CLI modifica gli eventi che possono essere verificati

ONTAP 9

NetApp
April 24, 2024

Sommario

CLI modifica gli eventi che possono essere verificati . . . 1
Panoramica degli eventi di cambiamento CLI che possono essere verificati . . . 1
Gestire l’evento di condivisione file . . . 2
Gestire l’evento audit-policy-change . . . 3
Gestire l’evento dell’account utente . . . 4
Gestire gli eventi del gruppo di sicurezza . . . 6
Gestire l’evento Authorization-policy-change . . . 7

CLI modifica gli eventi che possono essere verificati

Panoramica degli eventi di cambiamento CLI che possono essere verificati

ONTAP è in grado di controllare alcuni eventi di modifica dell'interfaccia CLI, tra cui determinati eventi di condivisione SMB, determinati eventi dei criteri di controllo, determinati eventi dei gruppi di protezione locali, eventi dei gruppi di utenti locali ed eventi dei criteri di autorizzazione. La comprensione degli eventi di modifica che è possibile verificare è utile quando si interpretano i risultati dei registri degli eventi.

È possibile gestire la macchina virtuale dello storage (SVM) per il controllo degli eventi di modifica della CLI ruotando manualmente i registri di controllo, attivando o disattivando il controllo, visualizzando le informazioni relative al controllo degli eventi di modifica, modificando gli eventi di modifica del controllo ed eliminando gli eventi di modifica del controllo.

In qualità di amministratore, se si esegue un comando per modificare la configurazione relativa agli eventi SMB-share, User-group locale, Security-group locale, Authorization-policy e audit-policy, viene generato un record e viene verificato l'evento corrispondente:

Categoria di controllo	Eventi	ID evento	Eseguire questo comando…
Mhost Auditing	cambiamento di policy	[4719] Configurazione dell'audit modificata	`vserver audit disable
enable	modify`	condivisione file	[5142] è stata aggiunta la condivisione di rete
`vserver cifs share create`	[5143] la condivisione di rete è stata modificata	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] condivisione di rete eliminata	`vserver cifs share delete`
Controllo	account utente	[4720] utente locale creato	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] utente locale abilitato	`vserver cifs users-and-groups local-user create	modify`	[4724] reimpostazione della password utente locale

`vserver cifs users-and-groups local-user set-password`	[4725] utente locale disattivato	`vserver cifs users-and-groups local-user create	modify`
[4726] utente locale cancellato	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] Modifica utente locale	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] Rinomina utente locale	`vserver cifs users-and-groups local-user rename`	security-group	[4731] Gruppo di sicurezza locale creato
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Gruppo di sicurezza locale cancellato	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Gruppo di sicurezza locale modificato
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] utente aggiunto al gruppo locale	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] utente rimosso dal gruppo locale	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	authorization-policy-change	[4704] diritti utente assegnati
`vserver cifs users-and-groups privilege add-privilege`	[4705] diritti utente rimossi	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Gestire l’evento di condivisione file

Quando viene configurato un evento di condivisione file per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi di condivisione file vengono generati quando la condivisione di rete SMB viene modificata

utilizzando `vserver cifs share` comandi correlati.

Gli eventi di file-share con gli id evento 5142, 5143 e 5144 vengono generati quando una condivisione di rete SMB viene aggiunta, modificata o eliminata per la SVM. La configurazione della condivisione di rete SMB viene modificata utilizzando `cifs share access control create|modify|delete` comandi.

Nell'esempio seguente viene visualizzato un evento di condivisione file con ID 5143, quando viene creato un oggetto di condivisione denominato '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)
```

Gestire l'evento audit-policy-change

Quando viene configurato un evento audit-policy-change per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi audit-policy-change vengono generati quando un criterio di audit viene modificato utilizzando `vserver audit` comandi correlati.

L'evento audit-policy-change con l'id evento 4719 viene generato ogni volta che un criterio di audit viene disattivato, attivato o modificato e aiuta a identificare quando un utente tenta di disattivare il controllo per coprire le tracce. È configurato per impostazione predefinita e richiede il privilegio di diagnostica per la disattivazione.

Nell'esempio riportato di seguito viene visualizzato un evento di modifica della policy di audit con l'ID 4719 generato, quando un audit viene disattivato:

```
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
```

Gestire l’evento dell’account utente

Quando viene configurato un evento account utente per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi dell’account utente con id evento 4720, 4722, 4724, 4725, 4726, 4738 e 4781 vengono generati quando un utente SMB o NFS locale viene creato o cancellato dal sistema, l’account utente locale viene attivato, disattivato o modificato e la password utente SMB locale viene reimpostata o modificata. Gli eventi dell’account utente vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local user>` e. `vserver services name-service <unix user>` comandi.

Nell’esempio seguente viene visualizzato un evento dell’account utente con l’ID 4720 generato, quando viene creato un utente SMB locale:

```
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 ~
```

Nell’esempio seguente viene visualizzato un evento dell’account utente con l’ID 4781 generato, quando l’utente SMB locale creato nell’esempio precedente viene rinominato:

```
 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 ~
```

Gestire gli eventi del gruppo di sicurezza

Quando viene configurato un evento di gruppo di sicurezza per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi del gruppo di sicurezza con id evento 4731, 4732, 4733, 4734 e 4735 vengono generati quando un gruppo SMB o NFS locale viene creato o cancellato dal sistema e l'utente locale viene aggiunto o rimosso dal gruppo. Gli eventi-gruppo-sicurezza vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local-group>` e. `vserver services name-service <unix-group>` comandi.

Nell'esempio seguente viene visualizzato un evento del gruppo di protezione con l'ID 4731 generato quando viene creato un gruppo di protezione UNIX locale:

```
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 ~
```

Gestire l'evento Authorization-policy-change

Quando l'evento Authorization-policy-change viene configurato per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi Authorization-policy-change con ID evento 4704 e 4705 vengono generati ogni volta che vengono concessi o revocati i diritti di autorizzazione per un utente SMB e un gruppo SMB. Gli eventi Authorization-policy-change vengono generati quando i diritti di autorizzazione vengono assegnati o revocati utilizzando `vserver cifs users-and-groups privilege` comandi correlati.

Nell'esempio seguente viene visualizzato un evento del criterio di autorizzazione con l'ID 4704 generato, quando vengono assegnati i diritti di autorizzazione per un gruppo di utenti 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
```