



Gruppenrichtlinienobjekte auf SMB-Server anwenden

ONTAP 9

NetApp
April 24, 2024

Inhalt

Gruppenrichtlinienobjekte auf SMB-Server anwenden	1
Gruppenrichtlinienobjekte auf SMB-Server anwenden – Übersicht	1
Unterstützte Gruppenrichtlinienobjekte	1
Anforderungen für die Verwendung von Gruppenrichtlinienobjekten mit Ihrem SMB-Server	7
Aktivieren oder deaktivieren Sie die GPO-Unterstützung auf einem CIFS-Server	7
Aktualisierung der Gruppenrichtlinienobjekte auf dem SMB-Server	8
Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server	9
Zeigt Informationen zu GPO-Konfigurationen an	9
Detaillierte Informationen zu Gruppenrichtlinienobjekten anzeigen	14
Informationen zu zentralen Zugriffsrichtlinien anzeigen	16
Informationen zu zentralen Zugriffsrichtlinien anzeigen	18

Gruppenrichtlinienobjekte auf SMB-Server anwenden

Gruppenrichtlinienobjekte auf SMB-Server anwenden – Übersicht

Ihr SMB-Server unterstützt Gruppenrichtlinienobjekte (Group Policy Objects, GPOs), einen Satz von Regeln, die als Gruppenrichtlinienattribute_ bezeichnet werden, die für Computer in einer Active Directory-Umgebung gelten. Mit Gruppenrichtlinienobjekten lassen sich Einstellungen aller Storage Virtual Machines (SVMs) im Cluster, die zur selben Active Directory-Domäne gehören, zentral managen.

Wenn Gruppenrichtlinienobjekte auf Ihrem SMB-Server aktiviert sind, sendet ONTAP LDAP-Anfragen an den Active Directory-Server und fordert Gruppenrichtlinieninformationen an. Wenn GPO-Definitionen vorhanden sind, die auf Ihren SMB-Server anwendbar sind, gibt der Active Directory-Server die folgenden GPO-Informationen zurück:

- GPO-Name
- Aktuelle GPO-Version
- Position der GPO-Definition
- Listen von UUIDs (Universally Unique Identifier) für GPO-Richtliniensätze

Verwandte Informationen

[Sichern des Dateizugriffs mithilfe von Dynamic Access Control \(DAC\)](#)

["SMB- und NFS-Auditing und Sicherheits-Tracing"](#)

Unterstützte Gruppenrichtlinienobjekte

Obwohl nicht alle Gruppenrichtlinienobjekte für Ihre CIFS-fähigen Storage Virtual Machines (SVMs) gelten, können SVMs die entsprechenden Gruppenrichtlinienobjekte erkennen und verarbeiten.

Die folgenden Gruppenrichtlinienobjekte werden derzeit auf SVMs unterstützt:

- Konfigurationseinstellungen für erweiterte Prüfungsrichtlinien:

Objektzugriff: Zentrale Zugriffsrichtlinien-Staging

Gibt die Art der zu prüfenden Ereignisse für die Durchführung der CAP-Strategie (Central Access Policy) an, einschließlich der folgenden Einstellungen:

- Nicht prüfen
- Nur erfolgreiche Ereignisse werden geprüft
- Nur Fehlerereignisse werden geprüft
- Prüfung von Erfolg- und Fehlerereignissen



Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

Verwenden Sie die `Audit Central Access Policy Staging` Einstellung im `Advanced Audit Policy Configuration/Audit Policies/Object Access GPO`.



Um Gruppenrichtlinieneinstellungen für die erweiterte Audit-Richtlinien zu verwenden, muss für die CIFS-fähige SVM, auf die Sie diese Einstellung anwenden möchten, eine Prüfung konfiguriert werden. Wenn keine Prüfung für die SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

- Registrierungseinstellungen:

- Aktualisierungsintervall für Gruppenrichtlinien für CIFS-fähige SVM

Verwenden Sie die `Registry` GPO.

- Gruppen-Policy aktualisieren zufälligen Offset

Verwenden Sie die `Registry` GPO.

- Hash-Publikation für BranchCache

Das Gruppenrichtlinienobjekt Hash Publication for BranchCache entspricht der Betriebsart BranchCache. Folgende drei unterstützte Betriebsmodi werden unterstützt:

- Pro Aktie
- Nur Freigaben
- Die Einstellung wird mithilfe des deaktiviert `Registry` GPO.

- Unterstützung der Hash-Version für BranchCache

Die folgenden drei Hash-Versionseinstellungen werden unterstützt:

- BranchCache Version 1
- BranchCache Version 2
- BranchCache Versionen 1 und 2 werden mithilfe der festgelegt `Registry` GPO.



Um Gruppenrichtlinieneinstellungen von BranchCache zu verwenden, muss BranchCache auf der CIFS-fähigen SVM konfiguriert werden, auf die Sie diese Einstellung anwenden möchten. Wenn BranchCache nicht auf der SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und werden verworfen.

- Sicherheitseinstellungen

- Audit-Richtlinie und Ereignisprotokoll

- Anmeldeereignisse überwachen

Gibt den Typ der zu prüfenden Anmeldeereignisse an, einschließlich der folgenden Einstellungen:

- Nicht prüfen
- Nur erfolgreiche Ereignisse werden geprüft
- Prüfung von Fehlerereignissen
- Prüfung von Erfolg- und Fehlerereignissen, die mithilfe des festgelegt wurden `Audit logon events` Einstellung im `Local Policies/Audit Policy GPO`.



Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

▪ Audit-Objektzugriff

Gibt den Typ des zu prüfenden Objektzugriffs an, einschließlich der folgenden Einstellungen:

- Nicht prüfen
- Nur erfolgreiche Ereignisse werden geprüft
- Prüfung von Fehlerereignissen
- Prüfung von Erfolg- und Fehlerereignissen, die mithilfe des festgelegt wurden `Audit object access` Einstellung im `Local Policies/Audit Policy GPO`.



Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

▪ Methode zur Protokollaufbewahrung

Gibt die Aufbewahrungsmethode für das Prüfprotokoll an, einschließlich der folgenden Einstellungen:

- Überschreiben Sie das Ereignisprotokoll, wenn die Größe der Protokolldatei die maximale Protokollgröße überschreitet
- Überschreiben Sie das mit dem eingestellte Ereignisprotokoll nicht (Protokoll manuell löschen) `Retention method for security log` Einstellung im `Event Log GPO`.

▪ Maximale Protokollgröße

Gibt die maximale Größe des Prüfprotokolls an.

Verwenden Sie die `Maximum security log size` Einstellung im `Event Log GPO`.



Um Richtlinien und GPO-Einstellungen für das Ereignisprotokoll zu verwenden, muss eine Prüfung auf der CIFS-fähigen SVM, auf die diese Einstellung angewendet werden soll, konfiguriert werden. Wenn keine Prüfung für die SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

◦ Dateisystemsicherheit

Gibt eine Liste von Dateien oder Verzeichnissen an, auf denen Dateisicherheit über ein Gruppenrichtlinienobjekt angewendet wird.

Verwenden Sie die `File System GPO`.



Der Volume-Pfad, zu dem das Gruppenrichtlinienobjekt für die Dateisystemsicherheit konfiguriert ist, muss in der SVM vorhanden sein.

- Kerberos-Richtlinie

- Maximale Taktabweichung

Gibt die maximale Toleranz in Minuten für die Synchronisierung der Computeruhr an.

Verwenden Sie die `Maximum tolerance for computer clock synchronization` Einstellung im `Account Policies/Kerberos Policy GPO`.

- Maximales Ticketalter

Gibt die maximale Lebensdauer in Stunden für das Benutzerticket an.

Verwenden Sie die `Maximum lifetime for user ticket` Einstellung im `Account Policies/Kerberos Policy GPO`.

- Maximales Alter der Ticketverlängerung

Gibt die maximale Lebensdauer in Tagen für die Verlängerung von Benutzertickets an.

Verwenden Sie die `Maximum lifetime for user ticket renewal` Einstellung im `Account Policies/Kerberos Policy GPO`.

- Zuweisung von Benutzerrechten (Berechtigungsrechte)

- Verantwortung

Gibt die Liste der Benutzer und Gruppen an, die das Recht haben, die Verantwortung für jedes seecable Objekt zu übernehmen.

Verwenden Sie die `Take ownership of files or other objects` Einstellung im `Local Policies/User Rights Assignment GPO`.

- Sicherheitsberechtigungen

Gibt die Liste der Benutzer und Gruppen an, die Überwachungsoptionen für den Objektzugriff einzelner Ressourcen wie Dateien, Ordner und Active Directory-Objekte festlegen können.

Verwenden Sie die `Manage auditing and security log` Einstellung im `Local Policies/User Rights Assignment GPO`.

- Berechtigung zur Benachrichtigung ändern (Bypass Traverse-Überprüfung)

Gibt die Liste der Benutzer und Gruppen an, die Verzeichnisbäume durchlaufen können, auch wenn Benutzer und Gruppen möglicherweise keine Berechtigungen im durchlaufenen Verzeichnis besitzen.

Die gleiche Berechtigung ist erforderlich, damit Benutzer Benachrichtigungen über Änderungen an Dateien und Verzeichnissen erhalten. Verwenden Sie die `Bypass traverse checking` Einstellung im `Local Policies/User Rights Assignment GPO`.

- Registrierungswerte

- Erforderliche Signatureinstellung

Gibt an, ob die erforderliche SMB-Signatur aktiviert oder deaktiviert ist.

Verwenden Sie die `Microsoft network server: Digitally sign communications (always)` Einstellung im Security Options GPO.

- Anonym beschränken

Legt fest, welche Einschränkungen für anonyme Benutzer gelten und enthält die folgenden drei GPO-Einstellungen:

- Keine Aufzählung von Security Account Manager (SAM)-Konten:

Durch diese Sicherheitseinstellung wird festgelegt, welche zusätzlichen Berechtigungen für anonyme Verbindungen zum Computer gewährt werden. Diese Option wird angezeigt als `no-enumeration` Wenn sie in ONTAP aktiviert ist.

Verwenden Sie die `Network access: Do not allow anonymous enumeration of SAM accounts` Einstellung im Local Policies/Security Options GPO.

- Keine Aufzählung von SAM-Konten und -Freigaben

Mit dieser Sicherheitseinstellung wird festgelegt, ob eine anonyme Aufzählung von SAM-Konten und -Freigaben zulässig ist. Diese Option wird angezeigt als `no-enumeration` Wenn sie in ONTAP aktiviert ist.

Verwenden Sie die `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Einstellung im Local Policies/Security Options GPO.

- Anonymen Zugriff auf Freigaben und benannte Pipes beschränken

Diese Sicherheitseinstellung schränkt den anonymen Zugriff auf Freigaben und Leitungen ein. Diese Option wird angezeigt als `no-access` Wenn sie in ONTAP aktiviert ist.

Verwenden Sie die `Network access: Restrict anonymous access to Named Pipes and Shares` Einstellung im Local Policies/Security Options GPO.

Wenn Informationen über definierte und angewendete Gruppenrichtlinien angezeigt werden, wird das angezeigt `Resultant restriction for anonymous user` Das Ausgabefeld enthält Informationen über die sich daraus ergebende Einschränkung der drei anonymen GPO-Einstellungen beschränken. Die möglichen daraus resultierenden Einschränkungen sind wie folgt:

- `no-access`

Dem anonymen Benutzer wird der Zugriff auf die angegebenen Freigaben und Named Pipes verweigert, und die Aufzählung von SAM-Konten und -Freigaben kann nicht verwendet werden. Diese resultierende Einschränkung wird angezeigt, wenn der `Network access: Restrict anonymous access to Named Pipes and Shares` GPO ist aktiviert.

- `no-enumeration`

Der anonyme Benutzer hat Zugriff auf die angegebenen Freigaben und Named Pipes, kann aber keine Aufzählung von SAM-Konten und -Freigaben verwenden. Diese resultierende Einschränkung wird angezeigt, wenn beide der folgenden Bedingungen erfüllt sind:

- Der Network access: Restrict anonymous access to Named Pipes and Shares GPO ist deaktiviert.
- Entweder im Network access: Do not allow anonymous enumeration of SAM accounts Oder im Network access: Do not allow anonymous enumeration of SAM accounts and shares Gruppenrichtlinienobjekte sind aktiviert.

° no-restriction

Der anonyme Benutzer hat vollen Zugriff und kann Enumeration verwenden. Diese resultierende Einschränkung wird angezeigt, wenn beide der folgenden Bedingungen erfüllt sind:

- Der Network access: Restrict anonymous access to Named Pipes and Shares GPO ist deaktiviert.
- Beide Network access: Do not allow anonymous enumeration of SAM accounts Und Network access: Do not allow anonymous enumeration of SAM accounts and shares Gruppenrichtlinienobjekte sind deaktiviert.

- Eingeschränkte Gruppen

Sie können eingeschränkte Gruppen so konfigurieren, dass sie die Mitgliedschaft von integrierten oder benutzerdefinierten Gruppen zentral verwalten können. Wenn Sie eine eingeschränkte Gruppe über eine Gruppenrichtlinie anwenden, wird die Mitgliedschaft einer lokalen CIFS-Server-Gruppe automatisch so eingestellt, dass sie den in der angewendeten Gruppenrichtlinie festgelegten Mitgliedschaftslisteneinstellungen entspricht.

Verwenden Sie die Restricted Groups GPO.

- Einstellungen für zentrale Zugriffsrichtlinien

Gibt eine Liste der zentralen Zugriffsrichtlinien an. Zentrale Zugriffsrichtlinien und die zugehörigen zentralen Zugriffsrichtlinien bestimmen die Zugriffsberechtigungen für mehrere Dateien auf der SVM.

Verwandte Informationen

[Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server](#)

[Sichern des Dateizugriffs mithilfe von Dynamic Access Control \(DAC\)](#)

["SMB- und NFS-Auditing und Sicherheits-Tracing"](#)

[Ändern der Kerberos-Sicherheitseinstellungen des CIFS-Servers](#)

[Nutzung von BranchCache zum Caching von SMB-Inhalten für Zweigstellen](#)

[Verwendung von SMB-Signing zur Verbesserung der Netzwerksicherheit](#)

[Konfigurieren der Umgehungsüberprüfung](#)

[Konfigurieren von Zugriffsbeschränkungen für anonyme Benutzer](#)

Anforderungen für die Verwendung von Gruppenrichtlinienobjekten mit Ihrem SMB-Server

Um Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) auf Ihrem SMB-Server zu verwenden, muss Ihr System mehrere Anforderungen erfüllen.

- SMB muss auf dem Cluster lizenziert sein. Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.
- Ein SMB Server muss konfiguriert und einer Windows Active Directory Domäne hinzugefügt werden.
- Der Status des SMB-Server-Administrators muss sich im befinden.
- Gruppenrichtlinienobjekte müssen konfiguriert und auf die Organisationseinheit (OU) von Windows Active Directory angewendet werden, die das SMB-Servercomputer-Objekt enthält.
- Die GPO-Unterstützung muss auf dem SMB-Server aktiviert sein.

Aktivieren oder deaktivieren Sie die GPO-Unterstützung auf einem CIFS-Server

Sie können die Unterstützung für Gruppenrichtlinienobjekt (GPO) auf einem CIFS-Server aktivieren oder deaktivieren. Wenn Sie die GPO-Unterstützung auf einem CIFS-Server aktivieren, werden die entsprechenden Gruppenrichtlinienobjekte, die in der Gruppenrichtlinie definiert sind - die Richtlinie, die auf die Organisationseinheit (OU) angewendet wird, die das Objekt des CIFS-Servercomputers enthält, auf den CIFS-Server angewendet.



Über diese Aufgabe

Gruppenrichtlinienobjekte können nicht im Workgroup-Modus auf CIFS-Servern aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Gruppenrichtlinienobjekte aktivieren	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Gruppenrichtlinienobjekte deaktivieren	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. Vergewissern Sie sich, dass die GPO-Unterstützung den gewünschten Status aufweist: `vserver cifs group-policy show -vserver +vserver_name_`

Der Gruppenrichtlinienstatus für CIFS-Server im Workgroup-Modus wird als „disabled“ angezeigt.

Beispiel

Das folgende Beispiel ermöglicht die GPO-Unterstützung für Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

      Vserver: vs1
Group Policy Status: enabled
```

Verwandte Informationen

[Unterstützte Gruppenrichtlinienobjekte](#)

[Anforderungen für die Verwendung von Gruppenrichtlinienobjekten mit Ihrem CIFS-Server](#)

[Aktualisierung der Gruppenrichtlinienobjekte auf dem CIFS-Server](#)

[Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server](#)

[Anzeigen von Informationen zu GPO-Konfigurationen](#)

Aktualisierung der Gruppenrichtlinienobjekte auf dem SMB-Server

Aktualisierung der Gruppenrichtlinienobjekte in der CIFS-Serverübersicht

Standardmäßig ruft ONTAP Änderungen des Gruppenrichtlinienobjekts (Gruppenrichtlinienobjekt) alle 90 Minuten ab und wendet sie an. Die Sicherheitseinstellungen werden alle 16 Stunden aktualisiert. Wenn Sie Gruppenrichtlinienobjekte aktualisieren möchten, um neue GPO-Richtlinieneinstellungen anzuwenden, bevor ONTAP sie automatisch aktualisiert, können Sie ein manuelles Update auf einem CIFS-Server mit einem ONTAP-Befehl auslösen.

- Standardmäßig werden alle Gruppenrichtlinienobjekte nach Bedarf alle 90 Minuten überprüft und aktualisiert.

Dieses Intervall ist konfigurierbar und kann mit dem festgelegt werden `Refresh interval` Und `Random offset` GPO-Einstellungen.

ONTAP fragt Active Directory nach Änderungen an Gruppenrichtlinienobjekten ab. Wenn die in Active Directory aufgezeichneten GPO-Versionsnummern höher sind als die auf dem CIFS-Server, ruft ONTAP die neuen Gruppenrichtlinienobjekte ab und wendet diese an. Wenn die Versionsnummern identisch sind, werden die Gruppenrichtlinienobjekte auf dem CIFS-Server nicht aktualisiert.

- Die Gruppenrichtlinienobjekte für Sicherheitseinstellungen werden alle 16 Stunden aktualisiert.

ONTAP ruft Gruppenrichtlinienobjekte alle 16 Stunden ab und wendet sie an, unabhängig davon, ob sich diese Gruppenrichtlinienobjekte geändert haben.



Der Standardwert für 16 Stunden kann in der aktuellen ONTAP-Version nicht geändert werden. Dies ist eine Windows-Client-Standardeinstellung.

- Alle Gruppenrichtlinienobjekte können manuell mit einem ONTAP-Befehl aktualisiert werden.

Dieser Befehl simuliert die Windows `gpupdate.exe /Force`-Befehl.

Verwandte Informationen

[Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server](#)

Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server

Wenn Sie die Gruppenrichtlinienobjekt-Einstellungen (GPO) auf Ihrem CIFS-Server sofort aktualisieren möchten, können Sie die Einstellungen manuell aktualisieren. Sie können nur geänderte Einstellungen aktualisieren oder ein Update für alle Einstellungen erzwingen, einschließlich der Einstellungen, die zuvor angewendet, aber nicht geändert wurden.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Aktualisieren...	Geben Sie den Befehl ein...
Die GPO-Einstellungen wurden geändert	<code>vserver cifs group-policy update -vserver vserver_name</code>
Alle GPO-Einstellungen	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

Verwandte Informationen

[Aktualisierung der Gruppenrichtlinienobjekte auf dem CIFS-Server](#)

Zeigt Informationen zu GPO-Konfigurationen an

Sie können Informationen zu Gruppenrichtlinienobjekt-Konfigurationen (GPO) anzeigen, die in Active Directory definiert sind, und zu GPO-Konfigurationen, die auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können Informationen zu allen GPO-Konfigurationen anzeigen, die im Active Directory der Domäne definiert sind, zu der der CIFS-Server gehört, oder Informationen zu GPO-Konfigurationen anzeigen, die auf einen CIFS-Server angewendet wurden.

Schritte

1. Zeigen Sie Informationen zu GPO-Konfigurationen an, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienkonfigurationen anzeigen möchten...	Geben Sie den Befehl ein...
In Active Directory definiert	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Anwendung auf eine CIFS-fähige Storage Virtual Machine (SVM)	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

Beispiel

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die im Active Directory definiert sind, zu dem die CIFS-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache : version1
```

```
Security Settings:
```

```
    Event Audit and Event Log:
```

```
        Audit Logon Events: none
```

```
        Audit Object Access: success
```

```
        Log Retention Method: overwrite-as-needed
```

```
        Max Log Size: 16384
```

```
File Security:
```

```
    /vol1/home
```

```
    /vol1/dir1
```

```
Kerberos:
```

```
    Max Clock Skew: 5
```

```
    Max Ticket Age: 10
```

```
    Max Renew Age: 7
```

```
Privilege Rights:
```

```
    Take Ownership: usr1, usr2
```

Security Privilege: usr1, usr2
Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
Status: enabled
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication for Mode BranchCache: per-share
 Hash Version Support for BranchCache: version1
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dir1
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:

```
No enumeration of SAM accounts: true
No enumeration of SAM accounts and shares: false
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die auf die CIFS-fähige SVM vs1 angewendet werden:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
Advanced Audit Settings:
    Object Access:
      Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
      Audit Logon Events: none
      Audit Object Access: success
      Log Retention Method: overwrite-as-needed
      Max Log Size: 16384
    File Security:
      /vol1/home
      /vol1/dir1
    Kerberos:
      Max Clock Skew: 5
      Max Ticket Age: 10
      Max Renew Age: 7
    Privilege Rights:
      Take Ownership: usr1, usr2
      Security Privilege: usr1, usr2
      Change Notify: usr1, usr2
```

Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
 Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
File Security:
 /vol1/home
 /vol1/dir1
Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false

```
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2
```

Verwandte Informationen

[Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server](#)

Detaillierte Informationen zu Gruppenrichtlinienobjekten anzeigen

Sie können detaillierte Informationen zu eingeschränkten Gruppen anzeigen, die als Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) in Active Directory definiert sind und auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

- Name der Gruppenrichtlinie
- Version der Gruppenrichtlinien
- Verlinken

Gibt die Ebene an, auf der die Gruppenrichtlinie konfiguriert ist. Mögliche Ausgabewerte sind:

- **Local** Wenn die Gruppenrichtlinie in ONTAP konfiguriert ist
 - **Site** Wenn die Gruppenrichtlinie auf Standortebene im Domänencontroller konfiguriert ist
 - **Domain** Wenn die Gruppenrichtlinie auf Domänenebene im Domänencontroller konfiguriert ist
 - **OrganizationalUnit** Wenn die Gruppenrichtlinie auf Organisationseinheit-Ebene (Organisationseinheit) im Domänencontroller konfiguriert ist
 - **RSOP** Für den daraus resultierenden Richtliniensatz, der aus allen Gruppenrichtlinien abgeleitet ist, die auf verschiedenen Ebenen definiert sind
- Eingeschränkter Gruppenname
 - Die Benutzer und Gruppen, die der Gruppe gehören und nicht zur eingeschränkten Gruppe gehören
 - Die Liste der Gruppen, denen die eingeschränkte Gruppe hinzugefügt wird

Eine Gruppe kann ein Mitglied von Gruppen sein, die nicht den hier aufgeführten Gruppen angehören.

Schritt

1. Informationen zu allen Gruppenrichtlinienobjekten anzeigen, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienobjekten anzeigen möchten...	Geben Sie den Befehl ein...
In Active Directory definiert	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Wird auf einen CIFS-Server angewendet	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

Beispiel

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die in der Active Directory-Domäne definiert sind, zu denen die CIFS-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1
```

```
Vserver: vs1
-----
```

```
    Group Policy Name: gp01
        Version: 16
        Link: OrganizationalUnit
    Group Name: group1
        Members: user1
    MemberOf: EXAMPLE\group9
```

```
    Group Policy Name: Resultant Set of Policy
        Version: 0
        Link: RSOP
    Group Name: group1
        Members: user1
    MemberOf: EXAMPLE\group9
```

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die auf die CIFS-fähige SVM vs1 angewendet wurden:

```
cluster1::> vserver cifs group-policy restricted-group show-applied  
-vserver vs1
```

Vserver: vs1

```
Group Policy Name: gp01  
Version: 16  
Link: OrganizationalUnit  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy  
Version: 0  
Link: RSOP  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

Verwandte Informationen

[Anzeigen von Informationen zu GPO-Konfigurationen](#)

Informationen zu zentralen Zugriffsrichtlinien anzeigen

Sie können detaillierte Informationen zu den zentralen Zugriffsrichtlinien anzeigen, die in Active Directory definiert sind. Sie können auch Informationen über die zentralen Zugriffsrichtlinien anzeigen, die über Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

- SVM-Name
- Name der zentralen Zugriffsrichtlinie
- SID
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Mitgliedsregeln



CIFS-Server im Workgroup-Modus werden nicht angezeigt, da sie GPOs nicht unterstützen.

Schritt

1. Zeigen Sie Informationen über zentrale Zugriffsrichtlinien an, indem Sie eine der folgenden Aktionen durchführen:

Wenn Informationen zu allen zentralen Zugriffsrichtlinien angezeigt werden sollen...	Geben Sie den Befehl ein...
In Active Directory definiert	<code>vserver cifs group-policy central-access-policy show-defined -vserver <i>vserver_name</i></code>
Wird auf einen CIFS-Server angewendet	<code>vserver cifs group-policy central-access-policy show-applied -vserver <i>vserver_name</i></code>

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, die in Active Directory definiert sind:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                      SID
-----  -
vs1      p1                          S-1-17-3386172923-1132988875-3044489393-3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                          S-1-17-1885229282-1100162114-134354072-822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                  r2
```

Das folgende Beispiel zeigt Informationen für alle zentralen Zugriffsrichtlinien, die auf die Storage Virtual Machines (SVMs) des Clusters angewendet werden:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

```
Vserver      Name                      SID
-----
-----
vs1          p1                      S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1          p2                      S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                      r2
```

Verwandte Informationen

[Sichern des Dateizugriffs mithilfe von Dynamic Access Control \(DAC\)](#)

[Anzeigen von Informationen zu GPO-Konfigurationen](#)

[Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln](#)

Informationen zu zentralen Zugriffsrichtlinien anzeigen

Sie können detaillierte Informationen zu zentralen Zugriffsrichtlinien anzeigen, die mit zentralen Zugriffsrichtlinien in Active Directory verknüpft sind. Sie können auch Informationen zu zentralen Zugriffsrichtlinien-Regeln anzeigen, die über zentrale Zugriffsrichtlinien-Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können detaillierte Informationen zu definierten und angewandten zentralen Zugriffsrichtlinien anzeigen. Standardmäßig werden die folgenden Informationen angezeigt:

- Name des Vserver
- Name der zentralen Zugriffsregel
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Aktuelle Berechtigungen

- Vorgeschlagene Berechtigungen
- Zielressourcen

Wenn Sie Informationen über alle zentralen Zugriffsrichtlinien anzeigen möchten, die mit zentralen Zugriffsrichtlinien verknüpft sind...	Geben Sie den Befehl ein...
In Active Directory definiert	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Wird auf einen CIFS-Server angewendet	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, die mit den in Active Directory definierten zentralen Zugriffsrichtlinien verknüpft sind:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinien, die mit zentralen Zugriffsrichtlinien auf Storage Virtual Machines (SVMs) auf dem Cluster verknüpft sind:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

Vserver	Name
vs1	r1
	Description: rule #1
	Creation Time: Tue Oct 22 09:33:48 2013
	Modification Time: Tue Oct 22 09:33:48 2013
	Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
	Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
vs1	r2
	Description: rule #2
	Creation Time: Tue Oct 22 10:27:57 2013
	Modification Time: Tue Oct 22 10:27:57 2013
	Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
	Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

Verwandte Informationen

[Sichern des Dateizugriffs mithilfe von Dynamic Access Control \(DAC\)](#)

[Anzeigen von Informationen zu GPO-Konfigurationen](#)

[Anzeigen von Informationen zu zentralen Zugriffsrichtlinien](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.