Les événements de modification de l'interface de ligne de commande peuvent être audités

ONTAP 9

NetApp
April 24, 2024

Sommaire

Les événements de modification de l’interface de ligne de commande peuvent être audités

Les événements de modification de la CLI pouvant être audités

ONTAP peut auditer certains événements de modification de l’interface de ligne de commandes, notamment certains événements de partage SMB, certains événements de stratégie d’audit, certains événements de groupe de sécurité local, des événements de groupe d’utilisateurs locaux et des événements de politique d’autorisation. Il est utile de savoir quels événements de modification peuvent être audités lors de l’interprétation des résultats des journaux d’événements.

Vous pouvez gérer les événements de modification de l’interface de ligne de commande d’audit des machines virtuelles de stockage (SVM) en faisant tourner manuellement les journaux d’audit, en activant ou désactivant l’audit, en affichant des informations sur l’audit des événements de modification, en modifiant l’audit des événements et en supprimant les événements d’audit des modifications.

En tant qu’administrateur, si vous exécutez une commande pour modifier la configuration relative aux événements SMB-share, local user-group, local Security-group, autorisation-policy et audit-policy, un enregistrement génère et l’événement correspondant est vérifié :

Catégorie d’audit	Événements	ID d’événement	Exécuter cette commande…
Audit Mhost	modification de règles	[4719] Configuration d’audit modifiée	`vserver audit disable
enable	modify`	partage de fichiers	[5142] le partage réseau a été ajouté
`vserver cifs share create`	[5143] le partage réseau a été modifié	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] partage réseau supprimé	`vserver cifs share delete`
Audit	compte utilisateur	[4720] utilisateur local créé	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`

[4722] utilisateur local activé	`vserver cifs users-and-groups local-user create	modify`	[4724] Réinitialisation du mot de passe de l'utilisateur local
`vserver cifs users-and-groups local-user set-password`	[4725] utilisateur local désactivé	`vserver cifs users-and-groups local-user create	modify`
[4726] utilisateur local supprimé	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] modification de l'utilisateur local	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] utilisateur local Renommer	`vserver cifs users-and-groups local-user rename`	groupe-de-sécurité	[4731] Groupe de sécurité local créé
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Groupe de sécurité local supprimé	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Groupe de sécurité local modifié
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] utilisateur ajouté au groupe local	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] utilisateur supprimé du groupe local	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	autorisation-stratégie-modification	[4704] droits d'utilisateur attribués
`vserver cifs users-and-groups privilege add-privilege`	[4705] droits d'utilisateur supprimés	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Gérer un événement de partage de fichiers

Lorsqu'un événement de partage de fichiers est configuré pour un SVM (Storage Virtual machine) et qu'un audit est activé, des événements d'audit sont générés. Les événements de partage de fichiers sont générés lorsque le partage réseau SMB est modifié à l'aide de `vserver cifs share` commandes associées

Les événements de partage de fichiers avec les id-événements 5142, 5143 et 5144 sont générés lorsqu'un partage réseau SMB est ajouté, modifié ou supprimé pour la SVM. La configuration du partage réseau SMB est modifiée à l'aide du `cifs share access control create|modify|delete` commandes.

L'exemple suivant affiche un événement de partage de fichiers avec l'ID 5143 est généré lorsqu'un objet de partage appelé « audit_dest » est créé :

```
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)
```

Gestion de l'événement audit-policy-change

Lorsqu'un événement d'audit-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés. Les événements audit-règle-modification sont générés lorsqu'une règle d'audit est modifiée à l'aide de `vserver audit` commandes associées

L'événement audit-policy-change avec l'ID-événement 4719 est généré chaque fois qu'une stratégie d'audit est désactivée, activée ou modifiée et aide à identifier quand un utilisateur tente de désactiver l'audit pour couvrir les pistes. Il est configuré par défaut et requiert un privilège de diagnostic pour être désactivé.

L'exemple suivant montre un événement de modification de règle d'audit avec l'ID 4719 généré lorsqu'un audit est désactivé :

```
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
```

Gérer un événement de compte utilisateur

Lorsqu'un événement de compte utilisateur est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du compte utilisateur avec les id-événements 4720, 4722, 4724, 4725, 4726, 4738 et 4781 sont générés lorsqu'un utilisateur SMB ou NFS local est créé ou supprimé du système, le compte d'utilisateur local est activé, désactivé ou modifié et le mot de passe de l'utilisateur SMB local est réinitialisé ou modifié. Les événements du compte utilisateur sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vserver cifs users-and-groups <local user>` et `vserver services name-service <unix user>` commandes.

L'exemple suivant montre un événement de compte d'utilisateur avec l'ID 4720 généré lors de la création d'un utilisateur 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 ~
```

L’exemple suivant affiche un événement de compte utilisateur avec l’ID 4781 généré lorsque l’utilisateur SMB local créé dans l’exemple précédent est renommé :

```
 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 ~
```

Gérer l'événement de groupe de sécurité

Lorsqu'un événement de groupe de sécurité est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du groupe de sécurité avec les id-événements 4731, 4732, 4733, 4734 et 4735 sont générés lorsqu'un groupe SMB ou NFS local est créé ou supprimé du système et que l'utilisateur local est ajouté ou supprimé du groupe. Les événements groupe-sécurité sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vserver cifs users-and-groups <local-group>` et `vserver services name-service <unix-group>` commandes.

L'exemple suivant montre un événement de groupe de sécurité avec l'ID 4731 généré lors de la création d'un groupe de sécurité UNIX local :

```
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 ~
```

Gérer l'événement autorisation-stratégie-modification

Lorsque l'événement autorisation-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements autorisation-policy-change avec les id-événements 4704 et 4705 sont générés chaque fois que les droits d'autorisation sont accordés ou révoqués pour un utilisateur SMB et un groupe SMB. Les événements autorisation-stratégie-modification sont générés lorsque les droits d'autorisation sont affectés ou révoqués à l'aide de `vserver cifs users-and-groups privilege` commandes associées

L'exemple suivant affiche un événement de stratégie d'autorisation avec l'ID 4704 généré lorsque les droits d'autorisation d'un groupe d'utilisateurs SMB sont affectés :

```
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
```