Eventos de mudança de CLI que podem ser auditados

ONTAP 9

NetApp
January 17, 2025

Índice

Eventos de mudança de CLI que podem ser auditados

CLI alterar eventos que podem ser auditados visão geral

O ONTAP pode auditar certos eventos de mudança de CLI, incluindo certos eventos de compartilhamento de SMB, certos eventos de política de auditoria, determinados eventos de grupo de segurança local, eventos de grupo de usuários locais e eventos de política de autorização. Entender quais eventos de mudança podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Você pode gerenciar eventos de alteração da CLI de auditoria de máquina virtual de storage (SVM) girando manualmente os logs de auditoria, habilitando ou desativando a auditoria, exibindo informações sobre auditoria de eventos de alterações, modificando eventos de auditoria de alterações e excluindo eventos de alteração de auditoria.

Como administrador, se você executar qualquer comando para alterar a configuração relacionada aos eventos SMB-share, grupo de usuários local, grupo de segurança local, política de autorização e política de auditoria, um Registro será gerado e o evento correspondente será auditado:

Categoria Auditoria	Eventos	IDs de eventos	Execute este comando…
Auditoria Mhost	mudança de política	[4719] Configuração de auditoria alterada	`vserver audit disable
enable	modify`	compartilhamento de arquivos	[5142] a partilha de rede foi adicionada
`vserver cifs share create`	[5143] a partilha de rede foi modificada	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] partilha de rede eliminada	`vserver cifs share delete`
Auditoria	conta de utilizador	[4720] usuário local criado	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] utilizador local ativado	`vserver cifs users-and-groups local-user create	modify`	[4724] Reposição da palavra-passe do utilizador local

`vserver cifs users-and-groups local-user set-password`	[4725] Utilizador local desativado	`vserver cifs users-and-groups local-user create	modify`
[4726] utilizador local eliminado	`vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete`	[4738] alteração do utilizador local	`vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify`
[4781] Renomear utilizador local	`vserver cifs users-and-groups local-user rename`	grupo de segurança	[4731] Grupo de Segurança local criado
`vserver cifs users-and-groups local-group create vserver services name-service unix-group create`	[4734] Grupo de Segurança local eliminado	`vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete`	[4735] Grupo de Segurança local modificado
`vserver cifs users-and-groups local-group rename`	modify` `vserver services name-service unix-group modify`	[4732] Usuário adicionado ao Grupo local	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] Usuário removido do Grupo local	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	autorização-política-alteração	[4704] Direitos de Usuário atribuídos
`vserver cifs users-and-groups privilege add-privilege`	[4705] Direitos de usuário removidos	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Gerenciar evento de compartilhamento de arquivos

Quando um evento de compartilhamento de arquivos é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de compartilhamento de arquivos são gerados quando o compartilhamento

de rede SMB é modificado usando `vserver cifs share` comandos relacionados.

Os eventos de compartilhamento de arquivos com as ids de eventos 5142, 5143 e 5144 são gerados quando um compartilhamento de rede SMB é adicionado, modificado ou excluído para o SVM. A configuração de compartilhamento de rede SMB é modificada usando os `cifs share access control create|modify|delete` comandos.

O exemplo a seguir exibe um evento de compartilhamento de arquivos com a ID 5143 é gerado, quando um objeto de compartilhamento chamado 'audit_dest' é criado:

```
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)
```

Gerenciar evento de mudança de política de auditoria

Quando um evento de alteração de política de auditoria é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de alteração de política de auditoria são gerados quando uma diretiva de auditoria é modificada usando `vserver audit` comandos relacionados.

O evento de alteração de política de auditoria com o ID de evento 4719 é gerado sempre que uma política de auditoria é desativada, ativada ou modificada e ajuda a identificar quando um usuário tenta desativar a auditoria para cobrir os trajetos. Ele é configurado por padrão e requer privilégio de diagnóstico para ser desativado.

O exemplo a seguir exibe um evento de mudança de diretiva de auditoria com a ID 4719 gerada, quando uma auditoria é desativada:

```
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
```

Gerenciar evento de conta de usuário

Quando um evento de conta de usuário é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos da conta de usuário com ids de eventos 4720, 4722, 4724, 4725, 4726, 4738 e 4781 são gerados quando um usuário SMB ou NFS local é criado ou excluído do sistema, a conta de usuário local é ativada, desativada ou modificada e a senha de usuário SMB local é redefinida ou alterada. Os eventos de conta de usuário são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local user>` comandos e `vserver services name-service <unix user>`.

O exemplo a seguir exibe um evento de conta de usuário com a ID 4720 gerada, quando um usuário SMB local é criado:

```
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 ~
```

O exemplo a seguir exibe um evento de conta de usuário com a ID 4781 gerada, quando o usuário local SMB criado no exemplo anterior é renomeado:

```
 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 ~
```

Gerenciar evento do grupo de segurança

Quando um evento de grupo de segurança é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos de grupo de segurança com ids de eventos 4731, 4732, 4733, 4734 e 4735 são gerados quando um grupo SMB ou NFS local é criado ou excluído do sistema e o usuário local é adicionado ou removido do grupo. Os eventos de grupo de segurança são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local-group>` comandos e `vserver services name-service <unix-group>`.

O exemplo a seguir exibe um evento de grupo de segurança com a ID 4731 gerada, quando um grupo de segurança UNIX local é criado:

```
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 ~
```

Gerenciar evento de alteração de política de autorização

Quando o evento de alteração de política de autorização é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos autorização-política-mudança com os ids de evento 4704 e 4705 são gerados sempre que os direitos de autorização são concedidos ou revogados para um usuário SMB e grupo SMB. Os eventos autorização-política-mudança são gerados quando os direitos de autorização são atribuídos ou revogados usando `vserver cifs users-and-groups privilege` comandos relacionados.

O exemplo a seguir exibe um evento de política de autorização com a ID 4704 gerada, quando os direitos de autorização para um grupo de usuários SMB são atribuídos:

```
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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais