



# Gerenciar syslog

SANtricity 11.9

NetApp

December 16, 2024

# Índice

- Gerenciar syslog ..... 1
  - Exibir atividade do log de auditoria ..... 1
  - Definir políticas de log de auditoria ..... 3
  - Excluir eventos do log de auditoria ..... 4
  - Configure o servidor syslog para logs de auditoria ..... 5
  - Edite as configurações do servidor syslog para Registros de log de auditoria ..... 6

# Gerenciar syslog

## Exibir atividade do log de auditoria

Ao visualizar logs de auditoria, os usuários com permissões de administrador de segurança podem monitorar as ações do usuário, falhas de autenticação, tentativas de login inválidas e a vida útil da sessão do usuário.

### Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.




### Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione a guia **Audit Log**.

A atividade do log de auditoria aparece em formato tabular, que inclui as seguintes colunas de informações:

- **Date/time** — Timestamp de quando a matriz de armazenamento detetou o evento (em GMT).
  - **Nome de usuário** — o nome de usuário associado ao evento. Para quaisquer ações não autenticadas na matriz de armazenamento, "N/A" aparece como o nome de usuário. Ações não autenticadas podem ser acionadas pelo proxy interno ou por algum outro mecanismo.
  - **Status Code** — Código de status HTTP da operação (200, 400, etc.) e texto descritivo associado ao evento.
  - **URL acessado** — URL completa (incluindo host) e string de consulta.
  - **Endereço IP do cliente** — Endereço IP do cliente associado ao evento.
  - **Source** — fonte de Registro associada ao evento, que pode ser System Manager, CLI, Web Services ou Support Shell.
  - **Descrição** — informações adicionais sobre o evento, se aplicável.
3. Utilize as seleções na página Registro de auditoria para ver e gerir eventos.

## Detalhes da seleção

Seleção	Descrição
Mostrar eventos do...	Limite eventos mostrados por intervalo de datas (últimas 24 horas, últimos 7 dias, últimos 30 dias ou um intervalo de datas personalizado).
Filtro	Limite eventos mostrados pelos caracteres inseridos no campo. Use aspas (""") para uma correspondência exata de palavras, digite OR para retornar uma ou mais palavras ou insira um traço ( — ) para omitir palavras.
Atualizar	Selecione <b>Atualizar</b> para atualizar a página para os eventos mais atuais.
Ver/Editar definições	Selecione <b>Exibir/Editar configurações</b> para abrir uma caixa de diálogo que permite especificar uma política de log completa e o nível de ações a serem registradas.
Eliminar eventos	Selecione <b>Excluir</b> para abrir uma caixa de diálogo que permite remover eventos antigos da página.
Mostrar/ocultar colunas	<p>Clique no ícone da coluna <b>Mostrar/Ocultar</b>  para selecionar colunas adicionais para exibição na tabela. Colunas adicionais incluem:</p> <ul style="list-style-type: none"><li>• <b>Método</b> — o método HTTP (por exemplo, POST, GET, DELETE, etc.).</li><li>• * Comando CLI executado* — o comando CLI (gramática) executado para solicitações de CLI segura.</li><li>• <b>CLI Return Status</b> — Um código de status CLI ou uma solicitação de arquivos de entrada do cliente.</li><li>• <b>Procedimento de símbolo</b> — procedimento de símbolo executado.</li><li>• * Tipo de evento SSH* — tipo de eventos Secure Shell (SSH), como login, logout e login_fail.</li><li>• <b>SSH Session PID</b> — número de ID do processo da sessão SSH.</li><li>• <b>Duração(s) da sessão SSH</b> — o número de segundos em que o usuário foi conectado.</li><li>• <b>Tipo de autenticação</b> — os tipos podem incluir usuário local, LDAP, SAML e token de acesso.</li><li>• <b>ID de autenticação</b> — ID da sessão autenticada.</li></ul>
Alternar filtros de coluna	Clique no ícone <b>alternar</b>  para abrir campos de filtragem para cada coluna. Insira caracteres dentro de um campo de coluna para limitar eventos mostrados por esses caracteres. Clique novamente no ícone para fechar os campos de filtragem.
Anular alterações	Clique no ícone <b>Desfazer</b>  para retornar a tabela à configuração padrão.

Seleção	Descrição
Exportação	Clique em <b>Export</b> para salvar os dados da tabela em um arquivo CSV (Comma Separated Value).

## Definir políticas de log de auditoria

Pode alterar a política de substituição e os tipos de eventos registrados no registo de auditoria.

### Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

### Sobre esta tarefa

Esta tarefa descreve como alterar as definições do registo de auditoria, que incluem a política de substituição de eventos antigos e a política de gravação de tipos de eventos.



### Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione o separador **Registro de auditoria**.
3. Selecione **Exibir/Editar configurações**.

A caixa de diálogo Configurações do Registro de auditoria é aberta.

4. Altere a política de substituição ou os tipos de eventos gravados.

## Detalhes do campo

Definição	Descrição
Substituir a política	<p>Determina a política de substituição de eventos antigos quando a capacidade máxima é atingida:</p> <ul style="list-style-type: none"><li>• <b>Permitir que os eventos mais antigos do log de auditoria sejam sobrescritos quando o log de auditoria estiver cheio</b> — sobrescreve os eventos antigos quando o log de auditoria atinge 50.000 Registros.</li><li>• <b>Exigir que os eventos de log de auditoria sejam excluídos manualmente</b> — especifica que os eventos não serão excluídos automaticamente; em vez disso, um aviso de limite aparece na porcentagem definida. Os eventos devem ser excluídos manualmente.</li></ul> <p> Se a política de substituição estiver desativada e as entradas do log de auditoria atingirem o limite máximo, o acesso ao System Manager será negado aos usuários sem permissões de Administrador de Segurança. Para restaurar o acesso do sistema a usuários sem permissões de Administrador de Segurança, um usuário atribuído à função Administrador de Segurança deve excluir os Registros de eventos antigos.</p> <p> As diretivas de substituição não se aplicam se um servidor syslog estiver configurado para arquivar logs de auditoria.</p>
Nível de ações a registrar	<p>Determina os tipos de eventos a serem registrados:</p> <ul style="list-style-type: none"><li>• <b>Gravar eventos de modificação somente</b> — mostra apenas os eventos em que uma ação do usuário envolve fazer uma alteração no sistema.</li><li>• <b>Grave todos os eventos de modificação e somente leitura</b> — mostra todos os eventos, incluindo uma ação do usuário que envolve a leitura ou download de informações.</li></ul>

5. Clique em **Salvar**.

## Excluir eventos do log de auditoria

Você pode limpar o log de auditoria de eventos antigos, o que torna a pesquisa através de eventos mais gerenciável. Você tem a opção de salvar eventos antigos em um arquivo CSV (valores separados por vírgulas) após a exclusão.

### Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança.

Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

### Passos

1. Selecione **Definições** > **Gestão de Acesso**.
2. Selecione o separador **Registo de auditoria**.
3. Selecione **Eliminar**.

A caixa de diálogo Excluir Registo de auditoria é aberta.

4. Selecione ou introduza o número de eventos mais antigos que pretende eliminar.
5. Se pretender exportar os eventos eliminados para um ficheiro CSV (recomendado), mantenha a caixa de verificação selecionada. Você será solicitado a inserir um nome de arquivo e um local quando clicar em **Excluir** na próxima etapa. Caso contrário, se você não quiser salvar eventos em um arquivo CSV, clique na caixa de seleção para desmarcá-lo.
6. Clique em **Excluir**.

Abre-se uma caixa de diálogo de confirmação.

7. Digite delete o campo e clique em **Excluir**.

Os eventos mais antigos são removidos da página Registo de Auditoria.

## Configure o servidor syslog para logs de auditoria

Se você quiser arquivar logs de auditoria em um servidor syslog externo, você pode configurar as comunicações entre esse servidor e o storage array. Depois que a conexão é estabelecida, os logs de auditoria são salvos automaticamente no servidor syslog.

### Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se o servidor usar um protocolo seguro (por exemplo, TLS), um certificado de autoridade de certificação (CA) deve estar disponível no sistema local. Os certificados CA identificam os proprietários de sites para conexões seguras entre servidores e clientes.

### Passos

1. Selecione **Definições** > **Gestão de Acesso**.
2. Na guia Registo de auditoria, selecione **Configurar servidores Syslog**.

A caixa de diálogo Configurar servidores Syslog é aberta.

3. Clique em **Add**.

A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Insira as informações do servidor e clique em **Adicionar**.

- **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- **Protocol** — Selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
- **Upload certificate (opcional)** — se você selecionou o protocolo TLS e ainda não carregou um certificado CA assinado, clique em **Browse** para carregar um arquivo de certificado. Os logs de auditoria não são arquivados em um servidor syslog sem um certificado confiável.



Se o certificado se tornar inválido mais tarde, o handshake TLS falhará. Como resultado, uma mensagem de erro é postada no log de auditoria e as mensagens não são mais enviadas para o servidor syslog. Para resolver este problema, tem de corrigir o certificado no servidor syslog e, em seguida, aceder ao **Definições > Registo de auditoria > Configurar servidores Syslog > testar tudo**.

- **Port** — Digite o número da porta para o recetor syslog. Depois de clicar em **Add**, a caixa de diálogo Configurar servidores Syslog abre e exibe o servidor syslog configurado na página.

5. Para testar a conexão do servidor com a matriz de armazenamento, selecione **Test All**.

### Resultados

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os registos anteriores não são transferidos. Para configurar ainda mais as configurações do syslog para alertas, "[Configure o servidor syslog para alertas](#)" consulte .

NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

## Edite as configurações do servidor syslog para Registros de log de auditoria

Você pode alterar as configurações do servidor syslog usado para arquivar logs de auditoria e também carregar um novo certificado de autoridade de certificação (CA) para o servidor.

### Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se você estiver carregando um novo certificado de CA, o certificado deve estar disponível no sistema local.

### Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Na guia Registro de auditoria, selecione **Configurar servidores Syslog**.

Os servidores syslog configurados são exibidos na página.



3. Para editar as informações do servidor, selecione o ícone **Edit** (lápiz) à direita do nome do servidor e, em seguida, faça as alterações desejadas nos seguintes campos:
  - **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
  - **Protocol** — Selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
  - **Port** — Digite o número da porta para o recetor syslog.
4. Se você alterou o protocolo para o protocolo TLS seguro (de UDP ou TCP), clique em **Importar certificado confiável** para carregar um certificado CA.
5. Para testar a nova conexão com a matriz de armazenamento, selecione **Test All**.

## Resultados

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os registros anteriores não são transferidos.

## **Informações sobre direitos autorais**

Copyright © 2024 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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; 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 DESTES SOFTWARES, 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.