Gerenciamento da autenticação

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

Gerenciamento da autenticação

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

Para ativar a autenticação remota, configurar serviços de autenticação e adicionar severs de autenticação, consulte a seção anterior em **Configurando o Unified Manager para enviar notificações de alerta**.

Editando servidores de autenticação

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

Antes de começar

Tem de ter a função Administrador de aplicações.

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 deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Eliminar 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 pretender alterar um servidor de autenticação com o qual o servidor de gestão está a comunicar, pode eliminar o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você exclui um servidor de autenticação, usuários remotos ou grupos 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 **Yes** para confirmar a solicitação de exclusão.

   Se a opção **usar conexão segura** estiver ativada, os certificados associados ao servidor de autenticação serão excluídos juntamente com o servidor de autenticação.

Autenticação com ative Directory ou OpenLDAP

Você pode ativar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento 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:

- Microsoft ative Directory

  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 os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o LDAP (Lightweight Directory Access Protocol) para autenticar usuários remotos no servidor de autenticação configurado.

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

Registo de auditoria

Você pode detetar se os logs de auditoria foram comprometidos com o uso de logs de auditoria. Todas as atividades realizadas por um utilizador são monitorizadas e registadas nos registos de auditoria. As auditorias são realizadas para todas as interfaces de usuário e funcionalidades do Active IQ Unified Manager das APIs expostas publicamente.

Você pode usar o **Registro de auditoria: Exibição de arquivo** para exibir e acessar todos os arquivos de log de auditoria disponíveis no Active IQ Unified Manager. Os arquivos no Audit Log: File View são listados com base em sua data de criação. Esta vista apresenta informações de todo o registo de auditoria que são capturados da instalação ou atualização para o presente no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e estão disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo "Status de integridade de arquivo" que é monitorado ativamente para detetar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando os logs de auditoria estão disponíveis no sistema:

Estado	Descrição
ATIVO	Ficheiro no qual os registos estão a ser registados atualmente.
NORMAL	Ficheiro inativo, comprimido e armazenado no sistema.

Estado	Descrição
ADULTERADO	Arquivo que foi comprometido por um usuário que editou manualmente o arquivo.
MANUAL_DELETE	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Ficheiro que foi eliminado devido à implementação com base na política de configuração contínua.
UNEXPECTED_DELETE	Arquivo que foi excluído devido a razões desconhecidas.

A página Registo de auditoria inclui os seguintes botões de comando:

- Configurar
- Eliminar
- Transferir

O botão **DELETE** permite excluir 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 juntamente com o nome do usuário que realizou a operação de exclusão.

A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela DB 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 "ADULTERADO" são baixados em um formato compactado `.gzip`.

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 registos de auditoria arquivados não estão incluídos.

Configurando logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de auditoria para configurar a política de rolagem para arquivos de log de auditoria e também ativar o log remoto para os Logs de auditoria.

Você pode definir os valores nos DIAS DE RETENÇÃO DO REGISTRO **MAX** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas dos dados que deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho dos dados totais do log de auditoria presentes no sistema. A política de rolagem é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO DO ARQUIVO MAX** 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 de arquivo continua disponível no banco de dados e é marcada como "Rollover Delete". O valor **AUDIT LOG RETENT DAYS** 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 é rolado.

Passos

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

   Se pretender ativar o registo remoto, deve selecionar **Ativar registo remoto**.

Ativar o registo remoto de registos de auditoria

Pode selecionar a caixa de verificação **Ativar registo remoto** na caixa de diálogo Configurar registos de auditoria para ativar o registo de auditoria remota. Você pode usar esse 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 no caso de os arquivos de log de auditoria no servidor Active IQ Unified Manager serem adulterados.

Passos

1. Na caixa de diálogo **Configurar registos de auditoria**, selecione a caixa de verificação **Ativar registo remoto**.

   São apresentados campos adicionais para configurar o registo remoto.

2. Introduza **HOSTNAME** e **PORT** do servidor remoto ao qual pretende ligar.
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` formato. Este certificado deve ser obtido a partir do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o nome do host selecionado como parte do `SubjectAltName` atributo (SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **TEMPO LIMITE DE CONEXÃO**, **ATRASO DE CONEXÃO**.

   Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog e a versão do protocolo TLS necessários nos campos **FORMAT** e **PROTOCOL**.
6. Marque a caixa de seleção **Ativar 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 para o servidor Syslog antes de salvar a configuração do Log de auditoria, caso contrário a conexão falhará. Dependendo do tipo de servidor Syslog, talvez seja necessário criar um hash do certificado de autenticação do cliente.

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

7. Clique em **Salvar** para configurar a conexão com o servidor e ativar o Registro remoto.

   Você será redirecionado para a página Logs de auditoria.

   O valor **tempo limite da conexão** pode afetar a configuração. Se a configuração demorar mais tempo a responder do que o valor definido, pode resultar em falha de configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor **tempo limite da conexão** e tente a configuração novamente.

Página Autenticação remota

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

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

Depois de selecionar a caixa de verificação Ativar autenticação remota, pode ativar a autenticação remota utilizando um servidor de autenticação.

- **Serviço de autenticação**

  Permite configurar o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como ative Directory, OpenLDAP ou especificar seu próprio mecanismo de autenticação. Você só pode especificar um serviço de autenticação se tiver habilitado a autenticação remota.

  - **Ative Directory**
    - Nome do administrador

      Especifica o nome de administrador do servidor de autenticação.

    - Palavra-passe

      Especifica a senha para acessar o servidor de autenticação.

    - Nome diferenciado base

      Especifica a localização dos usuários remotos no 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

    - Desative a Pesquisa de grupos aninhados

      Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

    - Utilize a ligação segura

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

- **OpenLDAP**
  - Vincular Nome distinto

    Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação.

  - Vincular senha

    Especifica a senha para acessar o servidor de autenticação.

  - Nome diferenciado base

    Especifica a localização dos usuários remotos no 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

  - Utilize a ligação segura

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

- **Outros**
  - Vincular Nome distinto

    Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação que você configurou.

  - Vincular senha

    Especifica a senha para acessar o servidor de autenticação.

  - Nome diferenciado base

    Especifica a localização dos usuários remotos no 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

  - Versão do protocolo

    Especifica a versão LDAP (Lightweight Directory Access Protocol) suportada pelo servidor de autenticação. Pode especificar se a versão do protocolo tem de ser detetada automaticamente ou definir a versão para 2 ou 3.

  - Atributo Nome Utilizador

    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 especificado no servidor de autenticação do usuário.

- UGID

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

- Desative a Pesquisa de grupos aninhados

  Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Membro

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

- Classe Objeto Utilizador

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

- Classe Objeto Grupo

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

  Os valores que você insere para os atributos *Member*, *User Object Class* e *Group Object Class* devem ser os mesmos que os adicionados nas configurações do ative Directory, OpenLDAP e LDAP. Caso contrário, a autenticação poderá falhar.

- Utilize a ligação segura

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

Se pretender modificar o serviço de autenticação, certifique-se de que elimina quaisquer servidores de autenticação existentes e adiciona novos servidores de autenticação.

Área 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 remotos ou grupos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite adicionar 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 está inacessível.

- Editar

  Permite editar as definições de um servidor de autenticação selecionado.

- Eliminar

  Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

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

- **Porto**

  Exibe o número da porta do servidor de autenticação.

- * Teste de Autenticação*

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

  Durante o teste, se você especificar apenas o nome de usuário, o servidor de gerenciamento pesquisará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se especificar o nome de utilizador e a palavra-passe, o servidor de gestão procura e autentica o utilizador remoto.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais