Registo de auditoria

Active IQ Unified Manager 9.13

NetApp
July 15, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-913/config/task_configure_audit_logs.html on July 15, 2026. Always check docs.netapp.com for the latest.

Índice

Registo de auditoria 1
Configurando logs de auditoria 2
Ativar o registo remoto de registos de auditoria 2

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.
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.

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.