



Log de auditoria

ONTAP 9

NetApp
January 17, 2025

Índice

- Log de auditoria 1
 - Como o ONTAP implementa o log de auditoria 1
 - Alterações ao registo de auditoria no ONTAP 9. 2
 - Exibir conteúdo do log de auditoria 2
 - Gerenciar as configurações de solicitação DE auditoria 3
 - Gerenciar destinos de log de auditoria 4

Log de auditoria

Como o ONTAP implementa o log de auditoria

As atividades de gerenciamento registradas no log de auditoria são incluídas nos relatórios padrão do AutoSupport e certas atividades de Registro são incluídas nas mensagens do EMS. Você também pode encaminhar o log de auditoria para destinos especificados e exibir arquivos de log de auditoria usando a CLI ou um navegador da Web.

A partir do ONTAP 9.11,1, você pode exibir o conteúdo do log de auditoria usando o Gerenciador do sistema.

A partir do ONTAP 9.12,1, o ONTAP fornece alertas de adulteração para logs de auditoria. O ONTAP executa um trabalho de segundo plano diário para verificar se há adulteração de arquivos `audit.log` e envia um alerta EMS se ele encontrar arquivos de log que foram alterados ou adulterados.

O ONTAP Registra as atividades de gerenciamento que são executadas no cluster, por exemplo, qual solicitação foi emitida, o usuário que acionou a solicitação, o método de acesso do usuário e a hora da solicitação.

As atividades de gestão podem ser um dos seguintes tipos:

- Definir solicitações, que normalmente se aplicam a comandos ou operações que não sejam exibidas:
 - Essas solicitações são emitidas quando você executa um `create` comando, `modify`, ou `delete`, por exemplo.
 - As solicitações de conjunto são registradas por padrão.
- OBTENHA solicitações, que recuperam informações e exibem na interface de gerenciamento:
 - Essas solicitações são emitidas quando você executa um `show` comando, por exemplo.
 - As SOLICITAÇÕES GET não são registradas por padrão, mas você pode controlar se as solicitações GET enviadas da CLI do ONTAP (`-cli`get), da API do ONTAP (`-ontapi`get) ou da API REST (`-http`get) estão registradas no arquivo.

O ONTAP Registra atividades de gerenciamento `/mroot/etc/log/mlog/audit.log` no arquivo de um nó. Comandos dos três shells para comandos CLI - o `clustershell`, o `nodeshell` e o `systemshell` não interativo (comandos do `systemshell` interativo não são registrados) - assim como os comandos API são registrados aqui. Os logs de auditoria incluem carimbos de data/hora para mostrar se todos os nós de um cluster estão sincronizados com a hora.

O `audit.log` arquivo é enviado pela ferramenta AutoSupport para os destinatários especificados. Você também pode encaminhar o conteúdo de forma segura para destinos externos especificados por você; por exemplo, um Splunk ou um servidor `syslog`.

O `audit.log` arquivo é girado diariamente. A rotação também ocorre quando atinge 100 MB de tamanho, e as 48 cópias anteriores são preservadas (com um total máximo de 49 arquivos). Quando o arquivo de auditoria executa sua rotação diária, nenhuma mensagem EMS é gerada. Se o arquivo de auditoria girar porque seu limite de tamanho de arquivo é excedido, uma mensagem EMS é gerada.

Alterações ao registo de auditoria no ONTAP 9

A partir do ONTAP 9, o `command-history.log` arquivo é substituído pelo `audit.log`, e o `mgwd.log` arquivo não contém mais informações de auditoria. Se você estiver atualizando para o ONTAP 9, revise todos os scripts ou ferramentas que se referem aos arquivos legados e seus conteúdos.

Após a atualização para o ONTAP 9, os arquivos existentes `command-history.log` são preservados. Eles são girados para fora (excluídos) à medida que novos `audit.log` arquivos são girados em (criados).

Ferramentas e scripts que verificam o `command-history.log` arquivo podem continuar funcionando, porque um link de software de `command-history.log` para `audit.log` é criado na atualização. No entanto, ferramentas e scripts que verificam o `mgwd.log` arquivo falharão, porque esse arquivo não contém mais informações de auditoria.

Além disso, os logs de auditoria no ONTAP 9 e posterior não incluem mais as seguintes entradas porque não são consideradas úteis e causam atividade de Registro desnecessária:

- Comandos internos executados pelo ONTAP (ou seja, onde o nome de usuário é root)
- Aliases de comando (separadamente do comando para o qual eles apontam)

A partir do ONTAP 9, você pode transmitir os logs de auditoria de forma segura para destinos externos usando os protocolos TCP e TLS.

Exibir conteúdo do log de auditoria

Você pode exibir o conteúdo dos arquivos do cluster `/mroot/etc/log/mlog/audit.log` usando a CLI do ONTAP, o Gerenciador de sistema ou um navegador da Web.

As entradas do arquivo de log do cluster incluem o seguinte:

Tempo

O carimbo de data/hora da entrada de registo.

Aplicação

A aplicação utilizada para ligar ao cluster. Exemplos de valores possíveis são `internal`, `console`, `ssh`, `http`, `,`, `ontapi`, `snmp`, `rsh`, `,`, `telnet` e `service-processor`.

Utilizador

O nome de utilizador do utilizador remoto.

Estado

O estado atual da solicitação de auditoria, que pode ser `success`, `pending` ou `error`.

Mensagem

Um campo opcional que pode conter erro ou informações adicionais sobre o status de um comando.

Session ID

O Session ID no qual o pedido é recebido. Cada SSH *session* recebe um Session ID, enquanto cada HTTP, ONTAPI ou SNMP *Request* recebe um Session ID exclusivo.

Armazenamento VM

O SVM por meio do qual o usuário se conectou.

Âmbito de aplicação

É exibido `svm` quando a solicitação está em uma VM de armazenamento de dados; caso contrário, exibe `cluster`.

ID do comando

O ID de cada comando recebido em uma sessão CLI. Isso permite correlacionar uma solicitação e uma resposta. As solicitações ZAPI, HTTP e SNMP não têm IDs de comando.

Você pode exibir as entradas de log do cluster a partir da CLI do ONTAP, de um navegador da Web e, começando com ONTAP 9.11.1, do Gerenciador do sistema.

System Manager

- Para exibir o inventário, selecione **Eventos e trabalhos > Logs de auditoria**. Cada coluna tem controles para filtrar, classificar, pesquisar, mostrar e categorias de inventário. Os detalhes do inventário podem ser baixados como uma pasta de trabalho do Excel.
- Para definir filtros, clique no botão **filtro** no canto superior direito e selecione os campos desejados. Você também pode visualizar todos os comandos executados na sessão em que ocorreu uma falha clicando no link Session ID.

CLI

Para exibir entradas de auditoria mescladas de vários nós no cluster, digite `security audit log show <[parameters]>`

Você pode usar o `security audit log show` comando para exibir entradas de auditoria para nós individuais ou mesclados de vários nós no cluster. Você também pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. Consulte a página de manual para obter detalhes.

Navegador da Web


Você pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. ["Saiba mais sobre como acessar os arquivos de log, despejo de memória e MIB de um nó usando um navegador da Web"](#).

Gerenciar as configurações de solicitação DE auditoria

Embora as SOLICITAÇÕES DE CONJUNTO sejam registradas por padrão, as SOLICITAÇÕES DE OBTENÇÃO não são. No entanto, você pode controlar se as solicitações GET enviadas do ONTAP HTML (`-httpget`), da CLI do ONTAP (`-cliget`) ou das APIs do ONTAP (`-ontapiget`) estão registradas no arquivo.

Você pode modificar as configurações de log de auditoria a partir da CLI do ONTAP e, a partir do ONTAP 9.11.1, do Gerenciador do sistema.

System Manager

1. Selecione **Eventos e trabalhos > Registos de auditoria**.
2. Clique  no canto superior direito e escolha as solicitações a serem adicionadas ou removidas.

CLI

- Para especificar que AS SOLICITAÇÕES GET da CLI ou APIs do ONTAP devem ser registradas no log de auditoria (o arquivo audit.log), além das solicitações de conjunto padrão, digite `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Para visualizar as definições atuais, introduza `security audit show`

Consulte as páginas de manual para obter detalhes.

Gerenciar destinos de log de auditoria

Você pode encaminhar o log de auditoria para um máximo de 10 destinos. Por exemplo, você pode encaminhar o log para um servidor Splunk ou syslog para fins de monitoramento, análise ou backup.

Sobre esta tarefa

Para configurar o encaminhamento, você deve fornecer o endereço IP do host syslog ou Splunk, seu número de porta, um protocolo de transmissão e a facilidade syslog para usar nos logs encaminhados. ["Saiba mais sobre as instalações do syslog"](#).

Pode selecionar um dos seguintes valores de transmissão utilizando o `-protocol` parâmetro:

UDP não encriptado

Protocolo de datagrama de usuário sem segurança (padrão)

TCP não criptografado

Protocolo de controlo da transmissão sem segurança

TCP criptografado

Protocolo de controle de transmissão com TLS (Transport Layer Security) e opção **Verify Server** está disponível quando o protocolo criptografado TCP é selecionado.

A porta padrão é 514 para UDP e 6514 para TCP, mas você pode designar qualquer porta que atenda às necessidades de sua rede.

Você pode selecionar um dos seguintes formatos de mensagem usando o `-message-format` comando:

legacy-NetApp




Uma variação do formato RFC-3164 Syslog (formato: <PRIVAL>)

rfc-5424

Formato syslog de acordo com RFC-5424 (formato: <PRIVAL>)

Você pode encaminhar logs de auditoria da CLI do ONTAP e, a partir do ONTAP 9.11,1, do Gerenciador de sistemas.

System Manager

- Para exibir destinos de log de auditoria, selecione **Cluster >Settings**. Uma contagem de destinos de log é mostrada no bloco **Notification Management**. Clique  para mostrar detalhes.
- Para adicionar, modificar ou eliminar destinos de registo de auditoria, selecione **Eventos e trabalhos > Registos de auditoria** e, em seguida, clique em **gerir destinos de auditoria** no canto superior direito do ecrã. Clique  **Add** em ou clique  na coluna **Endereço do host** para editar ou excluir entradas.

CLI

1. Para cada destino para o qual você deseja encaminhar o log de auditoria, especifique o endereço IP de destino ou o nome do host e quaisquer opções de segurança.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

- Se o `cluster log-forwarding create` comando não puder fazer ping no host de destino para verificar a conectividade, o comando falhará com um erro. Embora não seja recomendado, usar o `-force` parâmetro com o comando ignora a verificação de conectividade.
 - Quando você define o `-verify-server` parâmetro como `true`, a identidade do destino de encaminhamento de log é verificada validando seu certificado. Pode definir o valor `true` apenas quando selecionar o `tcp-encrypted` valor no `-protocol` campo.
2. Verifique se os Registros de destino estão corretos usando o `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

Destination Host          Port    Protocol          Verify Syslog
-----
192.168.123.96           514    udp-unencrypted  false  user
192.168.123.98           6514   tcp-encrypted    true   user
2 entries were displayed.
```

Consulte a `cluster log-forwarding create` página de manual para obter detalhes.

Informações sobre direitos autorais

Copyright © 2025 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.