



Gerenciar configurações de auditoria

ONTAP 9

NetApp
January 17, 2025

Índice

- Gerenciar configurações de auditoria 1
 - Rode manualmente os registos de eventos de auditoria 1
 - Ativar e desativar a auditoria em SVMs 1
 - Exibir informações sobre configurações de auditoria 2
 - Comandos para modificar configurações de auditoria 4
 - Excluir uma configuração de auditoria 5
 - Entenda as implicações de reverter o cluster 5

Gerenciar configurações de auditoria

Rode manualmente os registros de eventos de auditoria

Antes de poder visualizar os registros de eventos de auditoria, os registros têm de ser convertidos para formatos legíveis pelo utilizador. Se você quiser exibir os logs de eventos de uma máquina virtual de storage específica (SVM) antes que o ONTAP gire automaticamente o log, você pode girar manualmente os logs de eventos de auditoria em uma SVM.

Passo

1. Gire os logs de eventos de auditoria usando o `vserver audit rotate-log` comando.

```
vserver audit rotate-log -vserver vs1
```

O log de eventos de auditoria é salvo no diretório de log de eventos de auditoria SVM com o formato especificado pela configuração de auditoria (XML ou EVTX) e pode ser visualizado usando o aplicativo apropriado.

Ativar e desativar a auditoria em SVMs

Você pode ativar ou desativar a auditoria em máquinas virtuais de armazenamento (SVMs). Talvez você queira interromper temporariamente a auditoria de arquivos e diretórios desativando a auditoria. Você pode ativar a auditoria a qualquer momento (se houver uma configuração de auditoria).

O que você vai precisar

Antes de habilitar a auditoria na SVM, a configuração de auditoria da SVM já deve existir.

["Crie a configuração de auditoria"](#)

Sobre esta tarefa

A desativação da auditoria não exclui a configuração de auditoria.

Passos

1. Execute o comando apropriado:

Se você quer que a auditoria seja...	Digite o comando...
Ativado	<code>vserver audit enable -vserver vserver_name</code>
Desativado	<code>vserver audit disable -vserver vserver_name</code>

2. Verifique se a auditoria está no estado desejado:

```
vserver audit show -vserver vserver_name
```

Exemplos

O exemplo a seguir permite a auditoria do SVM VS1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
                Auditing state: true
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10
```

O exemplo a seguir desativa a auditoria para SVM VS1:

```
cluster1::> vserver audit disable -vserver vs1

                Vserver: vs1
                Auditing state: false
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10
```

Exibir informações sobre configurações de auditoria

Você pode exibir informações sobre configurações de auditoria. As informações podem ajudá-lo a determinar se a configuração é o que você deseja em vigor para cada SVM. As informações exibidas também permitem verificar se uma configuração de auditoria

está ativada.

Sobre esta tarefa

Você pode exibir informações detalhadas sobre configurações de auditoria em todos os SVMs ou pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Se não especificar nenhum dos parâmetros opcionais, é apresentado o seguinte:

- Nome do SVM ao qual a configuração de auditoria se aplica
- O estado de auditoria, que pode ser `true` ou `false`

Se o estado de auditoria for `true`, a auditoria será ativada. Se o estado de auditoria for `false`, a auditoria será desativada.

- As categorias de eventos a auditar
- O formato do log de auditoria
- O diretório de destino onde o subsistema de auditoria armazena logs de auditoria consolidados e convertidos

Passo

1. Exiba informações sobre a configuração de auditoria usando o `vserver audit show` comando.

Para obter mais informações sobre como usar o comando, consulte as páginas de manual.

Exemplos

O exemplo a seguir exibe um resumo da configuração de auditoria de todos os SVMs:

```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

O exemplo a seguir exibe, em forma de lista, todas as informações de configuração de auditoria para todos os SVMs:

```

cluster1::> vserver audit show -instance

                Vserver: vs1
                Auditing state: true
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 0

```

Comandos para modificar configurações de auditoria

Se você quiser alterar uma configuração de auditoria, você pode modificar a configuração atual a qualquer momento, incluindo modificar o destino do caminho de log e o formato de log, modificar as categorias de eventos a auditar, como salvar automaticamente arquivos de log e especificar o número máximo de arquivos de log a serem salvos.

Se você quiser...	Use este comando...
Modifique o caminho de destino do log	<code>vserver audit modify</code> com o <code>-destination</code> parâmetro
Modifique a categoria de eventos para auditoria	<code>vserver audit modify</code> com o <code>-events</code> parâmetro <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Para auditar eventos de preparação de políticas de acesso central, a opção servidor SMB de controle de acesso dinâmico (DAC) deve estar ativada na máquina virtual de armazenamento (SVM). </div>
Modifique o formato do log	<code>vserver audit modify</code> com o <code>-format</code> parâmetro
Ativar gravações automáticas com base no tamanho do ficheiro de registo interno	<code>vserver audit modify</code> com o <code>-rotate-size</code> parâmetro

Ativar as gravações automáticas com base num intervalo de tempo	<code>vserver audit modify</code> com os <code>-rotate</code> , <code>-schedule-month</code> parâmetros, <code>-rotate</code> , <code>-schedule-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate-schedule-hour</code> e <code>-rotate-schedule-minute</code>
Especificar o número máximo de ficheiros de registo guardados	<code>vserver audit modify</code> com o <code>-rotate-limit</code> parâmetro

Excluir uma configuração de auditoria

Se você não quiser mais auditar eventos de arquivo e diretório na máquina virtual de storage (SVM) e não quiser manter uma configuração de auditoria na SVM, é possível excluir a configuração de auditoria.

Passos

1. Desative a configuração de auditoria:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Excluir a configuração de auditoria:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

Entenda as implicações de reverter o cluster

Se você pretende reverter o cluster, deve estar ciente do processo de reversão que o ONTAP segue quando houver máquinas virtuais de storage (SVMs) habilitadas para auditoria no cluster. Você deve tomar certas ações antes de reverter.

Revertendo para uma versão do ONTAP que não suporte a auditoria de eventos de logon e logoff SMB e eventos de preparação de políticas de acesso central

O suporte para auditoria de eventos de logon e logoff SMB e para eventos de preparação de políticas de acesso central começa com o Clustered Data ONTAP 8.3. Se você estiver revertendo para uma versão do ONTAP que não ofereça suporte a esses tipos de eventos e tiver configurações de auditoria que monitorem esses tipos de eventos, será necessário alterar a configuração de auditoria desses SVMs habilitados para auditoria antes de reverter. Você deve modificar a configuração para que apenas eventos de arquivo operacional sejam auditados.

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.