL (Secure Sockets Layer).

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

Desativando grupos aninhados da autenticação remota

Se a autenticação remota estiver ativada, você poderá desativar a autenticação de grupo aninhado para que somente usuários individuais, e não membros de grupo, possam se autenticar remotamente no Unified Manager. Você pode desativar grupos aninhados quando quiser melhorar o tempo de resposta de autenticação do ative Directory.

Antes de começar

- Tem de ter a função Administrador de aplicações.
- A desativação de grupos aninhados só é aplicável ao usar o ative Directory.

Sobre esta tarefa

Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desativado 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 grupos aninhados**.
3. Clique em **Salvar**.

Adicionando servidores de autenticação

Você pode adicionar servidores de autenticação e ativar a autenticação remota no servidor de gerenciamento para que os usuários remotos no 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 o serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários remotos ou grupos no servidor de autenticação.
- Tem de ter a função Administrador de aplicações.

Sobre esta tarefa

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 de parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Ative ou desative a opção **Use secure Connection**:

Se você quiser...	Então faça isso...
Ative-o.	<ol style="list-style-type: none">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 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 Yes. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>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 o 636 como porta padrão para comunicação segura e o número de porta 389 para comunicação não segura.</p></div>
Desative-o.	<ol style="list-style-type: none">a. Desmarque a opção Use Secure Connection.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 Add.

O servidor de autenticação adicionado é exibido na área servidores.

3. Execute uma autenticação de teste para confirmar que é possível autenticar usuários no servidor de autenticação que você adicionou.

Testando a configuração dos servidores de autenticação

Você pode validar a configuração de seus servidores de autenticação para garantir que o servidor de gerenciamento seja capaz de se comunicar com eles. É possível validar a configuração pesquisando um usuário remoto ou grupo remoto de seus servidores de autenticação e autenticando-os usando as configurações configuradas.

Antes de começar

- Você deve ter habilitado a autenticação remota e configurado o 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 pesquisar o usuário remoto ou grupo remoto desses servidores e autenticá-los.
- Tem de ter a função Administrador de aplicações.

Sobre esta tarefa

Se o serviço de autenticação estiver definido como ativo 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 de autenticação.

Passos

1. No painel de navegação esquerdo, 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 de usuário do grupo remoto e clique em **Test**.

Se estiver a autenticar um grupo remoto, não deve introduzir a palavra-passe.

Adicionando usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página usuários. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base no Privileges das funções, os usuários podem gerenciar os objetos de storage e dados com o Unified Manager, ou exibir os dados em um banco de dados.

Antes de começar

- Tem de ter a função Administrador de aplicações.
- Para adicionar um utilizador ou grupo remoto, tem de ter ativado a autenticação remota e configurado o servidor de autenticação.

- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IDP) autentique usuários acessando a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários "remode".

O acesso à IU não é permitido para usuários do tipo "local" ou "Manutenção" quando a autenticação SAML está ativada.

Sobre esta tarefa

Se você adicionar um grupo do Windows ative Directory, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página **usuários**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar usuário**, selecione o tipo de usuário que deseja adicionar e insira as informações necessárias.

Ao inserir as informações de usuário necessárias, você deve especificar um endereço de e-mail exclusivo para esse usuário. Você deve evitar especificar endereços de e-mail compartilhados por vários usuários.

4. Clique em **Add**.

Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico é 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 configurações de notificação, como endereço de e-mail do usuário, servidor SMTP e host de intercetação SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e 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, você deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

Você pode criar um alerta diretamente da página de detalhes do evento depois de 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 cadeia de texto no campo **Name contains** para selecionar um grupo de recursos. Com base na cadeia de texto especificada, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto especificada é sensível a maiúsculas e minúsculas.

Se um recurso estiver em conformidade com as regras incluir e excluir que você especificou, a regra excluir terá precedência sobre a regra incluir 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 os quais 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, escolha se uma trap SNMP será enviada ao recetor de trap 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 será exibido em branco porque o endereço de e-mail modificado não será mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificou 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 através de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de 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 "ample@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:

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` o campo **Name contains** para exibir os volumes cujo nome contém `"abc"`.
 - b. Selecione **todos os volumes cujo nome contém 'abc'** na área recursos disponíveis e mova-o para a área recursos selecionados.
 - c. Clique em **Excluir**, digite `xyz` o campo **Nome contém** e clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítica** 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 esses usuários.
6. Selecione **lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

Você pode configurar um alerta para enviar repetidamente notificações aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta.

7. No menu Selecionar Script para execução, selecione **Test** script.
8. Clique em **Salvar**.

Informações sobre direitos autorais

Copyright © 2024 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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO 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 DESTES SOFTWARES, 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.