Aplique objetos de Diretiva de Grupo a servidores SMB

ONTAP 9

NetApp
January 17, 2025

Índice

Aplique objetos de Diretiva de Grupo a servidores SMB

Aplicar objetos de Diretiva de Grupo à visão geral dos servidores SMB

Seu servidor SMB oferece suporte a objetos de Diretiva de Grupo (GPOs), um conjunto de regras conhecidas como *atributos de diretiva de grupo* que se aplicam a computadores em um ambiente do ative Directory. Você pode usar GPOs para gerenciar centralmente as configurações de todas as máquinas virtuais de storage (SVMs) no cluster que pertence ao mesmo domínio do ative Directory.

Quando os GPOs estão ativados no servidor SMB, o ONTAP envia consultas LDAP ao servidor do ative Directory solicitando informações de GPO. Se houver definições de GPO aplicáveis ao servidor SMB, o servidor do ative Directory retornará as seguintes informações de GPO:

- Nome GPO
- Versão GPO atual
- Localização da definição GPO
- Listas de UUIDs (identificadores universalmente exclusivos) para conjuntos de políticas GPO

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

GPOs compatíveis

Embora nem todos os objetos de Diretiva de Grupo (GPOs) sejam aplicáveis às máquinas virtuais de storage (SVMs) habilitadas para CIFS, os SVMs podem reconhecer e processar o conjunto relevante de GPOs.

Os GPOs a seguir são compatíveis atualmente com SVMs:

- Definições avançadas de configuração da política de auditoria:

  Acesso a objetos: Preparação da Política de Acesso Central

  Especifica o tipo de eventos a serem auditados para o estadiamento da política de acesso central (CAP), incluindo as seguintes configurações:

  - Não faça auditoria
  - Audite apenas eventos de sucesso
  - Auditar apenas eventos de falha
  - Audite eventos de sucesso e falha

Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

Defina utilizando a `Audit Central Access Policy Staging` definição no `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

Para usar configurações avançadas de GPO de diretiva de auditoria, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições do registo:
  - Intervalo de atualização da política de grupo para SVM habilitado para CIFS

    Defina utilizando o `Registry` GPO.
  - Atualizar desvio aleatório da política de grupo

    Defina utilizando o `Registry` GPO.
  - Publicação hash para BranchCache

    A publicação Hash para o GPO BranchCache corresponde ao modo de operação BranchCache. Os três modos de operação suportados a seguir são suportados:

    - Por compartilhamento
    - Todos os compartilhamentos
    - Desativado definido utilizando o `Registry` GPO.
  - Suporte à versão hash para BranchCache

    As seguintes três configurações de versão hash são suportadas:

    - BranchCache versão 1
    - BranchCache versão 2
    - BranchCache versões 1 e 2 definidas usando o `Registry` GPO.

Para usar as configurações de GPO do BranchCache, o BranchCache deve ser configurado no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se o BranchCache não estiver configurado no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições de segurança
  - Política de auditoria e log de eventos
    - Audite eventos de logon

      Especifica o tipo de eventos de logon a serem auditados, incluindo as seguintes configurações:

- Não faça auditoria
- Audite apenas eventos de sucesso
- Auditoria em eventos de falha
- Audite eventos de sucesso e falha definidos usando a `Audit logon events` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Auditar o acesso a objeto

  Especifica o tipo de acesso a objeto a ser auditado, incluindo as seguintes configurações:

  - Não faça auditoria
  - Audite apenas eventos de sucesso
  - Auditoria em eventos de falha
  - Audite eventos de sucesso e falha definidos usando a `Audit object access` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Método de retenção de log

  Especifica o método de retenção do log de auditoria, incluindo as seguintes configurações:

  - Substituir o registo de eventos quando o tamanho do ficheiro de registo exceder o tamanho máximo do registo
  - Não substituir o registo de eventos (limpar registo manualmente) definido utilizando a `Retention method for security log` definição no `Event Log` GPO.

- Tamanho máximo do registo

  Especifica o tamanho máximo do log de auditoria.

  Defina utilizando a `Maximum security log size` definição no `Event Log` GPO.

> Para usar a diretiva de auditoria e as configurações de GPO de log de eventos, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

◦ Segurança do sistema de arquivos

Especifica uma lista de arquivos ou diretórios nos quais a segurança de arquivos é aplicada por meio de um GPO.

Defina utilizando o `File System` GPO.

O caminho do volume para o qual o GPO de segurança do sistema de arquivos está configurado deve existir na SVM.

- Política Kerberos
  - Inclinação máxima do relógio

    Especifica a tolerância máxima em minutos para a sincronização do relógio do computador.

    Defina utilizando a `Maximum tolerance for computer clock synchronization` definição no `Account Policies/Kerberos Policy` GPO.

  - Idade máxima do bilhete

    Especifica a vida útil máxima em horas para o ticket de usuário.

    Defina utilizando a `Maximum lifetime for user ticket` definição no `Account Policies/Kerberos Policy` GPO.

  - Idade máxima de renovação do bilhete

    Especifica o tempo de vida máximo em dias para a renovação do ticket do usuário.

  Defina utilizando a `Maximum lifetime for user ticket renewal` definição no `Account Policies/Kerberos Policy` GPO.

- Atribuição de direitos de utilizador (direitos de privilégio)
  - Assuma a propriedade

    Especifica a lista de usuários e grupos que têm o direito de assumir a propriedade de qualquer objeto que possa ser protegido.

    Defina utilizando a `Take ownership of files or other objects` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio de segurança

    Especifica a lista de usuários e grupos que podem especificar opções de auditoria para acesso a objetos de recursos individuais, como arquivos, pastas e objetos do ative Directory.

    Defina utilizando a `Manage auditing and security log` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio Change Notify (verificação de desvio transversal)

    Especifica a lista de usuários e grupos que podem atravessar árvores de diretório, mesmo que os usuários e grupos possam não ter permissões no diretório atravessado.

  O mesmo privilégio é necessário para que os usuários recebam notificações de alterações em arquivos e diretórios. Defina utilizando a `Bypass traverse checking` definição no `Local Policies/User Rights Assignment` GPO.

- Valores do registo

- Definição de assinatura necessária

  Especifica se a assinatura SMB necessária está ativada ou desativada.

Defina utilizando a `Microsoft network server: Digitally sign communications (always)` definição no `Security Options` GPO.

◦ Restringir o anonimato

Especifica quais são as restrições para usuários anônimos e inclui as seguintes três configurações de GPO:

- Sem enumeração de contas SAM (Security Account Manager):

  Esta configuração de segurança determina quais permissões adicionais são concedidas para conexões anônimas ao computador. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts` definição no `Local Policies/Security Options` GPO.

- Nenhuma enumeração de contas e compartilhamentos SAM

  Esta configuração de segurança determina se a enumeração anônima de contas e compartilhamentos SAM é permitida. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts and shares` definição no `Local Policies/Security Options` GPO.

- Restringir o acesso anônimo a compartilhamentos e pipes nomeados

  Essa configuração de segurança restringe o acesso anônimo a compartilhamentos e pipes. Esta opção é apresentada como `no-access` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Restrict anonymous access to Named Pipes and Shares` definição no `Local Policies/Security Options` GPO.

  Ao exibir informações sobre políticas de grupo definidas e aplicadas, o `Resultant restriction for anonymous user` campo de saída fornece informações sobre a restrição resultante das três configurações de GPO anônimo restrito. As possíveis restrições resultantes são as seguintes:

◦ `no-access`

O usuário anônimo tem acesso negado aos compartilhamentos especificados e pipes nomeados e não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se o `Network access: Restrict anonymous access to Named Pipes and Shares` GPO estiver ativado.

◦ `no-enumeration`

O usuário anônimo tem acesso aos compartilhamentos especificados e pipes nomeados, mas não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se

ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O ou os `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs estão ativados.

° `no-restriction`

O usuário anônimo tem acesso total e pode usar enumeração. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`Os GPOs e `Network access: Do not allow anonymous enumeration of SAM accounts and shares` os GPOs estão desativados.
  - Grupos restritos

    Você pode configurar grupos restritos para gerenciar centralmente a associação de grupos internos ou definidos pelo usuário. Quando você aplica um grupo restrito por meio de uma política de grupo, a associação de um grupo local de servidor CIFS é definida automaticamente para corresponder às configurações da lista de membros definidas na política de grupo aplicada.

Defina utilizando o `Restricted Groups` GPO.

- Definições da política de acesso central

  Especifica uma lista de políticas de acesso central. As políticas de acesso central e as regras de política de acesso central associadas determinam permissões de acesso para vários arquivos no SVM.

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

Modificação das configurações de segurança Kerberos do servidor CIFS

Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Utilizar a assinatura SMB para melhorar a segurança da rede

Configuração da verificação transversal de derivação

Configurando restrições de acesso para usuários anônimos

Requisitos para usar GPOs com seu servidor SMB

Para usar objetos de diretiva de grupo (GPOs) com seu servidor SMB, o sistema deve atender a vários requisitos.

- O SMB deve ser licenciado no cluster. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.
- Um servidor SMB deve ser configurado e Unido a um domínio do ative Directory do Windows.
- O status de administrador do servidor SMB deve estar ativado.
- Os GPOs devem ser configurados e aplicados à Unidade organizacional do ative Directory (ou) do Windows que contém o objeto de computador servidor SMB.
- O suporte ao GPO deve estar ativado no servidor SMB.

Ative ou desative o suporte de GPO em um servidor CIFS

Você pode ativar ou desativar o suporte de GPO (Group Policy Object) em um servidor CIFS. Se você habilitar o suporte a GPO em um servidor CIFS, os GPOs aplicáveis definidos na diretiva de grupo - a diretiva aplicada à unidade organizacional (ou) que contém o objeto computador servidor CIFS - serão aplicados ao servidor CIFS.

Sobre esta tarefa

Os GPOs não podem ser ativados em servidores CIFS no modo de grupo de trabalho.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Desativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Verifique se o suporte GPO está no estado desejado: `vserver cifs group-policy show -vserver +vserver_name_`

   O status da Diretiva de Grupo para servidores CIFS no modo de grupo de trabalho é exibido como "habilitado".

Exemplo

O exemplo a seguir habilita o suporte a GPO na máquina virtual de storage (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
```

Informações relacionadas

GPOs compatíveis

Requisitos para usar GPOs com seu servidor CIFS

Como os GPOs são atualizados no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Exibindo informações sobre as configurações do GPO

Como os GPOs são atualizados no servidor SMB

Como os GPOs são atualizados na visão geral do servidor CIFS

Por padrão, o ONTAP recupera e aplica alterações de Objeto de Diretiva de Grupo (GPO) a cada 90 minutos. As configurações de segurança são atualizadas a cada 16 horas. Se você quiser atualizar os GPOs para aplicar novas configurações de política de GPO antes que o ONTAP as atualize automaticamente, você pode acionar uma atualização manual em um servidor CIFS com um comando ONTAP.

- Por padrão, todos os GPOs são verificados e atualizados conforme necessário a cada 90 minutos.

  Este intervalo é configurável e pode ser definido utilizando as `Refresh interval` definições e `Random offset` GPO.

  O ONTAP consulta o ative Directory quanto a alterações nos GPOs. Se os números de versão do GPO registrados no ative Directory forem maiores do que os do servidor CIFS, o ONTAP recuperará e aplicará os novos GPOs. Se os números de versão forem os mesmos, os GPOs no servidor CIFS não serão atualizados.

- Os GPOs são atualizados a cada 16 horas.

  O ONTAP recupera e aplica GPOs de configurações de segurança a cada 16 horas, independentemente de estes GPOs terem sido alterados ou não.

  > O valor padrão de 16 horas não pode ser alterado na versão atual do ONTAP. É uma configuração padrão do cliente Windows.

- Todos os GPOs podem ser atualizados manualmente com um comando ONTAP.

  Este comando simula o comando Windows `gpupdate.exe`/force.

Informações relacionadas

Atualizar manualmente as definições de GPO no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Se pretender atualizar imediatamente as definições do GPO (Group Policy Object) no servidor CIFS, pode atualizar manualmente as definições. Você pode atualizar apenas as configurações alteradas ou forçar uma atualização para todas as configurações, incluindo as configurações que foram aplicadas anteriormente, mas não foram alteradas.

Passo

1. Execute a ação apropriada:

Se você quiser atualizar…	Digite o comando…
Definições GPO alteradas	`vserver cifs group-policy update -vserver` *`vserver_name`*
Todas as definições do GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informações relacionadas

Como os GPOs são atualizados no servidor CIFS

Apresentar informações sobre as configurações do GPO

Você pode exibir informações sobre configurações de GPO (Group Policy Object) definidas no ative Directory e sobre configurações GPO aplicadas ao servidor CIFS.

Sobre esta tarefa

Você pode exibir informações sobre todas as configurações de GPO definidas no ative Directory do domínio ao qual o servidor CIFS pertence, ou você pode exibir informações apenas sobre as configurações de GPO aplicadas a um servidor CIFS.

Passos

1. Exiba informações sobre as configurações do GPO executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy show-defined -vserver vserver_name`

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo…	Digite o comando…
Aplicado a uma máquina virtual de storage habilitada por CIFS (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe as configurações de GPO definidas no ative Directory ao qual pertence o SVM habilitado para CIFS chamado 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
```

O exemplo a seguir exibe as configurações de GPO aplicadas ao SVM VS1 habilitado para 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
```

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Exibir informações detalhadas sobre GPOs de grupo restrito

Você pode exibir informações detalhadas sobre grupos restritos definidos como objetos de Diretiva de Grupo (GPOs) no ative Directory e aplicados ao servidor CIFS.

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome da política de grupo
- Versão da política de grupo
- Link

  Especifica o nível no qual a diretiva de grupo está configurada. Os possíveis valores de saída incluem o seguinte:

  - `Local` Quando a política de grupo é configurada no ONTAP
  - `Site` quando a política de grupo é configurada no nível do site no controlador de domínio
  - `Domain` quando a política de grupo é configurada no nível do domínio no controlador de domínio
  - `OrganizationalUnit` Quando a política de grupo é configurada no nível de unidade organizacional (ou) no controlador de domínio
  - `RSOP` para o conjunto resultante de políticas derivadas de todas as políticas de grupo definidas em vários níveis
- Nome do grupo restrito
- Os usuários e grupos que pertencem e que não pertencem ao grupo restrito
- A lista de grupos aos quais o grupo restrito é adicionado

  Um grupo pode ser membro de grupos que não sejam os listados aqui.

Passo

1. Exiba informações sobre todos os GPOs de grupo restrito executando uma das seguintes ações:

Se você quiser exibir informações sobre todos os GPOs de grupo restrito…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`

Se você quiser exibir informações sobre todos os GPOs de grupo restrito…	Digite o comando…
Aplicado a um servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações sobre GPOs de grupo restrito definidos no domínio do ative Directory ao qual pertence o SVM habilitado para CIFS chamado 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
```

O exemplo a seguir exibe informações sobre GPOs de grupos restritos aplicados ao SVM VS1 habilitado para 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
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibir informações sobre políticas de acesso centrais

Você pode exibir informações detalhadas sobre as políticas de acesso central definidas no ative Directory. Você também pode exibir informações sobre as políticas de acesso central aplicadas ao servidor CIFS por meio de objetos de diretiva de grupo (GPOs).

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da política de acesso central
- SID
- Descrição
- Tempo de criação
- Tempo de modificação
- Regras dos membros

Os servidores CIFS no modo de grupo de trabalho não são exibidos porque não suportam GPOs.

Passo

1. Exiba informações sobre políticas de acesso central executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

Exemplo

O exemplo a seguir exibe informações de todas as políticas de acesso central definidas no ative 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
```

O exemplo a seguir exibe informações de todas as políticas de acesso central aplicadas às máquinas virtuais de armazenamento (SVMs) no 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
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre as regras da política de acesso central

Exibir informações sobre as regras da política de acesso central

Você pode exibir informações detalhadas sobre regras de política de acesso central associadas a políticas de acesso centrais definidas no ative Directory. Você também pode exibir informações sobre regras de políticas de acesso centrais aplicadas ao servidor CIFS por meio de GPOs de diretiva de acesso central (objetos de diretiva de grupo).

Sobre esta tarefa

Você pode exibir informações detalhadas sobre regras de política de acesso central definidas e aplicadas. Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da regra de acesso central
- Descrição
- Tempo de criação
- Tempo de modificação

- Permissões atuais
- Permissões propostas
- Direcionar recursos

Se você quiser exibir informações sobre todas as regras de política de acesso central associadas às políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central definidas no ative 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)
```

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central aplicadas a máquinas virtuais de armazenamento (SVMs) no 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)
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Informações sobre direitos autorais

Informações sobre marcas comerciais