Gerenciar autenticação

Active IQ Unified Manager

NetApp
October 15, 2025

Índice

Gerenciar autenticação

Você pode habilitar a autenticação usando LDAP ou Active Directory no servidor do Unified Manager e configurá-lo para funcionar com seus servidores para autenticar usuários remotos.

Para habilitar a autenticação remota, configurar serviços de autenticação e adicionar servidores de autenticação, consulte a seção anterior sobre **Configurando o Unified Manager para enviar notificações de alerta**.

Editar servidores de autenticação

Você pode alterar a porta que o servidor do Unified Manager usa para se comunicar com seu servidor de autenticação.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Na área **Servidores de autenticação**, selecione o servidor de autenticação que você deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Excluir servidores de autenticação

Você pode excluir um servidor de autenticação se quiser impedir que o servidor do Unified Manager se comunique com o servidor de autenticação. Por exemplo, se você quiser alterar um servidor de autenticação com o qual o servidor de gerenciamento está se comunicando, você pode excluir o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você exclui um servidor de autenticação, usuários ou grupos remotos do servidor de autenticação não poderão mais acessar o Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Selecione um ou mais servidores de autenticação que você deseja excluir e clique em **Excluir**.
3. Clique em **Sim** para confirmar a solicitação de exclusão.

   Se a opção **Usar conexão segura** estiver habilitada, os certificados associados ao servidor de autenticação serão excluídos junto com o servidor de autenticação.

Autenticação com Active Directory ou OpenLDAP

Você pode habilitar a autenticação remota no servidor de gerenciamento e configurá-lo para se comunicar com seus servidores de autenticação para que os usuários dentro dos servidores de autenticação possam acessar o Unified Manager.

Você pode usar um dos seguintes serviços de autenticação predefinidos ou especificar seu próprio serviço de autenticação:

- Diretório Ativo da Microsoft

  Você não pode usar o Microsoft Lightweight Directory Services.

- OpenLDAP

Você pode selecionar o serviço de autenticação necessário e adicionar os servidores de autenticação apropriados para permitir que usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários ou grupos remotos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o Lightweight Directory Access Protocol (LDAP) para autenticar usuários remotos dentro do servidor de autenticação configurado.

Para usuários locais criados no Unified Manager, o servidor de gerenciamento mantém seu próprio banco de dados de nomes de usuários e senhas. O servidor de gerenciamento executa a autenticação e não usa o Active Directory ou o OpenLDAP para autenticação.

Registro de auditoria

Você pode detectar se os logs de auditoria foram comprometidos usando Logs de Auditoria. Todas as atividades realizadas por um usuário são monitoradas e registradas nos Logs de Auditoria. As auditorias são realizadas para todas as funcionalidades da interface do usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar o **Registro de auditoria: Visualização de arquivo** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos no Log de auditoria: Exibição de arquivos são listados com base na data de criação. Esta exibição exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o presente no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e ficam disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo “File Integrity Status”, que é monitorado ativamente para detectar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando estão disponíveis no sistema:

Estado	Descrição
ATIVO	Arquivo no qual os logs estão sendo registrados atualmente.
NORMAL	Arquivo que está inativo, compactado e armazenado no sistema.

Estado	Descrição
VIOLADO	Arquivo que foi comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO_MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo que foi excluído devido à descontinuação com base na Política de configuração de descontinuação.
EXCLUSÃO_INESPERADA	Arquivo que foi excluído por motivos desconhecidos.

A página Log de Auditoria inclui os seguintes botões de comando:

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite que você exclua qualquer um dos logs de auditoria listados na exibição Logs de Auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajudará no futuro a determinar uma exclusão válida. A coluna MOTIVO lista o motivo junto com o nome do usuário que executou a operação de exclusão.

A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela do banco de dados não será excluída.

Você pode baixar os logs de auditoria do Active IQ Unified Manager usando o botão **DOWNLOAD** na seção Logs de auditoria e exportar os arquivos de log de auditoria. Os arquivos marcados como “NORMAL” ou “TAMPERED” são baixados em um formato compactado `.gzip` formatar.

Os arquivos de log de auditoria são arquivados periodicamente e salvos no banco de dados para referência. Antes do arquivamento, os logs de auditoria são assinados digitalmente para manter a segurança e a integridade.

Quando um pacote AutoSupport completo é gerado, o pacote de suporte inclui arquivos de log de auditoria arquivados e ativos. Mas quando um pacote de suporte leve é gerado, ele inclui apenas os logs de auditoria ativos. Os logs de auditoria arquivados não estão incluídos.

Configurar logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de Auditoria para configurar a política contínua para arquivos de Log de Auditoria e também habilitar o registro remoto para os Logs de Auditoria.

Você pode definir os valores em **TAMANHO MÁXIMO DO ARQUIVO** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas de dados que você deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO MÁXIMO DO ARQUIVO** e **TAMANHO TOTAL DO LOG**

DE AUDITORIA. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TAMANHO TOTAL DO LOG DE AUDITORIA**, o arquivo que foi arquivado primeiro é excluído. Isso significa que o arquivo mais antigo é excluído. Mas a entrada do arquivo continua disponível no banco de dados e é marcada como "Rollover Delete". O valor **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** é para o número de dias em que os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo será substituído.

Passos

1. Clique em **Registros de auditoria** > > **Configurar**.
2. Insira valores em **TAMANHO MÁXIMO DO ARQUIVO**, **TAMANHO TOTAL DO LOG DE AUDITORIA** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**.

   Se você quiser habilitar o registro remoto, selecione **Habilitar registro remoto**. /// 2025-6-11, OUTRODOC-133

Habilitar registro remoto de logs de auditoria

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar registros de auditoria para habilitar o registro de auditoria remota. Você pode usar este recurso para transferir logs de auditoria para um servidor Syslog remoto. Isso permitirá que você gerencie seus logs de auditoria quando houver restrições de espaço.

O registro remoto de logs de auditoria fornece um backup à prova de violação caso os arquivos de log de auditoria no servidor Active IQ Unified Manager sejam adulterados.

Passos

1. Na caixa de diálogo **Configurar logs de auditoria**, marque a caixa de seleção **Habilitar registro remoto**.

   Campos adicionais para configurar o registro remoto são exibidos.

2. Digite o **HOSTNAME** e a **PORTA** do servidor remoto ao qual você deseja se conectar.
3. No campo **CERTIFICADO DE CA DO SERVIDOR**, clique em **PROCURAR** para selecionar um certificado público do servidor de destino.

   O certificado deve ser carregado em `.pem` formatar. Este certificado deve ser obtido do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o "hostname" selecionado como parte do `SubjectAltName` Atributo (SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog necessário e a versão do protocolo TLS nos campos **FORMAT** e **PROTOCOL**.
6. Marque a caixa de seleção **Habilitar autenticação do cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

   Você precisará baixar o certificado de autenticação do cliente e enviá-lo ao servidor Syslog antes de salvar a configuração do Log de Auditoria, caso contrário, a conexão falhará. Dependendo do tipo de servidor Syslog, pode ser necessário criar um hash do certificado de autenticação do cliente.

Exemplo: syslog-ng requer que um <hash> do certificado seja criado usando o comando `openssl x509 -noout -hash -in cert.pem`, e então você deve vincular simbolicamente o certificado de autenticação do cliente a um arquivo nomeado após <hash> .0.

7. Clique em **Salvar** para configurar a conexão com seu servidor e habilitar o registro remoto.

   Você será redirecionado para a página Logs de Auditoria.

> O valor **Tempo limite de conexão** pode afetar a configuração. Se a configuração demorar mais tempo para responder do que o valor definido, isso poderá levar à falha de configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor **Tempo limite de conexão** e tente a configuração novamente.

Página de autenticação remota

Você pode usar a página Autenticação Remota para configurar o Unified Manager para se comunicar com seu servidor de autenticação para autenticar usuários remotos que tentam fazer login na interface da Web do Unified Manager.

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

Depois de marcar a caixa de seleção Habilitar autenticação remota, você pode habilitar a autenticação remota usando um servidor de autenticação.

- **Serviço de Autenticação**

  Permite que você configure o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como Active Directory, OpenLDAP, ou especifique seu próprio mecanismo de autenticação. Você pode especificar um serviço de autenticação somente se tiver habilitado a autenticação remota.

  - **Diretório Ativo**
    - Nome do Administrador

      Especifica o nome do administrador do servidor de autenticação.

    - Senha

      Especifica a senha para acessar o servidor de autenticação.

    - Nome Distinto Base

      Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.

    - Desativar pesquisa de grupo aninhado

      Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

- Usar conexão segura

  Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

- **OpenLDAP**
  - Vincular nome distinto

    Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação.

  - Senha de vinculação

    Especifica a senha para acessar o servidor de autenticação.

  - Nome Distinto Base

    Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.

  - Usar conexão segura

    Especifica que o LDAP seguro é usado para comunicação com servidores de autenticação LDAP.

- **Outros**
  - Vincular nome distinto

    Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação que você configurou.

  - Senha de vinculação

    Especifica a senha para acessar o servidor de autenticação.

  - Nome Distinto Base

    Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.

  - Versão do Protocolo

    Especifica a versão do Lightweight Directory Access Protocol (LDAP) suportada pelo seu servidor de autenticação. Você pode especificar se a versão do protocolo deve ser detectada automaticamente ou definir a versão como 2 ou 3.

  - Atributo de nome de usuário

    Especifica o nome do atributo no servidor de autenticação que contém nomes de login de usuário a serem autenticados pelo servidor de gerenciamento.

  - Atributo de Associação de Grupo

    Especifica um valor que atribui a associação do grupo do servidor de gerenciamento a usuários

remotos com base em um atributo e valor especificados no servidor de autenticação do usuário.

- UGID

  Se os usuários remotos forem incluídos como membros de um objeto GroupOfUniqueNames no servidor de autenticação, esta opção permitirá que você atribua a associação de grupo do servidor de gerenciamento aos usuários remotos com base em um atributo especificado nesse objeto GroupOfUniqueNames.

- Desativar pesquisa de grupo aninhado

  Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

- Membro

  Especifica o nome do atributo que seu servidor de autenticação usa para armazenar informações sobre os membros individuais de um grupo.

- Classe de objeto do usuário

  Especifica a classe de objeto de um usuário no servidor de autenticação remota.

- Classe de Objeto de Grupo

  Especifica a classe de objeto de todos os grupos no servidor de autenticação remota.

> Os valores inseridos para os atributos *Membro*, *Classe de Objeto de Usuário* e *Classe de Objeto de Grupo* devem ser os mesmos adicionados nas configurações do Active Directory, OpenLDAP e LDAP. Caso contrário, a autenticação poderá falhar.

- Usar conexão segura

  Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

> Se você quiser modificar o serviço de autenticação, certifique-se de excluir todos os servidores de autenticação existentes e adicionar novos servidores de autenticação.

Área de Servidores de Autenticação

A área Servidores de autenticação exibe os servidores de autenticação com os quais o servidor de gerenciamento se comunica para localizar e autenticar usuários remotos. As credenciais para usuários ou grupos remotos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite que você adicione um servidor de autenticação.

  Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade

(usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação do parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação estiver inacessível.

  - Editar

    Permite que você edite as configurações de um servidor de autenticação selecionado.

  - Excluir

    Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

  Exibe o nome do host ou endereço IP do servidor de autenticação usado para autenticar o usuário no servidor de gerenciamento.

- **Porta**

  Exibe o número da porta do servidor de autenticação.

- **Teste de Autenticação**

  Este botão valida a configuração do seu servidor de autenticação autenticando um usuário ou grupo remoto.

  Durante o teste, se você especificar apenas o nome do usuário, o servidor de gerenciamento procurará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se você especificar o nome de usuário e a senha, o servidor de gerenciamento pesquisará e autenticará o usuário remoto.

  Não é possível testar a autenticação se a autenticação remota estiver desabilitada.

Informações sobre direitos autorais

Informações sobre marcas comerciais