SMB 서버에 그룹 정책 개체를 적용합니다

ONTAP 9

NetApp
February 12, 2026

목차

SMB 서버에 그룹 정책 개체를 적용합니다

그룹 정책 개체를 ONTAP SMB 서버에 적용하는 방법에 대해 알아봅니다

SMB 서버는 Active Directory 환경의 컴퓨터에 적용되는 _group 정책 특성_이라는 규칙 집합인 GPO(그룹 정책 개체)를 지원합니다. GPO를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM(스토리지 가상 머신)에 대한 설정을 중앙에서 관리할 수 있습니다.

SMB 서버에서 GPO를 사용하도록 설정하면 ONTAP가 GPO 정보를 요청하는 Active Directory 서버에 LDAP 쿼리를 보냅니다. SMB 서버에 적용할 수 있는 GPO 정의가 있는 경우 Active Directory 서버는 다음 GPO 정보를 반환합니다.

- GPO 이름입니다
- 현재 GPO 버전입니다
- GPO 정의의 위치입니다
- GPO 정책 집합에 대한 UUID(Universally Unique Identifier) 목록입니다

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요
- "SMB 및 NFS 감사 및 보안 추적"

지원되는 ONTAP SMB GPO에 대해 알아봅니다

모든 GPO(그룹 정책 개체)가 CIFS 지원 SVM(스토리지 가상 머신)에 적용되는 것은 아니지만 SVM은 관련 GPO 세트를 인식하고 처리할 수 있습니다.

현재 SVM에서 지원되는 GPO는 다음과 같습니다.

- 고급 감사 정책 구성 설정:

  객체 액세스: 중앙 액세스 정책 스테이징

  다음 설정을 포함하여 중앙 액세스 정책(CAP) 스테이징에 대해 감사할 이벤트 유형을 지정합니다.

  - 감사 금지
  - 성공 이벤트만 감사합니다
  - 오류 이벤트만 감사합니다
  - 성공 및 실패 이벤트를 모두 감사합니다

  > ⓘ 세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

  Advanced Audit Policy Configuration/Audit Policies/Object Access GPO에서 Audit Central Access Policy Staging 설정을 이용하여 설정한다.

고급 감사 정책 구성 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 대해 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 레지스트리 설정:
  - CIFS 지원 SVM에 대한 그룹 정책 업데이트 간격

    레지스트리 GPO를 사용하여 설정합니다.
  - 그룹 정책 무작위 오프셋을 새로 고칩니다

    레지스트리 GPO를 사용하여 설정합니다.
  - BranchCache에 대한 해시 게시

    BranchCache GPO의 해시 게시는 BranchCache 운영 모드에 해당합니다. 지원되는 세 가지 작동 모드가 지원됩니다.

    - 공유당
    - 전체 공유
    - '레지스트리' GPO를 사용하여 설정을 비활성화했습니다.
  - BranchCache에 대한 해시 버전 지원

    다음 세 가지 해시 버전 설정이 지원됩니다.

    - BranchCache 버전 1
    - BranchCache 버전 2
    - BranchCache 버전 1 및 2는 레지스트리 GPO를 사용하여 설정합니다.

BranchCache GPO 설정을 사용하려면 이러한 설정을 적용할 CIFS 지원 SVM에 BranchCache를 구성해야 합니다. SVM에 BranchCache가 구성되어 있지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 보안 설정
  - 감사 정책 및 이벤트 로그
    - 로그온 이벤트를 감사합니다

      다음 설정을 포함하여 감사할 로그온 이벤트의 유형을 지정합니다.

      - 감사 금지
      - 성공 이벤트만 감사합니다
      - 장애 이벤트 감사
      - Local Policies/Audit Policy GPO에서 Audit logon events 설정을 이용하여 성공 및 실패 이벤트를 모두 Audit한다.

세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 개체 액세스를 감사합니다

  다음 설정을 포함하여 감사할 개체 액세스 유형을 지정합니다.

  - 감사 금지
  - 성공 이벤트만 감사합니다
  - 장애 이벤트 감사
  - Local Policies/Audit Policy GPO의 Audit object access 설정을 이용하여 성공 이벤트와 실패 이벤트를 모두 Audit한다.

  세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 로그 보존 방법입니다

  다음 설정을 포함하여 감사 로그 보존 방법을 지정합니다.

  - 로그 파일의 크기가 최대 로그 크기를 초과할 경우 이벤트 로그를 덮어씁니다
  - 이벤트 로그 GPO의 보안 로그 보관 방법 설정을 사용하여 이벤트 로그(수동으로 로그 지우기) 집합을 덮어쓰지 마십시오.

- 최대 로그 크기입니다

  감사 로그의 최대 크기를 지정합니다.

  이벤트 로그 GPO에서 최대 보안 로그 크기 설정을 사용하여 설정합니다.

  감사 정책 및 이벤트 로그 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

◦ 파일 시스템 보안

GPO를 통해 파일 보안을 적용할 파일 또는 디렉터리 목록을 지정합니다.

파일 시스템 GPO를 사용하여 설정합니다.

파일 시스템 보안 GPO를 구성하는 볼륨 경로가 SVM 내에 있어야 합니다.

◦ Kerberos 정책

- 최대 클럭 불균형

  컴퓨터 시계 동기화에 대한 최대 허용 시간(분)을 지정합니다.

  계정 정책/Kerberos 정책 GPO에서 컴퓨터 시계 동기화에 대한 최대 허용 한도를 사용하여 설정합니다.

- 최대 항공권 사용 기간

  사용자 티켓의 최대 수명(시간)을 지정합니다.

  계정 정책/Kerberos 정책 GPO에서 사용자 티켓의 최대 수명 설정을 사용하여 설정합니다.

- 최대 티켓 갱신 기간

  사용자 티켓 갱신에 대한 최대 수명(일)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓 갱신을 위한 최대 수명 설정을 사용하여 설정합니다.

◦ 사용자 권한 할당(권한 권한)

- 소유권 가져오기

  보안 개체의 소유권을 가져올 권한이 있는 사용자 및 그룹 목록을 지정합니다.

  Local Policies/User Rights Assignment GPO에서 파일 또는 기타 개체의 소유권 가져오기 설정을 사용하여 설정합니다.

- 보안 권한

  파일, 폴더 및 Active Directory 개체와 같은 개별 리소스의 개체 액세스에 대한 감사 옵션을 지정할 수 있는 사용자 및 그룹 목록을 지정합니다.

  Local Policies/User Rights Assignment GPO에서 MManage auditing and security log 설정을 이용하여 설정한다.

- 알림 권한 변경(통과 확인 무시)

  사용자 및 그룹에 통과 디렉터리에 대한 권한이 없더라도 디렉터리 트리를 통과할 수 있는 사용자 및 그룹 목록을 지정합니다.

사용자가 파일 및 디렉토리의 변경 알림을 수신하는 경우에도 동일한 권한이 필요합니다. Local Policies/User Rights Assignment GPO에서 통과 확인 무시 설정을 사용하여 설정합니다.

◦ 레지스트리 값

- 서명 필요 설정

  필요한 SMB 서명을 설정 또는 해제할지 여부를 지정합니다.

보안 옵션 GPO의 'Microsoft 네트워크 서버: 디지털 서명 통신(항상)' 설정을 사용하여 설정합니다.

◦ 익명 제한

익명 사용자의 제한 사항을 지정하고 다음 세 가지 GPO 설정을 포함합니다.

- SAM(보안 계정 관리자) 계정의 열거 없음:

  이 보안 설정은 컴퓨터에 대한 익명 연결에 대해 부여되는 추가 권한을 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 설정을 사용하여 설정합니다.

- SAM 계정 및 공유의 열거 없음

  이 보안 설정은 SAM 계정과 공유의 익명 열거가 허용되는지 여부를 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

  Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts and 공유 설정을 이용하여 설정한다.

- 공유 및 명명된 파이프에 대한 익명 액세스를 제한합니다

  이 보안 설정은 공유 및 파이프에 대한 익명 액세스를 제한합니다. 이 옵션이 활성화된 경우 ONTAP에서 이 옵션이 "no-access"로 표시됩니다.

  Local Policies/Security Options GPO에서 Network access: restrict anonymous access to named pipes and Shares 설정을 이용하여 설정한다.

  정의된 그룹 정책과 적용된 그룹 정책에 대한 정보를 표시할 때 "익명 사용자에 대한 결과 제한" 출력 필드는 세 가지 익명 GPO 제한 설정의 결과 제한에 대한 정보를 제공합니다. 가능한 결과 제한은 다음과 같습니다.

◦ "접근 불가"

익명 사용자는 지정된 공유 및 명명된 파이프에 대한 액세스가 거부되며 SAM 계정과 공유의 열거를 사용할 수 없습니다. 네트워크 액세스: 명명된 파이프 및 공유에 대한 익명 액세스 제한 GPO가 설정된 경우 이러한 제한이 나타납니다.

◦ 번호 매기기

익명 사용자는 지정된 공유 및 명명된 파이프에 액세스할 수 있지만 SAM 계정과 공유의 열거를 사용할 수는 없습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 또는 Network access: do not allow anonymous enumeration of SAM accounts and 공유 GPO(SAM 계정과 공유의 익명 열거 허용 안 함) 중 하나가 활성화됩니다.

◦ 무제한입니다

익명 사용자는 모든 액세스 권한이 있으며 열거형을 사용할 수 있습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 및 Network access: do not allow anonymous enumeration of SAM accounts and ses(SAM 계정과 공유의 익명 열거 허용 안 함) GPO가 모두 비활성화됩니다.
  - 제한된 그룹

    제한된 그룹을 구성하여 기본 제공 그룹 또는 사용자 정의 그룹의 구성원을 중앙에서 관리할 수 있습니다. 그룹 정책을 통해 제한된 그룹을 적용하면 CIFS 서버 로컬 그룹의 구성원은 적용된 그룹 정책에 정의된 멤버 자격 목록 설정과 일치하도록 자동으로 설정됩니다.

제한 그룹 GPO를 사용하여 설정합니다.

- 중앙 액세스 정책 설정

  중앙 액세스 정책 목록을 지정합니다. 중앙 액세스 정책과 관련 중앙 액세스 정책 규칙에 따라 SVM의 여러 파일에 대한 액세스 권한이 결정됩니다.

관련 정보

- 서버에서 GPO 지원 활성화 또는 비활성화
- 서버의 파일 액세스 보안에 대해 알아보세요
- "SMB 및 NFS 감사 및 보안 추적"
- 서버 보안 설정 수정
- 지점 사무실에서 공유 콘텐츠를 캐시하기 위해 BranchCache를 사용하는 방법에 대해 알아보세요.
- ONTAP 서명을 사용하여 네트워크 보안을 강화하는 방법에 대해 알아보세요.
- 바이패스 트래버스 검사 구성에 대해 알아보세요
- 익명 사용자의 액세스 제한을 구성합니다

GPO에 대한 ONTAP SMB 서버 요구 사항

SMB 서버에서 GPO(그룹 정책 개체)를 사용하려면 시스템이 여러 요구 사항을 충족해야 합니다.

- SMB는 클러스터에서 라이센스가 있어야 합니다. SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오 "있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- SMB 서버는 Windows Active Directory 도메인에 구성 및 가입해야 합니다.
- SMB 서버 관리자 상태는 켜져야 합니다.
- GPO를 구성하고 SMB 서버 컴퓨터 개체가 포함된 Windows Active Directory OU(조직 단위)에 적용해야 합니다.
- SMB 서버에서 GPO 지원을 활성화해야 합니다.

ONTAP SMB 서버에서 GPO 지원을 설정하거나 해제합니다

CIFS 서버에서 GPO(그룹 정책 개체) 지원을 설정하거나 해제할 수 있습니다. CIFS 서버에서 GPO 지원을 설정하면 CIFS 서버 컴퓨터 개체가 포함된 OU(조직 구성 단위)에 적용되는 그룹 정책에 정의된 적용 가능한 GPO가 CIFS 서버에 적용됩니다.

이 작업에 대해

워크그룹 모드에서는 CIFS 서버에서 GPO를 설정할 수 없습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
GPO를 활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status enabled'
GPO를 비활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status disabled'

2. GPO 지원이 'vserver cifs group-policy show-vserver+vserver_name_'(SVM CIFS 그룹 정책 표시) 상태로 설정되어 있는지 확인합니다

   워크그룹 모드의 CIFS 서버에 대한 그룹 정책 상태는 "사용 안 함"으로 표시됩니다.

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에 대한 GPO 지원을 설정합니다.

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

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

            Vserver: vs1
Group Policy Status: enabled
```

관련 정보

지원되는 GPO에 대해 알아보세요

GPO에 대한 서버 요구 사항

SMB 서버에서 GPO 업데이트에 대해 알아보세요

SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.

GPO 구성에 대한 정보를 표시합니다

SMB 서버에서 GPO를 업데이트하는 방법

ONTAP SMB 서버에서 GPO를 업데이트하는 방법에 대해 알아봅니다

기본적으로 ONTAP는 90분마다 GPO(그룹 정책 개체) 변경 내용을 검색하고 적용합니다. 보안 설정은 16시간마다 새로 고쳐집니다. ONTAP에서 GPO를 자동으로 업데이트하기 전에 GPO를 업데이트하여 새 GPO 정책 설정을 적용하려면 ONTAP 명령을 사용하여 CIFS 서버에서 수동 업데이트를 트리거하면 됩니다.

- 기본적으로 모든 GPO는 90분마다 확인 및 업데이트됩니다.

  이 간격은 구성 가능하며 '새로 고침 간격' 및 '임의 오프셋' GPO 설정을 사용하여 설정할 수 있습니다.

ONTAP는 Active Directory에 GPO 변경 사항을 쿼리합니다. Active Directory에 기록된 GPO 버전 번호가 CIFS 서버의 GPO 버전 번호보다 높을 경우 ONTAP는 새 GPO를 검색하고 적용합니다. 버전 번호가 같으면 CIFS 서버의 GPO가 업데이트되지 않습니다.

- 보안 설정 GPO는 16시간마다 새로 고쳐집니다.

  ONTAP는 이러한 GPO의 변경 여부에 관계없이 보안 설정 GPO를 16시간마다 검색하고 적용합니다.

  현재 ONTAP 버전에서는 16시간 기본값을 변경할 수 없습니다. Windows 클라이언트 기본 설정입니다.

- 모든 GPO는 ONTAP 명령을 사용하여 수동으로 업데이트할 수 있습니다.

  이 명령은 Windows 'gpupdate.exe' /force' 명령을 시뮬레이션합니다.

관련 정보

SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.

ONTAP SMB 서버에서 GPO 설정을 수동으로 업데이트합니다

CIFS 서버에서 GPO(그룹 정책 개체) 설정을 즉시 업데이트하려면 설정을 수동으로 업데이트할 수 있습니다. 변경된 설정만 업데이트하거나 이전에 적용되었지만 변경되지 않은 설정을 포함하여 모든 설정에 대해 업데이트를 적용할 수 있습니다.

단계

1. 적절한 작업을 수행합니다.

업데이트하려면...	명령 입력...
GPO 설정이 변경되었습니다	'vserver cifs group-policy update-vserver_vserver_name_'
모든 GPO 설정	'vserver cifs group-policy update-vserver_vserver_name_-force-re애플리케이션-all -settings true'

관련 정보

SMB 서버에서 GPO 업데이트에 대해 알아보세요

ONTAP SMB GPO 구성에 대한 정보를 표시합니다

Active Directory에 정의된 GPO(그룹 정책 개체) 구성과 CIFS 서버에 적용된 GPO 구성에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

CIFS 서버가 속한 도메인의 Active Directory에 정의된 모든 GPO 구성에 대한 정보를 표시하거나 CIFS 서버에 적용된

GPO 구성에 대한 정보만 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 GPO 구성에 대한 정보를 표시합니다.

모든 그룹 정책 구성에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy show-defined-vserver vserver_name'
CIFS 지원 스토리지 가상 시스템(SVM)에 적용	'vserver cifs group-policy show-applied-vserver vserver_name'

예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory에 정의된 GPO 구성을 보여 줍니다.

```
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
```

다음 예에서는 CIFS 지원 SVM VS1 V1에 적용된 GPO 구성을 보여 줍니다.

```
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
```

관련 정보

서버에서 GPO 지원 활성화 또는 비활성화

ONTAP SMB의 제한된 그룹 GPO에 대한 정보를 표시합니다

Active Directory에서 GPO(그룹 정책 개체)로 정의되고 CIFS 서버에 적용되는 제한된 그룹에 대한 자세한 정보를 표시할 수 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- 그룹 정책 이름입니다
- 그룹 정책 버전입니다
- 링크

  그룹 정책이 구성되는 수준을 지정합니다. 가능한 출력 값은 다음과 같습니다.

  - ONTAP에서 그룹 정책이 구성되면 Local이 됩니다
  - 도메인 컨트롤러의 사이트 수준에서 그룹 정책이 구성되면 '사이트'입니다
  - 도메인 컨트롤러의 도메인 수준에서 그룹 정책이 구성되면 "domain"입니다
  - 조직 단위(OrganizationalUnit) - 도메인 컨트롤러의 조직 단위(OU) 수준에서 그룹 정책이 구성된 경우
  - 다양한 수준에서 정의된 모든 그룹 정책에서 파생된 정책의 결과 집합에 대한 RSoP
- 제한된 그룹 이름입니다
- 제한된 그룹에 속하고 속하지 않는 사용자 및 그룹
- 제한된 그룹이 추가되는 그룹의 목록입니다

  그룹은 여기에 나열된 그룹 이외의 그룹의 구성원이 될 수 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 모든 제한된 그룹 GPO에 대한 정보를 표시합니다.

모든 제한된 그룹 **GPO**에 대한 정보를 표시하려면…	명령 입력…
Active Directory에 정의되어 있습니다	'vserver cifs group-policy restricted-group show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy restricted-group show-applied-vserver vserver_name'

예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory 도메인에 정의된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
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
```

다음 예에서는 CIFS 지원 SVM VS1 에 적용된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
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
```

관련 정보

GPO 구성에 대한 정보를 표시합니다

ONTAP SMB 중앙 액세스 정책에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책에 대한 자세한 정보를 표시할 수 있습니다. GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 정책의 이름입니다
- SID
- 설명
- 생성 시간
- 수정 시간
- 구성원 규칙

CIFS 서버는 GPO를 지원하지 않으므로 워크그룹 모드의 CIFS 서버는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행하여 중앙 액세스 정책에 대한 정보를 표시합니다.

모든 중앙 액세스 정책에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-policy show-defined-vserver_vserver_name_'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-policy show-applied-vserver_vserver_name_'

예

다음 예에서는 Active Directory에 정의된 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
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
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
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
```

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

ONTAP SMB 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책과 연결된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 중앙 액세스 정책 GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책 규칙에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

정의되고 적용된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 규칙의 이름입니다
- 설명
- 생성 시간
- 수정 시간
- 현재 권한
- 제안된 권한

- 타겟 리소스

중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-rule show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-rule show-applied-vserver vserver_name'

예

다음 예에서는 Active Directory에 정의된 중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
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)
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 중앙 액세스 정책과 연결된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
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)
```

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다

저작권 정보

상표 정보