Configurando o Unified Manager para enviar notificações de alerta

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

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.

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.

   Notas:

   - Se o endereço de e-mail for pré-preenchido 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 de e-mail sejam entregues com sucesso.
   - Se o nome do host do servidor SMTP não puder ser resolvido, você poderá especificar o endereço IP (IPv4 ou IPv6) do servidor SMTP em vez do nome do host.
3. Clique em **Salvar**.
4. Se você tiver selecionado a opção **Use STARTTLS** ou **Use SSL**, uma página de certificado será exibida após clicar no botão **Save**. Verifique os detalhes do certificado e aceite o certificado para salvar as configurações de notificação.

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

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 conetado 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 ativar a autenticação remota usando LDAP aberto ou ative 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 Serviço de autenticação, selecione o tipo de serviço e configure o serviço de autenticação.

Para tipo de autenticação…	Digite as seguintes informações…
Ative 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 do administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome diferenciado da base

   Se a autenticação de um usuário do ative 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. **Opcional:** 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.

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**.

Configurando serviços de autenticação

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

Antes de começar

- Tem de ter ativado a autenticação remota.
- Tem de ter a função Administrador de aplicações.

Passos

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

Se selecionar…	Então faça isso…
Ative Directory	a. Introduza o nome e a palavra-passe do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é

Se selecionar…	Então faça isso…
OpenLDAP	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é
Outros	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação. d. Introduza o nome de utilizador, a associação ao grupo, o grupo de utilizadores e os atributos de membro.

Se você quiser modificar o serviço de autenticação, você deve excluir quaisquer servidores de autenticação existentes e adicionar novos servidores de autenticação.

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.

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.	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**. 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.
Desative-o.	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.

Se o serviço de autenticação estiver definido como ative 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 testar usuário, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Teste**.

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

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.

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 "sample@domain.com", um script "Teste", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

Passos

1. Clique em **Nome** e insira **Teste de integridade** no campo **Nome do alerta**.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.

a. Digite **abc** no campo **Nome contém** para exibir os volumes cujo nome contém "'abc'".
b. Selecione *[All Volumes whose name contains 'abc'] na área recursos disponíveis e mova-o para a área recursos selecionados.
c. Clique em **Excluir**, digite **xyz** no 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 digite **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

Informações sobre marcas comerciais