Eventos de cambio de la interfaz de línea de comandos que se pueden auditar

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/nas-audit/cli-change-events-concept.html on April 16, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Eventos de cambio de la interfaz de línea de comandos que se pueden auditar . . . 1
Eventos de cambio de la CLI que se pueden auditar de información general . . . 1
Gestione el evento de archivos compartidos . . . 2
Gestionar evento de cambio de política de auditoría . . . 3
Gestionar evento de cuenta de usuario . . . 4
Gestionar evento de grupo de seguridad . . . 6
Gestionar evento de cambio de directiva-autorización . . . 7

Eventos de cambio de la interfaz de línea de comandos que se pueden auditar

Eventos de cambio de la CLI que se pueden auditar de información general

ONTAP puede auditar determinados eventos de cambio de CLI, como determinados eventos de uso compartido de SMB, determinados eventos de política de auditoría, determinados eventos de grupo de seguridad local, eventos de grupo de usuarios local y eventos de política de autorización. Comprender qué eventos de cambio se pueden auditar resulta útil al interpretar los resultados de los registros de eventos.

Puede gestionar los eventos de cambio de la CLI de la máquina virtual de almacenamiento (SVM) mediante la rotación manual de los registros de auditoría, la habilitación o la deshabilitación de la auditoría, la visualización de información sobre los eventos de cambio de auditoría, la modificación de los eventos de cambio de auditoría y la eliminación de eventos de cambio de auditoría.

Como administrador, si ejecuta cualquier comando para cambiar la configuración relacionada con los eventos de recurso compartido de SMB, grupo de usuarios local, grupo de seguridad local, política de autorización y política de auditoría, se genera un registro y se auditan el evento correspondiente:

Categoría de auditoría	Eventos	ID de evento	Ejecute este comando…
Auditoría de Mhost	cambio de políticas	[4719] Configuración de auditoría modificada	`vserver audit disable
enable	modify`	recurso compartido de archivos	[5142] se ha añadido un recurso compartido de red
`vserver cifs share create`	[5143] se ha modificado el recurso compartido de red	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] recurso compartido de red eliminado	`vserver cifs share delete`
Auditoría	cuenta de usuario	[4720] Usuario local creado	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] Usuario local activado	`vserver cifs users-and-groups local-user create	modify`	[4724] restablecimiento de contraseña de usuario local

`vserver cifs users-and-groups local-user set-password`	[4725] Usuario local desactivado	`vserver cifs users-and-groups local-user create	modify`
[4726] Usuario local eliminado	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] Cambio de usuario local	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] Cambiar nombre de usuario local	`vserver cifs users-and-groups local-user rename`	grupo de seguridad	[4731] Grupo de seguridad local creado
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Grupo de seguridad local eliminado	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Grupo de seguridad local modificado
`vserver cifs users-and-groups local-group rename`	modify` `vserver services name-service unix-group modify`	[4732] Usuario agregado al grupo local	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] el usuario ha eliminado del grupo local	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	autorización-cambio de política	[4704] Derechos de usuario asignados
`vserver cifs users-and-groups privilege add-privilege`	[4705] Derechos de usuario eliminados	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Gestione el evento de archivos compartidos

Cuando se configura un evento de recurso compartido de archivos para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría. Los eventos de uso compartido de archivos se generan cuando se modifica el

recurso compartido de red de SMB mediante `vserver cifs share` comandos relacionados.

Los eventos de uso compartido de archivos con los id de evento 5142, 5143 y 5144 se generan cuando se añade, se modifica o se elimina un recurso compartido de red de SMB para la SVM. La configuración de recursos compartidos de red de SMB se modifica con el `cifs share access control create|modify|delete` comandos.

En el siguiente ejemplo, se muestra un evento de recurso compartido de archivos con el ID 5143 que se genera cuando se crea un objeto compartido denominado 'audit_dest':

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Gestionar evento de cambio de política de auditoría

Cuando se configura un evento de cambio de política de auditoría para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría. Los eventos de cambio de directiva de auditoría se generan cuando se modifica una directiva de auditoría mediante `vserver audit` comandos relacionados.

El evento audit-policy-change con el event-id 4719 se genera siempre que se deshabilita, habilita o modifica una directiva de auditoría y ayuda a identificar cuándo un usuario intenta deshabilitar la auditoría para cubrir las pistas. Se configura de forma predeterminada y requiere que se deshabilite los privilegios de diagnóstico.

En el siguiente ejemplo, se muestra un evento de cambio de política de auditoría con el ID 4719 generado cuando se deshabilita una auditoría:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Gestionar evento de cuenta de usuario

Cuando se configura un evento de cuenta de usuario para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de cuenta de usuario con los id de evento 4720, 4722, 4724, 4725, 4726, 4738, y 4781 se generan cuando se crea o se elimina un usuario local de SMB o NFS del sistema, se habilita la cuenta de usuario local, se deshabilita o se modifica, y se restablece o se cambia la contraseña de usuario local de SMB. Los eventos de la cuenta de usuario se generan cuando se modifica una cuenta de usuario mediante `vserver cifs users-and-groups <local user>` y.. `vserver services name-service <unix user>` comandos.

En el siguiente ejemplo, se muestra un evento de cuenta de usuario con el ID 4720 generado cuando se crea un usuario de SMB local:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

En el siguiente ejemplo se muestra un evento de cuenta de usuario con el ID 4781 generado, cuando se cambia el nombre de usuario de SMB local creado en el ejemplo anterior:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Gestionar evento de grupo de seguridad

Cuando se configura un evento de grupo de seguridad para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de los grupos de seguridad con los id de evento 4731, 4732, 4733, 4734 y 4735 se generan cuando se crea o elimina un grupo SMB o NFS local del sistema y se agrega o se elimina el usuario local del grupo. Los eventos de grupo de seguridad se generan cuando se modifica una cuenta de usuario mediante `vserver cifs users-and-groups <local-group>` y.. `vserver services name-service <unix-group>` comandos.

En el ejemplo siguiente se muestra un evento de grupo de seguridad con el ID 4731 generado cuando se crea un grupo de seguridad local UNIX:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Gestionar evento de cambio de directiva-autorización

Cuando se configura un evento de cambio de política de autorización para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de cambio de política de autorización con los id de evento 4704 y 4705 se generan cada vez que se otorgan o revocan los derechos de autorización para un usuario de SMB y un grupo de SMB. Los eventos de cambio de directiva-autorización se generan cuando se asignan o revocan los derechos de autorización utilizando `vserver cifs users-and-groups privilege` comandos relacionados.

En el ejemplo siguiente se muestra un evento de directiva de autorización con el ID 4704 generado cuando se asignan los derechos de autorización para un grupo de usuarios de SMB:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.