Gerenciar syslog

SANtricity software

NetApp
March 17, 2026

Índice

Gerenciar syslog

Visualizar atividade do log de auditoria no SANtricity System Manager

Ao visualizar os logs de auditoria, os usuários com permissões de Security Admin podem monitorar ações do usuário, falhas de autenticação, tentativas de login inválidas e a duração da sessão do usuário.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.

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

   - **Data/Hora** — Registro de data e hora de quando o array de storage detectou o evento (em GMT).
   - **Nome de usuário** — O nome de usuário associado ao evento. Para quaisquer ações não autenticadas no array de storage, "N/A" aparece como o nome de usuário. Ações não autenticadas podem ser acionadas pelo proxy interno ou por algum outro mecanismo.
   - **Código de Status** — Código de status HTTP da operação (200, 400, etc.) e texto descritivo associado ao evento.
   - **URL acessada** — URL completa (incluindo host) e string de consulta.
   - **Endereço IP do cliente** — endereço IP do cliente associado ao evento.
   - **Origem** — 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 opções da página de log de auditoria para visualizar e gerenciar eventos.

Detalhes da seleção

Seleção	Descrição
Exibir eventos de…	Limite os eventos exibidos por intervalo de datas (últimas 24 horas, últimos 7 dias, últimos 30 dias ou um intervalo de datas personalizado).
Filtro	Limite os eventos exibidos aos caracteres inseridos no campo. Use aspas ("") para uma correspondência exata de palavras, insira `OR` para retornar uma ou mais palavras ou insira um hífen (—) para omitir palavras.
Atualizar	Selecione **Atualizar** para atualizar a página para os eventos mais atuais.
Ver/Editar configurações	Selecione **Exibir/Editar configurações** para abrir uma caixa de diálogo que permite especificar uma política de log completa e o nível de ações a serem registradas.
Excluir eventos	Selecione **Delete** para abrir uma caixa de diálogo que permite remover eventos antigos da página.
Mostrar/ocultar colunas	Clique no ícone da coluna **Mostrar/Ocultar** para selecionar colunas adicionais para exibição na tabela. Colunas adicionais incluem: • **Método** — O método HTTP (por exemplo, POST, GET, DELETE, etc.). • **Comando CLI executado** — O comando CLI (gramática) executado para solicitações Secure CLI. • **Status de retorno da CLI** — Um código de status da CLI ou uma solicitação de arquivos de entrada do cliente. • **Procedimento SYMbol** — O procedimento SYMbol foi executado. • **Tipo de evento SSH** — Tipo de evento Secure Shell (SSH), como login, logout e login_fail. • **PID da sessão SSH** — Número de identificação do processo da sessão SSH. • **Duração da sessão SSH (s)** — O número de segundos em que o usuário esteve conectado. • **Tipo de autenticação** — Tipos podem incluir usuário local, LDAP, SAML e token de acesso. • **ID de autenticação** — ID da sessão autenticada.
Alternar filtros de coluna	Clique no ícone **Alternar** para abrir os campos de filtro de cada coluna. Digite caracteres em um campo da coluna para limitar os eventos exibidos por esses caracteres. Clique no ícone novamente para fechar os campos de filtro.
Desfazer alterações	Clique no ícone **Desfazer** para retornar a tabela à configuração padrão.

Seleção	Descrição
Exportar	Clique em **Exportar** para salvar os dados da tabela em um arquivo CSV (comma separated value).

Defina as políticas de log de auditoria no SANtricity System Manager

Você pode alterar a política de sobrescrita e os tipos de eventos registrados no log de auditoria.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Esta tarefa descreve como alterar as configurações do log de auditoria, que incluem a política para sobrescrever eventos antigos e a política para registrar tipos de eventos.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.
3. Selecione **Visualizar/Editar Settings**.

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

4. Altere a política de sobrescrita ou os tipos de eventos registrados.

Detalhes do campo

Configuração	Descrição
Política de sobrescrita	Determina a política para sobrescrever eventos antigos quando a capacidade máxima é atingida: • **Permitir que os eventos mais antigos no log de auditoria sejam sobrescritos quando o log de auditoria estiver cheio** — Sobrescreve os eventos antigos quando o log de auditoria atinge 50,000 registros. • **Exigir que os eventos do log de auditoria sejam excluídos manualmente** — Especifica que os eventos não serão excluídos automaticamente; em vez disso, um aviso de limite será exibido na porcentagem definida. Os eventos devem ser excluídos manualmente. Se a política de sobrescrita 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 Security Admin. Para restaurar o acesso ao sistema para usuários sem permissões de Security Admin, um usuário atribuído à função de Security Admin deve excluir os registros de eventos antigos. As políticas de sobrescrita não se aplicam se um servidor syslog estiver configurado para arquivamento de logs de auditoria.
Nível de ações a serem registradas	Determina os tipos de eventos a serem registrados: • **Somente eventos de modificação de registros** — Mostra apenas os eventos em que uma ação do usuário envolve uma alteração no sistema. • **Registrar todos os eventos de modificação e somente leitura** — Exibe todos os eventos, incluindo uma ação do usuário que envolva a leitura ou o download de informações.

5. Clique em **Salvar**.

Excluir eventos do log de auditoria no SANtricity System Manager

Você pode limpar o log de auditoria de eventos antigos, o que torna a busca por eventos mais gerenciável. Você tem a opção de salvar eventos antigos em um arquivo CSV (valores separados por vírgula) ao excluí-los.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.
3. Selecione **Delete**.

   A caixa de diálogo Excluir log de auditoria é aberta.

4. Selecione ou insira o número de eventos mais antigos que você deseja excluir.
5. Se desejar exportar os eventos excluídos para um arquivo CSV (recomendado), mantenha a caixa de seleção marcada. Você será solicitado a inserir um nome e um local para o arquivo ao clicar em **Excluir** na próxima etapa. Caso contrário, se não quiser salvar os eventos em um arquivo CSV, clique na caixa de seleção para desmarcá-la.
6. Clique em **Delete**.

   Uma caixa de diálogo de confirmação é aberta.

7. Digite `delete` no campo e clique em **Excluir**.

   Os eventos mais antigos são removidos da página de log de auditoria.

Configurar o servidor syslog para log de auditoria no SANtricity System Manager

Se você quiser arquivar logs de auditoria em um servidor syslog externo, pode configurar a comunicação entre esse servidor e o array de storage. Após a conexão ser estabelecida, os logs de auditoria são salvos automaticamente no servidor syslog.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se o seu servidor utiliza um protocolo seguro (por exemplo, TLS), um certificado de Autoridade Certificadora (CA) deve estar disponível no seu sistema local. Os certificados de CA identificam os proprietários de websites para conexões seguras entre servidores e clientes.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Na guia log de auditoria, selecione **Configurar servidores syslog**.

   A caixa de diálogo Configurar servidores syslog é aberta.

3. Clique em **Add**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

4. Insira as informações do servidor e clique em **Adicionar**.
   - **Endereço do servidor** — Insira um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
   - **Protocolo** — selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
   - **Carregar certificado (opcional)** — Se você selecionou o protocolo TLS e ainda não carregou um certificado de CA assinado, clique em **Procurar** 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 posteriormente, o handshake TLS falhará. Como resultado, uma mensagem de erro será registrada no log de auditoria e as mensagens não serão mais enviadas para o servidor syslog. Para resolver esse problema, você deve corrigir o certificado no servidor syslog e então acessar menu:Configurações [Log de Auditoria > Configurar Servidores Syslog > Testar Todos].

   - **Porta** — Insira o número da porta para o syslog receiver. Depois de clicar em **Adicionar**, a caixa de diálogo Configurar Servidores Syslog será aberta e exibirá o seu servidor syslog configurado na página.
5. Para testar a conexão do servidor com o array de storage, selecione **Test All**.

Resultados

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os logs anteriores não são transferidos. Para configurar ainda mais as definições do syslog para alertas, consulte "Configurar servidor syslog para alertas".

```
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 no SANtricity System Manager

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

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um 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 seu sistema local.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Na guia log de auditoria, selecione **Configurar servidores syslog**.

Os servidores syslog configurados são exibidos na página.

3. Para editar as informações do servidor, selecione o ícone **Editar** (lápis) à direita do nome do servidor e, em seguida, faça as alterações desejadas nos seguintes campos:
   - **Endereço do servidor** — Insira um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
   - **Protocolo** — selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
   - **Porta** — Insira o número da porta para o receptor syslog.
4. Se você alterou o protocolo para o protocolo seguro TLS (de UDP ou TCP), clique em **Import Trusted Certificate** para carregar um certificado de CA.
5. Para testar a nova conexão com o array de storage, selecione **Test All**.

Resultados

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

Informações sobre direitos autorais

Informações sobre marcas comerciais