Applicare oggetti Criteri di gruppo ai server SMB

ONTAP 9

NetApp
April 24, 2024

Sommario

Applicare oggetti Criteri di gruppo ai server SMB

Panoramica sull'applicazione degli oggetti Criteri di gruppo ai server SMB

Il server SMB supporta gli oggetti Criteri di gruppo (GPO), un insieme di regole note come *attributi dei criteri di gruppo* che si applicano ai computer in un ambiente Active Directory. È possibile utilizzare gli oggetti Criteri di gruppo per gestire centralmente le impostazioni di tutte le macchine virtuali di storage (SVM) nel cluster appartenente allo stesso dominio Active Directory.

Quando gli oggetti Criteri di gruppo sono attivati sul server SMB, ONTAP invia query LDAP al server Active Directory per richiedere informazioni sull'oggetto Criteri di gruppo. Se esistono definizioni di GPO applicabili al server SMB, il server Active Directory restituisce le seguenti informazioni di GPO:

- Nome dell'oggetto Criteri di gruppo
- Versione attuale dell'oggetto Criteri di gruppo
- Posizione della definizione dell'oggetto Criteri di gruppo
- Elenchi di UUID (universally unique identifier) per set di criteri GPO

Informazioni correlate

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

"Controllo SMB e NFS e tracciamento della sicurezza"

GPO supportati

Sebbene non tutti gli oggetti Criteri di gruppo (GPO) siano applicabili alle SVM (Storage Virtual Machine) abilitate per CIFS, le SVM sono in grado di riconoscere ed elaborare il relativo set di GPO.

I seguenti GPO sono attualmente supportati sulle SVM:

- Impostazioni avanzate di configurazione dei criteri di controllo:

  Accesso a oggetti: Staging dei criteri di accesso centrale

  Specifica il tipo di eventi da sottoporre a verifica per lo staging dei criteri di accesso centrale (CAP), incluse le seguenti impostazioni:

  - Non eseguire audit
  - Controllare solo gli eventi di successo
  - Controllare solo gli eventi di errore
  - Controllare gli eventi di successo e di guasto

> Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

Impostare utilizzando `Audit Central Access Policy Staging` in `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

> Per utilizzare le impostazioni dell'oggetto Criteri di gruppo per la configurazione avanzata dei criteri di controllo, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni del Registro di sistema:
  - Intervallo di aggiornamento dei criteri di gruppo per SVM abilitato CIFS

    Impostare utilizzando `Registry` GPO.
  - Offset casuale di refresh dei criteri di gruppo

    Impostare utilizzando `Registry` GPO.
  - Pubblicazione hash per BranchCache

    La pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde alla modalità operativa BranchCache. Sono supportate le seguenti tre modalità operative:
    - Per-share
    - All-share
    - Disattivato tramite `Registry` GPO.
  - Supporto della versione hash per BranchCache

    Sono supportate le seguenti tre impostazioni di versione hash:
    - BranchCache versione 1
    - BranchCache versione 2
    - BranchCache versioni 1 e 2 impostate tramite `Registry` GPO.

> Per utilizzare le impostazioni dell'oggetto Criteri di gruppo BranchCache, è necessario configurare BranchCache sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se BranchCache non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni di sicurezza
  - Policy di audit e registro eventi
    - Controllare gli eventi di accesso

      Specifica il tipo di eventi di accesso da sottoporre a verifica, incluse le seguenti impostazioni:

    - Non eseguire audit
    - Controllare solo gli eventi di successo
    - Verifica degli eventi di guasto
    - Controllare gli eventi di successo e di guasto impostati utilizzando `Audit logon events` in `Local Policies/Audit Policy` GPO.

    > Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

  - Controllare l'accesso agli oggetti

    Specifica il tipo di accesso a oggetti da sottoporre a controllo, incluse le seguenti impostazioni:

    - Non eseguire audit
    - Controllare solo gli eventi di successo
    - Verifica degli eventi di guasto
    - Controllare gli eventi di successo e di guasto impostati utilizzando `Audit object access` in `Local Policies/Audit Policy` GPO.

    > Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

  - Metodo di conservazione dei log

    Specifica il metodo di conservazione del registro di controllo, incluse le seguenti impostazioni:

    - Sovrascrivere il registro eventi quando la dimensione del file di registro supera la dimensione massima
    - Non sovrascrivere il registro eventi (cancellare manualmente il registro) impostato utilizzando `Retention method for security log` in `Event Log` GPO.

  - Dimensione massima del log

    Specifica la dimensione massima del registro di controllo.

    Impostare utilizzando `Maximum security log size` in `Event Log` GPO.

    > Per utilizzare le impostazioni dell'oggetto Criteri di gruppo dei criteri di controllo e del registro eventi, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Sicurezza del file system

  Specifica un elenco di file o directory su cui viene applicata la protezione dei file tramite un GPO.

  Impostare utilizzando `File System` GPO.

> Il percorso del volume in cui è configurato l'oggetto Criteri di gruppo di protezione del file system deve esistere all'interno della SVM.

- Policy Kerberos
  - Massima inclinazione dell'orologio

    Specifica la tolleranza massima in minuti per la sincronizzazione dell'orologio del computer.

    Impostare utilizzando `Maximum tolerance for computer clock synchronization` in `Account Policies/Kerberos Policy` GPO.

  - Età massima del biglietto

    Specifica la durata massima in ore per il ticket utente.

    Impostare utilizzando `Maximum lifetime for user ticket` in `Account Policies/Kerberos Policy` GPO.

  - Età massima per il rinnovo del biglietto

    Specifica la durata massima in giorni per il rinnovo del ticket utente.

  Impostare utilizzando `Maximum lifetime for user ticket renewal` in `Account Policies/Kerberos Policy` GPO.

- Assegnazione dei diritti dell'utente (diritti di privilegio)
  - Assuma la proprietà

    Specifica l'elenco di utenti e gruppi che hanno il diritto di assumere la proprietà di qualsiasi oggetto a protezione diretta.

    Impostare utilizzando `Take ownership of files or other objects` in `Local Policies/User Rights Assignment` GPO.

  - Privilegio di sicurezza

    Specifica l'elenco di utenti e gruppi che possono specificare le opzioni di controllo per l'accesso a oggetti di singole risorse, come file, cartelle e oggetti Active Directory.

    Impostare utilizzando `Manage auditing and security log` in `Local Policies/User Rights Assignment` GPO.

  - Modifica del privilegio di notifica (ignora il controllo incrociato)

    Specifica l'elenco di utenti e gruppi che possono attraversare gli alberi di directory anche se gli utenti e i gruppi potrebbero non disporre delle autorizzazioni per la directory attraversata.

  Lo stesso privilegio è richiesto per gli utenti per ricevere notifiche delle modifiche apportate a file e directory. Impostare utilizzando `Bypass traverse checking` in `Local Policies/User Rights Assignment` GPO.

- Valori del Registro di sistema

- Firma obbligatoria

  Specifica se la firma SMB richiesta è attivata o disattivata.

Impostare utilizzando `Microsoft network server: Digitally sign communications (always)` in `Security Options` GPO.

- Limitare l'anonimato

Specifica quali sono le restrizioni per gli utenti anonimi e include le seguenti tre impostazioni dell'oggetto Criteri di gruppo:

- Nessuna enumerazione degli account SAM (Security account Manager):

  Questa impostazione di protezione determina le autorizzazioni aggiuntive concesse per le connessioni anonime al computer. Questa opzione viene visualizzata come `no-enumeration` In ONTAP, se abilitato.

  Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts` in `Local Policies/Security Options` GPO.

- Nessuna enumerazione di account e condivisioni SAM

  Questa impostazione di protezione determina se è consentita l'enumerazione anonima di account e condivisioni SAM. Questa opzione viene visualizzata come `no-enumeration` In ONTAP, se abilitato.

  Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts and shares` in `Local Policies/Security Options` GPO.

- Limitare l'accesso anonimo alle condivisioni e alle named pipe

  Questa impostazione di sicurezza limita l'accesso anonimo alle condivisioni e alle pipe. Questa opzione viene visualizzata come `no-access` In ONTAP, se abilitato.

  Impostare utilizzando `Network access: Restrict anonymous access to Named Pipes and Shares` in `Local Policies/Security Options` GPO.

  Quando si visualizzano informazioni sui criteri di gruppo definiti e applicati, il `Resultant restriction for anonymous user` Il campo di output fornisce informazioni sulla restrizione risultante delle tre impostazioni di restrizione anonime dell'oggetto Criteri di gruppo. Le possibili restrizioni risultanti sono le seguenti:

- `no-access`

All'utente anonimo viene negato l'accesso alle condivisioni e alle named pipe specificate e non è possibile utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è attivato.

- `no-enumeration`

L'utente anonimo ha accesso alle condivisioni e alle named pipe specificate, ma non può utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se

vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Sia il `Network access: Do not allow anonymous enumeration of SAM accounts` o il `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti GPO sono abilitati.

° `no-restriction`

L'utente anonimo ha accesso completo e può utilizzare l'enumerazione. Questa restrizione risultante si verifica se vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Entrambi i modelli `Network access: Do not allow anonymous enumeration of SAM accounts` e. `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti Criteri di gruppo sono disattivati.
  - Gruppi con restrizioni

    È possibile configurare gruppi con restrizioni per gestire centralmente l'appartenenza a gruppi integrati o definiti dall'utente. Quando si applica un gruppo con restrizioni tramite un criterio di gruppo, l'appartenenza di un gruppo locale del server CIFS viene impostata automaticamente in modo che corrisponda alle impostazioni dell'elenco di appartenenze definite nel criterio di gruppo applicato.

Impostare utilizzando `Restricted Groups` GPO.

- Impostazioni dei criteri di accesso centrale

  Specifica un elenco di criteri di accesso centrale. I criteri di accesso centrale e le relative regole dei criteri di accesso centrale determinano le autorizzazioni di accesso per più file sulla SVM.

Informazioni correlate

Attivazione o disattivazione del supporto GPO su un server CIFS

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

"Controllo SMB e NFS e tracciamento della sicurezza"

Modifica delle impostazioni di sicurezza Kerberos del server CIFS

Utilizzo di BranchCache per memorizzare nella cache SMB i contenuti vengono condivisi in una filiale

Utilizzo della firma SMB per migliorare la sicurezza della rete

Configurazione del controllo incrociato bypass

Configurazione delle restrizioni di accesso per utenti anonimi

Requisiti per l'utilizzo degli oggetti Criteri di gruppo con il server SMB

Per utilizzare gli oggetti Criteri di gruppo (GPO) con il server SMB, il sistema deve soddisfare diversi requisiti.

- SMB deve essere concesso in licenza sul cluster. La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.
- Un server SMB deve essere configurato e collegato a un dominio Active Directory di Windows.
- Lo stato dell'amministratore del server SMB deve essere attivo.
- Gli oggetti Criteri di gruppo devono essere configurati e applicati all'unità organizzativa (OU) di Windows Active Directory contenente l'oggetto computer server SMB.
- Il supporto GPO deve essere attivato sul server SMB.

Attivare o disattivare il supporto GPO su un server CIFS

È possibile attivare o disattivare il supporto degli oggetti Criteri di gruppo (GPO) su un server CIFS. Se si attiva il supporto GPO su un server CIFS, gli oggetti Criteri di gruppo applicabili definiti nel criterio di gruppo, ovvero il criterio applicato all'unità organizzativa (OU) che contiene l'oggetto computer server CIFS, vengono applicati al server CIFS.

A proposito di questa attività

I GPO non possono essere abilitati sui server CIFS in modalità workgroup.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Abilitare gli oggetti Criteri di gruppo	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Disattivare gli oggetti Criteri di gruppo	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Verificare che il supporto GPO sia nello stato desiderato: `vserver cifs group-policy show -vserver +vserver_name_`

   Lo stato dei criteri di gruppo per i server CIFS in modalità gruppo di lavoro viene visualizzato come "disabled".

Esempio

L'esempio seguente abilita il supporto GPO su 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
```

Informazioni correlate

GPO supportati

Requisiti per l'utilizzo degli oggetti Criteri di gruppo con il server CIFS

Come vengono aggiornati gli oggetti Criteri di gruppo sul server CIFS

Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Modalità di aggiornamento degli oggetti Criteri di gruppo sul server SMB

Come vengono aggiornati gli oggetti Criteri di gruppo nella panoramica del server CIFS

Per impostazione predefinita, ONTAP recupera e applica le modifiche dell'oggetto Criteri di gruppo ogni 90 minuti. Le impostazioni di sicurezza vengono aggiornate ogni 16 ore. Se si desidera aggiornare gli oggetti Criteri di gruppo per applicare le nuove impostazioni dei criteri dell'oggetto Criteri di gruppo prima che ONTAP li aggiorni automaticamente, è possibile attivare un aggiornamento manuale su un server CIFS con un comando ONTAP.

- Per impostazione predefinita, tutti gli oggetti Criteri di gruppo vengono verificati e aggiornati in base alle necessità ogni 90 minuti.

  Questo intervallo è configurabile e può essere impostato utilizzando `Refresh interval` e. `Random offset` Impostazioni dell'oggetto Criteri di gruppo.

  ONTAP interroga Active Directory per le modifiche apportate agli oggetti Criteri di gruppo. Se i numeri di versione dell'oggetto Criteri di gruppo registrati in Active Directory sono superiori a quelli del server CIFS, ONTAP recupera e applica i nuovi oggetti Criteri di gruppo. Se i numeri di versione sono gli stessi, gli oggetti Criteri di gruppo sul server CIFS non vengono aggiornati.

- Gli oggetti Criteri di gruppo delle impostazioni di sicurezza vengono aggiornati ogni 16 ore.

  ONTAP recupera e applica gli oggetti Criteri di gruppo delle impostazioni di protezione ogni 16 ore, indipendentemente dal fatto che questi oggetti Criteri di gruppo siano stati modificati o meno.

> Il valore predefinito di 16 ore non può essere modificato nella versione corrente di ONTAP. Si tratta di un'impostazione predefinita del client Windows.

- Tutti gli oggetti Criteri di gruppo possono essere aggiornati manualmente con un comando ONTAP.

  Questo comando simula le finestre `gpupdate.exe`/force` command.

Informazioni correlate

Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

Se si desidera aggiornare immediatamente le impostazioni dell'oggetto Criteri di gruppo (GPO) sul server CIFS, è possibile aggiornare manualmente le impostazioni. È possibile aggiornare solo le impostazioni modificate oppure forzare un aggiornamento per tutte le impostazioni, incluse quelle applicate in precedenza ma non modificate.

Fase

1. Eseguire l'azione appropriata:

Se si desidera eseguire l'aggiornamento…	Immettere il comando…
Impostazioni GPO modificate	`vserver cifs group-policy update -vserver` *`vserver_name`*
Tutte le impostazioni dell'oggetto Criteri di gruppo	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informazioni correlate

Come vengono aggiornati gli oggetti Criteri di gruppo sul server CIFS

Visualizza informazioni sulle configurazioni dell'oggetto Criteri di gruppo

È possibile visualizzare informazioni sulle configurazioni degli oggetti Criteri di gruppo (GPO) definite in Active Directory e sulle configurazioni degli oggetti Criteri di gruppo applicate al server CIFS.

A proposito di questa attività

È possibile visualizzare informazioni su tutte le configurazioni GPO definite in Active Directory del dominio a cui appartiene il server CIFS oppure solo sulle configurazioni GPO applicate a un server CIFS.

Fasi

1. Visualizzare le informazioni sulle configurazioni dell'oggetto Criteri di gruppo eseguendo una delle seguenti

operazioni:

Se si desidera visualizzare informazioni su tutte le configurazioni di Criteri di gruppo…	Immettere il comando…
Definito in Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Applicato a una SVM (Storage Virtual Machine) abilitata per CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Esempio

Nell'esempio seguente vengono visualizzate le configurazioni GPO definite in Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

```
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
```

Nell'esempio seguente vengono visualizzate le configurazioni GPO applicate a SVM vs1 abilitato CIFS:

```
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
```

Informazioni correlate

Attivazione o disattivazione del supporto GPO su un server CIFS

Visualizzare informazioni dettagliate sugli oggetti GPO di gruppo con restrizioni

È possibile visualizzare informazioni dettagliate sui gruppi con restrizioni definiti come oggetti Criteri di gruppo (GPO) in Active Directory e applicati al server CIFS.

A proposito di questa attività

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del criterio di gruppo
- Versione dei criteri di gruppo
- Collegamento

  Specifica il livello di configurazione dei criteri di gruppo. I valori di output possibili includono:

  - `Local` Quando il criterio di gruppo è configurato in ONTAP
  - `Site` quando il criterio di gruppo è configurato a livello di sito nel controller di dominio
  - `Domain` quando il criterio di gruppo è configurato a livello di dominio nel controller di dominio
  - `OrganizationalUnit` Quando il criterio di gruppo è configurato a livello di unità organizzativa (OU) nel controller di dominio
  - `RSOP` per l'insieme risultante di criteri derivati da tutti i criteri di gruppo definiti a vari livelli
- Nome del gruppo con restrizioni
- Gli utenti e i gruppi che appartengono al gruppo con restrizioni e che non ne fanno parte
- L'elenco dei gruppi a cui viene aggiunto il gruppo con restrizioni

  Un gruppo può essere un membro di gruppi diversi dai gruppi elencati qui.

Fase

1. Visualizzare le informazioni su tutti gli oggetti Criteri di gruppo con restrizioni eseguendo una delle seguenti operazioni:

Se si desidera visualizzare informazioni su tutti gli oggetti Criteri di gruppo con restrizioni…	Immettere il comando…
Definito in Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Applicato a un server CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Esempio

Nell'esempio seguente vengono visualizzate informazioni sugli oggetti Criteri di gruppo con restrizioni definiti nel dominio Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

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

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

     Group Policy Name: gpo1
               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
```

Nell'esempio seguente vengono visualizzate informazioni sui GPO a gruppi limitati applicati a SVM vs1 abilitato a CIFS:

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

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

     Group Policy Name: gpo1
               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
```

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizza informazioni sui criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sui criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sui criteri di accesso centrale applicati al server CIFS tramite oggetti Criteri di gruppo (GPO).

A proposito di questa attività

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome SVM
- Nome della policy di accesso centrale
- SID
- Descrizione
- Tempo di creazione
- Tempo di modifica
- Regole dei membri

> I server CIFS in modalità gruppo di lavoro non vengono visualizzati perché non supportano gli oggetti Criteri di gruppo.

Fase

1. Visualizzare le informazioni sui criteri di accesso centrale eseguendo una delle seguenti operazioni:

Se si desidera visualizzare informazioni su tutti i criteri di accesso centrale…	Immettere il comando…
Definito in Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Applicato a un server CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Esempio

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale definiti in Active Directory:

```
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
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale applicati alle macchine virtuali dello storage (SVM) sul cluster:

```
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
```

Informazioni correlate

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Visualizza informazioni sulle regole dei criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sulle regole dei criteri di accesso centrale applicate al server CIFS attraverso gli oggetti Criteri di gruppo (GPO) dei criteri di accesso centrale.

A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale definite e applicate. Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del server virtuale
- Nome della regola di accesso centrale
- Descrizione
- Tempo di creazione
- Tempo di modifica

- Permessi correnti
- Permessi proposti
- Risorse di destinazione

Se si desidera visualizzare informazioni su tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale…	Immettere il comando…
Definito in Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Applicato a un server CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Esempio

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory:

```
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)
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale applicati alle macchine virtuali di storage (SVM) sul cluster:

```
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)
```

Informazioni correlate

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale