Registro de auditoria

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/config/concept_audit_logging.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Registro de auditoria 1
Saiba mais sobre os registros de auditoria no Active IQ Unified Manager 1
Configurar os registros de auditoria do Active IQ Unified Manager 2
Ative o registro remoto de logs de auditoria no Active IQ Unified Manager 2

Registro de auditoria

Saiba mais sobre os registros de auditoria no Active IQ Unified Manager

É possível detectar se os logs de auditoria foram comprometidos usando os 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 de usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar a **Visualização de arquivos: log de auditoria** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos na Visualização de arquivos: log de auditoria são listados com base na data de criação. Essa visualização exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o momento 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 inativo, compactado e armazenado no sistema.
ADULTERADO	Arquivo comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo excluído devido à remoção com base na Política de Configuração de Rotação.
UNEXPECTED_DELETE	Arquivo que foi excluído por motivos desconhecidos.

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

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite excluir qualquer um dos logs de auditoria listados na visualização Logs de auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajuda no futuro a determinar se a exclusão foi válida. A coluna MOTIVO lista o motivo juntamente com o nome do usuário que realizou a operação de exclusão.

Excluir um arquivo de log remove o arquivo do sistema, mas não exclui a entrada na tabela do DB.

Você pode baixar os logs de auditoria do Active IQ Unified Manager usando o botão **DOWNLOAD** na seção Audit Logs e exportar os arquivos de log de auditoria. Os arquivos marcados como “NORMAL” ou

“TAMPERED” são baixados em formato `.gzip` compactado.

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

Configurar os registros de auditoria do Active IQ Unified Manager

Você pode usar o botão **Configure** na seção Logs de Auditoria para configurar a política de rotação dos arquivos de log de auditoria e também habilitar o registro remoto dos Logs de Auditoria.

Você pode definir os valores em **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** de acordo com a quantidade e a frequência de dados que deseja armazenar no sistema. O valor no campo **TOTAL AUDIT LOG SIZE** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** e **TOTAL AUDIT LOG SIZE**. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TOTAL AUDIT LOG SIZE**, 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 de **AUDIT LOG RETENTION DAYS** corresponde ao número de dias durante os quais os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo passa por rollover.

Passos

1. Clique em **Logs 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**.

   Para ativar o registro remoto, selecione **Ativar registro remoto**.

Ative o registro remoto de logs de auditoria no Active IQ Unified Manager

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar logs de auditoria para habilitar o registro remoto de auditoria. 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 dos logs de auditoria fornece um backup à prova de adulteração 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**, selecione a caixa de seleção **Habilitar registro remoto**.

   São exibidos campos adicionais para configurar o registro remoto.

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

   O certificado deve ser carregado no formato `.pem`. Este certificado deve ser obtido do servidor Syslog de destino e não deve estar expirado. O certificado deve conter o "hostname" selecionado como parte do atributo `SubjectAltName`(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. Selecione a caixa de seleção **Habilitar autenticação de cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

   Você precisará baixar o certificado de autenticação de cliente e carregá-lo no 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 de cliente.

   Exemplo: o syslog-ng requer que uma <hash> do certificado seja criada usando o comando `openssl x509 -noout -hash -in cert.pem`, e então você deve criar simbolicamente um link do certificado de autenticação de cliente para um arquivo nomeado com <hash> .0.

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

   Você será redirecionado para a página de Registros de Auditoria.

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