



SMB 서버를 관리합니다

ONTAP 9

NetApp
April 24, 2024

목차

SMB 서버를 관리합니다	1
SMB 서버를 수정합니다	1
옵션을 사용하여 SMB 서버를 사용자 지정합니다	2
SMB 서버 보안 설정을 관리합니다	10
성능 및 이중화를 위해 SMB 멀티 채널을 구성합니다	41
SMB 서버에서 기본 Windows 사용자를 UNIX 사용자 매핑으로 구성합니다	43
SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시합니다	46
과도한 Windows 클라이언트 리소스 사용을 제한하는 명령 옵션입니다	47
기존 oplocks 및 리스 oplocks로 클라이언트 성능 향상	48
SMB 서버에 그룹 정책 개체를 적용합니다	54
SMB 서버 컴퓨터 계정 암호를 관리하는 명령입니다	73
도메인 컨트롤러 연결을 관리합니다	73
null 세션을 사용하여 Kerberos가 아닌 환경의 스토리지에 액세스합니다	77
SMB 서버의 NetBIOS 별칭을 관리합니다	79
기타 SMB 서버 작업을 관리합니다	83
SMB 액세스 및 SMB 서비스에 IPv6를 사용합니다	89

SMB 서버를 관리합니다

SMB 서버를 수정합니다

"vserver cifs modify" 명령을 사용하여 작업 그룹에서 Active Directory 도메인으로, 작업 그룹에서 다른 작업 그룹으로 또는 Active Directory 도메인에서 작업 그룹으로 SMB 서버를 이동할 수 있습니다.

이 작업에 대해

SMB 서버 이름 및 관리 상태와 같은 SMB 서버의 다른 속성을 수정할 수도 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

선택

- 작업 그룹에서 Active Directory 도메인으로 SMB 서버 이동:

- a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. 작업 그룹에서 Active Directory 도메인으로 SMB 서버를 이동합니다: 'vserver cifs modify -vserver_vserver_name_-domain_domain_name_'

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=_example_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

- 작업 그룹에서 다른 작업 그룹으로 SMB 서버 이동:

- a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버의 워크그룹을 수정합니다. 'vserver cifs modify -vserver_vserver_name_-workgroup_new_workgroup_name_'

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory 도메인에서 작업 그룹으로 SMB 서버 이동:

- a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버를 Active Directory 도메인에서 작업 그룹('vserver cifs modify -vserver_vserver_name_-workgroup_workgroup_name_')으로 이동합니다

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



워크그룹 모드로 전환하려면 모든 도메인 기반 기능을 사용하지 않도록 설정하고 지속적으로 사용 가능한 공유, 새도우 복제본 및 AES를 포함하여 시스템에서 해당 구성을 자동으로 제거해야 합니다. 그러나 "EXAMPLE.COM\userName" 같은 도메인 구성 공유 ACL은 제대로 작동하지 않지만 ONTAP에서는 제거할 수 없습니다. 명령이 완료된 후 외부 툴을 사용하여 가능한 한 빨리 이러한 공유 ACL을 제거합니다. AES가 활성화된 경우 "example.com" 도메인에서 Windows 계정을 비활성화할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다.

- 'vserver cifs modify' 명령의 적절한 매개 변수를 사용하여 다른 속성을 수정합니다.

옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

사용 가능한 **SMB** 서버 옵션

SMB 서버를 사용자 지정하는 방법을 고려할 때 사용할 수 있는 옵션을 파악하는 것이 유용합니다. 일부 옵션은 SMB 서버에서 일반적으로 사용되지만 일부 옵션은 특정 SMB 기능을 설정하고 구성하는 데 사용됩니다. SMB 서버 옵션은 'vserver cifs options modify' 옵션으로 제어됩니다.

다음 목록은 관리자 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * SMB 세션 시간 초과 값 구성 *

이 옵션을 구성하면 SMB 세션의 연결이 끊기까지의 유향 시간(초)을 지정할 수 있습니다. 유향 세션은 사용자가 클라이언트에 열려 있는 파일이나 디렉토리가 없는 세션입니다. 기본값은 900초입니다.

- * 기본 UNIX 사용자 구성 *

이 옵션을 구성하면 SMB 서버에서 사용하는 기본 UNIX 사용자를 지정할 수 있습니다. ONTAP는 ""pcuser""(UID 65534)라는 기본 사용자를 자동으로 만들고 ""pcuser""(GID가 65534)라는 그룹을 만든 다음 기본 사용자를 ""pcuser"" 그룹에 추가합니다. SMB 서버를 생성하면 ONTAP는 자동으로 ""pcuser""를 기본 UNIX 사용자로 구성합니다.

- * 게스트 UNIX 사용자 구성 *

이 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 매핑될 UNIX 사용자의 이름을 지정할 수 있으므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결할 수 있습니다. 기본적으로 이 옵션은 구성되지 않음(기본값 없음)이므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결하도록 허용하지 않습니다.

- * 모드 비트에 대한 읽기 권한 실행 활성화 또는 비활성화 *

이 옵션을 설정하거나 해제하면 UNIX 실행 가능 비트가 설정되지 않은 경우에도 SMB 클라이언트가 읽기 액세스 권한이 있는 UNIX 모드 비트를 사용하여 실행 파일을 실행하도록 허용할지 여부를 지정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

- * NFS 클라이언트에서 읽기 전용 파일을 삭제하는 기능을 활성화 또는 비활성화합니다

이 옵션을 설정하거나 해제하면 NFS 클라이언트가 읽기 전용 속성이 설정된 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. NTFS 삭제 의미 체계에서는 읽기 전용 특성이 설정된 경우 파일 또는 폴더를 삭제할 수 없습니다. UNIX 삭제 의미 체계는 읽기 전용 비트를 무시하고 상위 디렉토리 권한을 사용하여 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. 기본 설정은 사용 안 함 으로 NTFS 삭제 의미를 가져옵니다.

- * Windows 인터넷 이름 서비스 서버 주소 구성 *

이 옵션을 구성하면 WINS(Windows Internet Name Service) 서버 주소 목록을 심표로 구분된 목록으로 지정할 수 있습니다. IPv4 주소를 지정해야 합니다. IPv6 주소는 지원되지 않습니다. 기본값이 없습니다.

다음 목록은 고급 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * CIFS 사용자에게 UNIX 그룹 권한 부여 *

이 옵션을 구성하면 파일 소유자가 아닌 수신 CIFS 사용자에게 그룹 권한을 부여할 수 있는지 여부를 결정합니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수를 "true"로 설정하면 해당 파일에 대한 그룹 권한이 부여됩니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수가 "false"로 설정된 경우 일반 UNIX 규칙을 적용하여 파일 권한을 부여할 수 있습니다. 이 매개 변수는 권한이 '모드 비트'로 설정되어 있고 NTFS 또는 NFSv4 보안 모드가 있는 파일에는 적용되지 않는 UNIX 보안 스타일 파일에 적용됩니다. 기본 설정은 false입니다.

- * SMB 1.0 * 활성화 또는 비활성화

SMB 1.0은 ONTAP 9.3에서 SMB 서버가 생성된 SVM에서 기본적으로 비활성화되어 있습니다.



ONTAP 9.3부터는 ONTAP 9.3에서 생성된 새 SMB 서버에 대해 SMB 1.0이 기본적으로 사용되지 않습니다. 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

- * SMB 2.x * 활성화 또는 비활성화

SMB 2.0은 LIF 페일오버를 지원하는 최소 SMB 버전입니다. SMB 2.x를 비활성화하면 ONTAP도 자동으로 SMB 3.X를 비활성화합니다

SMB 2.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.0 * 활성화 또는 비활성화

SMB 3.0은 지속적으로 사용 가능한 공유를 지원하는 최소 SMB 버전입니다. Windows Server 2012 및 Windows 8은 SMB 3.0을 지원하는 최소 Windows 버전입니다.

SMB 3.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.1 * 활성화 또는 비활성화

Windows 10은 SMB 3.1을 지원하는 유일한 Windows 버전입니다.

SMB 3.1은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * ODX 복사 오프로드 설정 또는 해제 *

ODX 복사 오프로드는 Windows 클라이언트에서 지원하는 데 자동으로 사용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- * ODX 복사 오프로드에 대한 직접 복사 메커니즘 설정 또는 해제 *

직접 복사 메커니즘은 Windows 클라이언트가 복사 진행 중에 파일이 변경되지 않도록 하는 모드에서 복사본의 소스 파일을 열려고 할 때 복제 오프로드 작업의 성능을 향상시킵니다. 기본적으로 직접 복사 메커니즘은 활성화되어 있습니다.

- * 자동 노드 참조 활성화 또는 비활성화 *

SMB 서버는 자동 노드 조회를 통해 요청된 공유를 통해 액세스한 데이터를 호스팅하는 노드에 대한 데이터 LIF 로컬 클라이언트를 자동으로 참조합니다.

- * SMB*에 대한 내보내기 정책 활성화 또는 비활성화

이 옵션은 기본적으로 비활성화되어 있습니다.

- * 교차점을 재분석 지점으로 사용하여 활성화 또는 비활성화 *

이 옵션을 활성화하면 SMB 서버는 재분석 지점으로 SMB 클라이언트에 연결 지점을 노출합니다. 이 옵션은 SMB 2.x 또는 SMB 3.0 연결에만 유효합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 옵션은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * TCP 연결당 최대 동시 작업 수 구성 *

기본값은 255입니다.

- * 로컬 Windows 사용자 및 그룹 기능 활성화 또는 비활성화 *

이 옵션은 기본적으로 활성화되어 있습니다.

- * 로컬 Windows 사용자 인증 활성화 또는 비활성화 *

이 옵션은 기본적으로 활성화되어 있습니다.

- * VSS 새도우 복제본 기능 활성화 또는 비활성화 *

ONTAP는 새도우 복제본 기능을 사용하여 SMB를 통한 Hyper-V 솔루션을 사용하여 저장된 데이터의 원격 백업을 수행합니다.

이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 새도 복사본 디렉토리 수준 구성 *

이 옵션을 구성하면 새도우 복제본 기능을 사용할 때 새도우 복제본을 생성할 디렉토리의 최대 깊이를 정의할 수 있습니다.

이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 이름 매핑에 대한 다중 도메인 검색 기능을 활성화 또는 비활성화합니다 *

활성화된 경우, UNIX 사용자가 Windows 사용자 이름의 도메인 부분에서 와일드카드(*)를 사용하여 Windows 도메인 사용자에게 매핑되면(예: *\\Joe) ONTAP는 양방향 트러스트가 있는 모든 도메인에서 홈 도메인으로 지정된 사용자를 검색합니다. 홈 도메인은 SMB 서버의 컴퓨터 계정이 포함된 도메인입니다.

양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 이 옵션을 사용하도록 설정하고 기본 설정 목록을 구성하면 다중 도메인 이름 매핑 검색을 수행하는 데 기본 설정 목록이 사용됩니다.

기본값은 다중 도메인 이름 매핑 검색을 사용하는 것입니다.

- * 파일 시스템 섹터 크기 구성 *

이 옵션을 구성하면 ONTAP에서 SMB 클라이언트에 보고하는 파일 시스템 섹터 크기를 바이트 단위로 구성할 수 있습니다. 이 옵션에는 4096과 512의 두 가지 유효한 값이 있습니다. 기본값은 4096입니다. Windows 응용 프로그램이 512바이트의 섹터 크기만 지원하는 경우 이 값을 '512'로 설정해야 할 수 있습니다.

- * 동적 액세스 제어 활성화 또는 비활성화 *

이 옵션을 활성화하면 DAC(Dynamic Access Control)를 사용하여 중앙 액세스 정책을 스테이징하고 그룹 정책 개체를 사용하여 중앙 액세스 정책을 구현하는 등 SMB 서버의 개체를 보호할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

이 옵션은 SVM에서만 지원됩니다.

- * 인증되지 않은 세션에 대한 액세스 제한 설정(익명 제한) *

이 옵션을 설정하면 인증되지 않은 세션에 대한 액세스 제한이 결정됩니다. 제한 사항은 익명 사용자에게 적용됩니다. 기본적으로 익명 사용자에게 대한 액세스 제한은 없습니다.

- * UNIX 효과적인 보안(UNIX 보안 스타일 볼륨 또는 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)이 있는 볼륨에서 NTFS ACL 표시를 활성화 또는 비활성화합니다. *

이 옵션을 설정하거나 해제하면 UNIX 보안이 있는 파일 및 폴더의 파일 보안이 SMB 클라이언트에 제공되는 방식이 결정됩니다. 이 옵션을 설정하면 ONTAP는 UNIX 보안 기능이 있는 볼륨의 파일 및 폴더를 NTFS ACL을 사용한 NTFS 파일 보안으로 SMB 클라이언트에 제공합니다. 사용하지 않도록 설정하면 ONTAP는 UNIX 보안이 설정된 볼륨을 파일 보안 없이 FAT 볼륨으로 제공합니다. 기본적으로 볼륨은 NTFS ACL을 사용한 NTFS 파일 보안을 갖는 것으로 표시됩니다.

- * SMB 가짜 열기 기능 활성화 또는 비활성화 *

이 기능을 사용하면 파일 및 디렉토리에 대한 속성 정보를 쿼리할 때 ONTAP에서 열기 및 닫기 요청을 수행하는 방식을 최적화하여 SMB 2.x 및 SMB 3.0 성능을 향상시킬 수 있습니다. 기본적으로 SMB 가짜 열기 기능이 활성화됩니다. 이 옵션은 SMB 2.x 이상에서 만들어진 연결에만 유용합니다.

- * UNIX 확장 활성화 또는 비활성화 *

이 옵션을 활성화하면 SMB 서버에서 UNIX 확장이 활성화됩니다. UNIX 확장을 사용하면 POSIX/UNIX 스타일 보안을 SMB 프로토콜을 통해 표시할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

Mac OSX 클라이언트와 같은 UNIX 기반 SMB 클라이언트가 있는 경우 UNIX 확장을 활성화해야 합니다. UNIX 확장을 사용하면 SMB 서버가 POSIX/UNIX 보안 정보를 SMB를 통해 UNIX 기반 클라이언트로 전송한 다음 보안 정보를 POSIX/UNIX 보안으로 변환합니다.

• * 간단한 이름 검색 지원 활성화 또는 비활성화 *

이 옵션을 활성화하면 SMB 서버가 짧은 이름으로 검색을 수행할 수 있습니다. 이 옵션을 사용하는 검색 쿼리는 8.3 파일 이름과 긴 파일 이름을 일치시키려고 합니다. 이 파라미터의 기본값은 'false'입니다.

• * DFS 기능 자동 보급에 대한 지원 활성화 또는 비활성화 *

이 옵션을 활성화 또는 비활성화하면 SMB 서버가 공유에 연결하는 SMB 2.x 및 SMB 3.0 클라이언트에 DFS 기능을 자동으로 보급할지 여부를 결정합니다. ONTAP은 SMB 액세스를 위한 심볼 링크 구현에 DFS 조회를 사용합니다. 활성화된 경우 SMB 서버는 심볼 링크 액세스가 설정되었는지 여부에 관계없이 항상 DFS 기능을 알립니다. 비활성화된 경우 SMB 서버는 클라이언트가 심볼 링크 액세스가 설정된 공유에 연결할 때만 DFS 기능을 알립니다.

• * 최대 SMB 크레딧 수 구성 *

ONTAP 9.4부터, '-max-credits' 옵션을 구성하면 클라이언트와 서버가 SMB 버전 2 이상을 실행하는 경우 SMB 연결에 부여할 크레딧 수를 제한할 수 있습니다. 기본값은 128입니다.

• * SMB 멀티 채널 * 에 대한 지원 활성화 또는 비활성화

ONTAP 9.4 이상 릴리스에서 '-is-multichannel-enabled' 옵션을 활성화하면 SMB 서버는 클러스터와 해당 클라이언트에 적절한 NIC가 구축될 때 단일 SMB 세션에 대해 여러 개의 연결을 설정할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다. 이 파라미터의 기본값은 'false'입니다.

SMB 멀티 채널이 활성화되면 다음 매개 변수도 지정할 수 있습니다.

- 다중 채널 세션당 허용되는 최대 연결 수입니다. 이 매개 변수의 기본값은 32입니다.
- Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 이 매개 변수의 기본값은 256입니다.

SMB 서버 옵션 구성

SVM(스토리지 가상 시스템)에서 SMB 서버를 생성한 후에는 언제든지 SMB 서버 옵션을 구성할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

SMB 서버 옵션을 구성하려면...	명령 입력...
관리 권한 수준에서 설정합니다	'vserver cifs options modify -vserver_vserver_name options_'

SMB 서버 옵션을 구성하려면...	명령 입력...
고급 권한 수준에서 설정합니다	a. 세트 프리빌리지 고급 b. 'vserver cifs options modify -vserver_vserver_name options_ c. 'Set-Privilege admin'입니다

SMB 서버 옵션 구성에 대한 자세한 내용은 'vserver cifs options modify' 명령의 man 페이지를 참조하십시오.

SMB 사용자에게 UNIX 그룹 권한 부여 를 구성합니다

들어오는 SMB 사용자가 파일 소유자가 아닌 경우에도 파일 또는 디렉토리에 액세스할 수 있는 그룹 권한을 부여하도록 이 옵션을 구성할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX 그룹 권한 부여를 적절히 구성합니다.

원하는 경우	명령을 입력합니다
사용자가 파일 소유자가 아니더라도 파일 또는 디렉토리에 대한 액세스를 활성화하여 그룹 권한을 얻습니다	'vserver cifs options modify --grant-unix-group-perms-to-others true'
파일 또는 디렉토리에 대한 액세스를 비활성화하여 사용자가 파일 소유자가 아니더라도 그룹 권한을 얻습니다	'vserver cifs options modify --grant-unix-group-perms-to-others false'

3. 이 옵션이 원하는 값으로 설정되어 있는지 확인합니다. 'vserver cifs options show --fields grant-unix-group-perms-to-others'
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

익명 사용자의 액세스 제한을 구성합니다

기본적으로 인증되지 않은 익명 사용자(*null user* 라고도 함)는 네트워크의 특정 정보에 액세스할 수 있습니다. SMB 서버 옵션을 사용하여 익명 사용자의 액세스 제한을 구성할 수 있습니다.

이 작업에 대해

익명 제한 SMB 서버 옵션은 Windows의 RestrictAnonymous 레지스트리 항목에 해당합니다.

익명 사용자는 사용자 이름 및 세부 정보, 계정 정책 및 공유 이름을 포함하여 네트워크의 Windows 호스트에서 특정 유형의 시스템 정보를 나열하거나 열거할 수 있습니다. 다음 세 가지 액세스 제한 설정 중 하나를 지정하여 익명 사용자에게 대한 액세스를 제어할 수 있습니다.

값	설명
무제한(기본값)	익명 사용자에게 대한 액세스 제한을 지정하지 않습니다.
번호 매기기	익명 사용자에게 대해서만 열거를 제한하도록 지정합니다.
"접근 불가"	익명 사용자에게 대한 액세스가 제한되도록 지정합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익명 제한 설정: 'vserver cifs options modify -vserver _vserver_name_ -restrict-anonymous{no-restriction|no-enumeration|no-access}'를 구성합니다
3. 옵션이 원하는 값('vserver cifs options show -vserver _vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

사용 가능한 SMB 서버 옵션

UNIX 보안 스타일 데이터를 위해 **SMB** 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

UNIX 보안 스타일 데이터 개요를 위해 **SMB** 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화하여 UNIX 보안 스타일 데이터용 파일 보안을 SMB 클라이언트에 제공하는 방법을 선택할 수 있습니다. 각 설정에는 비즈니스 요구 사항에 가장 적합한 설정을 선택해야 한다는 점을 이해해야 합니다.

기본적으로 ONTAP은 UNIX 보안 스타일 볼륨에 대한 UNIX 권한을 SMB 클라이언트에 NTFS ACL로 제공합니다. 다음과 같이 이 방법이 필요한 시나리오가 있습니다.

- Windows 속성 상자의 * 보안 * 탭을 사용하여 UNIX 권한을 보고 편집하려는 경우

UNIX 시스템에서 작업이 허용되지 않는 경우 Windows 클라이언트에서 권한을 수정할 수 없습니다. 예를 들어 UNIX 시스템에서는 이 작업을 허용하지 않으므로 소유하지 않는 파일의 소유권을 변경할 수 없습니다. 이 제한 사항으로 인해 SMB 클라이언트가 파일 및 폴더에 설정된 UNIX 권한을 우회하지 못합니다.

- 사용자는 Microsoft Office와 같은 특정 Windows 응용 프로그램을 사용하여 UNIX 보안 스타일 볼륨에서 파일을 편집 및 저장하고 있습니다. 여기서 ONTAP는 저장 작업 중에 UNIX 권한을 유지해야 합니다.
- 사용자 환경에는 사용 중인 파일에 대해 NTFS ACL을 읽을 것으로 예상되는 특정 Windows 애플리케이션이 있습니다.

경우에 따라 UNIX 사용 권한을 NTFS ACL로 표시하지 않도록 설정할 수 있습니다. 이 기능을 비활성화하면 ONTAP는 UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 제공합니다. UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 표시하는 이유는 다음과 같습니다.

- UNIX 클라이언트에서 마운트를 사용하여 UNIX 사용 권한만 변경할 수 있습니다.

UNIX 보안 스타일 볼륨이 SMB 클라이언트에 매핑된 경우에는 보안 탭을 사용할 수 없습니다. 매핑된 드라이브는

파일 권한이 없는 FAT 파일 시스템으로 포맷된 것 같습니다.

- 액세스 파일 및 폴더에 NTFS ACL을 설정하는 SMB를 통해 애플리케이션을 사용 중이며, UNIX 보안 스타일 볼륨에 데이터가 있는 경우 오류가 발생할 수 있습니다.

ONTAP가 볼륨을 FAT로 보고하는 경우 응용 프로그램은 ACL을 변경하지 않습니다.

관련 정보

[FlexVol 볼륨에서 보안 스타일 구성](#)

[Qtree에서 보안 스타일 구성](#)

UNIX 보안 스타일 데이터에 대한 **NTFS ACL** 표시를 활성화 또는 비활성화합니다

UNIX 보안 스타일 데이터(UNIX 보안 스타일 볼륨 및 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)를 위해 SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화할 수 있습니다.

이 작업에 대해

이 옵션을 설정하면 ONTAP는 효율적인 UNIX 보안 스타일을 사용하는 볼륨의 파일 및 폴더를 NTFS ACL을 갖는 것으로 SMB 클라이언트에 제공합니다. 이 옵션을 비활성화하면 볼륨이 SMB 클라이언트에 FAT 볼륨으로 표시됩니다. 기본값은 NTFS ACL을 SMB 클라이언트에 제공하는 것입니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX NTFS ACL 옵션 설정을 구성합니다. 'vserver cifs options modify -vserver_vserver_name_-is-unix-NT -acl-enabled{true|false}'
3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

ONTAP에서 **UNIX** 사용 권한을 유지하는 방법

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

Windows 보안 탭을 사용하여 **UNIX** 사용 권한을 관리합니다

SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

SMB 서버 보안 설정을 관리합니다

ONTAP가 SMB 클라이언트 인증을 처리하는 방법

사용자가 SVM에 포함된 데이터에 액세스하기 위해 SMB 연결을 생성하려면 먼저 SMB 서버가 속해 있는 도메인에서 인증을 받아야 합니다. SMB 서버는 Kerberos와 NTLM(NTLMv1 또는 NTLMv2)의 두 가지 인증 방법을 지원합니다. Kerberos는 도메인 사용자를 인증하는 데 사용되는 기본 방법입니다.

Kerberos 인증

ONTAP는 인증된 SMB 세션을 생성할 때 Kerberos 인증을 지원합니다.

Kerberos는 Active Directory의 기본 인증 서비스입니다. Kerberos 서버 또는 Kerberos KDC(Key Distribution Center) 서비스는 Active Directory에 보안 원칙에 대한 정보를 저장하고 검색합니다. NTLM 모델과 달리 SMB 서버와 같은 다른 컴퓨터와 세션을 설정하려는 Active Directory 클라이언트는 KDC에 직접 문의하여 세션 자격 증명을 얻습니다.

NTLM 인증

NTLM 클라이언트 인증은 암호를 기반으로 사용자별 비밀번호에 대한 공유 지식을 기반으로 하는 본인 확인 응답 프로토콜을 사용하여 수행됩니다.

사용자가 로컬 Windows 사용자 계정을 사용하여 SMB 연결을 만들면 NTLMv2를 사용하여 SMB 서버에서 로컬로 인증이 수행됩니다.

SVM 재해 복구 구성의 SMB 서버 보안 설정 지침

ID가 보존되지 않는 재해 복구 대상으로 구성된 SVM(SnapMirror 구성에서 'identity-preserve' 옵션이 'false'로 설정됨)을 생성하기 전에 SVM 대상에서 SMB 서버 보안 설정이 관리되는 방식을 알아야 합니다.

- 기본이 아닌 SMB 서버 보안 설정은 대상에 복제되지 않습니다.

대상 SVM에서 SMB 서버를 생성할 때 모든 SMB 서버 보안 설정이 기본값으로 설정됩니다. SVM 재해 복구 대상이 초기화, 업데이트 또는 재동기화되면 소스의 SMB 서버 보안 설정이 타겟으로 복제되지 않습니다.

- 기본이 아닌 SMB 서버 보안 설정을 수동으로 구성해야 합니다.

소스 SVM에 기본값이 아닌 SMB 서버 보안 설정이 구성되어 있는 경우 SnapMirror 관계가 깨진 후, 대상이 읽기-쓰기 상태가 되면 대상 SVM에서 동일한 설정을 수동으로 구성해야 합니다.

SMB 서버 보안 설정에 대한 정보를 표시합니다

SMB 서버 보안 설정에 대한 정보를 SVM(스토리지 가상 머신)에 표시할 수 있습니다. 이 정보를 사용하여 보안 설정이 올바른지 확인할 수 있습니다.

이 작업에 대해

표시된 보안 설정은 해당 개체의 기본값이거나 ONTAP CLI를 사용하거나 Active Directory 그룹 정책 개체(GPO)를 사용하여 구성된 기본값이 아닌 값일 수 있습니다.

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 SMB 서버에 대해 "vserver cifs security show" 명령을 사용하지 마십시오.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 모든 보안 설정	'vserver cifs security show -vserver_vserver_name_'
SVM의 특정 보안 설정 또는 설정	'vserver cifs security show -vserver_vserver_name_ - 필드 [fieldname,...]'를 입력하면 '-fields?'를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

예

다음 예는 SVM VS1 보안 설정을 모두 보여줍니다.

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

표시되는 설정은 실행 중인 ONTAP 버전에 따라 다릅니다.

다음 예에서는 SVM VS1 Kerberos 클럭 편중을 보여 줍니다.

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew
```

```
vserver kerberos-clock-skew
-----
vs1      5
```

관련 정보

[GPO 구성에 대한 정보 표시](#)

로컬 **SMB** 사용자에게 대해 필요한 암호 복잡성을 설정하거나 해제합니다

필수 비밀번호 복잡성은 스토리지 가상 시스템(SVM)의 로컬 SMB 사용자를 위해 향상된 보안을 제공합니다. 필요한 암호 복잡성 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지 않도록 설정하고 언제든지 다시 사용하도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버에서 로컬 사용자, 로컬 그룹 및 로컬 사용자 인증을 설정해야 합니다.



이 작업에 대해

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 CIFS 서버에 대해 "vserver cifs security modify" 명령을 사용하면 안 됩니다.

단계

1. 다음 작업 중 하나를 수행합니다.

로컬 SMB 사용자에게 대한 암호 복잡성에 필요한 경우...	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required false'

2. 필요한 암호 복잡성에 대한 보안 설정을 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 용 로컬 SMB 사용자에게 대해 필요한 암호 복잡성이 활성화된 것을 보여 줍니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password  
-complexity-required true  
  
cluster1::> vserver cifs security show -vserver vs1 -fields is-password-  
complexity-required  
vserver is-password-complexity-required  
-----  
vs1      true
```

관련 정보

[CIFS 서버 보안 설정에 대한 정보를 표시합니다](#)

[로컬 사용자 및 그룹을 인증 및 인증에 사용합니다](#)

[로컬 사용자 암호 요구 사항](#)

[로컬 사용자 계정 암호 변경](#)

CIFS 서버 Kerberos 보안 설정을 수정합니다

허용되는 최대 Kerberos 클록 비뿔어짐 시간, Kerberos 티켓 수명 및 티켓 갱신 최대 일 수를 비롯한 특정 CIFS 서버 Kerberos 보안 설정을 수정할 수 있습니다.

이 작업에 대해

'vserver cifs security modify' 명령을 사용하여 CIFS 서버 Kerberos 설정을 수정하면 '-vserver' 매개 변수로 지정한 단일 SVM(스토리지 가상 머신)에서만 설정이 수정됩니다. Active Directory 그룹 정책 개체(GPO)를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM에 대한 Kerberos 보안 설정을 중앙에서 관리할 수 있습니다.

단계

1. 다음 작업 중 하나 이상을 수행합니다.

원하는 작업	입력...
허용되는 최대 Kerberos 클럭 편중 시간을 분(9.13.1 이상) 또는 초(9.12.1 이하)로 지정합니다.	<code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-clock-suts_integer_in_minutes_'</code> 기본 설정은 5분입니다.
Kerberos 티켓 수명(시간)을 지정합니다.	<code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-티켓-age integer_in_hours'</code> 를 선택합니다 기본 설정은 10시간입니다.
티켓 갱신 최대 일 수를 지정하십시오.	<code>'vserver cifs security modify -vserver_vserver_name_- Kerberos - renew - age_integer_in_days _'</code> 기본 설정은 7일입니다.
모든 KDC가 도달할 수 없음으로 표시되는 KDC의 소켓에 대한 시간 제한을 지정합니다.	<code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-KDC -timeout_integer_in_seconds _'</code> 기본 설정은 3초입니다.

2. Kerberos 보안 설정을 확인합니다.

`'vserver cifs security show -vserver_vserver_name_'`

예

다음 예에서는 Kerberos 보안을 다음과 같이 변경합니다. ""Kerberos Clock Skew""는 3분으로 설정되고 ""Kerberos Ticket Age""는 SVM VS1 v1의 경우 8시간으로 설정됩니다.


```
cluster1::> vservice cifs security modify -vservice vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vservice cifs security show -vservice vs1

Vservice: vs1

Kerberos Clock Skew: 3 minutes
Kerberos Ticket Age: 8 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
```

관련 정보

"CIFS 서버 보안 설정에 대한 정보를 표시합니다"

"지원되는 GPO"

"CIFS 서버에 그룹 정책 객체 적용"

SMB 서버 최소 인증 보안 수준을 설정합니다

SMB 클라이언트 액세스에 대한 비즈니스 보안 요구 사항을 충족하도록 SMB 서버에서 `_LMCompatibilityLevel_` 이라고도 하는 SMB 서버 최소 보안 수준을 설정할 수 있습니다. 최소 보안 수준은 SMB 서버가 SMB 클라이언트에서 허용하는 최소 보안 토큰입니다.



이 작업에 대해

- 워크그룹 모드의 SMB 서버는 NTLM 인증만 지원합니다. Kerberos 인증은 지원되지 않습니다.
- `LMCompatibilityLevel` 관리자 인증이 아닌 SMB 클라이언트 인증에만 적용됩니다.

최소 인증 보안 수준을 지원되는 네 가지 보안 수준 중 하나로 설정할 수 있습니다.

값	설명
lm-NTLM-NTLMv2-KRB(기본값)	SVM(스토리지 가상 시스템)은 LM, NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다.
NTLM-NTLMv2-KRB	SVM은 NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 인증을 거부합니다.

값	설명
NTLMv2-KRB	SVM은 NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 및 NTLM 인증을 거부합니다.
KRB	SVM은 Kerberos 인증 보안만 수락합니다. SVM은 LM, NTLM 및 NTLMv2 인증을 거부합니다.

단계

1. 최소 인증 보안 수준을 설정합니다. 'vserver cifs security modify -vserver_vserver_name_-lm -compatibility -level{lm-NTLM-NTLMv2-KRB | NTLM-NTLMv2-KRB | NTLMv2-KRB | KRB | KRB}'
2. 인증 보안 수준이 원하는 수준('vserver cifs security show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다

관련 정보

[Kerberos 기반 통신을 위한 AES 암호화 활성화 또는 비활성화](#)

AES 암호화를 사용하여 Kerberos 기반 통신을 위한 강력한 보안을 구성합니다

Kerberos 기반 통신을 사용하여 보안을 강화하기 위해 SMB 서버에서 AES-256 및 AES-128 암호화를 활성화할 수 있습니다. 기본적으로 SVM에서 SMB 서버를 생성할 때 AES(고급 암호화 표준) 암호화가 사용되지 않습니다. AES 암호화로 제공되는 강력한 보안을 활용하려면 이 기능을 활성화해야 합니다.

SMB를 위한 Kerberos 관련 통신은 SVM에서 SMB 서버를 생성하는 동안이나 SMB 세션 설정 단계에서 사용됩니다. SMB 서버는 Kerberos 통신을 위해 다음과 같은 암호화 유형을 지원합니다.

- AES 256
- AES 128
- DES
- RC4-HMAC

Kerberos 통신에 가장 높은 보안 암호화 유형을 사용하려면 SVM에서 Kerberos 통신에 AES 암호화를 사용하도록 설정해야 합니다.

SMB 서버가 생성되면 도메인 컨트롤러는 Active Directory에 컴퓨터 시스템 계정을 만듭니다. 이때 KDC는 특정 컴퓨터 계정의 암호화 기능을 인식합니다. 그런 다음 인증 중에 클라이언트가 서버에 제공하는 서비스 티켓을 암호화하기 위해 특정 암호화 유형을 선택합니다.

ONTAP 9.12.1부터 Active Directory(AD) KDC에 알릴 암호화 유형을 지정할 수 있습니다. 를 사용할 수 있습니다 -advertised-enc-types 권장 암호화 유형을 활성화하는 옵션으로, 약한 암호화 유형을 비활성화하는 데 사용할 수 있습니다. 자세한 내용을 알아보십시오 ["Kerberos 기반 통신을 위한 암호화 유형을 활성화 및 비활성화합니다"](#).



인텔 AES 새 명령어(인텔 AES NI)는 SMB 3.0에서 사용할 수 있으며, AES 알고리즘을 개선하고 지원되는 프로세서 제품군에서 데이터 암호화를 가속화합니다. SMB 3.1.1부터 AES-128-GCM은 SMB 암호화에 사용되는 해시 알고리즘으로 AES-128-CCM을 대체합니다.

관련 정보

Kerberos 기반 통신을 위해 **AES** 암호화를 사용하거나 사용하지 않도록 설정합니다

Kerberos 기반 통신에서 가장 강력한 보안을 활용하려면 SMB 서버에서 AES-256 및 AES-128 암호화를 사용해야 합니다. ONTAP 9.13.1부터 AES 암호화는 기본적으로 사용하도록 설정됩니다. SMB 서버가 AD(Active Directory) KDC와 Kerberos 기반 통신을 위해 AES 암호화 유형을 선택하지 않도록 하려면 AES 암호화를 사용하지 않도록 설정할 수 있습니다.

AES 암호화가 기본적으로 사용되는지 여부와 암호화 유형을 지정하는 옵션이 있는지 여부는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	AES 암호화 사용...	암호화 유형을 지정할 수 있습니까?
9.13.1 이상	기본적으로 사용됩니다	예
9.12.1	수동	예
9.11.1 이하	수동	아니요

ONTAP 9.12.1부터 AES 암호화는 `을` 사용하여 활성화 및 비활성화됩니다 `-advertised-enc-types` 옵션: AD KDC에 보급된 암호화 유형을 지정할 수 있습니다. 기본 설정은 `입니다 rc4 및 des` 그러나 AES 유형이 지정되면 AES 암호화가 활성화됩니다. 이 옵션을 사용하여 약한 RC4 및 DES 암호화 유형을 명시적으로 비활성화할 수도 있습니다. ONTAP 9.11.1 이하 버전에서는 을 사용해야 합니다 -is-aes-encryption-enabled AES 암호화를 활성화 및 비활성화하는 옵션과 암호화 유형을 지정할 수 없습니다.`

보안을 강화하기 위해 SVM(Storage Virtual Machine)은 AES 보안 옵션을 수정할 때마다 AD에서 시스템 계정 암호를 변경합니다. 암호를 변경하려면 컴퓨터 계정이 포함된 OU(조직 구성 단위)에 대한 관리 AD 자격 증명이 필요할 수 있습니다.

SVM이 ID가 보존되지 않는 재해 복구 대상으로 구성된 경우(`-identity-preserve` 옵션이 `로 설정되어 있습니다 false SnapMirror 구성에서 기본 SMB 서버가 아닌 보안 설정은 대상에 복제되지 않습니다. 소스 SVM에서 AES 암호화를 사용하도록 설정한 경우 수동으로 활성화해야 합니다.`

예 1. 단계

ONTAP 9.12.1 이상

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우...	명령 입력...
활성화됨	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
사용 안 함	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

◦ 참고: * -is-aes-encryption-enabled 옵션은 ONTAP 9.12.1에서 사용되지 않으며 이후 릴리스에서 제거될 수 있습니다.

2. AES 암호화가 필요에 따라 활성화 또는 비활성화되었는지 확인합니다. `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-----
vs1      aes-128,aes-256
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsserver cifs security modify -vsserver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsserver cifs security show -vsserver vs2 -fields advertised-
enc-types
```

```
vsserver  advertised-enc-types
-----  -
vs2       aes-128,aes-256
```

ONTAP 9.11.1 이전 버전

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우...	명령 입력...
활성화됨	'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled true'
사용 안 함	'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled false'

2. AES 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vsserver cifs security show -vsserver vsserver_name -fields is -aes-encryption-enabled'

AES 암호화가 활성화된 경우 is-aes-encryption-enabled 필드가 true로 표시되고, 비활성화된 경우 false로 표시됩니다.

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vsriver cifs security modify -vsriver vs1 -is-aes
-encryption-enabled true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-aes-
encryption-enabled

vsriver  is-aes-encryption-enabled
-----
vs1      true
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vsriver cifs security show -vsriver vs2 -fields is-aes-
encryption-enabled

vsriver  is-aes-encryption-enabled
-----
vs2      true
```

SMB 서명을 사용하여 네트워크 보안을 강화합니다

SMB 서명을 사용하여 네트워크 보안 개요를 개선합니다

SMB 서명을 사용하면 SMB 서버와 클라이언트 사이의 네트워크 트래픽이 손상되지 않도록 할 수 있으며, 재생 공격을 차단하여 이 작업을 수행합니다. 기본적으로 ONTAP는 클라이언트가 요청할 때 SMB 서명을 지원합니다. 필요에 따라 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버를 구성할 수 있습니다.

SMB 서명 정책이 CIFS 서버와의 통신에 미치는 영향

CIFS 서버 SMB 서명 보안 설정 외에도 Windows 클라이언트의 두 SMB 서명 정책은 클라이언트와 CIFS 서버 간의 디지털 통신 서명을 제어합니다. 비즈니스 요구 사항에 맞게 설정을 구성할 수 있습니다.

클라이언트 SMB 정책은 MMC(Microsoft Management Console) 또는 Active Directory GPO를 사용하여 구성되는 Windows 로컬 보안 정책 설정을 통해 제어됩니다. 클라이언트 SMB 서명 및 보안 문제에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

다음은 Microsoft 클라이언트에 대한 두 가지 SMB 서명 정책에 대한 설명입니다.

- 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)'

이 설정은 클라이언트의 SMB 서명 기능이 설정되었는지 여부를 제어합니다. 기본적으로 활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 CIFS 서버와의 클라이언트 통신은 CIFS 서버의 SMB 서명 설정에 따라 달라집니다.

- 마이크로네트워크 클라이언트: 디지털 서명 통신(항상)

이 설정은 클라이언트가 서버와 통신하기 위해 SMB 서명을 필요로 하는지 제어합니다. 기본적으로 비활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 SMB 서명 동작은 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)' 및 CIFS 서버의 설정에 대한 정책 설정을 기반으로 합니다.



환경에 SMB 서명이 필요하도록 구성된 Windows 클라이언트가 포함된 경우 CIFS 서버에서 SMB 서명을 설정해야 합니다. 그렇지 않으면 CIFS 서버가 이러한 시스템에 데이터를 제공할 수 없습니다.

클라이언트 및 CIFS 서버 SMB 서명 설정의 효과적인 결과는 SMB 세션이 SMB 1.0 또는 SMB 2.x 이상을 사용하는지 여부에 따라 달라집니다.

다음 표에는 세션이 SMB 1.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

클라이언트	ONTAP — 서명이 필요하지 않습니다	ONTAP — 서명이 필요합니다
서명이 비활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 비활성화되었으며 필수입니다	서명됨	서명됨
서명이 설정되어 있어야 합니다	서명됨	서명됨



클라이언트에서 서명이 비활성화되었지만 CIFS 서버에서 필요한 경우 이전 Windows SMB 1 클라이언트와 일부 비 Windows SMB 1 클라이언트가 연결되지 않을 수 있습니다.

다음 표에는 세션에서 SMB 2.x 또는 SMB 3.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.



SMB 2.x 및 SMB 3.0 클라이언트의 경우 SMB 서명이 항상 사용하도록 설정됩니다. 비활성화할 수 없습니다.

클라이언트	ONTAP — 서명이 필요하지 않습니다	ONTAP — 서명이 필요합니다
서명이 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 필요합니다	서명됨	서명됨

다음 표에는 기본 Microsoft 클라이언트 및 서버 SMB 서명 동작이 요약되어 있습니다.

프로토콜	해시 알고리즘입니다	활성화/비활성화할 수 있습니다	필요/필요하지 않습니다	클라이언트 기본값입니다	서버 기본값	DC 기본값
SMB 1.0	MD5	예	예	활성화됨(필요하지 않음)	사용 안 함(필수 아님)	필수 요소입니다
SMB 2.x	HMAC SHA-256	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다
SMB 3.0	AES-CMAC	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다



Microsoft는 더 이상 '고유 서명 통신(클라이언트에서 동의한 경우)' 또는 '고유 서명 통신(서버에서 동의한 경우)' 그룹 정책 설정을 사용할 것을 권장하지 않습니다. Microsoft는 또한 "EnableSecuritySignature" 레지스트리 설정을 더 이상 사용하지 않을 것을 권장합니다. 이러한 옵션은 SMB 1 동작에만 영향을 미치며 Digitally sign communications (Always)(항상 서명 통신) 그룹 정책 설정 또는 RequireSecuritySignature(요구 보안 서명) 레지스트리 설정으로 대체할 수 있습니다. 또한 Microsoft 블로그에서 자세한 정보를 얻을 수 있습니다. [The SMB 서명의 기본 사항\(SMB1 및 SMB2 모두 포함\)](#)

SMB 서명의 성능 영향

SMB 세션에서 SMB 서명을 사용하면 Windows 클라이언트와 주고 받는 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드) 모두에 영향을 미칩니다.

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 서명된 SMB 트래픽의 성능을 향상시킬 수 있습니다. SMB 서명 오프로드는 SMB 서명이 설정된 경우 기본적으로 설정됩니다.

향상된 SMB 서명 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 서명의 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경에서 테스트를 통해서만 확인할 수 있습니다.

대부분의 Windows 클라이언트는 서버에서 SMB 서명을 사용하는 경우 기본적으로 협상합니다. 일부 Windows 클라이언트에 대해 SMB 보호가 필요하고 SMB 서명으로 인해 성능 문제가 발생하는 경우 재생 공격에 대한 보호가 필요하지 않은 Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정할 수 있습니다. Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

SMB 서명 구성을 위한 권장 사항입니다

SMB 클라이언트와 CIFS 서버 간에 SMB 서명 동작을 구성하여 보안 요구 사항을 충족할 수 있습니다. CIFS 서버에서 SMB 서명을 구성할 때 선택하는 설정은 보안 요구 사항에 따라 다릅니다.

클라이언트 또는 CIFS 서버에서 SMB 서명을 구성할 수 있습니다. SMB 서명을 구성할 때 다음 권장 사항을 고려하십시오.

만약...	권장 사항...
클라이언트와 서버 간의 통신 보안을 강화하려는 경우	클라이언트에서 'Require Option(Sign Always)' 보안 설정을 활성화하여 클라이언트에서 SMB 서명이 필요하도록 합니다.
모든 SMB 트래픽이 특정 SVM(스토리지 가상 머신)에 서명하기를 원합니다	SMB 서명이 필요하도록 보안 설정을 구성하여 CIFS 서버에 SMB 서명이 필요합니다.

Windows 클라이언트 보안 설정 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

여러 데이터 **LIF**가 구성된 경우 **SMB** 서명을 위한 지침입니다

SMB 서버에서 필요한 SMB 서명을 설정하거나 해제하는 경우 SVM에 대한 여러 데이터 LIF 구성에 대한 지침을 숙지해야 합니다.

SMB 서버를 구성할 때 여러 데이터 LIF가 구성되어 있을 수 있습니다. 이 경우 DNS 서버에 동일한 SMB 서버 호스트 이름을 사용하는 CIFS 서버에 대한 여러 개의 "A" 레코드 항목이 포함되어 있고 각 항목은 고유한 IP 주소를 사용합니다. 예를 들어, 두 개의 데이터 LIF가 구성된 SMB 서버의 DNS 'A' 레코드 항목은 다음과 같습니다.

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

일반적으로 필요한 SMB 서명 설정을 변경하면 클라이언트의 새 연결만 SMB 서명 설정의 변경 사항에 영향을 받습니다. 그러나 이 동작에 대한 예외는 있습니다. 클라이언트가 공유에 대한 기존 연결을 가지고 있고, 원래 연결을 유지하면서 설정을 변경한 후 클라이언트가 동일한 공유에 대한 새 연결을 생성하는 경우가 있습니다. 이 경우 새로운 SMB 연결과 기존 SMB 연결이 모두 새로운 SMB 서명 요구 사항을 적용합니다.

다음 예제를 고려해 보십시오.

1. CLIENT1은 'O:\' 경로를 사용하여 SMB 서명이 필요 없이 공유에 연결합니다.
2. 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버 구성을 수정합니다.
3. CLIENT1은 '\:' 경로를 사용하여('O:\' 경로를 사용하여 연결을 유지하면서) 필요한 SMB 서명과 동일한 공유에 연결합니다.
4. 그 결과, "O:\"와 "s:\" 드라이브 모두에서 데이터에 액세스할 때 SMB 서명이 사용됩니다.

수신 **SMB** 트래픽에 필요한 **SMB** 서명을 설정하거나 해제합니다

필요한 SMB 서명을 설정하여 클라이언트가 SMB 메시지에 서명하도록 요구 사항을 적용할 수 있습니다. 활성화된 경우 ONTAP은 유효한 서명이 있는 경우에만 SMB 메시지를 수락합니다. SMB 서명을 허용하되 SMB 서명이 필요하지 않은 경우 필요한 SMB 서명을 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

기본적으로 필요한 SMB 서명은 사용되지 않습니다. 필요한 SMB 서명을 언제든지 설정하거나 해제할 수 있습니다.



다음과 같은 상황에서는 SMB 서명이 기본적으로 비활성화되어 있지 않습니다.

1. 필요한 SMB 서명이 설정되어 있고 클러스터가 SMB 서명을 지원하지 않는 ONTAP 버전으로 되돌려집니다.
2. 이후 클러스터는 SMB 서명을 지원하는 ONTAP 버전으로 업그레이드됩니다.

이러한 경우 지원되는 ONTAP 버전에 원래 구성된 SMB 서명 구성은 재버전과 후속 업그레이드를 통해 유지됩니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 필요한 SMB 서명을 사용하도록 설정한 경우, 대상 SVM에서 필요한 SMB 서명을 수동으로 활성화해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 서명이 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-signing-required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-signing-required false'

2. 다음 명령의 출력에서 "is signing required" 필드의 값이 원하는 값으로 설정되어 있는지 확인하여 필요한 SMB 서명이 활성화되어 있는지 또는 비활성화되어 있는지 확인합니다. 'vserver cifs security show

-vserver_vserver_name_-fields is-signing-required'

예

다음 예에서는 SVM VS1 에 필요한 SMB 서명을 활성화합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----  -
vs1      true
```



암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

SMB 세션이 서명되었는지 확인합니다

CIFS 서버에서 연결된 SMB 세션에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 SMB 세션이 서명되었는지 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 스토리지 가상 시스템(SVM)에서 서명된 모든 세션	'vserver cifs session show -vserver_vserver_name_-is-session-signed true'
SVM에서 특정 세션 ID와 서명된 세션의 세부 정보	'vserver cifs session show -vserver_vserver_name_-session-id integer-instance'

예

다음 명령을 실행하면 SVM VS1 에서 서명된 세션에 대한 세션 정보가 표시됩니다. 기본 요약 출력에는 ""세션 서명됨" 출력 필드가 표시되지 않습니다.

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation    Windows User    Open    Idle
-----  -----  -
3151272279  1          10.1.1.1      DOMAIN\joe      2       23s
```

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 세션의 서명 여부를 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

관련 정보

SMB 서명 세션 통계 모니터링

SMB 서명 세션 통계를 모니터링합니다

SMB 세션 통계를 모니터링하고 서명된 설정된 세션과 그렇지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 서명된 SMB 세션 수를 모니터링하는 데 사용할 수 있는 'signed_sessions' 카운터를 제공합니다. 'Signed_sessions' 카운터는 다음과 같은 통계 객체와 함께 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 세션에 대해 SMB 서명을 모니터링할 수 있습니다.
- 'MB1'을 사용하면 SMB 1.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.
- 'MB2'를 사용하면 SMB 2.x 및 SMB 3.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.

SMB 3.0 통계는 'MB2' 객체의 출력에 포함됩니다.

서명된 세션의 수를 총 세션 수와 비교하려면 'signed_sessions' 카운터의 출력을 '설정된_sessions' 카운터의 출력과 비교할 수 있습니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데

사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 `advanced:+et-Privilege advanced`로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

4. SMB 서명 통계 보기:

에 대한 정보를 보려면...	입력...
서명된 세션	shope-sample-id sample_ID-counter signed_sessions
node_name[-node_node_name_]	서명된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter signed_sessions	ESTANCE_SECURIONS

단일 노드에 대한 정보만 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 2.x 및 SMB 3.0 서명 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 서명된 SMB 세션과 샘플의 노드별 설정된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smb signing_sample -counter  
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

다음 명령을 실행하면 샘플에서 노드 2에 대해 서명된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smb signing_sample -counter  
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

다음 명령을 실행하면 admin 권한 레벨로 다시 이동됩니다.

```
cluster1::*> set -privilege admin
```

SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화를 구성합니다

SMB 암호화 개요

SMB를 통한 데이터 전송을 위한 SMB 암호화는 SMB 서버에서 활성화 또는 비활성화할 수 있는 향상된 보안 기능입니다. 공유 속성 설정을 통해 공유별로 원하는 SMB 암호화 설정을 구성할 수도 있습니다.

기본적으로 SVM(스토리지 가상 머신)에 SMB 서버를 생성할 때 SMB 암호화는 사용하지 않도록 설정됩니다. SMB 암호화를 통해 제공되는 향상된 보안을 활용하려면 이 기능을 활성화해야 합니다.

암호화된 SMB 세션을 생성하려면 SMB 클라이언트가 SMB 암호화를 지원해야 합니다. Windows Server 2012 및 Windows 8부터 시작되는 Windows 클라이언트는 SMB 암호화를 지원합니다.

SVM의 SMB 암호화는 두 가지 설정을 통해 제어됩니다.

- SVM에서 기능을 활성화하는 SMB 서버 보안 옵션
- 공유 단위로 SMB 암호화 설정을 구성하는 SMB 공유 속성입니다

SVM의 모든 데이터에 액세스하려면 암호화를 사용할지, 선택한 공유에서만 데이터에 액세스하려면 SMB 암호화가 필요한지 여부를 결정할 수 있습니다. SVM 레벨 설정이 공유 레벨 설정보다 우선합니다.

효과적인 SMB 암호화 구성은 두 가지 설정의 조합에 따라 달라지며 다음 표에 설명되어 있습니다.

SMB 서버 SMB 암호화가 활성화되었습니다	공유 암호화 데이터 설정이 활성화되었습니다	서버측 암호화 동작
참	거짓	SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
참	참	공유 레벨 암호화와 관계없이 SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
거짓	참	특정 공유에 대해 공유 수준 암호화가 설정됩니다. 이 구성을 사용하면 트리 연결로부터 암호화가 수행됩니다.
거짓	거짓	암호화가 활성화되지 않았습니다.

암호화를 지원하지 않는 SMB 클라이언트는 암호화가 필요한 SMB 서버 또는 공유에 연결할 수 없습니다.

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

SMB 암호화가 성능에 미치는 영향

SMB 세션에서 SMB 암호화를 사용하면 Windows 클라이언트와 서버 간의 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버 모두에 영향을 미칩니다(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드).

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 암호화된 SMB 트래픽에서 성능을 향상시킬 수 있습니다. SMB 암호화 오프로드는 SMB 암호화가 활성화된 경우 기본적으로 활성화됩니다.

향상된 SMB 암호화 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 암호화가 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경의 테스트를 통해서만 확인할 수 있습니다.

SMB 서버에서 SMB 암호화는 기본적으로 비활성화되어 있습니다. 암호화가 필요한 SMB 공유 또는 SMB 서버에서만 SMB 암호화를 활성화해야 합니다. SMB 암호화를 통해 ONTAP는 요청을 암호 해독하고 모든 요청에 대한 응답을 암호화하는 추가 처리를 수행합니다. 따라서 필요한 경우에만 SMB 암호화를 활성화해야 합니다.

수신 **SMB** 트래픽에 필요한 **SMB** 암호화를 설정하거나 해제합니다

수신 SMB 트래픽에 SMB 암호화가 필요한 경우 CIFS 서버 또는 공유 레벨에서 설정할 수 있습니다. 기본적으로 SMB 암호화는 필요하지 않습니다.

이 작업에 대해

CIFS 서버에서 SMB 암호화를 설정하면 CIFS 서버의 모든 공유에 적용됩니다. CIFS 서버의 모든 공유에 대해 SMB 암호화가 필요하지 않거나 공유 단위로 수신 SMB 트래픽에 대해 필요한 SMB 암호화를 설정하려는 경우 CIFS 서버에서 필요한 SMB 암호화를 해제할 수 있습니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napmirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 SMB 암호화를 사용하도록 설정한 경우 대상에서 CIFS 서버 SMB 암호화를 수동으로 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

CIFS 서버에서 들어오는 SMB 트래픽에 대해 SMB 암호화가 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required false'

2. CIFS 서버에서 필요한 SMB 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_-fields is-smb-encryption-required'

CIFS 서버에 필요한 SMB 암호화가 설정되어 있으면 is-smb-encryption-required 필드에 true가 표시되고, 비활성화된 경우에는 false가 표시됩니다.

예

다음 예에서는 SVM VS1에서 CIFS 서버에 대해 수신 SMB 트래픽에 필요한 SMB 암호화를 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true
```

클라이언트가 암호화된 **SMB** 세션을 사용하여 연결되어 있는지 확인합니다

연결된 SMB 세션에 대한 정보를 표시하여 클라이언트가 암호화된 SMB 연결을 사용하는지 여부를 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

SMB 클라이언트 세션은 다음 세 가지 암호화 수준 중 하나를 가질 수 있습니다.

- "암호화되지 않음"

SMB 세션이 암호화되지 않았습니다. SVM(스토리지 가상 시스템) 레벨 또는 공유 레벨 암호화가 구성되지 않았습니다.

- 부분적으로 암호화되었습니다

트리 연결이 발생하면 암호화가 시작됩니다. 공유 수준 암호화가 구성됩니다. SVM 레벨 암호화가 활성화되지 않았습니다.

- '암호화됨'

SMB 세션이 완전히 암호화됩니다. SVM 레벨 암호화가 활성화됩니다. 공유 수준 암호화가 활성화되어 있거나 활성화되어 있지 않을 수 있습니다. SVM 레벨 암호화 설정이 공유 레벨 암호화 설정보다 우선합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 세션에 대해 지정된 암호화 설정을 갖는 세션	'vserver cifs session show -vserver_vserver_name_{encrypted
sPartially-encrypted	encrypted}-instance'
지정된 SVM에서 특정 세션 ID의 암호화 설정입니다	'vserver cifs session show -vserver_vserver_name_-session-id_integer_-instance'

예

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 암호화 설정을 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

SMB 암호화 통계를 모니터링합니다

SMB 암호화 통계를 모니터링하고 설정된 세션 및 공유 연결이 암호화되고 암호화되지 않은

세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 다음 카운터를 제공하며, 이 카운터를 사용하여 암호화된 SMB 세션 수를 모니터링하고 연결을 공유할 수 있습니다.

카운터 이름	설명
'암호화 세션'	암호화된 SMB 3.0 세션의 수를 제공합니다
'암호화_공유_연결'	트리 연결이 발생한 암호화된 공유 수를 제공합니다
"암호화되지 않은 세션"이 끼어들었습니다	에서는 클라이언트 암호화 기능이 부족하여 거부된 세션 설정 수를 제공합니다
"암호화되지 않은_공유"가 있습니다	에서는 클라이언트 암호화 기능이 없어 거부된 공유 매핑 수를 제공합니다

이러한 카운터는 다음 통계 개체에서 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 3.0 세션에 대해 SMB 암호화를 모니터링할 수 있습니다.

SMB 3.0 통계는 'CIFS' 객체의 출력에 포함됩니다. 암호화된 세션의 수를 총 세션 수와 비교하려면 "encrypted_sessions" 카운터의 출력과 "encrypted_sessions" 카운터의 출력을 비교할 수 있습니다.

암호화된 공유 연결 수와 총 공유 연결 수를 비교하려면 에 대한 출력을 비교할 수 있습니다 encrypted_share_connections 에 대한 출력이 있는 카운터 connected_shares 카운터.

- reped_cencrypted_sessions는 SMB 암호화를 지원하지 않는 클라이언트로부터 암호화를 요구하는 SMB 세션을 설정하려고 시도한 횟수를 제공합니다.
- refened_cencrypted_share는 SMB 암호화를 지원하지 않는 클라이언트의 암호화가 필요한 SMB 공유에 연결하려고 시도한 횟수를 제공합니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:'+et-Privilege advanced로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

4. SMB 암호화 통계 보기:

에 대한 정보를 보려면...	입력...
암호화된 세션	'shope-sample-id_sample_ID_-counter encrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter encrypted_sessions	encrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화된 공유 연결
'shope-sample-id_sample_ID_-counter encrypted_share_connections	<i>node_name</i> [-node_node_name_]
암호화된 공유 연결 및 연결된 공유	'sHow-sample-id_sample_ID_-counter encrypted_share_connections
Connected_share	<i>node_name</i> [-node_node_name_]
암호화되지 않은 세션이 거부되었습니다	shope-sample-id_sample_ID_-counter rejected_sencrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화되지 않은 공유 연결이 거부되었습니다
'shd-sample-id_sample_ID_-counter rejected_sencrypted_share	<i>node_name</i> [-node_node_name_]

단일 노드에 대해서만 정보를 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 해당 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 암호화된 SMB 세션 및 샘플의 노드에 의해 설정된 SMB 세션이 표시됩니다.

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 세션이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

다음 명령을 실행하면 샘플의 노드에 의해 연결된 SMB 공유 및 암호화된 SMB 공유의 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 공유 연결이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

관련 정보

[사용할 수 있는 통계 개체 및 카운터 결정](#)

["성능 모니터링 및 관리 개요"](#)

보안 **LDAP** 세션 통신

LDAP 서명 및 봉인 개념

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록

서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

CIFS 서버에서 LDAP 서명 및 봉인을 설정합니다

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-session-security-for-ad-ldap{none|sign|seal}'

서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_'



SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

TLS를 통해 LDAP를 구성합니다

자체 서명된 루트 CA 인증서의 복사본을 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: technet.microsoft.com"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"Microsoft TechNet 라이브러리"

SVM에 자체 서명된 루트 CA 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS를 통한 LDAP가 활성화된 경우 SVM의 ONTAP LDAP 클라이언트는 ONTAP 9.0 및 9.1에서 해지된 인증서를 지원하지 않습니다.

ONTAP 9.2부터 TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:

- a. 인증서 설치를 시작합니다. 'Security certificate install - vserverserver_name -type server -ca'

콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

- b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 ---- '-----'로 끝나는 종료 인증서 ---- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.

- c. 인증서가 올바르게 표시되는지 확인합니다.

- d. Enter 키를 눌러 설치를 완료합니다.

2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserverserver_name_'

서버에서 TLS를 통해 LDAP를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(Active Directory) 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 'vservers cifs security modify' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- "LDAP 개요"

- "Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver_vserver_name_



SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.

성능 및 이중화를 위해 **SMB** 멀티 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- * 클라이언트와 ONTAP 클러스터의 1G NIC *

클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- * 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC *

클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- * '-max-connections-per-session' *

다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- * '-max-liff-per-session' *

Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. SMB 서버에서 SMB 멀티 채널 활성화: 'vserver cifs options modify -vserver_vserver_name_-is-multichannel -enabled true
3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다. 'vserver cifs session show_options_'
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                                Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s
Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance
```

```
Vserver: vs1
```

```
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

SMB 서버에서 기본 Windows 사용자를 UNIX 사용자 매핑으로 구성합니다

기본 UNIX 사용자를 구성합니다

기본 UNIX 사용자는 사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우에 사용하도록 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 UNIX 사용자를 구성하지 않아야 합니다.

이 작업에 대해

기본적으로 기본 UNIX 사용자의 이름은 "pcuser"입니다. 즉, 기본적으로 기본 UNIX 사용자에 대한 사용자 매핑이 설정됩니다. 기본 UNIX 사용자로 사용할 다른 이름을 지정할 수 있습니다. 지정하는 이름은 SVM(스토리지 가상 머신)용으로 구성된 네임 서비스 데이터베이스에 있어야 합니다. 이 옵션이 null 문자열로 설정된 경우 CIFS 서버를 UNIX 기본 사용자로 액세스할 수 없습니다. 즉, 각 사용자는 CIFS 서버를 액세스하기 전에 암호 데이터베이스에 계정이 있어야 합니다.

사용자가 기본 UNIX 사용자 계정을 사용하여 CIFS 서버에 접속하려면 다음과 같은 사전 요구 사항을 충족해야 합니다.

- 사용자가 인증됩니다.
- 사용자가 CIFS 서버의 로컬 Windows 사용자 데이터베이스, CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인에 있습니다(CIFS 서버에서 다중 도메인 이름 매핑 검색이 설정된 경우).

- 사용자 이름이 null 문자열에 명시적으로 매핑되어 있지 않습니다.

단계

1. 기본 UNIX 사용자 구성:

원하는 작업	입력...
기본 UNIX 사용자 ""pcuser"" 사용	'vserver cifs options modify-default-unix-user pcuser'
다른 UNIX 사용자 계정을 기본 사용자로 사용합니다	'vserver cifs options modify-default-unix-user _user_name_'
기본 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-default-unix-user''

'vserver cifs options modify-default-unix-user pcuser'

2. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver_vserver_name_'

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec       : disabled
Read Only Delete       : disabled
WINS Servers           : -
```

게스트 UNIX 사용자를 구성합니다

게스트 UNIX 사용자 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 게스트 UNIX 사용자에게 매핑되고 CIFS 서버에 연결할 수 있습니다. 또는 신뢰할 수 없는 도메인의 사용자 인증에 실패하도록 하려면 게스트 UNIX 사용자를 구성하지 않아야 합니다. 기본값은 신뢰할 수 없는 도메인의 사용자가 CIFS 서버에 접속할 수 없도록 하는 것입니다(게스트 UNIX 계정이 구성되지 않음).

이 작업에 대해

게스트 UNIX 계정을 구성할 때 다음 사항을 염두에 두어야 합니다.

- CIFS 서버가 홈 도메인 또는 신뢰할 수 있는 도메인 또는 로컬 데이터베이스에 대한 도메인 컨트롤러에 대해

사용자를 인증할 수 없고 이 옵션이 설정된 경우 CIFS 서버는 사용자를 게스트 사용자로 간주하고 지정된 UNIX 사용자에게 매핑합니다.

- 이 옵션을 null 문자열로 설정하면 게스트 UNIX 사용자가 비활성화됩니다.
- SVM(Storage Virtual Machine) 이름 서비스 데이터베이스 중 하나에서 게스트 UNIX 사용자로 사용할 UNIX 사용자를 생성해야 합니다.
- 게스트 사용자로 로그인한 사용자는 자동으로 CIFS 서버에 있는 BUILTIN\guests 그룹의 구성원입니다.
- 'homedirs-public' 옵션은 인증된 사용자에게만 적용됩니다. 게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	입력...
게스트 UNIX 사용자를 구성합니다	'vserver cifs options modify-guest-unix-user_unix_name_'
게스트 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-guest-unix-user''

'vserver cifs options modify-guest-unix-user pcuser'

2. 게스트 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver_vserver_name_'

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

관리자 그룹을 루트에 매핑합니다

사용자 환경에 CIFS 클라이언트만 있고 SVM(스토리지 가상 시스템)을 멀티프로토콜 스토리지 시스템으로 설정한 경우, SVM에서 파일에 액세스할 수 있는 루트 권한이 있는 Windows 계정이 하나 이상 있어야 합니다. 그렇지 않으면 충분한 사용자 권한이 없기 때문에 SVM을 관리할 수 없습니다.

이 작업에 대해

그러나 스토리지 시스템이 NTFS 전용으로 설정된 경우, '/etc' 디렉토리에는 관리자 그룹이 ONTAP 구성 파일에 액세스할 수 있도록 하는 파일 레벨 ACL이 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 관리자 그룹을 루트에 적절하게 매핑하는 CIFS 서버 옵션을 구성합니다.

원하는 작업	그러면...
관리자 그룹 구성원을 루트에 매핑합니다	'vserver cifs options modify -vserver_vserver_name _is-admin-users-mapped-to -root-enabled true' 계정을 루트로 매핑하는 '/etc/usermap.cfg' 항목이 없는 경우에도 administrators 그룹의 모든 계정은 루트로 간주됩니다. administrators 그룹에 속하는 계정을 사용하여 파일을 생성하는 경우 UNIX 클라이언트에서 파일을 볼 때 파일은 루트에서 소유합니다.
관리자 그룹 구성원을 루트에 매핑하도록 해제합니다	"vserver cifs options modify -vserver_vserver_name _is-admin-users-mapped-to -root-enabled false" administrators 그룹의 계정은 더 이상 루트에 매핑되지 않습니다. 단일 사용자만 루트에 명시적으로 매핑할 수 있습니다.

3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시합니다

SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시할 수 있습니다. 따라서 적절한 유형의 사용자만 SVM(스토리지 가상 머신)의 SMB 세션을 통해 연결할 수 있습니다.

이 작업에 대해

다음 유형의 사용자는 SMB 세션을 통해 연결할 수 있습니다.

- '로컬 사용자'

로컬 CIFS 사용자로 인증되었습니다

- '다민 사용자'입니다

도메인 사용자로 인증됨(CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인)

- 'guest-user'입니다

게스트 사용자로 인증되었습니다

- 익명의 사용자

익명 또는 null 사용자로 인증되었습니다

단계

1. SMB 세션을 통해 연결된 사용자 유형을 확인합니다. 'vserver cifs session show -vserver _vserver_name_ -windows-user _windows_user_name_ -fields windows-user, address, lif-address, user-type'

설정된 세션에 대한 사용자 유형 정보를 표시하려면...	다음 명령을 입력합니다...
사용자 유형이 지정된 모든 세션에 대해	'vserver cifs session show -vserver _vserver_name_ -user-type{local-user
domain-user	guest-user
anonymous-user}'입니다	특정 사용자의 경우

예

다음 명령을 실행하면 ""iepubs\user1" 사용자가 설정한 SVM VS1 세션의 사용자 유형에 대한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user      user-type
-----
pub1node1 pub1      1          3439441860    10.0.0.1    10.1.1.1
IEPUBS\user1      domain-user
```

과도한 Windows 클라이언트 리소스 사용을 제한하는 명령 옵션입니다

'vserver cifs options modify' 명령 옵션을 사용하면 Windows 클라이언트의 리소스 사용을 제어할 수 있습니다. 이 기능은 클라이언트가 리소스 사용의 정상적인 범위를 벗어난 경우(예: 열려 있는 파일의 수가 비정상적으로 많거나 세션이 열려 있거나 변경 알림 요청이 있는 경우) 유용합니다.

Windows 클라이언트 리소스 사용을 제어하기 위해 'vserver cifs options modify' 명령에 대한 다음 옵션이 추가되었습니다. 이 옵션 중 최대값이 초과되면 요청이 거부되고 EMS 메시지가 전송됩니다. 이 옵션에 대해 구성된 제한값의 80%에 도달하면 EMS 경고 메시지도 전송됩니다.

- '-max-오픈-파일-트리 단위'

CIFS 트리당 동일한 파일에 대한 최대 열기 수입니다

- '-max-same-user-sessions-per-connection'

동일한 사용자가 접속당 연 최대 세션 수입니다

- '-max-same-tree-connect-per-session'

세션당 동일한 공유에 대한 최대 트리 연결 수입니다

- '-max-s위치-세트당-트리'

트리당 설정된 최대 시계 수(_CHANGE ALBERS_라고도 함)입니다

기본 제한 및 현재 구성을 표시하려면 man 페이지를 참조하십시오.

ONTAP 9.4부터 SMB 버전 2 이상을 실행하는 서버는 클라이언트가 SMB 연결을 통해 서버로 전송할 수 있는 미해결 요청(*smb* 크레딧) 수를 제한할 수 있습니다. SMB 크레딧의 관리는 클라이언트가 시작하고 서버에 의해 제어됩니다.

SMB 연결에서 허용할 수 있는 최대 요청 수는 '-max-credits' 옵션으로 제어됩니다. 이 옵션의 기본값은 128입니다.

기존 **oplocks** 및 리스 **oplocks**로 클라이언트 성능 향상

기존 및 리스 **oplocks** 개요를 통해 클라이언트 성능 향상

기존 **oplocks**(기회 잠금) 및 리스 **oplocks**는 특정 파일 공유 시나리오에서 SMB 클라이언트가 미리 읽기, 쓰기 후 및 잠금 정보의 클라이언트측 캐싱을 수행할 수 있도록 합니다. 그러면 클라이언트는 해당 파일에 액세스해야 한다는 사실을 서버에 정기적으로 알려주지 않고 파일을 읽거나 파일에 쓸 수 있습니다. 이렇게 하면 네트워크 트래픽이 줄어들어 성능이 향상됩니다.

리스 **oplocks**는 SMB 2.1 프로토콜 이상에서 사용할 수 있는 향상된 형태의 **oplocks**입니다. 리스 **oplocks**를 사용하면 클라이언트가 자체적으로 시작된 여러 SMB에서 클라이언트 캐싱 상태를 확보하고 유지할 수 있습니다.

oplocks는 다음 두 가지 방법으로 제어할 수 있습니다.

- 공유를 생성할 때 공유 속성에 의해 'vserver cifs share create' 명령을 사용하거나 생성 후 'vserver share properties' 명령을 사용합니다.
- *qtree*가 생성될 때 'volume qtree create' 명령을 사용하거나 생성 후 'volume qtree oplock' 명령을 사용하여 *qtree* 속성에 의해 생성됩니다.

oplocks 사용 시 캐시 데이터 손실 고려 사항 쓰기

경우에 따라 프로세스에 파일에 배타적 **oplock**이 있고 두 번째 프로세스에서 파일을 열려고 시도할 경우 첫 번째 프로세스에서는 캐시된 데이터를 무효화하고 쓰기 및 잠금을 플러시해야 합니다. 그런 다음 클라이언트는 **oplock** 및 파일에 대한 액세스를 양도해야 합니다. 이 플러시 중에 네트워크 장애가 발생하면 캐시된 쓰기 데이터가 손실될 수 있습니다.

- 데이터 손실 가능성

다음과 같은 상황에서는 쓰기 캐싱된 데이터가 있는 모든 애플리케이션에서 해당 데이터가 손실될 수 있습니다.

- 연결은 SMB 1.0을 사용하여 이루어집니다.

- 파일에 배타적 oplock이 있습니다.
 - 해당 oplock을 깨거나 파일을 닫도록 합니다.
 - 쓰기 캐시를 플러시하는 프로세스 중에 네트워크 또는 타겟 시스템에서 오류가 발생합니다.
- 오류 처리 및 쓰기 완료

캐시 자체는 오류 처리를 하지 않습니다. 애플리케이션에서 캐시에 쓰기를 수행할 때는 항상 쓰기가 완료됩니다. 캐시가 네트워크를 통해 타겟 시스템에 쓰기를 수행하는 경우 쓰기가 완료된 것으로 가정해야 합니다. 그렇지 않으면 데이터가 손실되기 때문입니다.

SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. oplocks는 스토리지 가상 시스템(SVM)에 상주하는 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수 있습니다. 공유별로 oplocks를 설정하거나 해제할 수 있습니다.


이 작업에 대해


공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 해제됩니다. 공유에서 oplocks를 비활성화하면 볼륨 oplock 설정보다 우선적으로 적용됩니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다.

심표로 구분된 목록을 사용하여 oplock 공유 속성을 지정하는 것 외에도 다른 공유 속성을 지정할 수 있습니다. 다른 공유 매개 변수를 지정할 수도 있습니다.

단계

1. 해당 작업을 수행합니다.

원하는 작업	그러면...
공유를 생성하는 동안 공유에 oplocks를 설정합니다	<p>'vserver cifs share create -vserver_vserver_name_-share-name share_name -path path_to_share-share-properties [oplocks,...]' 명령을 입력합니다</p> <div>  <p>공유에서 oplocks, browsable, changentify의 기본 공유 속성만 사용하려면 SMB 공유를 생성할 때 '-share-properties' 매개 변수를 지정하지 않아도 됩니다. 기본값 이외의 공유 속성을 조합하려면 해당 공유에 사용할 공유 속성 목록과 함께 '-share-properties' 매개 변수를 지정해야 합니다.</p> </div>

원하는 작업	그러면...
공유를 생성하는 동안 공유에 oplocks를 사용하지 않도록 설정합니다	<p>'vserver cifs share create-vserver_vserver_name_-share-name_share_name_-path_to_share_-share-properties[other_share_property,...]' 명령을 입력합니다</p> <div>  <p>oplocks를 해제할 때는 공유를 생성할 때 공유 속성 목록을 지정해야 하지만 "oplocks" 속성을 지정해서는 안 됩니다.</p> </div>

관련 정보

[기존 SMB 공유에서 oplocks 설정 또는 해제](#)

[oplock 상태 모니터링](#)

볼륨 및 qtree에서 oplocks를 설정하거나 해제하는 명령입니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. 볼륨 또는 qtree에서 oplocks를 설정하거나 해제하는 명령을 알아야 합니다. 또한 볼륨 및 qtree에서 oplocks를 설정하거나 해제할 수 있는 시기를 알아야 합니다.

- oplocks는 기본적으로 볼륨에 설정됩니다.
- 볼륨을 생성할 때는 oplocks를 해제할 수 없습니다.
- 언제든지 기존 볼륨에서 SVM에 대한 oplocks를 설정하거나 해제할 수 있습니다.
- SVM에 대해 qtree에서 oplocks를 설정할 수 있습니다.

oplock 모드 설정은 qtree ID 0의 속성으로, 모든 볼륨에 있는 기본 qtree입니다. qtree를 생성할 때 oplock 설정을 지정하지 않으면 qtree가 기본적으로 사용되는 상위 볼륨의 oplock 설정을 상속합니다. 그러나 새 qtree에 oplock 설정을 지정하면 볼륨의 oplock 설정보다 우선합니다.

원하는 작업	이 명령 사용...
볼륨 또는 qtree에 oplocks를 설정합니다	'-oplock-mode' 매개 변수가 'enable'로 설정된 볼륨 qtree oplocks
볼륨 또는 qtree에서 oplocks를 해제합니다	'-oplock-mode' 매개 변수가 '사용할 수 있음'으로 설정된 볼륨 qtree oplocks입니다

관련 정보

[oplock 상태 모니터링](#)

기존 SMB 공유에서 oplocks를 설정하거나 해제합니다

oplocks는 기본적으로 스토리지 가상 시스템(SVM)의 SMB 공유에 설정됩니다. 경우에 따라



oplocks를 해제할 수도 있습니다. 이전에 공유에서 oplocks를 해제한 경우에는 oplocks를 다시 설정할 수도 있습니다.

이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 비활성화됩니다. 공유에 oplocks를 사용하지 않도록 설정하면 볼륨에서 oplocks를 설정하는 것이 우선합니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다. 언제든지 기존 공유에 oplocks를 설정하거나 해제할 수 있습니다.

단계

- 1. 해당 작업을 수행합니다.

원하는 작업	그러면...
기존 공유를 수정하여 공유에 oplocks를 설정합니다	<div>'vserver cifs share properties add -vserver_vserver_name_-share-name share_name-share-properties oplocks' 명령을 입력합니다</div> <div><div></div><div>심표로 구분된 목록을 사용하여 추가할 추가 공유 속성을 지정할 수 있습니다.</div></div> <div>새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다. 이전에 지정한 공유 속성은 그대로 유지됩니다.</div>
기존 공유를 수정하여 공유에 oplocks를 사용하지 않도록 설정합니다	<div>'vserver cifs share properties remove-vserver_vserver_name_-share-name share_name_-share-properties oplocks' 명령을 입력합니다</div> <div><div></div><div>심표로 구분된 목록을 사용하여 제거할 추가 공유 속성을 지정할 수 있습니다.</div></div> <div>제거한 공유 속성은 기존 공유 속성 목록에서 삭제되지만 이전에 구성한 공유 속성은 제거하지 않습니다.</div>

예

다음 명령을 실행하면 스토리지 가상 시스템(SVM, 이전 명칭 Vserver) VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 설정됩니다.

```
cluster1::> vservers cifs share properties add -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

다음 명령을 실행하면 SVM VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 해제됩니다.

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

관련 정보

[SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)

[oplock 상태 모니터링](#)

[기존 SMB 공유에서 공유 속성 추가 또는 제거](#)

oplock 상태를 모니터링합니다

oplock 상태에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보를 사용하여 oplocks가 있는 파일, oplock 레벨 및 oplock 상태 수준이 무엇인지, oplock 리스가 사용되는지 여부를 확인할 수 있습니다. 수동으로 해제해야 하는 잠금에 대한 정보를 확인할 수도 있습니다.

이 작업에 대해

모든 oplocks에 대한 정보를 요약 양식 또는 세부 목록 양식에 표시할 수 있습니다. 선택적 매개 변수를 사용하여 기존 잠금의 하위 집합에 대한 정보를 표시할 수도 있습니다. 예를 들어, 지정된 클라이언트 IP 주소 또는 지정된 경로를 사용하여 출력 반환만 잠그도록 지정할 수 있습니다.

기존 및 리스 oplocks에 대한 다음 정보를 표시할 수 있습니다.

- oplock이 설정된 SVM, 노드, 볼륨 및 LIF입니다
- UUID를 잠급니다

- oplock을 사용하는 클라이언트의 IP 주소입니다
- oplock이 설정된 경로입니다
- 잠금 프로토콜(SMB) 및 유형(oplock)
- 잠금 상태
- oplock 레벨
- 연결 상태 및 SMB 만료 시간입니다
- 임대 oplock이 부여된 경우 그룹 ID를 엽니다

각 매개변수에 대한 자세한 설명은 'vserver oplocks show' man 페이지를 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 oplock 상태를 표시합니다.

예

다음 명령을 실행하면 모든 잠금에 대한 기본 정보가 표시됩니다. 표시된 파일의 oplock은 "임시 배치" oplock 레벨로 허가됩니다.

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1	cifs	share-level	192.168.1.5
Sharelock Mode: read_write-deny_delete				op-lock	192.168.1.5
Oplock Level: read-batch					

다음 예제는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 잠금에 대한 자세한 정보를 표시합니다. IP 주소가 10.3.1.3 인 클라이언트에 배치 oplock 레벨이 있는 파일에 리스 oplock이 부여됩니다.



자세한 정보를 표시할 때 이 명령은 oplock 및 sharelock 정보에 대한 별도의 출력을 제공합니다. 이 예제는 oplock 섹션의 출력만 보여 줍니다.

```
cluster1::> vservers lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
  Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

관련 정보

[SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)

[기존 SMB 공유에서 oplocks 설정 또는 해제](#)

[볼륨 및 qtree에서 oplocks를 설정하거나 해제하는 명령입니다](#)

SMB 서버에 그룹 정책 개체를 적용합니다

SMB 서버에 그룹 정책 개체 적용 개요

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

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

["SMB 및 NFS 감사 및 보안 추적"](#)

지원되는 GPO

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

- 로그인 이벤트를 감사합니다

다음 설정을 포함하여 감사할 로그인 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 사용자에게 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

[CIFS 서버에서 GPO 지원을 설정하거나 해제합니다](#)

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

["SMB 및 NFS 감사 및 보안 추적"](#)

CIFS 서버 Kerberos 보안 설정을 수정합니다

BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

SMB 서명을 사용하여 네트워크 보안을 강화합니다

통과 확인 우회 구성

익명 사용자에게 대한 액세스 제한 구성

SMB 서버에 GPO를 사용하기 위한 요구 사항

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

- SMB는 클러스터에서 라이선스가 있어야 합니다. SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). 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.

CIFS 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 GPO](#)

[GPO를 CIFS 서버와 함께 사용하기 위한 요구 사항](#)

[CIFS 서버에서 GPO를 업데이트하는 방법](#)

[CIFS 서버에서 GPO 설정을 수동으로 업데이트합니다](#)

[GPO 구성에 대한 정보 표시](#)

SMB 서버에서 GPO를 업데이트하는 방법

CIFS 서버 개요에서 **GPO**를 업데이트하는 방법

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.

CIFS 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'

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::> vsriver cifs group-policy show-defined -vsriver vs1
```

```
Vsriver: 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:
```

```
    /voll/home
```

```
    /voll/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/dirl

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

[CIFS 서버에서 GPO 지원을 설정하거나 해제합니다](#)

제한된 그룹 **GPO**에 대한 자세한 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 vservice_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy restricted-group show-applied-vserver vservice_name'

예

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

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

```
Vsriver: 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
```

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

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

```
Vsriver: 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
```

관련 정보

[GPO 구성에 대한 정보 표시](#)

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::> vsriver 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::> vsriver 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

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

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

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

[GPO 구성에 대한 정보 표시](#)

[중앙 액세스 정책에 대한 정보 표시](#)

SMB 서버 컴퓨터 계정 암호를 관리하는 명령입니다

암호를 변경, 재설정 및 비활성화하고 자동 업데이트 일정을 구성하기 위한 명령을 알아야 합니다. SMB 서버에서 자동으로 업데이트되도록 스케줄을 구성할 수도 있습니다.

원하는 작업	이 명령 사용...
도메인 계정 암호를 변경하거나 재설정하면 암호를 알 수 있습니다	'vserver cifs domain password change'를 선택합니다
도메인 계정 암호를 재설정하며 암호를 모르는 경우	'vserver cifs domain password reset'
자동 컴퓨터 계정 암호 변경을 위해 SMB 서버를 구성합니다	'vserver cifs domain password schedule modify -vserver vs1-is-schedule -enabled true'
SMB 서버에서 자동 컴퓨터 계정 암호 변경을 비활성화합니다	'vserver cifs domain password schedule modify -vserver vs1-is-schedule -enabled false'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

도메인 컨트롤러 연결을 관리합니다

검색된 서버에 대한 정보를 표시합니다

CIFS 서버에서 검색된 LDAP 서버 및 도메인 컨트롤러와 관련된 정보를 표시할 수 있습니다.

단계

1. 검색된 서버와 관련된 정보를 표시하려면 'vserver cifs domain discovered-servers show' 명령을 입력합니다

예

다음 예에서는 SVM VS1 에서 검색된 서버를 보여 줍니다.

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

관련 정보

서버 재설정 및 재검색

CIFS 서버를 중지 또는 시작하는 중입니다

서버를 재설정하고 재검색합니다

CIFS 서버에서 서버를 재설정하고 재검색하면 CIFS 서버가 LDAP 서버 및 도메인 컨트롤러에 대한 저장된 정보를 삭제할 수 있습니다. 서버 정보를 폐기한 후 CIFS 서버는 이러한 외부 서버에 대한 현재 정보를 다시 가져옵니다. 이 기능은 연결된 서버가 적절하게 응답하지 않는 경우에 유용할 수 있습니다.

단계

1. 'vserver cifs domain discovered - servers reset -servers -vserver_vserver_name_' 명령을 입력합니다
2. 새로 재검색된 서버에 대한 정보를 표시합니다. 'vserver cifs domain discovered-servers show -vserver_vserver_name_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 VS1 용 서버를 재설정하고 다시 검색합니다.

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

관련 정보

검색된 서버에 대한 정보 표시

CIFS 서버를 중지 또는 시작하는 중입니다

도메인 컨트롤러 검색을 관리합니다

ONTAP 9.3부터는 DC(도메인 컨트롤러)가 검색되는 기본 프로세스를 수정할 수 있습니다. 이렇게 하면 사이트 또는 기본 DC 풀로 검색을 제한할 수 있으며, 이는 환경에 따라 성능 개선을 초래할 수 있습니다.

이 작업에 대해

기본적으로 동적 검색 프로세스는 기본 DC, 로컬 사이트의 모든 DC 및 모든 원격 DC를 포함하여 사용 가능한 모든 DC를 검색합니다. 이 구성을 사용하면 특정 환경에서 인증 및 공유 액세스에 지연 시간이 발생할 수 있습니다. 사용하려는 DC 풀을 이미 결정했거나 원격 DC가 부적절하거나 액세스할 수 없는 경우 검색 방법을 변경할 수 있습니다.

ONTAP 9.3 이상 릴리즈에서는 "cifs domain discovered-servers" 명령의 discovery-mode 매개 변수를 사용하여 다음 검색 옵션 중 하나를 선택할 수 있습니다.

- 도메인의 모든 DC가 검색됩니다.
- 로컬 사이트의 DC만 검색됩니다.

를 클릭합니다 default-site 사이트 및 서비스의 사이트에 할당되지 않은 LIF와 함께 이 모드를 사용하도록 SMB 서버에 대한 매개 변수를 정의할 수 있습니다.

- 서버 검색은 수행되지 않으며, SMB 서버 구성은 기본 DC에만 의존합니다.

이 모드를 사용하려면 먼저 SMB 서버의 기본 DC를 정의해야 합니다.

단계

1. 원하는 검색 옵션을 지정합니다. 'vserver cifs domain discovered-servers discovery-mode modify -vserver_vserver_name_-mode{all|site|none}'

'모드' 파라미터 옵션:

- 모두

사용 가능한 모든 DC를 검색합니다(기본값).

- '사이트'입니다

사이트에 대한 DC 검색을 제한합니다.

- "없음"

검색을 수행하지 않고 기본 DC만 사용하십시오.

기본 도메인 컨트롤러를 추가합니다

ONTAP는 DNS를 통해 도메인 컨트롤러를 자동으로 검색합니다. 필요에 따라 특정 도메인의 기본 도메인 컨트롤러 목록에 하나 이상의 도메인 컨트롤러를 추가할 수 있습니다.

이 작업에 대해

지정된 도메인에 대한 기본 도메인 컨트롤러 목록이 이미 있는 경우 새 목록이 기존 목록과 병합됩니다.

단계

1. 기본 도메인 컨트롤러 목록에 추가하려면 + "vserver cifs domain preferred-dc add-vserver_vserver_name_-domain_domain_name_-preferred-dc ip_address,...+" 명령을 입력합니다

'-vserver_vserver_name_'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-domain_domain_name_'은 지정된 도메인 컨트롤러가 속한 도메인의 정규화된 Active Directory 이름을

지정합니다.

'-preferred-dc_ip_address_',... 기본 설정 도메인 컨트롤러의 IP 주소를 심표로 구분된 목록으로 지정합니다.

예

다음 명령을 실행하면 cifs.lab.example.com 도메인에 대한 외부 액세스를 관리하기 위해 SVM VS1의 SMB 서버가 사용하는 기본 도메인 컨트롤러 목록에 도메인 컨트롤러 172.17.102.25 및 172.17.102.24가 추가됩니다.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain  
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

관련 정보

[기본 도메인 컨트롤러를 관리하는 명령입니다](#)

기본 도메인 컨트롤러를 관리하는 명령입니다

기본 도메인 컨트롤러를 추가, 표시 및 제거하는 명령을 알아야 합니다.

원하는 작업	이 명령 사용...
기본 도메인 컨트롤러를 추가합니다	'vserver cifs domain preferred-dc add'
기본 도메인 컨트롤러를 표시합니다	'vserver cifs domain preferred-dc show'
기본 도메인 컨트롤러를 제거합니다	'vserver cifs domain preferred-dc remove'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

관련 정보

[기본 도메인 컨트롤러 추가 중](#)

도메인 컨트롤러에 대한 **SMB2** 연결을 설정합니다

ONTAP 9.1부터 SMB 버전 2.0을 사용하여 도메인 컨트롤러에 연결할 수 있습니다. 도메인 컨트롤러에서 SMB 1.0을 사용하지 않도록 설정한 경우 이 작업이 필요합니다. ONTAP 9.2부터는 SMB2가 기본적으로 설정됩니다.

이 작업에 대해

'MB2-enabled-for-dc-connections' 명령 옵션을 사용하면 사용 중인 ONTAP 릴리스에 대한 시스템 기본값을 사용할 수 있습니다. ONTAP 9.1의 시스템 기본값은 SMB 1.0에 대해 사용되고 SMB 2.0에는 사용되지 않습니다. ONTAP 9.2의 시스템 기본값은 SMB 1.0에 대해 활성화되어 있고 SMB 2.0에 대해 활성화되어 있습니다. 도메인 컨트롤러가 처음에 SMB 2.0을 협상할 수 없는 경우 SMB 1.0을 사용합니다.

SMB 1.0은 ONTAP에서 도메인 컨트롤러로 비활성화할 수 있습니다. ONTAP 9.1에서 SMB 1.0을 사용하지 않도록 설정한 경우 도메인 컨트롤러와 통신하려면 SMB 2.0을 활성화해야 합니다.

자세히 알아보기:

- "활성화된 SMB 버전을 확인하는 중입니다".
- "지원되는 SMB 버전 및 기능".



SMB1-enabled-for-dc-connections가 false로 설정되어 있고 -SMB1-enabled가 true로 설정되어 있으면 ONTAP은 SMB 1.0 연결을 클라이언트로 거부하지만 인바운드 SMB 1.0 연결을 서버로 계속 허용합니다.

단계

1. SMB 보안 설정을 변경하기 전에 어떤 SMB 버전이 활성화되어 있는지 확인하십시오: "vserver cifs security show"
2. 목록을 아래로 스크롤하여 SMB 버전을 확인합니다.
3. 'SMB2 enabled-for-dc-connections' 옵션을 사용하여 적절한 명령을 수행합니다.

SMB2가 다음과 같은 상태가 되도록 하려면...	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-SMB2-enabled-for-dc-connections true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-SMB2-enabled-for-dc-connections false'

도메인 컨트롤러에 대한 암호화된 연결을 활성화합니다

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다.

이 작업에 대해

ONTAP는 '-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러(DC) 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다.

암호화된 DC 통신이 필요한 경우 ONTAP는 SMB3 연결만 협상하므로 '-SMB2-enabled-for-DC-connections' 옵션이 무시됩니다. DC가 SMB3 및 암호화를 지원하지 않는 경우 ONTAP가 이를 통해 연결되지 않습니다.

단계

1. DC와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver_svm_name_-encryption-required-for-dc-connection true'

null 세션을 사용하여 Kerberos가 아닌 환경의 스토리지에 액세스합니다

Null 세션을 사용하여 Kerberos가 아닌 환경의 스토리지에 액세스 개요

null 세션 액세스는 스토리지 시스템 데이터와 같은 네트워크 리소스 및 로컬 시스템에서

실행되는 클라이언트 기반 서비스에 대한 권한을 제공합니다. 클라이언트 프로세스가 "시스템" 계정을 사용하여 네트워크 리소스에 액세스할 때 Null 세션이 발생합니다. Null 세션 구성은 비 Kerberos 인증에만 적용됩니다.

스토리지 시스템에서 null 세션 액세스를 제공하는 방법

null 세션 공유는 인증이 필요하지 않으므로 null 세션 액세스가 필요한 클라이언트의 IP 주소가 스토리지 시스템에 매핑되어야 합니다.

기본적으로 매핑되지 않은 null 세션 클라이언트는 공유 열거형과 같은 특정 ONTAP 시스템 서비스에 액세스할 수 있지만 스토리지 시스템 데이터에 액세스하지 못하도록 제한됩니다.



ONTAP는 '-restricting-anonymous' 옵션을 사용하여 Windows RestrictAnonymous 레지스트리 설정 값을 지원합니다. 이렇게 하면 매핑되지 않은 null 사용자가 시스템 리소스를 보거나 액세스할 수 있는 범위를 제어할 수 있습니다. 예를 들어 공유 열거를 사용하지 않도록 설정하고 IPC\$ 공유(숨겨진 명명된 파이프 공유)에 액세스할 수 있습니다. 'vserver cifs options modify' 및 'vserver cifs options'에 man page가 표시되어 '-restrict-anonymous' 옵션에 대한 자세한 정보를 제공합니다.

달리 구성하지 않는 한 null 세션을 통해 스토리지 시스템 액세스를 요청하는 로컬 프로세스를 실행하는 클라이언트는 ""Everyone""과 같은 제한적이지 않은 그룹의 구성원입니다. 선택한 스토리지 시스템 리소스에 대해 null 세션 액세스를 제한하려면 모든 null 세션 클라이언트가 속한 그룹을 생성해야 합니다. 이 그룹을 생성하면 스토리지 시스템 액세스를 제한하고 null 세션 클라이언트에 적용되는 스토리지 시스템 리소스 권한을 설정할 수 있습니다.

ONTAP는 'vserver name-mapping' 명령 세트에서 null 사용자 세션을 사용하여 스토리지 시스템 리소스에 액세스할 수 있는 클라이언트의 IP 주소를 지정하는 매핑 구문을 제공합니다. Null 사용자에게 그룹을 생성한 후에는 null 세션에만 적용되는 스토리지 시스템 리소스 및 리소스 권한에 대한 액세스 제한을 지정할 수 있습니다. Null 사용자는 익명 로그온으로 식별됩니다. Null 사용자는 홈 디렉토리에 액세스할 수 없습니다.

매핑된 IP 주소에서 스토리지 시스템을 액세스하는 모든 null 사용자에게 매핑된 사용자 권한이 부여됩니다. null 사용자로 매핑된 스토리지 시스템에 대한 무단 액세스를 방지하려면 적절한 예방 조치를 고려하십시오. 최대한의 보호를 위해, IP 주소 "스포크"의 가능성을 제거하기 위해, 별도의 네트워크에 null 사용자 스토리지 시스템 액세스를 필요로 하는 모든 클라이언트와 스토리지 시스템을 배치하십시오.

관련 정보

익명 사용자에게 대한 액세스 제한 구성

Null 사용자에게 파일 시스템 공유에 대한 액세스 권한을 부여합니다

null 세션 클라이언트가 사용할 그룹을 할당하고 null 세션 클라이언트의 IP 주소를 기록하여 null 세션을 사용하여 데이터를 액세스할 수 있는 스토리지 시스템의 클라이언트 목록에 추가하는 방식으로 null 세션 클라이언트를 통해 스토리지 시스템 리소스에 대한 액세스를 허용할 수 있습니다.

단계

1. "vserver name-mapping create" 명령을 사용하여 Null 사용자를 IP 한정자를 사용하여 유효한 Windows 사용자에게 매핑합니다.

다음 명령을 실행하면 유효한 호스트 이름이 google.com 인 user1에 null 사용자가 매핑됩니다.


```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

다음 명령을 실행하면 유효한 IP 주소가 10.238.2.54/32인 user1에 null 사용자가 매핑됩니다.

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 이름 매핑을 확인하려면 'vserver name-mapping show' 명령을 사용하십시오.

```
vserver name-mapping show

Vserver:    vs1
Direction:  win-unix
Position Hostname      IP Address/Mask
-----
1          -            10.72.40.83/32      Pattern: anonymous logon
                                      Replacement: user1
```

3. "vserver cifs options modify -win-name -for-null-user" 명령을 사용하여 null 사용자에게 Windows 구성원을 할당합니다.

이 옵션은 Null 사용자에게 대해 유효한 이름 매핑이 있는 경우에만 적용할 수 있습니다.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. "vserver cifs options show" 명령을 사용하여 null 사용자가 Windows 사용자 또는 그룹에 매핑되었는지 확인합니다.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

SMB 서버의 NetBIOS 별칭을 관리합니다

SMB 서버의 NetBIOS 별칭 관리 개요

NetBIOS 별칭은 SMB 클라이언트가 SMB 서버에 연결할 때 사용할 수 있는 SMB 서버의 대체

이름입니다. SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 파일 서버의 이름에 응답하도록 할 때 유용할 수 있습니다.

SMB 서버를 생성할 때 또는 SMB 서버를 생성한 후 언제든지 NetBIOS 별칭 목록을 지정할 수 있습니다. 목록에서 NetBIOS 별칭을 언제든지 추가하거나 제거할 수 있습니다. NetBIOS 별칭 목록에 있는 이름을 사용하여 SMB 서버에 연결할 수 있습니다.

관련 정보

[TCP 연결을 통한 NetBIOS에 대한 정보 표시](#)

NetBIOS 별칭 목록을 SMB 서버에 추가합니다

SMB 클라이언트가 별칭을 사용하여 SMB 서버에 접속하도록 하려면 NetBIOS 별칭 목록을 만들거나 NetBIOS 별칭의 기존 목록에 NetBIOS 별칭을 추가할 수 있습니다.

이 작업에 대해

- NetBIOS 별칭 이름은 최대 15자까지 지정할 수 있습니다.
- SMB 서버에서 최대 200개의 NetBIOS 별칭을 구성할 수 있습니다.
- 다음 문자는 허용되지 않습니다.

@# * ()=+[]!,:";<>V?

단계

1. NetBIOS 별칭: + 'vserver cifs add-netbios-alias-vserver_vserver_name_-NetBIOS-alias_netbios_alias,...'를 추가합니다

```
'vserver cifs add-netbios-alias-vserver vs1-netbios-alias alias_1, alias_2, alias_3'
```

- 쉼표로 구분된 목록을 사용하여 하나 이상의 NetBIOS 별칭을 지정할 수 있습니다.
- 지정된 NetBIOS 별칭이 기존 목록에 추가됩니다.
- 목록이 현재 비어 있는 경우 새 NetBIOS 별칭 목록이 생성됩니다.

2. NetBIOS 별칭이 올바르게 추가되었는지 확인합니다. 'vserver cifs show -vserver vserver_name -display -netbios -aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

관련 정보

[NetBIOS 별칭 목록에서 NetBIOS 별칭을 제거합니다](#)

[CIFS 서버에서 NetBIOS 별칭 목록을 표시합니다](#)

NetBIOS 별칭 목록에서 NetBIOS 별칭을 제거합니다

CIFS 서버에 대한 특정 NetBIOS 별칭이 필요하지 않은 경우 목록에서 해당 NetBIOS 별칭을 제거할 수 있습니다. 목록에서 모든 NetBIOS 별칭을 제거할 수도 있습니다.

이 작업에 대해

쉼표로 구분된 목록을 사용하여 둘 이상의 NetBIOS 별칭을 제거할 수 있습니다. '-NetBIOS-aliases' 매개 변수의 값으로 '.'를 지정하여 CIFS 서버에서 모든 NetBIOS 별칭을 제거할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

을(를) 제거하려면...	입력...
목록에서 특정 NetBIOS 별칭	'vserver cifs remove-netbios-alias-vserver_name_-netbios-alias_netbios_alias,...'
목록에서 모든 NetBIOS 별칭	'vserver cifs remove-netbios-aliases-vserver_vserver_name_-netbios-aliases-'

```
'vserver cifs remove-netbios-alias-vserver vs1-netbios-alias_1'
```

2. 지정된 NetBIOS 별칭이 제거되었는지 확인합니다. 'vserver cifs show -vserver_vserver_name_-display-netbios-aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

CIFS 서버의 NetBIOS 별칭 목록을 표시합니다

NetBIOS 별칭 목록을 표시할 수 있습니다. 이 기능은 SMB 클라이언트가 CIFS 서버에 접속할 수 있는 이름 목록을 확인하려는 경우에 유용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	입력...
CIFS 서버의 NetBIOS 별칭입니다	'vserver cifs show-display-netbios-aliases'
자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록입니다	'vserver cifs show-instance'

다음 예에서는 CIFS 서버의 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs show-display-netbios-aliases'

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

다음 예에서는 자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록을 표시합니다.

'vserver cifs show-instance'

```
Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

관련 정보

[CIFS 서버에 NetBIOS 별칭 목록을 추가합니다](#)

[CIFS 서버를 관리하는 명령입니다](#)

SMB 클라이언트가 NetBIOS 별칭을 사용하여 연결되어 있는지 확인합니다

SMB 클라이언트가 NetBIOS 별칭을 사용하여 연결되어 있는지 여부와 연결된 경우 연결에 사용되는 NetBIOS 별칭을 확인할 수 있습니다. 이 기능은 연결 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

SMB 연결에 연결된 NetBIOS 별칭(있는 경우)을 표시하려면 '-instance' 매개 변수를 사용해야 합니다. CIFS 서버 이름 또는 IP 주소를 사용하여 SMB 연결을 수행하는 경우 NetBIOS 이름 필드의 출력은 "-"(하이픈)입니다.

단계

1. 원하는 작업을 수행합니다.

다음에 대한 NetBIOS 정보를 표시하려면...	입력...
SMB 연결	'vserver cifs session show-instance'
지정된 NetBIOS 별칭을 사용하는 연결:	'vserver cifs session show-instance-netbios-name_netbios_name_'

다음 예에서는 세션 ID 1과 SMB 연결을 설정하는 데 사용되는 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs session show-session-id 1-instance'

```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted

```

기타 **SMB** 서버 작업을 관리합니다

CIFS 서버를 중지하거나 시작합니다

사용자가 SMB 공유를 통해 데이터에 액세스하지 않는 상태에서 작업을 수행할 때 유용할 수 있는 SVM에서 CIFS 서버를 중지할 수 있습니다. CIFS 서버를 시작하여 SMB 액세스를 재시작할 수 있습니다. CIFS 서버를 중지하면 스토리지 가상 시스템(SVM)에서 허용되는 프로토콜도 수정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
CIFS 서버를 중지합니다	'vserver cifs stop-vserver_vserver_name_[-foreground{true
false}]'	CIFS 서버를 시작합니다
'vserver cifs start -vserver_vserver_name_[-foreground{true	false}]'

'-foreground'는 포그라운드와 배경에서 명령을 실행할지 여부를 지정합니다. 이 매개 변수를 입력하지 않으면 true로 설정되고 포그라운드에서 명령이 실행됩니다.

2. 'vserver cifs show' 명령을 사용하여 CIFS 서버 관리 상태가 올바른지 확인합니다.

예

다음 명령은 SVM VS1 에서 CIFS 서버를 시작합니다.

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: VS1
NetBIOS Domain/Workgroup Name: DOMAIN
Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
```

관련 정보

[검색된 서버에 대한 정보 표시](#)

[서버 재설정 및 재검색](#)

CIFS 서버를 다른 OU로 이동합니다

CIFS 서버 생성 프로세스는 다른 OU를 지정하지 않는 한 설정 중에 기본 OU(조직 구성 단위) CN=컴퓨터를 사용합니다. 설정 후 CIFS 서버를 다른 OU로 이동할 수 있습니다.

단계

1. Windows 서버에서 * Active Directory 사용자 및 컴퓨터 * 트리를 엽니다.
2. SVM(스토리지 가상 머신)에 대한 Active Directory 개체를 찾습니다.
3. 개체를 마우스 오른쪽 단추로 클릭하고 * 이동 * 을 선택합니다.
4. SVM과 연결할 OU를 선택합니다

결과

SVM 객체가 선택한 OU에 배치됩니다.

SMB 서버를 이동하기 전에 **SVM**에서 동적 **DNS** 도메인을 수정합니다

SMB 서버를 다른 도메인으로 이동할 때 Active Directory 통합 DNS 서버가 DNS에 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SMB 서버를 이동하기 전에 SVM(스토리지 가상 시스템)에서 DDNS(동적 DNS)를 수정해야 합니다.

시작하기 전에

SMB 서버 컴퓨터 계정이 포함될 새 도메인의 서비스 위치 레코드가 포함된 DNS 도메인을 사용하려면 SVM에서 DNS 이름 서비스를 수정해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 합니다.

이 작업에 대해

DDNS(SVM에서 구성된 경우)는 데이터 LIF의 DNS 레코드를 자동으로 새 도메인에 추가하지만 원래 도메인의 DNS 레코드는 원래 DNS 서버에서 자동으로 삭제되지 않습니다. 수동으로 삭제해야 합니다.

SMB 서버를 이동하기 전에 DDNS 수정을 완료하려면 다음 항목을 참조하십시오.

["동적 DNS 서비스를 구성합니다"](#)

SVM을 **Active Directory** 도메인에 연결합니다

"vserver cifs modify" 명령을 사용하여 도메인을 수정하여 기존 SMB 서버를 삭제하지 않고 SVM(스토리지 가상 시스템)을 Active Directory 도메인에 연결할 수 있습니다. 현재 도메인에 다시 참가하거나 새 도메인에 가입할 수 있습니다.

시작하기 전에

- SVM에는 이미 DNS 구성이 있어야 합니다.
- SVM을 위한 DNS 구성은 타겟 도메인을 지원할 수 있어야 합니다.

DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가 포함되어 있어야 합니다.

이 작업에 대해

- Active Directory 도메인 수정을 진행하려면 CIFS 서버의 관리 상태를 "down"으로 설정해야 합니다.
- 명령이 성공적으로 완료되면 관리 상태가 자동으로 ""설정""으로 설정됩니다.
- 도메인에 가입할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

단계

1. SVM을 CIFS 서버 도메인에 가입합니다. 'vserver cifs modify -vserver_vserver_name_-domain_domain_name_-status -admin down'

자세한 내용은 'vserver cifs modify' 명령에 대한 man 페이지를 참조하십시오. 새 도메인에 대한 DNS를 재구성해야 하는 경우 'vserver DNS modify' 명령에 대한 man 페이지를 참조하십시오.

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=_example_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-uri' 매개 변수에 vserver cifs 명령을 포함하여 포함시키십시오.

2. CIFS 서버가 원하는 Active Directory 도메인에 있는지 확인합니다. 'vserver cifs show'

예

다음 예에서는 SVM VS1 의 SMB 서버 ""CIFSSERVER1""이 keytab 인증을 사용하여 example.com 도메인에 연결됩니다.

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

NetBIOS over TCP 연결에 대한 정보를 표시합니다

NBT(NetBIOS over TCP) 연결에 대한 정보를 표시할 수 있습니다. 이는 NetBIOS 관련 문제를 해결할 때 유용할 수 있습니다.

단계

1. 'vserver cifs nbtstat' 명령을 사용하여 NetBIOS over TCP 연결에 대한 정보를 표시합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

예

다음 예제에서는 ""cluster1""에 대해 표시되는 NetBIOS 이름 서비스 정보를 보여 줍니다.


```
cluster1::> vservice cifs nbtstat
```

```
Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2  (active  )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State    Time Left  Type
-----
CLUSTER_1     00                wins     57
CLUSTER_1     20                wins     57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2  (active  )
CLUSTER_1     00                wins     58
CLUSTER_1     20                wins     58
4 entries were displayed.
```

SMB 서버 관리를 위한 명령입니다

생성, 표시, 수정, 중지, 시작 명령을 알아야 합니다. 및 SMB 서버 삭제. 또한 서버를 재설정 및 재검색, 컴퓨터 계정 암호 변경 또는 재설정, 컴퓨터 계정 암호 변경 예약, NetBIOS 별칭 추가 또는 제거 등의 명령도 있습니다.

원하는 작업	이 명령 사용...
SMB 서버를 생성합니다	'vservice cifs create
SMB 서버에 대한 정보를 표시합니다	'vservice cifs show'
SMB 서버를 수정합니다	'vservice cifs modify(가상 CIFS 수정)
SMB 서버를 다른 도메인으로 이동합니다	'vservice cifs modify(가상 CIFS 수정)

SMB 서버를 중지합니다	'vserver cifs stop'
SMB 서버를 시작합니다	'vserver cifs start'를 선택합니다
SMB 서버를 삭제합니다	'vserver cifs delete'
SMB 서버의 서버를 재설정하고 다시 검색합니다	'vserver cifs domain discovered - servers reset-servers'
SMB 서버의 컴퓨터 계정 암호를 변경합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정 암호를 재설정합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정에 대한 자동 암호 변경을 예약합니다	'vserver cifs domain password schedule modify'를 참조하십시오
SMB 서버에 대한 NetBIOS 별칭을 추가합니다	'vserver cifs add-netbios-aliases'
SMB 서버의 NetBIOS 별칭을 제거합니다	'vserver cifs remove-netbios-aliases'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

관련 정보

"SMB 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까"

NetBIOS 이름 서비스를 활성화합니다

ONTAP 9부터는 NetBIOS 이름 서비스(NBNS, Windows 인터넷 이름 서비스 또는 WINS라고도 함)가 기본적으로 사용되지 않습니다. 이전에는 CIFS 지원 SVM(스토리지 가상 머신)이 네트워크에서 WINS가 활성화되었는지 여부에 관계없이 이름 등록 브로드캐스트를 전송했습니다. NBNS가 필요한 구성으로 이러한 브로드캐스트를 제한하려면 새 CIFS 서버에 대해 NBNS를 명시적으로 설정해야 합니다.

시작하기 전에

- 이미 NBNS를 사용하고 있으며 ONTAP 9로 업그레이드하는 경우 이 작업을 완료할 필요가 없습니다. NBNS는 이전과 마찬가지로 계속 작동합니다.
- NBNS는 UDP(포트 137)를 통해 활성화됩니다.
- IPv6을 통한 NBNS는 지원되지 않습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. CIFS 서버에서 NBNS를 설정합니다.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

3. 관리자 권한 수준으로 돌아갑니다.

```
set -privilege admin
```

SMB 액세스 및 SMB 서비스에 IPv6를 사용합니다

IPv6을 사용하기 위한 요구 사항

SMB 서버에서 IPv6를 사용하려면 먼저 IPv6를 지원하는 ONTAP 및 SMB 버전과 라이선스 요구 사항이 무엇인지 알아야 합니다.

ONTAP 라이선스 요구 사항

SMB 라이선스가 있는 경우 IPv6에 대한 특수 라이선스가 필요하지 않습니다. SMB 라이선스는 에 포함되어 있습니다 "[ONTAP 1 을 참조하십시오](#)". ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 버전의 SMB 프로토콜에서 IPv6를 지원합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

SMB 액세스 및 CIFS 서비스를 통해 IPv6를 지원합니다

CIFS 서버에서 IPv6를 사용하려면 ONTAP가 CIFS 서비스에 대한 SMB 액세스 및 네트워크 통신을 위해 IPv6를 지원하는 방법을 알고 있어야 합니다.

Windows 클라이언트 및 서버 지원

ONTAP는 IPv6를 지원하는 Windows 서버 및 클라이언트를 지원합니다. 다음은 Microsoft Windows 클라이언트 및 서버 IPv6 지원에 대한 설명입니다.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 이상에서는 DNS, LDAP, CLDAP 및 Kerberos 서비스를 포함한 SMB 파일 공유 및 Active Directory 서비스에 대해 IPv6를 지원합니다.

IPv6 주소가 구성된 경우 Windows 7 및 Windows Server 2008 이상 릴리즈에서는 Active Directory 서비스에 대해 기본적으로 IPv6를 사용합니다. IPv6 연결을 통한 NTLM 및 Kerberos 인증이 모두 지원됩니다.

ONTAP에서 지원하는 모든 Windows 클라이언트는 IPv6 주소를 사용하여 SMB 공유에 연결할 수 있습니다.

ONTAP가 지원하는 Windows 클라이언트에 대한 최신 정보는 ["상호 운용성 매트릭스"](#).



NT 도메인은 IPv6에서 지원되지 않습니다.

추가 **CIFS** 서비스 지원

ONTAP는 SMB 파일 공유 및 Active Directory 서비스에 대한 IPv6 지원 외에도 다음에 대한 IPv6 지원을 제공합니다.

- 오프라인 폴더, 로밍 프로필, 폴더 리디렉션 및 이전 버전을 포함한 클라이언트측 서비스입니다
- 동적 홈 디렉토리(홈 디렉토리 기능), symlink 및 Widelink, BranchCache, ODX 복사 오프로드, 자동 노드 추천 등의 서버 측 서비스 및 이전 버전
- Windows 로컬 사용자 및 그룹을 사용하여 액세스 제어 및 권한 관리, CLI를 사용한 파일 권한 및 감사 정책 설정, 보안 추적, 파일 잠금 관리, SMB 작업 모니터링 등의 파일 액세스 관리 서비스입니다
- NAS 멀티 프로토콜 감사
- FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유, Witness 프로토콜 및 원격 VSS(SMB 구성 기반 Hyper-V에 사용)

네임 서비스 및 인증 서비스 지원

IPv6에서는 다음 이름 서비스와의 통신이 지원됩니다.

- 도메인 컨트롤러
- DNS 서버
- LDAP 서버
- KDC 서버
- NIS 서버

CIFS 서버가 **IPv6**를 사용하여 외부 서버에 연결하는 방법

요구 사항을 충족하는 구성을 생성하려면 CIFS 서버가 외부 서버에 연결할 때 IPv6을 사용하는 방법을 알고 있어야 합니다.

- 원본 주소 선택

외부 서버에 연결하려고 시도하면 선택한 소스 주소는 대상 주소와 같은 유형이어야 합니다. 예를 들어, IPv6 주소에 연결하는 경우 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)에는 소스 주소로 사용할 IPv6 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다. 마찬가지로, SVM을 IPv4 주소에 연결할 경우 소스 주소로 사용할 IPv4 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다.

- DNS를 사용하여 동적으로 검색된 서버의 경우 서버 검색은 다음과 같이 수행됩니다.
 - 클러스터에서 IPv6이 비활성화되어 있으면 IPv4 서버 주소만 검색됩니다.
 - 클러스터에서 IPv6이 활성화되어 있으면 IPv4 및 IPv6 서버 주소가 모두 검색됩니다. 주소가 속한 서버의 적합성과 IPv6 또는 IPv4 데이터 또는 관리 LIF의 가용성에 따라 두 유형 중 하나를 사용할 수 있습니다. 동적 서버 검색은 도메인 컨트롤러 및 LSA, NETLOGON, Kerberos 및 LDAP와 같은 관련 서비스를 검색하는 데 사용됩니다.

- DNS 서버 연결

DNS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 DNS 이름 서비스 구성에 따라 달라집니다. DNS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 DNS 이름 서비스 구성에서 IPv4 주소를 사용하여 DNS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. DNS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

- LDAP 서버 접속 구성

LDAP 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 LDAP 클라이언트 구성에 따라 달라집니다. LDAP 클라이언트가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결됩니다. 필요한 경우 LDAP 클라이언트 구성에서 IPv4 주소를 사용하여 LDAP 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. LDAP 클라이언트 구성을 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



LDAP 클라이언트 구성은 UNIX 사용자, 그룹 및 넷그룹 이름 서비스에 대해 LDAP를 구성할 때 사용됩니다.

- NIS 서버 접속

NIS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 NIS 이름 서비스 구성에 따라 달라집니다. NIS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 NIS 이름 서비스 구성에서 IPv4 주소를 사용하여 NIS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. NIS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



NIS 이름 서비스는 UNIX 사용자, 그룹, 넷그룹 및 호스트 이름 객체를 저장하고 관리하는 데 사용됩니다.

관련 정보

[SMB를 위한 IPv6 사용\(클러스터 관리자만 해당\)](#)

[IPv6 SMB 세션에 대한 정보 모니터링 및 표시](#)

SMB용 IPv6 사용(클러스터 관리자만 해당)

클러스터 설정 중에 IPv6 네트워크가 활성화되지 않습니다. SMB용 IPv6를 사용하려면 클러스터 설정이 완료된 후 클러스터 관리자가 IPv6을 사용하도록 설정해야 합니다. 클러스터 관리자가 IPv6을 사용하도록 설정하면 전체 클러스터에 대해 설정됩니다.

단계

1. IPv6 사용:'네트워크 옵션 IPv6 수정 사용 참'을 선택합니다

클러스터에서 IPv6 사용 및 IPv6 LIF 구성에 대한 자세한 내용은 [_Network Management Guide_](#)를 참조하십시오.

IPv6이 활성화되었습니다. SMB 액세스를 위한 IPv6 데이터 LIF를 구성할 수 있습니다.

관련 정보

[IPv6 SMB 세션에 대한 정보 모니터링 및 표시](#)

SMB에 대해 IPv6을 사용하지 않도록 설정합니다

네트워크 옵션을 사용하여 클러스터에 IPv6이 설정되어 있어도 동일한 명령을 사용하여 SMB용 IPv6를 해제할 수 없습니다. 대신 ONTAP은 클러스터 관리자가 클러스터에서 마지막 IPv6 사용 인터페이스를 비활성화할 때 IPv6를 비활성화합니다. IPv6 지원 인터페이스 관리에 대해서는 클러스터 관리자와 통신해야 합니다.

클러스터에서 IPv6을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [_Network Management Guide_](#)를 참조하십시오.

관련 정보

["네트워크 관리"](#)

IPv6 SMB 세션에 대한 정보를 모니터링하고 표시합니다

IPv6 네트워크를 사용하여 연결된 SMB 세션에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보는 IPv6 SMB 세션에 대한 기타 유용한 정보와 함께 IPv6를 사용하여 연결 중인 클라이언트를 확인하는 데 유용합니다.

단계

1. 원하는 작업을 수행합니다.

다음 사항을 확인할 수 있습니다.	명령 입력...
SVM(스토리지 가상 시스템)에 대한 SMB 세션은 IPv6를 사용하여 연결됩니다	'vserver cifs session show -vserver_vserver_name_-instance'
IPv6은 지정된 LIF 주소를 통해 SMB 세션에 사용됩니다	'vserver cifs session show -vserver_vserver_name_-lif-address_LIF_ip_address_-instance' 'LIF_IP_address'는 데이터 LIF의 IPv6 주소입니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.