CLI에서 NFS를 관리합니다

ONTAP 9

NetApp
April 24, 2024

목차

CLI에서 NFS를 관리합니다

NFS 참조 개요

ONTAP에는 NFS 프로토콜에 사용할 수 있는 파일 액세스 기능이 포함되어 있습니다. NFS 서버를 사용하도록 설정하고 볼륨 또는 qtree를 내보낼 수 있습니다.

다음과 같은 상황에서 이러한 절차를 수행합니다.

- ONTAP NFS 프로토콜의 기능 범위를 이해하고자 합니다.
- 기본 NFS 구성이 아닌, 덜 일반적인 구성 및 유지보수 작업을 수행하려는 경우
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

NAS 파일 액세스 이해

네임스페이스 및 교차점

네임스페이스 및 교차점 개요

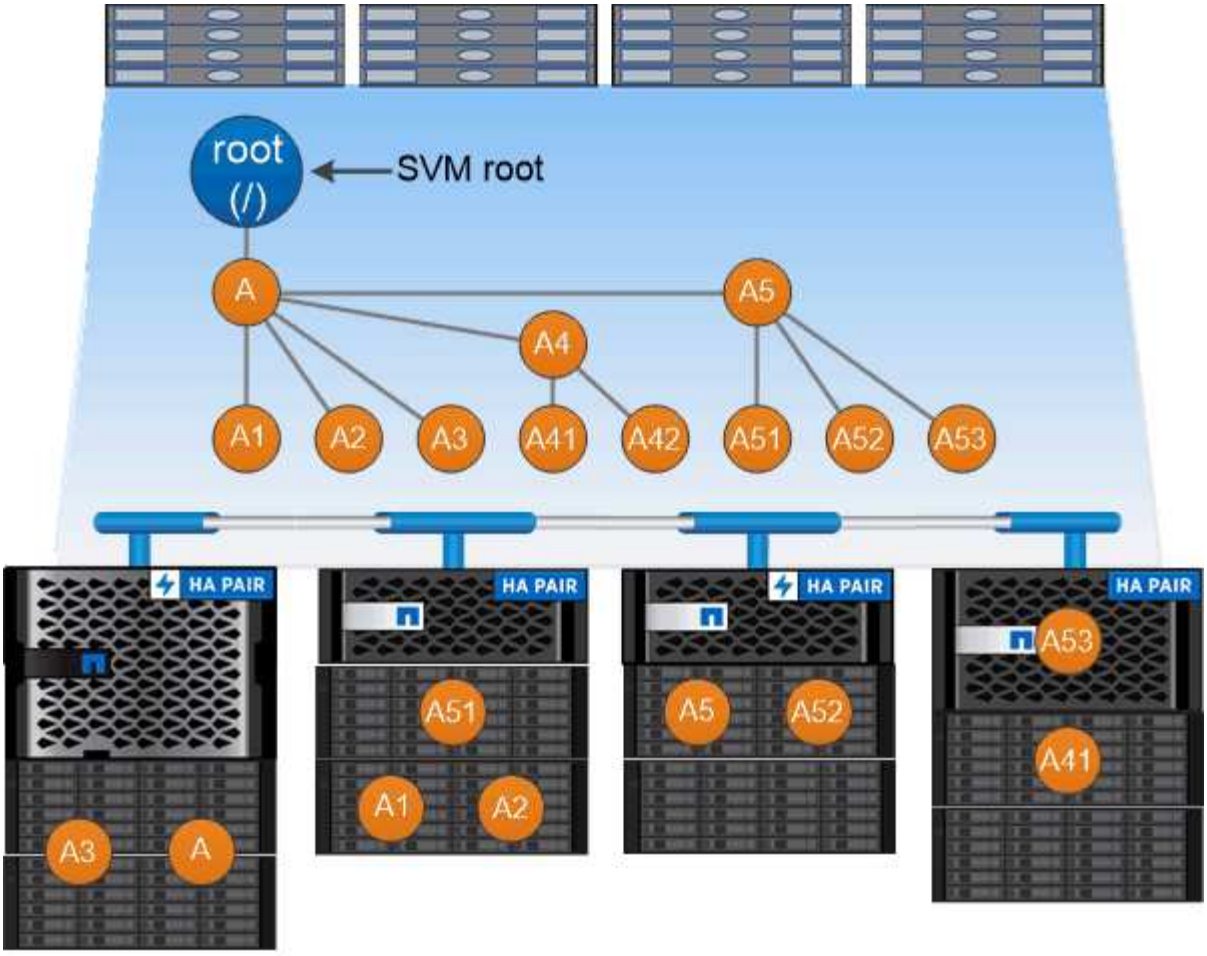
nas_namespace_는 단일 파일 시스템 계층을 생성하기 위해 _junction points_에 함께 결합된 볼륨의 논리적 그룹입니다. 권한이 충분한 클라이언트는 저장소에 있는 파일의 위치를 지정하지 않고 네임스페이스의 파일에 액세스할 수 있습니다. Junced 볼륨은 클러스터의 모든 위치에 상주할 수 있습니다.

관심 파일이 포함된 모든 볼륨을 마운트하는 대신 NAS 클라이언트는 nfs_export_를 마운트하거나 smb_share에 액세스합니다. _ 내보내기 또는 공유는 전체 네임스페이스 또는 네임스페이스 내의 중간 위치를 나타냅니다. 클라이언트는 해당 액세스 지점 아래에 마운트된 볼륨만 액세스합니다.

필요에 따라 네임스페이스에 볼륨을 추가할 수 있습니다. 상위 볼륨 접합 바로 아래 또는 볼륨 내의 디렉토리에 접합 지점을 생성할 수 있습니다. "vol3"이라는 이름의 볼륨에 대한 볼륨 접합부의 경로는 "/vol1/vol2/vol3" 또는 "/vol1/dir2/vol3" 또는 "/dir1/dir2/vol3"일 수 있습니다. 이 경로를 _junction path ._라고 합니다

모든 SVM에는 고유한 네임스페이스가 있습니다. SVM 루트 볼륨은 네임스페이스 계층 구조의 진입점입니다.

> 노드 운영 중단 또는 페일오버 발생 시에도 데이터가 계속 사용 가능하도록 하려면 SVM 루트 볼륨에 대해 _load-sharing mirror_copy를 생성해야 합니다.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

일반적인 **NAS** 네임스페이스 아키텍처란 무엇입니까

SVM 이름 공간을 생성할 때 사용할 수 있는 몇 가지 일반적인 NAS 네임스페이스 아키텍처가 있습니다. 비즈니스 및 워크플로우 요구사항에 맞는 네임스페이스 아키텍처를 선택할 수 있습니다.

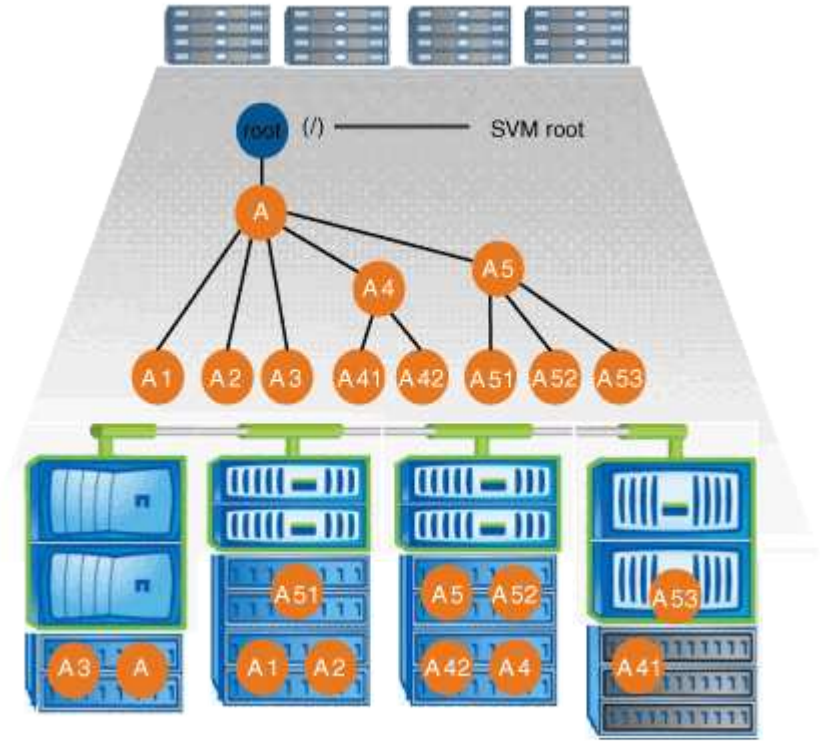
네임스페이스 맨 위에는 항상 루트 볼륨이 있으며, 이 볼륨은 슬래시(/)로 표시됩니다. 루트 아래의 네임스페이스 아키텍처는 세 가지 기본 범주로 분류됩니다.

- 네임스페이스 루트에 대한 단일 분기만 있는 단일 분기 트리

- 여러 개의 분기된 나무는 여러 교차점이 네임스페이스의 루트를 가리킵니다
- 각각 별도의 연결 지점이 있는 여러 독립형 볼륨이 이름 공간의 루트를 가리킵니다

단일 분기 트리가 있는 네임스페이스입니다

단일 분기 트리가 있는 아키텍처는 SVM 네임스페이스의 루트에 대한 단일 삽입 지점을 갖습니다. 단일 삽입 지점은 접합된 볼륨이거나 루트 아래의 디렉토리일 수 있습니다. 다른 모든 볼륨은 단일 삽입 지점(볼륨 또는 디렉토리 가능) 아래의 접합 지점에 마운트됩니다.

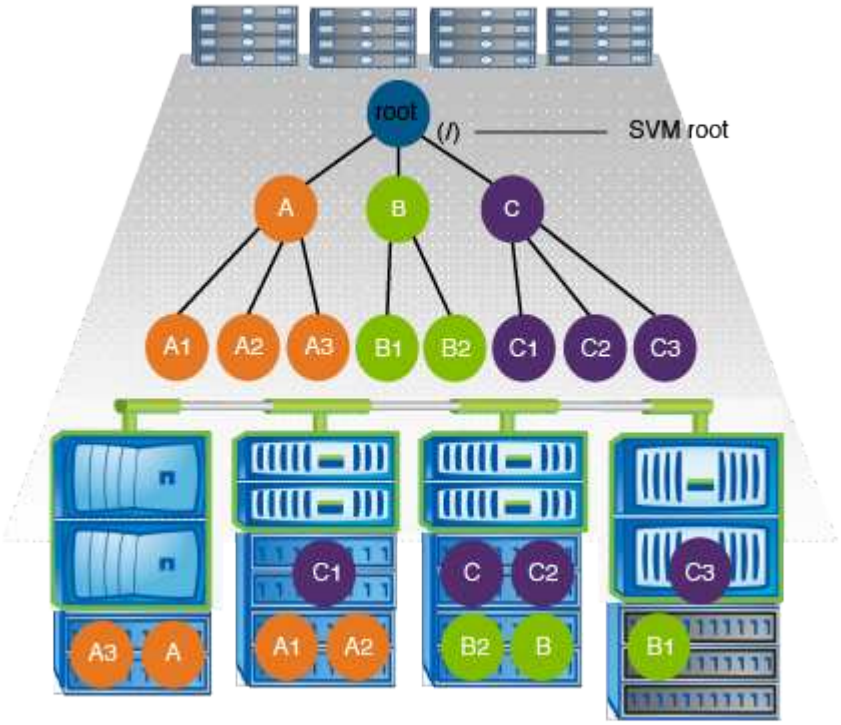


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 연결 구성은 "데이터"라는 디렉토리인 단일 삽입 지점 아래에 모든 볼륨이 접합되는 다음과 같은 구성으로 보일 수 있습니다.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     corp1        true     /data/dir1/corp1       RW_volume
vs1     corp2        true     /data/dir1/corp2       RW_volume
vs1     data1        true     /data/data1            RW_volume
vs1     eng1         true     /data/data1/eng1       RW_volume
vs1     eng2         true     /data/data1/eng2       RW_volume
vs1     sales        true     /data/data1/sales      RW_volume
vs1     vol1         true     /data/vol1             RW_volume
vs1     vol2         true     /data/vol2             RW_volume
vs1     vol3         true     /data/vol3             RW_volume
vs1     vs1_root     -        /                      -
```

여러 개의 분기 트리가 있는 네임스페이스입니다

여러 개의 분기 트리가 있는 아키텍처에는 SVM 네임스페이스의 루트에 대한 여러 삽입 지점이 있습니다. 삽입 지점은 루트 아래의 분기된 볼륨 또는 디렉토리일 수 있습니다. 다른 모든 볼륨은 삽입 지점(볼륨 또는 디렉토리일 수 있음) 아래의 접합 지점에 마운트됩니다.



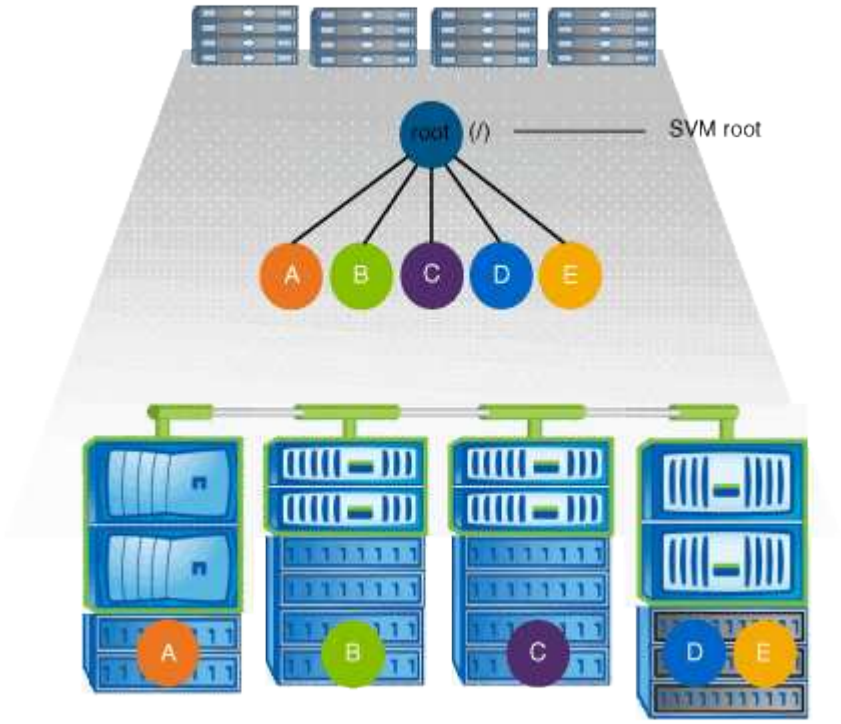
예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 SVM의 루트 볼륨에 세 개의 삽입 지점이 있는 다음과 같은 구성을 예로 들 수 있습니다. 두 개의 삽입 지점은 "다타"와 "프로젝트"라는 디렉토리입니다. 한 삽입 지점은 "audit"이라는 이름의 접합부입니다.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     audit        true     /audit                 RW_volume
vs1     audit_logs1  true     /audit/logs1           RW_volume
vs1     audit_logs2  true     /audit/logs2           RW_volume
vs1     audit_logs3  true     /audit/logs3           RW_volume
vs1     eng          true     /data/eng              RW_volume
vs1     mktg1        true     /data/mktg1            RW_volume
vs1     mktg2        true     /data/mktg2            RW_volume
vs1     project1     true     /projects/project1     RW_volume
vs1     project2     true     /projects/project2     RW_volume
vs1     vs1_root     -        /                      -
```

여러 개의 독립 실행형 볼륨이 있는 네임스페이스

독립 실행형 볼륨이 있는 아키텍처에서 모든 볼륨은 SVM 네임스페이스의 루트에 대한 삽입 지점을 갖습니다. 하지만 볼륨이 다른 볼륨 아래에 접합되지 않습니다. 각 볼륨은 고유한 경로를 가지고 있으며, 루트 바로 아래에 접합되거나

루트 아래의 디렉토리 아래에 접합됩니다.



예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 다음 구성과 비슷합니다. 여기서 SVM의 루트 볼륨에 5개의 삽입 지점을 두고 각 삽입 지점을 단일 볼륨의 경로를 나타냅니다.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     eng           true     /eng                   RW_volume
vs1     mktg          true     /vol/mktg              RW_volume
vs1     project1      true     /project1              RW_volume
vs1     project2      true     /project2              RW_volume
vs1     sales         true     /sales                 RW_volume
vs1     vs1_root      -        /                      -
```

ONTAP에서 파일 액세스를 제어하는 방법

ONTAP에서 파일 액세스를 제어하는 방법 개요

ONTAP는 사용자가 지정하는 인증 기반 및 파일 기반 제한 사항에 따라 파일에 대한 액세스를 제어합니다.

클라이언트가 스토리지 시스템에 접속하여 파일을 액세스하는 경우 ONTAP는 다음 두 가지 작업을 수행해야 합니다.

- 인증

  ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트를 인증해야 합니다. 또한 클라이언트의 인증 유형은

클라이언트가 내보내기 정책을 구성할 때 데이터에 액세스할 수 있는지 여부를 결정하는 데 사용할 수 있는 방법 중 하나입니다(CIFS의 경우 선택 사항).

- 권한 부여

  ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하고 제공할 액세스 유형(있는 경우)을 확인하여 사용자를 승인해야 합니다.

파일 액세스 제어를 제대로 관리하려면 ONTAP가 NIS, LDAP 및 Active Directory 서버와 같은 외부 서비스와 통신해야 합니다. CIFS 또는 NFS를 사용하여 파일 액세스를 위한 스토리지 시스템을 구성하려면 ONTAP의 환경에 따라 적절한 서비스를 설정해야 합니다.

인증 기반 제한

인증 기반 제한 사항을 사용하여 SVM(스토리지 가상 머신)에 연결할 수 있는 클라이언트 시스템과 사용자를 지정할 수 있습니다.

ONTAP는 UNIX 서버와 Windows 서버 모두에서 Kerberos 인증을 지원합니다.

파일 기반 제한 사항

ONTAP은 세 가지 보안 수준을 평가하여 엔티티가 SVM에 있는 파일 및 디렉토리에 대해 요청된 작업을 수행할 수 있는 권한이 있는지 확인합니다. 액세스는 세 가지 보안 수준을 평가한 후 유효한 권한에 의해 결정됩니다.

모든 스토리지 객체에는 최대 3가지 유형의 보안 계층이 포함될 수 있습니다.

- 내보내기(NFS) 및 공유(SMB) 보안

  내보내기 및 공유 보안은 지정된 NFS 내보내기 또는 SMB 공유에 대한 클라이언트 액세스에 적용됩니다. 관리 권한이 있는 사용자는 SMB 및 NFS 클라이언트의 내보내기 및 공유 수준 보안을 관리할 수 있습니다.

- 스토리지 레벨 Access Guard 파일 및 디렉토리 보안

  스토리지 레벨 액세스 가드 보안은 SMB 및 NFS 클라이언트가 SVM 볼륨에 액세스하는 데 적용됩니다. NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

  > NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다.

- NTFS, UNIX 및 NFSv4 네이티브 파일 레벨 보안

  네이티브 파일 레벨 보안은 스토리지 객체를 나타내는 파일 또는 디렉토리에 존재합니다. 클라이언트에서 파일 수준 보안을 설정할 수 있습니다. 파일 권한은 SMB 또는 NFS를 사용하여 데이터를 액세스하든 관계없이 유효합니다.

ONTAP가 NFS 클라이언트 인증을 처리하는 방식

ONTAP에서 NFS 클라이언트 인증을 처리하는 방법 개요

NFS 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 제대로 인증되어야 합니다. ONTAP는 UNIX 자격 증명을 구성하는 이름 서비스와 비교하여 클라이언트를 인증합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 SVM의 이름 서비스 구성에 따라 다른 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. ONTAP는 로컬 UNIX 계정, NIS 도메인 및 LDAP 도메인에 대한 자격 증명을 확인할 수 있습니다. ONTAP가 사용자를 성공적으로 인증할 수 있도록 하나 이상의 사용자를 구성해야 합니다. 여러 개의 이름 서비스와 ONTAP가 서비스를 검색하는 순서를 지정할 수 있습니다.

UNIX 볼륨 보안 스타일을 사용하는 순수 NFS 환경에서는 이 구성으로 NFS 클라이언트에서 접속하는 사용자에 대해 적절한 파일 액세스를 인증하고 제공할 수 있습니다.

혼합, NTFS 또는 통합 볼륨 보안 스타일을 사용하는 경우 ONTAP는 Windows 도메인 컨트롤러에서 인증을 위해 UNIX 사용자의 SMB 사용자 이름을 얻어야 합니다. 이 문제는 로컬 UNIX 계정이나 LDAP 도메인을 사용하여 개별 사용자를 매핑하거나 기본 SMB 사용자를 대신 사용하여 발생할 수 있습니다. ONTAP에서 검색할 이름 서비스를 순서대로 지정하거나 기본 SMB 사용자를 지정할 수 있습니다.

ONTAP에서 이름 서비스를 사용하는 방법

ONTAP는 이름 서비스를 사용하여 사용자 및 클라이언트에 대한 정보를 얻습니다. ONTAP는 이 정보를 사용하여 스토리지 시스템의 데이터에 액세스하거나 데이터를 관리하는 사용자를 인증하고 혼합 환경에서 사용자 자격 증명을 매핑합니다.

스토리지 시스템을 구성할 때 ONTAP에서 인증에 사용할 사용자 자격 증명을 얻기 위해 사용할 이름 서비스를 지정해야 합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자(파일)
- 외부 NIS 도메인(NIS)
- 외부 LDAP 도메인(LDAP)

'vserver services name-service ns-switch' 명령 제품군을 사용하여 소스로 SVM을 구성하여 네트워크 정보 및 검색 순서를 검색할 수 있습니다. 이러한 명령은 UNIX 시스템에서 '/etc/nsswitch.conf' 파일과 동일한 기능을 제공합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 지정된 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. 이름 서비스가 올바르게 구성되어 있고 ONTAP에서 UNIX 자격 증명을 얻을 수 있는 경우 ONTAP는 사용자를 성공적으로 인증합니다.

보안 스타일이 혼합된 환경에서는 ONTAP가 사용자 자격 증명을 매핑해야 할 수 있습니다. ONTAP가 사용자 자격 증명을 적절하게 매핑할 수 있도록 사용자 환경에 맞게 이름 서비스를 구성해야 합니다.

ONTAP에서는 SVM 관리자 계정을 인증하는 데에도 이름 서비스를 사용합니다. 이름 서비스 스위치를 구성하거나 수정할 때 실수로 SVM 관리자 계정에 대한 인증을 비활성화하지 않도록 주의해야 합니다. SVM 관리 사용자에 대한 자세한 내용은 를 참조하십시오 "관리자 인증 및 RBAC".

ONTAP가 NFS 클라이언트에서 SMB 파일 액세스를 허용하는 방법

ONTAP는 Windows NT 파일 시스템(NTFS) 보안 의미를 사용하여 NFS 클라이언트의 UNIX

사용자가 NTFS 권한이 있는 파일에 액세스할 수 있는지 여부를 결정합니다.

ONTAP는 사용자의 UNIX UID(사용자 ID)를 SMB 자격 증명으로 변환한 다음 SMB 자격 증명을 사용하여 사용자에게 파일에 대한 액세스 권한이 있는지 확인합니다. SMB 자격 증명은 일반적으로 사용자의 Windows 사용자 이름인 기본 SID(보안 식별자)와 사용자가 구성원인 Windows 그룹에 해당하는 하나 이상의 그룹 SID로 구성됩니다.

프로세스가 도메인 컨트롤러에 접속하기 때문에 ONTAP가 UNIX UID를 SMB 자격 증명으로 변환하는 데 걸리는 시간은 수십 밀리초에서 수백 밀리초로 지정할 수 있습니다. ONTAP는 UID를 SMB 자격 증명에 매핑하고 자격 증명 캐시에 매핑을 입력하여 변환으로 인한 검증 시간을 줄입니다.

NFS 자격 증명 캐시의 작동 방식

NFS 사용자가 스토리지 시스템의 NFS 내보내기에 대한 액세스를 요청할 경우 ONTAP는 외부 이름 서버 또는 로컬 파일에서 사용자 자격 증명을 검색하여 사용자를 인증해야 합니다. 그런 다음 ONTAP는 나중에 참조할 수 있도록 이러한 자격 증명을 내부 자격 증명 캐시에 저장합니다. NFS 자격 증명 캐시의 작동 방식을 이해하면 잠재적인 성능 및 액세스 문제를 처리할 수 있습니다.

자격 증명 캐시가 없으면 ONTAP는 NFS 사용자가 액세스를 요청할 때마다 이름 서비스를 쿼리해야 합니다. 사용량이 많은 스토리지 시스템에서 많은 사용자가 액세스하는 경우 심각한 성능 문제가 신속하게 발생하여 원치 않는 지연이 발생하거나 NFS 클라이언트 액세스가 거부 될 수 있습니다.

ONTAP는 자격 증명 캐시를 사용하여 사용자 자격 증명을 검색한 다음 NFS 클라이언트가 다른 요청을 보낼 때 빠르고 쉽게 액세스할 수 있도록 미리 결정된 시간 동안 저장합니다. 이 방법은 다음과 같은 이점을 제공합니다.

- NIS 또는 LDAP와 같은 외부 이름 서버에 대한 요청 수를 줄여 스토리지 시스템의 로드를 간소화합니다.
- 외부 네임 서버에 대한 요청 수를 줄여 부하를 덜어줍니다.
- 외부 소스에서 자격 증명을 얻기 위한 대기 시간을 없애 사용자 액세스 속도를 높입니다.

ONTAP는 자격 증명 캐시에 양의 자격 증명과 음의 자격 증명을 모두 저장합니다. 양의 자격 증명은 사용자가 인증되고 액세스 권한이 부여되었음을 의미합니다. 음수 자격 증명은 사용자가 인증되지 않고 액세스가 거부되었음을 의미합니다.

기본적으로 ONTAP는 24시간 동안 양의 자격 증명을 저장합니다. 즉, 처음에 사용자를 인증한 후 ONTAP는 해당 사용자의 액세스 요청에 대해 24시간 동안 캐시된 자격 증명을 사용합니다. 사용자가 24시간 후에 액세스를 요청하면 주기가 다시 시작됩니다. ONTAP 는 캐시된 자격 증명을 삭제하고 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 24시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 24시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

기본적으로 ONTAP는 2시간 동안 부정 자격 증명을 저장합니다. 즉, 처음에 사용자에 대한 액세스를 거부하면 ONTAP는 해당 사용자의 액세스 요청을 2시간 동안 계속 거부합니다. 사용자가 2시간 후에 액세스를 요청하는 경우 주기가 다시 시작됩니다. ONTAP 는 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 2시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 2시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

지정된 교차점으로 데이터 볼륨을 생성합니다

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1 부터는 용량 분석 및 활동 추적 기능이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 을 실행합니다 `volume create` 명령을 사용합니다 `-analytics-state` 또는 `-activity -tracking-state` 를 로 설정합니다 `on`.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 파일 시스템 분석 설정.

> 다음 문자는 접합 경로에 사용할 수 없습니다. *#"><|? \

또한, 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. 교차점으로 볼륨을 생성합니다.

   'volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size{integer[KB|MB|GB|TB|PB]}-security-style{NTFS|UNIX|MIXED}-junction-path_junction_path_'입니다

   접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

   볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

   교차경로는 대/소문자를 구분하지 않고 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, 교차점이 /eng인 경우 SMB 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

   데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 자세한 내용은 볼륨 만들기 명령에 대한 man 페이지를 참조하십시오.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

   'volume show -vserver_vserver_name_-volume_volume_name_-junction'

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                   Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

교차점을 지정하지 않고 데이터 볼륨을 생성합니다

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1 부터는 용량 분석 및 활동 추적 기능이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 을 실행합니다 `volume create` 명령을 사용합니다 `-analytics-state` 또는 `-activity -tracking-state` 를 로 설정합니다 `on`.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 파일 시스템 분석 설정.

단계

1. 다음 명령을 사용하여 교차점 없이 볼륨을 생성합니다.

   'volume create-vserver vserver_name-volume volume_name-aggregate aggregate_name-size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'입니다

   볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

   데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 자세한 내용은 볼륨 만들기 명령에 대한 man 페이지를 참조하십시오.

2. 볼륨이 교차점 없이 생성되었는지 확인합니다.

   'volume show -vserver vserver_name -volume volume_name -junction'

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NAS 네임스페이스에서 기존 볼륨을 마운트 또는 마운트 해제합니다

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.

> 볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오.
>
> "ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 엑스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
볼륨을 마운트합니다	'volume mount-vserver_svm_name_-volume_volume_name_-junction-path_junction_path_'

원하는 작업	명령 입력...

볼륨을 마운트 해제합니다	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

예

다음 예에서는 SVM ""VS1""에 있는 ""판매""라는 볼륨을 접합 지점 """/판매""에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

다음 예에서는 SVM ""VS1""에 있는 ""데이터""라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이

정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

를 표시하려면…	명령 입력…
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보	'volume show -vserver_vserver_name_-junction'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보	'volume show -vserver_vserver_name_-volume_volume_name_ -instance'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보	a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다 b. '-fields' 매개 변수 'volume show-vserver_vserver_name_-fields_fieldname_,…'를 사용하여 원하는 정보를 표시합니다

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data            RW_volume
vs1       home4       true     /eng/home        RW_volume
vs1       vs1_root    -        /                -
vs1       sales       true     /sales           RW_volume
```

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

보안 스타일과 그 효과는 무엇입니까

UNIX, NTFS, 혼합 및 통합 등 네 가지 보안 유형이 있습니다. 각 보안 스타일은 데이터에 대한 사용 권한이 처리되는 방식에 다른 영향을 줍니다. 용도에 맞는 적절한 보안 스타일을 선택할 수 있도록 다양한 효과를 이해해야 합니다.

보안 스타일은 클라이언트 유형이 데이터에 액세스할 수 있거나 액세스할 수 없는 형식을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 ONTAP에서 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

예를 들어, 볼륨이 UNIX 보안 스타일을 사용하는 경우에도 SMB 클라이언트는 ONTAP의 멀티 프로토콜 특성으로 인해 데이터에 액세스(적절하게 인증 및 승인)할 수 있습니다. 그러나 ONTAP에서는 UNIX 클라이언트만 기본 툴을 사용하여 수정할 수 있는 UNIX 권한을 사용합니다.

보안 스타일	사용 권한을 수정할 수 있는 클라이언트입니다	클라이언트가 사용할 수 있는 권한	결과적으로 효율적인 보안 스타일을 제공합니다	파일에 액세스할 수 있는 클라이언트입니다
Unix	NFS 를 참조하십시오	NFSv3 모드 비트	Unix	NFS 및 SMB
		NFSv4.x ACL		
NTFS입니다	중소기업	NTFS ACL	NTFS입니다	
혼합	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.ACL		
		NTFS ACL	NTFS입니다	
통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당)	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.1 ACL		
		NTFS ACL	NTFS입니다	

FlexVol 볼륨은 UNIX, NTFS 및 혼합 보안 스타일을 지원합니다. 보안 스타일이 혼합 또는 통합된 경우 사용자가 보안 스타일을 개별적으로 설정하므로 사용자가 마지막으로 권한을 수정한 클라이언트 유형에 따라 유효 사용 권한이 달라집니다. 권한을 수정한 마지막 클라이언트가 NFSv3 클라이언트인 경우 사용 권한은 UNIX NFSv3 모드 비트입니다. 마지막 클라이언트가 NFSv4 클라이언트인 경우 사용 권한은 NFSv4 ACL입니다. 마지막 클라이언트가 SMB 클라이언트인 경우 사용 권한은 Windows NTFS ACL입니다.

통합 보안 스타일은 ONTAP 9.5 이상 릴리스에서 더 이상 지원되지 않는 무한 볼륨에서만 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexGroup 볼륨 관리 개요.

ONTAP 9.2부터 vserver security file-directory 명령에 대한 'show-Effective-permissions' 매개 변수를 사용하면 지정된 파일 또는 폴더 경로에서 Windows 또는 UNIX 사용자에게 부여된 유효한 권한을 표시할 수 있습니다. 또한 선택적 매개 변수 '-share-name'을 사용하면 유효 공유 권한을 표시할 수 있습니다.

> ONTAP는 처음에 일부 기본 파일 권한을 설정합니다. 기본적으로 UNIX, 혼합 및 통합 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 UNIX이고, 기본 보안 스타일에 의해 허용되는 대로 클라이언트에 의해 구성될 때까지 유효 사용 권한 유형은 UNIX 모드 비트(별도로 지정하지 않는 경우 0755)입니다. 기본적으로 NTFS 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 NTFS이며 ACL을 통해 모든 사람에게 모든 권한을 제공할 수 있습니다.

보안 스타일을 설정하는 위치 및 시기

보안 스타일은 FlexVol 볼륨(루트 또는 데이터 볼륨) 및 qtree에서 설정할 수 있습니다. 보안 스타일은 생성 시 수동으로 설정하거나 자동으로 상속하거나 나중에 변경할 수 있습니다.

SVM에 사용할 보안 유형을 결정합니다

볼륨에 사용할 보안 스타일을 결정하는 데 도움이 되도록 두 가지 요소를 고려해야 합니다. 기본 요소는 파일 시스템을 관리하는 관리자 유형입니다. 2차 요소는 볼륨의 데이터에 액세스하는 사용자 또는 서비스의 유형입니다.

볼륨에 보안 스타일을 구성할 때는 최상의 보안 스타일을 선택하고 사용 권한 관리 문제를 피하기 위해 환경의 요구 사항을 고려해야 합니다. 다음 고려 사항을 통해 결정을 내릴 수 있습니다.

보안 스타일	다음 경우에 선택…
Unix	• 파일 시스템은 UNIX 관리자가 관리합니다. • 대부분의 사용자는 NFS 클라이언트입니다. • 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.
NTFS입니다	• 파일 시스템은 Windows 관리자가 관리합니다. • 대부분의 사용자는 SMB 클라이언트입니다. • 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.
혼합	• 파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

보안 스타일 상속의 작동 방식

새 FlexVol 볼륨 또는 qtree를 생성할 때 보안 스타일을 지정하지 않으면 보안 스타일이 다른 방식으로 상속됩니다.

보안 스타일은 다음과 같은 방식으로 상속됩니다.

- FlexVol 볼륨은 SVM이 포함된 루트 볼륨의 보안 스타일을 상속합니다.
- qtree는 포함된 FlexVol 볼륨의 보안 스타일을 상속합니다.
- 파일 또는 디렉토리는 포함된 FlexVol 볼륨 또는 qtree의 보안 스타일을 상속합니다.

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.

SVM 루트 볼륨에 보안 스타일을 구성합니다

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

   루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

2. 생성한 SVM의 루트 볼륨 보안 유형을 포함하여 구성을 표시하고 확인합니다.

   'vserver show -vserver_vserver_name_'

FlexVol 볼륨에서 보안 스타일을 구성합니다

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

FlexVol 볼륨이	명령 사용…
아직 없습니다	보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다.
이미 있습니다	볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.

FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

   'volume show-volume volume_name-instance'

Qtree에서 보안 스타일 구성

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

qtree가…	명령 사용…
아직 없습니다	볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다.
이미 있습니다	볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.

   qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합 입니다.

   Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

   '볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 'volume qtree show-qtree_qtree_name_-instance' 명령을 입력합니다

NFS를 사용하여 파일 액세스를 설정합니다

NFS 개요를 사용하여 파일 액세스 설정

고객이 NFS를 사용하여 SVM(스토리지 가상 시스템)의 파일에 액세스할 수 있도록 하려면 여러 단계를 완료해야 합니다. 환경의 현재 구성에 따라 몇 가지 추가 단계가 선택적으로 제공됩니다.

클라이언트가 NFS를 사용하여 SVM의 파일에 액세스할 수 있으려면 다음 작업을 완료해야 합니다.

1. SVM에서 NFS 프로토콜을 활성화합니다.

   NFS를 통해 클라이언트에서 데이터에 액세스할 수 있도록 SVM을 구성해야 합니다.

2. SVM에서 NFS 서버를 생성합니다.

   NFS 서버는 SVM에서 NFS를 통해 파일을 처리할 수 있는 논리적 엔터티입니다. NFS 서버를 생성하고 허용할 NFS 프로토콜 버전을 지정해야 합니다.

3. SVM에 엑스포트 정책을 구성합니다.

   클라이언트에서 볼륨 및 qtree를 사용할 수 있도록 엑스포트 정책을 구성해야 합니다.

4. 네트워크 및 스토리지 환경에 따라 적절한 보안 및 기타 설정으로 NFS 서버를 구성합니다.

   이 단계에는 Kerberos, LDAP, NIS, 이름 매핑 및 로컬 사용자 구성이 포함될 수 있습니다.

내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

엑스포트 정책이 볼륨 또는 **qtree**에 대한 클라이언트 액세스를 제어하는 방법

엑스포트 정책에는 각 클라이언트 액세스 요청을 처리하는 _export rules_이 하나 이상 포함되어 있습니다. 프로세스 결과에 따라 클라이언트가 거부되었는지, 액세스 권한이 부여되었는지, 액세스 수준이 결정됩니다. 클라이언트가 데이터에 액세스할 수 있도록 SVM(스토리지 가상 시스템)에 엑스포트 규칙과 함께 엑스포트 정책이 있어야 합니다.

볼륨 또는 qtree에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨 또는 qtree에 정확히 하나의 엑스포트 정책을 연결합니다. SVM에는 여러 엑스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨 또는 qtree를 사용하는 SVM에 대해 다음을 수행할 수 있습니다.

- 개별 클라이언트 액세스 제어를 SVM의 각 볼륨 또는 qtree에 서로 다른 엑스포트 정책을 지정하여 각 볼륨 또는 qtree에 대한 볼륨 또는 qtree를 관리할 수 있습니다.
- 각 볼륨 또는 qtree에 대해 새로운 엑스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨 또는 qtree에 동일한 엑스포트 정책을 할당합니다.

클라이언트가 해당 엑스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우 권한 거부 메시지와 함께 요청이 실패합니다. 클라이언트가 엑스포트 정책의 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다.

ONTAP를 실행하는 시스템에서 엑스포트 정책을 동적으로 수정할 수 있습니다.

SVM에 대한 기본 엑스포트 정책

각 SVM에는 규칙이 없는 기본 엑스포트 정책이 있습니다. 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 규칙과 함께 엑스포트 정책이 있어야 합니다. SVM에 포함된 각 FlexVol 볼륨은 엑스포트 정책과 연결되어야 합니다.

SVM을 생성할 때 스토리지 시스템은 SVM의 루트 볼륨에 대한 기본 엑스포트 정책인 'Default'를 자동으로 생성합니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다. 또는 규칙을 사용하여 사용자 지정 엑스포트 정책을 생성할 수도 있습니다. 기본 엑스포트 정책을 수정 및 변경할 수 있지만, 기본 엑스포트 정책은 삭제할 수 없습니다.

SVM이 포함된 FlexVol 볼륨에서 스토리지 시스템은 볼륨을 생성한 후 SVM의 루트 볼륨에 대한 기본 엑스포트 정책과 연결합니다. 기본적으로 SVM에서 생성된 각 볼륨은 루트 볼륨의 기본 엑스포트 정책과 연결됩니다. SVM에 포함된

모든 볼륨에 기본 엑스포트 정책을 사용하거나, 각 볼륨에 대해 고유한 엑스포트 정책을 생성할 수 있습니다. 여러 볼륨을 동일한 엑스포트 정책에 연결할 수 있습니다.

엑스포트 규칙의 작동 방식

내보내기 규칙은 엑스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성한 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 엑스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 엑스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
- 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.

  '-clientmatch' 필드의 최대 크기는 4096자입니다.

- Kerberos v5, NTLM 또는 AUTH_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.

> ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하고 결과를 표시하며, 이 명령을 사용하여 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다.
>
> 명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS

- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

목록에 없는 보안 유형으로 클라이언트를 관리합니다

클라이언트가 엑스포트 규칙의 액세스 매개 변수에 나열되지 않은 보안 유형을 자체적으로 표시할 경우, 액세스 매개 변수에서 "없음" 옵션을 사용하는 대신 클라이언트에 대한 액세스를 거부하거나 익명 사용자 ID에 매핑할 수 있습니다.

클라이언트는 다른 보안 유형으로 인증되었거나 전혀 인증되지 않았기 때문에 액세스 매개 변수에 나열되지 않은 보안 형식(security type AUTH_none)으로 자신을 나타낼 수 있습니다. 기본적으로 클라이언트는 해당 수준에 대한 액세스가 자동으로 거부됩니다. 그러나, 액세스 파라미터에 'none' 옵션을 추가할 수 있습니다. 따라서 목록에 없는 보안 스타일이 있는 클라이언트는 대신 익명 사용자 ID에 매핑됩니다. '-anon' 매개 변수는 해당 클라이언트에 할당되는 사용자 ID를 결정합니다. '-anon' 매개 변수에 지정된 사용자 ID는 익명 사용자에게 적합한 권한으로 구성된 유효한 사용자여야 합니다.

'-anon' 파라미터의 유효 값은 0부터 65535까지입니다.

'-anon'에 할당된 사용자 **ID**입니다	이로 인해 클라이언트 액세스 요청이 처리되었습니다
0-65533	클라이언트 액세스 요청은 익명 사용자 ID에 매핑되며 이 사용자에 대해 구성된 권한에 따라 액세스를 가져옵니다.

'-anon'에 할당된 사용자 ID입니다	이로 인해 클라이언트 액세스 요청이 처리되었습니다
65534	클라이언트 액세스 요청이 nobody 사용자에게 매핑되고 이 사용자에 대해 구성된 권한에 따라 액세스 권한이 부여됩니다. 이것이 기본값입니다.
65,535입니다	이 ID에 매핑되면 클라이언트의 액세스 요청이 거부되고 클라이언트는 보안 유형 AUTH_NONE으로 표시됩니다. 사용자 ID가 0인 클라이언트의 액세스 요청은 이 ID에 매핑될 때 거부되며 클라이언트는 다른 보안 유형을 제공합니다.

none 옵션을 사용할 때는 읽기 전용 매개변수가 먼저 처리된다는 점을 기억해야 합니다. 목록에 없는 보안 유형의 클라이언트에 대한 내보내기 규칙을 구성할 때 다음 지침을 고려하십시오.

읽기 전용에는 없음 이 포함됩니다	읽기-쓰기에는 없음도 있습니다	목록에 없는 보안 유형의 클라이언트에 대한 액세스
아니요	아니요	거부됨
아니요	예	읽기 전용이 먼저 처리되므로 거부됩니다
예	아니요	익명 읽기 전용
예	예	익명으로서 읽기-쓰기

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- "어이, 없습니다.
- '어다나'
- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개

변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 모든 보안 유형에 대해 읽기-쓰기 액세스를 허용하지만 이 경우에는 읽기 전용 규칙에 의해 이미 필터링된 클라이언트에만 적용됩니다.

따라서 클라이언트 #1과 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 고유한 사용자 ID를 사용하여 읽기-쓰기 권한을 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- "어이, 없습니다.
- '-rwrule' none
- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개 변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 익명 사용자로만 읽기-쓰기 액세스를 허용합니다.

따라서 클라이언트 #1과 클라이언트 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 자체 사용자 ID를 사용하여 읽기 전용 액세스를 얻지만 읽기-쓰기 액세스는 거부됩니다.

보안 유형이 클라이언트 액세스 수준을 결정하는 방법

클라이언트가 에서 인증한 보안 유형은 내보내기 규칙에서 특별한 역할을 합니다. 보안 유형에 따라 클라이언트가 볼륨 또는 qtree에 액세스하는 액세스 수준이 어떻게 결정되는지 이해해야 합니다.

세 가지 액세스 수준은 다음과 같습니다.

1. 읽기 전용
2. 읽기-쓰기
3. 슈퍼유저(사용자 ID가 0인 클라이언트의 경우)

보안 유형별 액세스 수준은 이 순서대로 평가되므로 내보내기 규칙에서 액세스 수준 매개 변수를 구성할 때 다음 규칙을 준수해야 합니다.

클라이언트가 액세스 레벨을 얻는 경우...	이러한 액세스 매개 변수는 클라이언트의 보안 유형과 일치해야 합니다.
일반 사용자 읽기 전용	읽기 전용('-rorule')
일반 사용자 읽기-쓰기	읽기 전용('-rorule') 및 읽기/쓰기('-rwrule')
고급 사용자 읽기 전용	읽기 전용('rorule') 및 '-superuser'
고급 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule') 및 '-superuser'

다음은 이러한 세 가지 액세스 매개 변수 각각에 대해 유효한 보안 유형입니다.

- 모두
- "없음"
- "안 돼.

  이 보안 유형은 '-superuser' 매개변수와 함께 사용할 수 없습니다.

- krb5
- krb5i
- 크르b5p
- NTLM
- '스'입니다

클라이언트의 보안 유형을 세 가지 액세스 매개 변수 각각에 일치시킬 경우 다음과 같은 세 가지 결과가 발생할 수 있습니다.

클라이언트의 보안 유형인 경우...	그러면 고객은...
access 매개 변수에 지정된 것과 일치합니다.	해당 사용자 ID를 사용하여 해당 수준에 대한 액세스를 가져옵니다.
지정된 옵션과 일치하지 않지만 액세스 매개 변수에는 '없음' 옵션이 포함됩니다.	'-anon' 매개 변수로 지정한 사용자 ID를 가진 익명 사용자로 해당 수준에 대한 액세스를 가져옵니다.
지정된 옵션과 일치하지 않으며 액세스 매개 변수에 '없음' 옵션이 포함되어 있지 않습니다.	이 수준은 지정되지 않은 경우에도 항상 '없음'을 포함하므로 '-superuser' 매개 변수에는 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'

- 모든 것
- '-rwrule"s, krb5'
- 슈퍼유저 krb5

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, 사용자 ID 0이 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, 인증하지 않았습니다(AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두와 일치합니다. 읽기 전용 매개 변수는 보안 유형에 관계없이 모든 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 AUTH_SYS 또는 Kerberos v5로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기-쓰기 액세스를 허용합니다. 슈퍼유저 매개 변수를 사용하면 Kerberos v5로 인증된 사용자 ID 0을 가진 클라이언트에 슈퍼유저 액세스가 가능합니다.

따라서 클라이언트 #1은 세 가지 액세스 매개 변수와 모두 일치하기 때문에 수퍼유저 읽기-쓰기 액세스 권한을 얻습니다. 클라이언트 #2에 읽기-쓰기 액세스 권한이 있지만 고급 사용자 액세스 권한이 없습니다. 클라이언트 #3은 읽기 전용 액세스 권한을 얻지만 고급 사용자 액세스는 받지 않습니다.

고급 사용자 액세스 요청을 관리합니다

엑스포트 정책을 구성할 때는 스토리지 시스템이 사용자 ID 0의 클라이언트 액세스 요청을 받으면 수행할 작업을 고려해야 합니다. 즉, 고급 사용자로서 엑스포트 규칙을 설정해야 합니다.

UNIX 환경에서 사용자 ID 0을 가진 사용자는 일반적으로 시스템에 대한 무제한 액세스 권한이 있는 슈퍼유저라고 합니다. 고급 사용자 권한을 사용하는 것은 시스템 위반 및 데이터 보안을 비롯한 여러 가지 이유로 위험할 수 있습니다.

기본적으로 ONTAP는 사용자 ID 0을 사용하는 클라이언트를 익명 사용자에게 매핑합니다. 그러나 내보내기 규칙에서 '-superuser' 매개 변수를 지정하여 보안 유형에 따라 사용자 ID 0으로 나타나는 클라이언트를 처리하는 방법을 결정할 수 있습니다. 다음은 '-superuser' 파라미터에 대한 유효한 옵션입니다.

- 모두
- "없음"

  이 설정은 '-superuser' 파라미터를 지정하지 않을 경우 기본 설정입니다.

- krb5
- NTLM
- '스'입니다

'-superuser' 매개 변수 구성에 따라 사용자 ID 0으로 표시하는 클라이언트가 처리되는 방법에는 두 가지가 있습니다.

'-superuser' 매개변수와 클라이언트의 보안 유형이...	그러면 고객은...
일치	사용자 ID 0을 사용하여 수퍼유저 액세스 권한을 가져옵니다.

'-superuser' 매개변수와 클라이언트의 보안 유형이...	그러면 고객은...
일치하지 않습니다	'-anon' 매개 변수에 지정된 사용자 ID와 할당된 사용 권한을 가진 익명 사용자로 액세스를 가져옵니다. 이는 읽기 전용 또는 읽기/쓰기 매개 변수가 '없음' 옵션을 지정하는지 여부에 관계없이 적용됩니다.

클라이언트가 NTFS 보안 스타일로 볼륨에 액세스하기 위해 사용자 ID 0을 제공하고 '-superuser' 매개 변수가 'none'으로 설정된 경우 ONTAP는 익명 사용자의 이름 매핑을 사용하여 적절한 자격 증명을 얻습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM
- '-anon"127

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID 746을 가지고 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5를 사용하여 인증합니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다.

클라이언트 #2에서 수퍼유저 액세스 권한을 얻을 수 없습니다. 대신 '-superuser' 매개 변수가 지정되지 않아 익명으로 매핑됩니다. 즉, 기본적으로 '없음'으로 설정되어 있으며 사용자 ID 0을 익명으로 자동 매핑합니다. 또한 보안 형식이 읽기-쓰기 매개 변수와 일치하지 않기 때문에 클라이언트 #2는 읽기 전용 액세스만 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM
- 슈퍼유저 krb5
- 0

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을

보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

내보내기 규칙은 사용자 ID가 0인 클라이언트에 대한 수퍼유저 액세스를 허용합니다. 클라이언트 #1은 읽기 전용 및 '-superuser' 매개 변수의 사용자 ID와 보안 유형과 일치하기 때문에 수퍼유저 액세스 권한을 얻습니다. 보안 유형이 읽기-쓰기 매개 변수나 '-superuser' 매개 변수와 일치하지 않기 때문에 클라이언트 #2에서 읽기-쓰기 또는 수퍼유저 액세스 권한을 얻지 못합니다. 대신 클라이언트 #2가 익명 사용자에게 매핑되며 이 경우 사용자 ID 0이 있습니다.

ONTAP에서 엑스포트 정책 캐시를 사용하는 방법

시스템 성능을 개선하기 위해 ONTAP는 로컬 캐시를 사용하여 호스트 이름 및 넷그룹과 같은 정보를 저장합니다. 이렇게 하면 ONTAP에서 외부 소스에서 정보를 검색하는 것보다 내보내기 정책 규칙을 더 빠르게 처리할 수 있습니다. 캐시의 정의 및 작업을 이해하면 클라이언트 액세스 문제를 해결하는 데 도움이 됩니다.

NFS 내보내기에 대한 클라이언트 액세스를 제어하기 위해 엑스포트 정책을 구성합니다. 각 엑스포트 정책에는 규칙이 포함되어 있으며, 각 규칙에는 액세스를 요청하는 클라이언트와 규칙을 일치시키는 매개 변수가 포함되어 있습니다. 이러한 매개 변수 중 일부는 도메인 이름, 호스트 이름 또는 넷그룹과 같은 개체를 확인하기 위해 ONTAP에서 DNS 또는 NIS 서버와 같은 외부 소스에 연결해야 합니다.

외부 소스와의 이러한 통신에는 약간의 시간이 소요됩니다. 성능을 높이기 위해 ONTAP는 여러 캐시의 각 노드에 정보를 로컬로 저장하여 엑스포트 정책 규칙 개체를 해결하는 데 걸리는 시간을 단축합니다.

캐시 이름입니다	저장된 정보의 유형입니다
액세스	해당 엑스포트 정책에 대한 클라이언트 매핑
이름	UNIX 사용자 이름을 해당 UNIX 사용자 ID에 매핑
ID입니다	UNIX 사용자 ID와 해당 UNIX 사용자 ID 및 확장 UNIX 그룹 ID의 매핑
호스트	호스트 이름을 해당 IP 주소에 매핑
넷그룹	구성원의 해당 IP 주소에 대한 넷그룹 매핑
쇼마운트	SVM 네임스페이스에서 내보낸 디렉토리 목록입니다

ONTAP에서 검색 및 로컬에 저장한 후 환경에 있는 외부 이름 서버의 정보를 변경하면 캐시에 오래된 정보가 포함될 수 있습니다. ONTAP를 새로 고치면 특정 기간이 지나면 자동으로 캐시가 새로 고쳐지지만 다른 캐시에 만료 및 새로 고침 시간과 알고리즘이 다릅니다.

캐시에 오래된 정보가 포함되는 또 다른 가능한 이유는 ONTAP가 캐시된 정보를 새로 고치려고 하지만 이름 서버와 통신하려고 할 때 오류가 발생하는 것입니다. 이 경우 ONTAP는 클라이언트 중단을 방지하기 위해 로컬 캐시에 현재 저장되어 있는 정보를 계속 사용합니다.

따라서 성공해야 하는 클라이언트 액세스 요청이 실패하고 실패해야 하는 클라이언트 액세스 요청이 성공할 수 있습니다. 이러한 클라이언트 액세스 문제를 해결할 때 일부 엑스포트 정책 캐시를 보고 수동으로 플러시할 수 있습니다.

액세스 캐시의 작동 방식

ONTAP은 액세스 캐시를 사용하여 클라이언트 액세스 작업에 대한 엑스포트 정책 규칙 평가 결과를 볼륨 또는 qtree에 저장합니다. 따라서 클라이언트가 입출력 요청을 보낼 때마다 내보내기 정책 규칙 평가 프로세스를 거치는 것보다 액세스 캐시에서 정보를 훨씬 빠르게 검색할 수 있기 때문에 성능이 향상됩니다.

NFS 클라이언트가 볼륨 또는 qtree의 데이터에 액세스하기 위해 I/O 요청을 보낼 때마다 ONTAP는 각 I/O 요청을 평가하여 I/O 요청을 허용하거나 거부할 것인지 결정해야 합니다. 이 평가에서는 볼륨 또는 qtree와 관련된 엑스포트 정책의 모든 엑스포트 정책 규칙을 검사합니다. 볼륨 또는 qtree에 대한 경로에 하나 이상의 접합 지점이 포함되는 경우, 경로를 따라 여러 엑스포트 정책을 위해 이 점검을 수행해야 할 수 있습니다.

이 평가는 초기 마운트 요청뿐만 아니라 읽기, 쓰기, 목록, 복사 및 기타 작업과 같이 NFS 클라이언트에서 전송된 모든 입출력 요청에 대해 수행됩니다.

ONTAP가 해당 엑스포트 정책 규칙을 식별하고 요청을 허용 또는 거부할지 결정한 후에는 ONTAP가 액세스 캐시에 이 정보를 저장하기 위한 항목을 생성합니다.

NFS 클라이언트가 I/O 요청을 보낼 때 ONTAP는 클라이언트의 IP 주소, SVM의 ID, 타겟 볼륨 또는 qtree와 관련된 엑스포트 정책을 기록한 다음, 액세스 캐시에서 일치하는 항목을 확인합니다. 액세스 캐시에 일치하는 항목이 있는 경우 ONTAP는 저장된 정보를 사용하여 I/O 요청을 허용하거나 거부합니다. 일치하는 항목이 없는 경우 ONTAP는 위에서 설명한 모든 해당 정책 규칙을 평가하는 일반적인 프로세스를 수행합니다.

활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않습니다. 이렇게 하면 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시에서 정보를 검색하는 것이 모든 입출력 요청에 대해 전체 엑스포트 정책 규칙 평가 프로세스를 수행하는 것보다 훨씬 빠릅니다. 따라서 액세스 캐시를 사용하면 클라이언트 액세스 검사의 오버헤드를 줄여 성능을 크게 향상시킬 수 있습니다.

액세스 캐시 매개 변수의 작동 방식

여러 매개 변수는 액세스 캐시의 항목에 대한 새로 고침 기간을 제어합니다. 이러한 매개 변수의 작동 방식을 이해하면 액세스 캐시를 조정하고 저장된 정보의 최근 성능과 균형을 유지하도록 매개 변수를 수정할 수 있습니다.

액세스 캐시는 볼륨 또는 qtree에 액세스하려는 클라이언트에 적용되는 하나 이상의 엑스포트 규칙으로 구성된 항목을 저장합니다. 이러한 항목은 새로 고쳐지기 전에 일정 시간 동안 저장됩니다. 새로 고침 시간은 액세스 캐시 매개 변수에 의해 결정되며 액세스 캐시 항목의 유형에 따라 달라집니다.

개별 SVM에 대한 액세스 캐시 매개 변수를 지정할 수 있습니다. 따라서 SVM 액세스 요구사항에 따라 매개 변수가 달라질 수 있습니다. 활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않으므로 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시 항목 유형입니다	설명	새로 고침 기간(초

양의 입력	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생되지 않았습니다.	최소: 300 최대: 86,400 기본값: 3,600
음수 항목	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생했습니다.	최소: 60 최대: 86,400 기본값: 3,600

예

NFS 클라이언트가 클러스터의 볼륨에 액세스하려고 합니다. ONTAP는 클라이언트를 엑스포트 정책 규칙과 일치시키고 클라이언트가 엑스포트 정책 규칙 구성에 따라 액세스할 수 있는지 확인합니다. ONTAP는 액세스 캐시에 있는 내보내기 정책 규칙을 양의 항목으로 저장합니다. 기본적으로 ONTAP는 액세스 캐시의 양의 항목을 1시간 (3,600초) 동안 유지한 다음 해당 항목을 자동으로 새로 고쳐 정보를 최신 상태로 유지합니다.

액세스 캐시가 불필요하게 가득 차는 것을 방지하기 위해 특정 기간 동안 사용하지 않은 기존 액세스 캐시 항목을 지우기 위한 추가 매개 변수가 있습니다. 이 '-하비스트-timeout' 매개 변수는 허용되는 범위는 60초에서 2,592,000초이며 기본 설정은 86,400초입니다.

qtree에서 엑스포트 정책을 제거합니다

특정 엑스포트 정책을 qtree에 더 이상 할당하지 않으려는 경우, qtree를 수정하여 포함하는 볼륨의 엑스포트 정책을 상속하도록 엑스포트 정책을 제거할 수 있습니다. 이렇게 하려면 '-export-policy' 매개 변수와 빈 이름 문자열("")을 사용하여 볼륨 qtree modify 명령을 사용할 수 있습니다.

단계

1. qtree에서 엑스포트 정책을 제거하려면 다음 명령을 입력합니다.

   "볼륨 qtree modify -vserver vserver_name -qtree -path /vol/volume_name /qtree_name -export-policy""

2. qtree가 적절히 수정되었는지 확인합니다.

   '볼륨 qtree show-qtree qtree_name-fields export-policy'입니다

qtree 파일 작업에 대해 **qtree ID**를 검증합니다

ONTAP에서는 qtree ID에 대한 선택적 추가 검증을 수행할 수 있습니다. 이 검증에서는 클라이언트 파일 작업 요청이 유효한 qtree ID를 사용하고 클라이언트가 동일한 qtree 내의 파일만 이동할 수 있는지 확인합니다. '-validate-qtree-export' 매개 변수를 수정하여 이 유효성 검사를 활성화 또는 비활성화할 수 있습니다. 이 매개 변수는 기본적으로 사용하도록 설정됩니다.

이 작업에 대해

이 매개 변수는 SVM(스토리지 가상 머신)에서 하나 이상의 qtree에 엑스포트 정책을 직접 할당한 경우에만 효과적입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

Qtree ID 검증을 원하는 경우…	다음 명령을 입력합니다…
활성화됨	'vserver nfs modify -vserver vserver_name -validate -qtree -export enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -validate -qtree -export disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

FlexVol 볼륨에 대한 정책 제한 및 중첩된 연결 지점을 내보냅니다

중첩 교차점에 덜 제한적인 정책을 설정하지만 상위 수준 교차점에 더 제한적인 정책을 설정하도록 내보내기 정책을 구성한 경우 하위 수준 교차점에 액세스하지 못할 수 있습니다.

상위 레벨의 교차로에서 낮은 레벨의 교차로보다 제한적인 엑스포트 정책이 있는지 확인해야 합니다.

강력한 보안을 위해 **NFS**와 **Kerberos** 사용

Kerberos에 대한 **ONTAP** 지원

Kerberos는 클라이언트/서버 응용 프로그램에 대해 강력한 보안 인증을 제공합니다. 인증을 통해 사용자 및 프로세스 ID를 서버에 확인할 수 있습니다. ONTAP 환경에서 Kerberos는 SVM(스토리지 가상 머신)과 NFS 클라이언트 간에 인증을 제공합니다.

ONTAP 9에서는 다음과 같은 Kerberos 기능이 지원됩니다.

- 무결성 검사를 통한 Kerberos 5 인증(krb5i)

  Krb5i는 체크섬을 사용하여 클라이언트와 서버 간에 전송되는 각 NFS 메시지의 무결성을 확인합니다. 이는 보안상의 이유(예: 데이터가 무단 변경되지 않도록 보장) 및 데이터 무결성을 위해(예: 불안정한 네트워크에서 NFS를 사용할 때 데이터 손상을 방지) 모두에 유용합니다.

- Kerberos 5 개인 정보 확인 인증(krb5p)

  Krb5p는 체크섬을 사용하여 클라이언트와 서버 사이의 모든 트래픽을 암호화합니다. 이는 보다 안전하며 부하가 더 많이 발생합니다.

- 128비트 및 256비트 AES 암호화

AES(Advanced Encryption Standard)는 전자 데이터의 보안을 위한 암호화 알고리즘입니다. ONTAP은 128비트 키(AES-128)로 AES와 256비트 키(AES-256) 암호화를 사용하여 Kerberos를 더욱 강력하게 지원합니다.

- SVM 레벨 Kerberos 영역 구성

  이제 SVM 관리자가 SVM 레벨에서 Kerberos 영역 구성을 생성할 수 있습니다. 즉, SVM 관리자는 더 이상 Kerberos 영역 구성을 위해 클러스터 관리자에 의존하지 않고 다중 테넌시 환경에서 개별 Kerberos 영역 구성을 생성할 수 있습니다.

NFS로 **Kerberos** 구성 요구 사항

시스템에서 NFS로 Kerberos를 구성하기 전에 네트워크 및 스토리지 환경의 특정 항목이 올바르게 구성되었는지 확인해야 합니다.

> 환경을 구성하는 단계는 사용 중인 클라이언트 운영 체제, 도메인 컨트롤러, Kerberos, DNS 등의 버전과 유형에 따라 다릅니다. 이러한 모든 변수를 문서화하는 것은 이 문서의 범위를 벗어납니다. 자세한 내용은 각 구성 요소에 대한 각 설명서를 참조하십시오.
>
> Windows Server 2008 R2 Active Directory 및 Linux 호스트를 사용하는 환경에서 NFSv3 및 NFSv4를 사용하여 ONTAP 및 Kerberos 5를 설정하는 방법에 대한 자세한 내용은 기술 보고서 4073을 참조하십시오.

다음 항목을 먼저 구성해야 합니다.

네트워크 환경 요구 사항

- Kerberos

  Windows Active Directory 기반 Kerberos 또는 MIT Kerberos와 같은 KDC(키 배포 센터)를 사용하여 작동하는 Kerberos 설정이 있어야 합니다.

  NFS 서버는 시스템 보안 주체의 주요 구성 요소로 NFS를 사용해야 합니다.

- 디렉터리 서비스

  SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다.

- NTP

  NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이 작업이 필요합니다.

- 도메인 이름 확인(DNS)

  각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

- 사용자 계정

  각 클라이언트에는 Kerberos 영역에 사용자 계정이 있어야 합니다. NFS 서버는 시스템 보안 주체의 기본 구성 요소로 "NFS"를 사용해야 합니다.

- NFS 를 참조하십시오

  NFSv3 또는 NFSv4를 사용하여 네트워크를 통해 통신하도록 각 클라이언트를 올바르게 구성해야 합니다.

  고객은 RFC1964 및 RFC2203을 지원해야 합니다.

- Kerberos

  각 클라이언트는 Kerberos 인증을 사용하도록 적절히 구성되어야 하며, 다음과 같은 세부 정보가 포함되어야 합니다.

  - TGS 통신에 대한 암호화가 활성화되었습니다.

    강력한 보안을 위한 AES-256.

  - TGT 통신을 위한 가장 안전한 암호화 유형이 활성화됩니다.
  - Kerberos 영역과 도메인이 올바르게 구성되었습니다.
  - GSS가 활성화되었습니다.

    시스템 자격 증명을 사용하는 경우:

  - gssd를 -n 매개변수로 실행하지 마십시오.
  - 루트 사용자로 "kinit"를 실행하지 마십시오.

- 각 클라이언트는 최신 및 업데이트된 운영 체제 버전을 사용해야 합니다.

  Kerberos와 AES 암호화를 위한 최고의 호환성과 안정성을 제공합니다.

- DNS

  올바른 이름 확인을 위해 DNS를 사용하도록 각 클라이언트를 올바르게 구성해야 합니다.

- NTP

  각 클라이언트는 NTP 서버와 동기화되어야 합니다.

- 호스트 및 도메인 정보

  각 클라이언트의 '/etc/hosts' 및 '/etc/resolv.conf' 파일은 각각 올바른 호스트 이름과 DNS 정보를 포함해야 합니다.

- keytab 파일

  각 클라이언트에는 KDC의 keytab 파일이 있어야 합니다. 영역은 대문자여야 합니다. 가장 강력한 보안을 위해서는 암호화 유형이 AES-256이어야 합니다.

- 선택 사항: 최상의 성능을 위해 클라이언트는 최소한 두 개의 네트워크 인터페이스를 가질 수 있습니다. 하나는 로컬 영역 네트워크와 통신하며 다른 하나는 스토리지 네트워크와 통신하기 위한 것입니다.

수행할 수 있습니다

- NFS 라이센스

  스토리지 시스템에 유효한 NFS 라이센스가 설치되어 있어야 합니다.

- CIFS 라이센스

  CIFS 라이센스는 선택 사항입니다. 멀티프로토콜 이름 매핑을 사용할 때는 Windows 자격 증명을 확인하는 데만 필요합니다. 엄격한 UNIX 전용 환경에서는 필요하지 않습니다.

- SVM

  시스템에 SVM이 하나 이상 구성되어 있어야 합니다.

- SVM의 DNS

  각 SVM에서 DNS를 구성해야 합니다.

- NFS 서버

  SVM에서 NFS를 구성해야 합니다.

- AES 암호화

  가장 강력한 보안을 위해서는 Kerberos에 AES-256 암호화만 허용하도록 NFS 서버를 구성해야 합니다.

- SMB 서버

  멀티프로토콜 환경을 실행 중인 경우 SVM에서 SMB를 구성해야 합니다. 멀티 프로토콜 이름 매핑에 SMB 서버가 필요합니다.

- 볼륨

  루트 볼륨과 SVM에서 사용하도록 구성된 데이터 볼륨이 하나 이상 있어야 합니다.

- 루트 볼륨

  SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름	설정
보안 스타일	Unix
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	777

  루트 볼륨과 달리 데이터 볼륨은 보안 스타일을 가질 수 있습니다.

- Unix 그룹

  SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 **ID**입니다
데몬	1
루트	0
pcuser	65534(SVM 생성 시 ONTAP에서 자동으로 생성)

- Unix 사용자

  SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함 NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다.
pcuser	65534	65534	NFS 및 CIFS를 멀티프로토콜 용도로 필요합니다 SVM을 생성할 때 ONTAP이 pcuser 그룹을 자동으로 생성하여 추가했습니다.
루트	0	0	마운팅에 필요합니다

  NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.

- 엑스포트 정책 및 규칙

  루트 및 데이터 볼륨 및 qtree에 필요한 엑스포트 규칙을 사용하여 엑스포트 정책을 구성해야 합니다. Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5', krb5i 또는 krb5p로 설정할 수 있습니다.

- Kerberos - UNIX 이름 매핑

  NFS 클라이언트 사용자 SPN에 의해 식별된 사용자에게 루트 권한을 부여하려면 루트에 대한 이름 매핑을 생성해야 합니다.

관련 정보

"NetApp 기술 보고서 4073: 안전한 통합 인증"

"NetApp 상호 운용성 매트릭스 툴"

"시스템 관리"

"논리적 스토리지 관리"

NFSv4의 사용자 **ID** 도메인을 지정합니다

사용자 ID 도메인을 지정하려면 '-v4-id-domain' 옵션을 설정합니다.

이 작업에 대해

기본적으로 ONTAP에서는 NFSv4 사용자 ID 매핑이 설정된 경우 NIS 도메인을 사용합니다. NIS 도메인이 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 예를 들어 여러 사용자 ID 도메인이 있는 경우 사용자 ID 도메인을 설정해야 할 수 있습니다. 도메인 이름은 도메인 컨트롤러의 도메인 구성과 일치해야 합니다. NFSv3에는 필요하지 않습니다.

단계

1. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name'

이름 서비스 구성

ONTAP 네임 서비스 스위치 구성의 작동 방식

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.

데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
호스트	호스트 이름을 IP 주소로 변환	파일, DNS
그룹	사용자 그룹 정보를 찾는 중입니다	파일, NIS, LDAP
암호	사용자 정보를 찾는 중입니다	파일, NIS, LDAP
넷그룹	넷그룹 정보를 찾는 중입니다	파일, NIS, LDAP

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
이름맵	사용자 이름 매핑 중	파일, LDAP

소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
파일	로컬 소스 파일	SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹 SVM 서비스 이름 서비스 넷그룹 SVM 서비스 이름-서비스 DNS 호스트
NIS를 선택합니다	SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버	'vserver services name-service nis-domain'을 선택합니다
LDAP를 지원합니다	SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버	'vserver services name-service ldap'
DNS	SVM의 DNS 구성에 지정된 외부 DNS 서버	SVM 서비스 이름-서비스 DNS

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
NIS를 선택합니다	UDP입니다
DNS	UDP입니다
LDAP를 지원합니다	TCP

예

다음 예는 SVM svm_1의 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

호스트의 IP 주소를 조회하기 위해 ONTAP는 먼저 로컬 소스 파일을 참조합니다. 쿼리가 결과를 반환하지 않으면 다음으로 DNS 서버가 선택됩니다.

사용자 또는 그룹 정보를 조회하기 위해 ONTAP는 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP는 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP는 기본적으로 로컬 소스 파일만 참조합니다.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

LDAP를 사용합니다

LDAP 개요

LDAP(Lightweight Directory Access Protocol) 서버를 사용하면 사용자 정보를 중앙에서 관리할 수 있습니다. 사용자 환경의 LDAP 서버에 사용자 데이터베이스를 저장하는 경우 기존 LDAP 데이터베이스에서 사용자 정보를 조회하도록 스토리지 시스템을 구성할 수 있습니다.

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
  - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.
  - LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
    - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
    - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
  - LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

    다음 세션 보안 옵션을 사용할 수 있습니다.

        - LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)
        - TLS를 시작합니다
        - LDAPS(TLS 또는 SSL을 통한 LDAP)
    - 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
        - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
        - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
        - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
    - 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
        - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
        - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서 TLS 또는 SSL에 대해 LDAP 서버를 활성화해야 합니다. SSL은 ONTAP 9.0-9.4에서 지원되지 않습니다.
        - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
    - ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
        - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
            - 양방향
            - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
            - 부모-자식
        - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
        - '--bind-as-cifs-server'가 true로 설정된 경우 도메인 암호가 인증을 위해 동일해야 합니다.

> LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.
>
> - 모든 ONTAP 버전:
> - 관리 SVM의 LDAP 클라이언트
> - ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
> - LDAP 서명 및 봉인('-session-security' 옵션)
> - 암호화된 TLS 연결('-use-start-tls' 옵션)
> - LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- ONTAP 9.11.1부터 를 사용할 수 있습니다 "nsswitch 인증을 위한 LDAP 빠른 바인딩."
- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

  대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

자세한 내용은 을 참조하십시오 "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법".

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 NFS 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. 테스트

SVM에서 '-session-security-for-ad-ldap' 옵션을 사용하여 SVM에서 SMB 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

LDAPS 개념

ONTAP가 LDAP 통신을 보호하는 방법에 대한 특정 용어와 개념을 이해해야 합니다. ONTAP는 Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버 간에 인증된 세션을 설정하기 위해 시작 TLS 또는 LDAPS를 사용할 수 있습니다.

용어

ONTAP에서 LDAPS를 사용하여 LDAP 통신을 보호하는 방법에 대해 이해해야 하는 특정 용어가 있습니다.

- * LDAP *

  (Lightweight Directory Access Protocol) 정보 디렉터리에 액세스하고 관리하는 프로토콜입니다. LDAP는 사용자, 그룹 및 넷그룹과 같은 객체를 저장하기 위한 정보 디렉토리로 사용됩니다. 또한 LDAP는 이러한 객체를 관리하고 LDAP 클라이언트의 LDAP 요청을 처리하는 디렉토리 서비스를 제공합니다.

- SSL *

  (Secure Sockets Layer) 인터넷을 통해 정보를 안전하게 전송하기 위해 개발된 프로토콜입니다. SSL은 ONTAP 9 이상에서 지원되지만 TLS 사용을 위해 더 이상 사용되지 않습니다.

- * TLS *

  (전송 계층 보안) IETF 표준 트랙 프로토콜로서 이전 SSL 사양에 기초합니다. SSL의 후속 제품입니다. TLS는 ONTAP 9.5 이상에서 지원됩니다.

- * LDAPS(SSL 또는 TLS를 통한 LDAP) *

  LDAP 클라이언트와 LDAP 서버 간의 보안 통신을 위해 TLS 또는 SSL을 사용하는 프로토콜입니다. SSL을 통한 _LDAP_와 TLS를 통한 _LDAP_라는 용어는 서로 바꿔 사용되기도 합니다. LDAPS는 ONTAP 9.5 이상에서 지원됩니다.

  - ONTAP 9.5-9.8에서 LDAPS는 포트 636에서만 활성화할 수 있습니다. 이렇게 하려면 '-use-ldaps-for-ad-ldap' 매개 변수를 'vserver cifs security modify' 명령과 함께 사용하십시오.
  - ONTAP 9.9.1부터 포트 636이 기본값으로 유지되지만 LDAPS는 모든 포트에서 활성화할 수 있습니다. 이렇게 하려면 '-ldaps-enabled' 매개 변수를 'true'로 설정하고 원하는 '-port' 매개 변수를 지정합니다. 자세한 내용은 'vserver services name-service ldap client create' man 페이지를 참조하십시오

  ⓘ LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.

- * TLS * 를 시작합니다

  (*start_tls*, *STARTTLS* 및 *StartTLS* 라고도 함) TLS 프로토콜을 사용하여 보안 통신을 제공하는 메커니즘입니다.

  ONTAP는 LDAP 통신 보안을 위해 STARTTLS를 사용하며 기본 LDAP 포트(389)를 사용하여 LDAP 서버와 통신합니다. LDAP 서버는 LDAP 포트 389를 통한 연결을 허용하도록 구성해야 합니다. 그렇지 않으면 SVM에서 LDAP 서버로의 LDAP TLS 연결이 실패합니다.

ONTAP에서 **LDAPS**를 사용하는 방법

ONTAP는 TLS 서버 인증을 지원하므로 SVM LDAP 클라이언트가 바인딩 작업 중에 LDAP 서버의 ID를 확인할 수 있습니다. TLS를 사용하는 LDAP 클라이언트는 공용 키 암호화의 표준 기술을 사용하여 서버의 인증서와 공용 ID가 유효하며 클라이언트의 신뢰할 수 있는 CA 목록에 나열된 CA(인증 기관)에서 발급되었는지 확인할 수 있습니다.

LDAP는 TLS를 사용하여 통신을 암호화하는 STARTTLS를 지원합니다. STARTTLS는 표준 LDAP 포트(389)를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다.

ONTAP는 다음을 지원합니다.

- Active Directory 통합 LDAP 서버와 SVM 간의 SMB 관련 트래픽을 위한 LDAPS
- 이름 매핑 및 기타 UNIX 정보를 위한 LDAP 트래픽용 LDAPS

  Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버를 사용하여 LDAP 이름 매핑과 사용자, 그룹 및 넷그룹과 같은 기타 UNIX 정보에 대한 정보를 저장할 수 있습니다.

- 자체 서명된 루트 CA 인증서

  Active-Directory 통합 LDAP를 사용하는 경우 도메인에 Windows Server 인증서 서비스가 설치될 때 자체 서명된 루트 인증서가 생성됩니다. LDAP 이름 매핑에 UNIX 기반 LDAP 서버를 사용하는 경우 자체 서명된 루트 인증서는 해당 LDAP 애플리케이션에 적합한 방법을 사용하여 생성 및 저장됩니다.

기본적으로 LDAPS는 비활성화되어 있습니다.

LDAP RFC2307bis 지원을 활성화합니다

LDAP를 사용하고 중첩된 그룹 구성원을 사용하는 추가 기능이 필요한 경우 ONTAP를 구성하여 LDAP RFC2307bis 지원을 활성화할 수 있습니다.

필요한 것

사용할 기본 LDAP 클라이언트 스키마 중 하나의 복사본을 만들어야 합니다.

이 작업에 대해

LDAP 클라이언트 스키마에서 그룹 개체는 memberUid 특성을 사용합니다. 이 속성은 여러 값을 포함할 수 있으며 해당 그룹에 속한 사용자의 이름을 나열합니다. RFC2307bis가 활성화된 LDAP 클라이언트 스키마에서 그룹 객체는 uniqueMember 속성을 사용합니다. 이 속성은 LDAP 디렉토리에 있는 다른 개체의 전체 DN(고유 이름)을 포함할 수 있습니다. 이렇게 하면 그룹이 다른 그룹을 구성원으로 포함할 수 있으므로 중첩된 그룹을 사용할 수 있습니다.

사용자는 중첩된 그룹을 포함하여 256개 이상의 그룹의 구성원이 아니어야 합니다. ONTAP는 256 그룹 제한을 초과하는 모든 그룹을 무시합니다.

기본적으로 RFC2307bis 지원은 비활성화되어 있습니다.

> RFC2307bis 지원은 MS-AD-BIS 스키마를 사용하여 LDAP 클라이언트를 생성할 때 ONTAP에서 자동으로 활성화됩니다.

자세한 내용은 을 참조하십시오 "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법".

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. RFC2307 LDAP 클라이언트 스키마를 수정하여 RFC2307bis 지원을 활성화합니다.

   'vserver services name-service ldap client schema modify -vserver vserver_name -schema schema -name -enable -rfc2307bis true'

3. LDAP 서버에서 지원되는 객체 클래스와 일치하도록 스키마를 수정합니다.

   'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -group-of-unique-names-object-class object_class'

4. LDAP 서버에서 지원되는 속성 이름과 일치하도록 스키마를 수정합니다.

   'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -unique-member-attribute attribute_name'

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

LDAP 디렉토리 검색에 대한 구성 옵션입니다

사용자, 그룹 및 넷그룹 정보를 포함한 LDAP 디렉토리 검색을 최적화하려면 ONTAP LDAP 클라이언트가 사용자 환경에 가장 적합한 방식으로 LDAP 서버에 접속하도록 구성해야 합니다. 기본 LDAP 기본 및 범위 검색 값이 충분하면 사용자 지정 값이 더 적합한 시기를 지정하는 매개변수가 무엇인지 이해해야 합니다.

사용자, 그룹 및 넷그룹 정보에 대한 LDAP 클라이언트 검색 옵션을 사용하면 LDAP 쿼리가 실패하여 스토리지 시스템에 대한 클라이언트 액세스가 실패하는 것을 방지할 수 있습니다. 또한 클라이언트 성능 문제를 방지하기 위해 가능한 한 효율적으로 검색을 수행할 수 있습니다.

기본 및 범위 검색 값입니다

LDAP 베이스는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 DN입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 DN을 사용하여 수행됩니다. 이 옵션은 LDAP 디렉토리가 상대적으로 작고 모든 관련 항목이 동일한 DN에 있을 때 적합합니다.

사용자 지정 기본 DN을 지정하지 않으면 기본값은 "root"입니다. 즉, 각 쿼리는 전체 디렉터리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

LDAP 기본 범위는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 검색 범위입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 범위를 사용하여 수행됩니다. LDAP 쿼리가 명명된 항목만 검색할지, DN 아래의 항목 하나 또는 DN 아래의 전체 하위 트리를 검색할지 여부를 결정합니다.

사용자 지정 기본 범위를 지정하지 않으면 기본값은 'Subtree'입니다. 즉, 각 쿼리는 DN 아래의 전체 하위 트리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

사용자 지정 기준 및 범위 검색 값

필요에 따라 사용자, 그룹 및 넷그룹 검색에 대해 별도의 기본 값과 범위 값을 지정할 수 있습니다. 이러한 방식으로 검색 기준 및 쿼리 범위를 제한하면 LDAP 디렉토리의 하위 섹션으로 검색이 제한되므로 성능이 크게 향상됩니다.

사용자 지정 기준 및 범위 값을 지정하면 사용자, 그룹 및 넷그룹 검색에 대한 일반 기본 검색 기준 및 범위가 재정의됩니다. 사용자 지정 기준 및 범위 값을 지정하는 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

LDAP 클라이언트 매개 변수…	사용자 지정…
'-base-dn'	필요한 경우 모든 LDAP 검색다중 값에 대한 기본 DN을 입력할 수 있습니다(예: ONTAP 9.5 이상 릴리스에서 LDAP 조회 추적을 사용하는 경우).
``기본범위''	모든 LDAP 검색에 대한 기본 범위입니다
'-user-dn'	모든 LDAP 사용자의 기본 DNS 검색이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
'- 사용자 범위'	모든 LDAP 사용자 검색에 대한 기본 범위 이 매개 변수는 사용자 이름 매핑 검색에도 적용됩니다.
``그룹-dn''	모든 LDAP 그룹 검색에 대한 기본 DNS입니다
그룹-범위	모든 LDAP 그룹 검색에 대한 기본 범위입니다
'-넷그룹-dn'	모든 LDAP 넷그룹 검색에 대한 기본 DNS입니다
넷그룹 범위	모든 LDAP 넷그룹 검색에 대한 기본 범위입니다

여러 사용자 정의 기본 **DN** 값

LDAP 디렉토리 구조가 더 복잡한 경우 여러 기본 DNS를 지정하여 LDAP 디렉토리의 여러 부분을 검색하여 특정 정보를 검색해야 할 수 있습니다. 사용자, 그룹 및 넷그룹 DN 매개 변수에 대해 여러 DNS를 지정할 수 있습니다. 이를 세미콜론(;)으로 분리하고 전체 DN 검색 목록을 큰따옴표(")로 둘러싸서 지정할 수 있습니다. DN에 세미콜론이 포함된 경우 DN의 세미콜론 바로 앞에 이스케이프 문자(\)를 추가해야 합니다.

범위는 해당 매개 변수에 지정된 DNS의 전체 목록에 적용됩니다. 예를 들어 사용자 범위에 대해 서로 다른 세 개의 사용자 DNS 및 하위 트리의 목록을 지정하면 LDAP 사용자는 지정된 세 DNS에 대해 전체 하위 트리를 검색합니다.

ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에서 반환되지 않는 경우 ONTAP LDAP 클라이언트가 다른

LDAP 서버에 조회 요청을 참조할 수 있도록 LDAP_READIAL DIADIGING_을 지정할 수도 있습니다. 클라이언트는 추천 데이터를 사용하여 추천 데이터에 설명된 서버에서 대상 객체를 검색합니다. 참조된 LDAP 서버에 있는 객체를 검색하려면, LDAP 클라이언트 구성의 일부로 참조된 객체의 base-dn을 base-dn에 추가할 수 있습니다. 그러나 LDAP 클라이언트 생성 또는 수정 중에 참조 추격이 활성화('-referral-enabled true' 옵션 사용)된 경우에만 참조 객체가 조회됩니다.

LDAP 디렉토리 **Netgroup-by-host** 검색 성능 향상

LDAP 환경이 호스트별 넷그룹 검색을 허용하도록 구성된 경우 ONTAP를 구성하여 이를 활용하고 호스트별 넷그룹 검색을 수행할 수 있습니다. 따라서 넷그룹 검색 속도를 크게 높이고 넷그룹 검색 중 대기 시간으로 인해 발생할 수 있는 NFS 클라이언트 액세스 문제를 줄일 수 있습니다.

필요한 것

LDAP 디렉토리에는 netgroup.byhost 맵이 포함되어야 합니다.

DNS 서버에는 NFS 클라이언트에 대한 정방향(A) 및 역방향(PTR) 조회 레코드가 모두 포함되어야 합니다.

넷그룹에 IPv6 주소를 지정할 때는 RFC 5952에 지정된 대로 항상 각 주소를 줄이고 압축해야 합니다.

이 작업에 대해

NIS 서버는 넷그룹, 넷그룹, byuser, netgroup.byhost라는 세 개의 개별 맵에 넷그룹 정보를 저장합니다. 넷그룹 byuser와 netgroup.byhost 맵의 목적은 넷그룹 검색 속도를 높이는 것입니다. ONTAP는 NIS 서버에서 호스트 별로 넷그룹 검색을 수행하여 마운트 응답 시간을 향상시킬 수 있습니다.

기본적으로 LDAP 디렉토리에는 NIS 서버와 같은 netgroup.byhost 맵이 없습니다. 하지만 타사 툴을 사용하여 NIS 넷그룹을 LDAP 디렉토리에 가져올 수도 있습니다. byhost 맵을 LDAP 디렉토리에 가져와서 빠르게 넷그룹을 통한 호스트 간 검색을 수행할 수 있습니다. 호스트 별로 넷그룹을 검색할 수 있도록 LDAP 환경을 구성한 경우 netgroup.byhost의 맵 이름, DN 및 검색 범위를 사용하여 ONTAP LDAP 클라이언트를 구성하여 더 빠른 호스트 기준 넷그룹을 검색할 수 있습니다.

Netgroup-by-host 검색에 대한 결과를 더 빨리 수신하면 NFS 클라이언트가 내보내기에 대한 액세스를 요청할 때 ONTAP에서 엑스포트 규칙을 더 빠르게 처리할 수 있습니다. 따라서 넷그룹 검색 지연 문제로 인해 액세스가 지연될 가능성이 줄어듭니다.

단계

1. LDAP 디렉토리로 가져온 NIS 넷그룹 byhost 맵의 정확한 전체 고유 이름을 가져옵니다.

   지도 DN은 가져오기에 사용한 타사 도구에 따라 다를 수 있습니다. 최상의 성능을 얻으려면 정확한 맵 DN을 지정해야 합니다.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

3. 스토리지 가상 시스템(SVM)의 LDAP 클라이언트 구성에서 Netgroup-by-host 검색을 설정합니다. 'vserver services name-service LDAP client modify -vserver vserver_name -client -config config config_name -is -netgroup-byhost-enabled true-netgroup-byhost-dn netgroup-by-host_map_ninggroup-byhost-scope netgroup-by-host_search_scope

   `-is-netgroup-byhost-enabled '{'true'|'false'}LDAP 디렉토리에 대한 호스트 별 넷그룹 검색을 설정하거나 해제합니다. 기본값은 false 입니다.

   dnetgroup-byhost-dn dnetgroup-by-host_map_ninged_name은 LDAP 디렉토리에 있는 netgroup.byhost 맵의

고유 이름을 지정합니다. 넷그룹별 검색에 대한 기본 DN을 재정의합니다. 이 매개 변수를 지정하지 않으면 ONTAP에서는 기본 DN을 대신 사용합니다.

`-netgroup-byhost-scope '{'base'|'onelel'|'ubtree'}는 넷그룹-호스트 검색 범위를 지정합니다. 이 매개변수를 지정하지 않으면 기본값은 'Subtree'입니다.

LDAP 클라이언트 구성이 아직 없는 경우 'vserver services name-service ldap client create' 명령을 사용하여 새 LDAP 클라이언트 구성을 생성할 때 이러한 매개 변수를 지정하여 Netgroup-by-host 검색을 설정할 수 있습니다.

> ONTAP 9.2부터 -ldap-servers 필드가 -servers 필드를 대체합니다. 이 새 필드는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 netgroup.byhost 맵 ""nisMapName="netgroup.byhost", dc=corp, dc=example, dc=com" 및 기본 검색 범위 'subtree'를 사용하여 넷그룹을 호스트별로 검색할 수 있도록 이름이 ""ldap_corp""인 기존 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

작업을 마친 후

클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다.

관련 정보

"IETF RFC 5952: IPv6 주소 텍스트 표현에 대한 권장 사항입니다"

nsswitch 인증에 **LDAP** 고속 바인딩을 사용합니다

ONTAP 9.11.1부터는 LDAP_Fast BIND_FUNGION(*CONNEC*동시 바인드)을 활용하여 클라이언트 인증 요청을 더 빠르고 간편하게 수행할 수 있습니다. 이 기능을 사용하려면 LDAP 서버가 빠른 바인딩 기능을 지원해야 합니다.

이 작업에 대해

빠른 바인딩이 없으면 ONTAP는 LDAP 단순 바인드를 사용하여 LDAP 서버에서 관리자 사용자를 인증합니다. 이 인증 방법을 사용하면 ONTAP에서 사용자 또는 그룹 이름을 LDAP 서버로 보내고, 저장된 해시 암호를 받고, 서버 해시 코드를 사용자 암호에서 로컬로 생성된 해시 암호와 비교합니다. 동일한 경우 ONTAP는 로그인 권한을 부여합니다.

빠른 바인딩 기능을 사용하면 ONTAP는 보안 연결을 통해 사용자 자격 증명(사용자 이름 및 암호)만 LDAP 서버로 전송합니다. 그런 다음 LDAP 서버가 이러한 자격 증명을 검증하고 ONTAP에 로그인 권한을 부여하도록 지시합니다.

빠른 바인딩의 한 가지 장점은 LDAP 서버에서 암호 해싱이 수행되기 때문에 ONTAP가 LDAP 서버에서 지원하는 모든 새로운 해싱 알고리즘을 지원할 필요가 없다는 것입니다.

"빠른 바인딩 사용에 대해 알아보십시오."

LDAP 고속 바인딩에 기존 LDAP 클라이언트 구성을 사용할 수 있습니다. 그러나 LDAP 클라이언트를 TLS 또는

LDAPS용으로 구성하는 것이 좋습니다. 그렇지 않으면 암호를 일반 텍스트로 유선으로 보냅니다.

ONTAP 환경에서 LDAP 고속 바인딩을 사용하려면 다음 요구 사항을 충족해야 합니다.

- ONTAP admin 사용자는 빠른 바인딩을 지원하는 LDAP 서버에 구성해야 합니다.
- ONTAP SVM은 이름 서비스 스위치(nsswitch) 데이터베이스에서 LDAP에 대해 구성해야 합니다.
- ONTAP admin 사용자 및 그룹 계정은 빠른 바인딩을 사용하여 nsswitch 인증에 맞게 구성해야 합니다.

단계

1. LDAP 관리자에게 LDAP 서버에서 LDAP 고속 바인딩이 지원되는지 확인하십시오.
2. ONTAP 관리자 사용자 자격 증명이 LDAP 서버에 구성되어 있는지 확인합니다.
3. LDAP 고속 바인딩에 대해 admin 또는 data SVM이 올바르게 구성되었는지 확인합니다.

   a. LDAP 빠른 바인딩 서버가 LDAP 클라이언트 구성에 나열되는지 확인하려면 다음을 입력합니다.

      'vserver services name-service ldap client show'

      "LDAP 클라이언트 구성에 대해 자세히 알아보십시오."

   b. LDAP가 nsswitch 'passwd' 데이터베이스에 대해 구성된 소스 중 하나인지 확인하려면 다음을 입력합니다.

      'vserver services name-service ns-switch show'

   "nsswitch 구성에 대해 알아봅니다."

4. admin 사용자가 nsswitch를 사용하여 인증하는지, 그리고 계정에서 LDAP 빠른 바인딩 인증이 활성화되어 있는지 확인합니다.

   - 기존 사용자의 경우 '보안 로그인 수정'을 입력하고 다음 파라미터 설정을 확인합니다.

     '-authentication-method nsswitch'

   '-is-ldap-fastbind true'

   - 새 관리자 사용자는 를 참조하십시오 "LDAP 또는 NIS 계정 액세스를 설정합니다."

LDAP 통계를 표시합니다

ONTAP 9.2부터는 스토리지 시스템의 SVM(스토리지 가상 머신)에 대한 LDAP 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

필요한 것

- SVM에서 LDAP 클라이언트를 구성해야 합니다.
- 데이터를 볼 수 있는 LDAP 객체를 식별해야 합니다.

단계

1. 카운터 객체에 대한 성능 데이터 보기:

   '스타티틱스 쇼'

예

다음 예제는 객체 'ECD_EXTERNAL_SERVICE_OP'에 대한 성능 데이터를 보여 줍니다.

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

이름 매핑을 구성합니다

이름 매핑 구성 개요

ONTAP는 이름 매핑을 사용하여 SMB ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 SMB ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 SMB 클라이언트에서 연결 중인지 여부와 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 SMB 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

  이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명이 동일한 기본

사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.

이름 매핑 작동 방식

ONTAP에서 사용자에 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 SMB 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

  컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

다중 도메인은 **UNIX** 사용자와 **Windows** 사용자 이름 매핑을 검색합니다

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 **UNIX** 사용자에게 **Windows** 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. SMB 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 신뢰나 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 SMB 서버가 속하는 도메인입니다.

- _양방향 트러스트 _

양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. SMB 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.

- _아웃바운드 트러스트 _

  아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 _not_sunfre검색되었습니다.

- _ 인바운드 신뢰 _

  인바운드 트러스트를 사용하면 다른 도메인이 SMB 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 _not_sound입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드(*)를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

패턴	교체	결과
루트	* {백슬래시} {백슬래시} 관리자	UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.

패턴	교체	결과
*	* {백슬래시} {백슬래시} *	유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다. * {백슬래시} {백슬래시} * 패턴은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법으로는 사용할 수 없습니다.

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다
- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

이름 매핑 변환 규칙

ONTAP 시스템은 각 SVM에 대해 일련의 전환 규칙을 유지합니다. 각 규칙은 A_pattern_과 A_replacement_의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

이름 매핑을 생성합니다

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을

사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

단계

1. 이름 매핑 생성:

   'vserver name-mapping create-vserver vserver_name-direction{KRB-unix|win-unix|unix-win} - position integer-pattern text-replacement text'

   > '-pattern' 및 '-replacement' 문은 정규식으로 공식화할 수 있습니다. 또한 '-replacement' 문을 사용하여 null 대체 문자열 ""(공백 문자)를 사용하여 사용자에 대한 매핑을 명시적으로 거부할 수 있습니다. 자세한 내용은 'vserver name-mapping create' man 페이지를 참조하십시오.

   Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB 클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnnDoe에 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 ""$"가 포함됩니다. 매핑은 Windows 사용자 ENG\John$ops를 UNIX 사용자 John_ops에 매핑합니다.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

기본 사용자를 구성합니다

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

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다…
기본 UNIX 사용자를 구성합니다	'vserver cifs options modify-default-unix-user user_name'을 선택합니다
기본 Windows 사용자를 구성합니다	'vserver nfs modify-default-win-user user_name'을 선택합니다

이름 매핑을 관리하는 명령입니다

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
이름 매핑을 생성합니다	'vserver name-mapping create'
특정 위치에 이름 매핑을 삽입합니다	'vserver name-mapping insert'
이름 매핑을 표시합니다	'vserver name-mapping show'
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	'vserver name-mapping swap'
이름 매핑을 수정합니다	'vserver name-mapping modify'입니다
이름 매핑을 삭제합니다	'vserver name-mapping delete
올바른 이름 매핑을 확인합니다	'vserver security file-directory show-Effective-permissions-vserver vs1-win-user-name user1-path/-share-name SH1'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

Windows NFS 클라이언트에 대한 액세스를 설정합니다

ONTAP는 Windows NFSv3 클라이언트에서 파일 액세스를 지원합니다. 즉, NFSv3을 지원하는 Windows 운영 체제를 실행하는 클라이언트가 클러스터의 NFSv3 내보내기에 있는 파일에 액세스할 수 있습니다. 이 기능을 성공적으로 사용하려면 SVM(스토리지 가상 시스템)을 올바르게 구성하고 특정 요구사항과 제한사항을 숙지해야 합니다.

이 작업에 대해

기본적으로 Windows NFSv3 클라이언트 지원은 비활성화되어 있습니다.

시작하기 전에

SVM에서 NFSv3을 활성화해야 합니다.

단계

1. Windows NFSv3 클라이언트 지원 설정:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly
   disabled
   ```

2. Windows NFSv3 클라이언트를 지원하는 모든 SVM에서 를 사용하지 않도록 설정합니다 `-enable-ejukebox` 및 `-v3-connection-drop` 매개 변수:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
   -drop disabled
   ```

   이제 Windows NFSv3 클라이언트가 스토리지 시스템에 내보내기를 마운트할 수 있습니다.

3. 각 Windows NFSv3 클라이언트가 '-o mtype=hard' 옵션을 지정하여 하드 마운트를 사용하는지 확인합니다.

   이 작업은 안정적인 마운트를 보장하기 위해 필요합니다.

   mount-o mtype=hard\\10.53.33.10\vol\vol1 z:\"

NFS 클라이언트에서 NFS 내보내기 표시를 설정합니다

NFS 클라이언트는 'howmount -e' 명령을 사용하여 ONTAP NFS 서버에서 사용할 수 있는 내보내기 목록을 볼 수 있습니다. 이렇게 하면 마운트할 파일 시스템을 식별하는 데 도움이 됩니다.

ONTAP 9.2부터 ONTAP는 NFS 클라이언트가 기본적으로 엑스포트 목록을 볼 수 있도록 지원합니다. 이전 릴리즈에서는 vserver nfs modify 명령의 'howmount' 옵션을 명시적으로 활성화해야 합니다. 엑스포트 목록을 보려면 SVM에서 NFSv3을 설정해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM의 showmount 기능이 표시됩니다.

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

NFS 클라이언트에서 실행된 다음 명령은 IP 주소가 10.63.21.9인 NFS 서버의 내보내기 목록을 표시합니다.

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

NFS를 사용하여 파일 액세스를 관리합니다

NFSv3을 사용하거나 사용하지 않도록 설정합니다

'-v3' 옵션을 수정하여 NFSv3을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv3 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. 기본적으로 NFSv3은 설정되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
NFSv3을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 enabled'
NFSv3을 사용하지 않도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 disabled'

NFSv4.0을 설정 또는 해제합니다

'-v4.0' 옵션을 수정하여 NFSv4.0을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv4.0 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. ONTAP 9.9.1에서는 NFSv4.0이 기본적으로 설정되어 있으며 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.0을 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 enabled'
NFSv4.0을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 disabled'

NFSv4.1을 설정 또는 해제합니다

'-v4.1' 옵션을 수정하여 NFSv4.1을 설정 또는 해제할 수 있습니다. 따라서 NFSv4.1 프로토콜을 사용하여 클라이언트에 파일을 액세스할 수 있습니다. ONTAP 9.9.1에서는 NFSv4.1이 기본적으로 활성화되어 있지만 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.1을 활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 enabled'
NFSv4.1을 비활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 disabled'

NFSv4 저장소 풀 제한을 관리합니다

ONTAP 9.13부터 관리자는 NFSv4 서버가 클라이언트 저장소 풀 리소스 제한당 한도에 도달하면 NFSv4 클라이언트에 대한 리소스를 거부하도록 설정할 수 있습니다. 클라이언트가 NFSv4 저장소 풀 리소스를 너무 많이 사용하면 NFSv4 저장소 풀 리소스를 사용할 수 없어 다른 NFSv4 클라이언트가 차단될 수 있습니다.

또한 이 기능을 사용하면 각 클라이언트에서 사용하는 활성 저장소 리소스를 볼 수 있습니다. 이렇게 하면 시스템 리소스가 소진되는 클라이언트를 쉽게 식별할 수 있으며 클라이언트 리소스 제한에 따라 적용할 수 있습니다.

사용된 저장소 풀 리소스를 봅니다

를 클릭합니다 `vserver nfs storepool show` 명령 사용된 저장소 리소스 수를 표시합니다. 저장소 풀은 NFSv4 클라이언트가 사용하는 리소스 풀입니다.

단계

1. 관리자 권한으로 를 실행합니다 `vserver nfs storepool show` NFSv4 클라이언트의 저장소 풀 정보를 표시하는 명령입니다.

예

이 예에서는 NFSv4 클라이언트의 저장소 풀 정보를 표시합니다.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정합니다

관리자는 다음 명령을 사용하여 저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정할 수 있습니다.

단계

1. 관리자는 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
저장소 풀 제한 컨트롤을 활성화합니다	`vserver nfs storepool config modify -limit-enforce enabled`
저장소 풀 제한 컨트롤을 비활성화합니다	`vserver nfs storepool config modify -limit-enforce disabled`

차단된 클라이언트 목록을 봅니다

저장소 풀 제한이 설정된 경우 관리자는 클라이언트별 리소스 임계값에 도달하면 차단된 클라이언트를 확인할 수 있습니다. 관리자는 다음 명령을 사용하여 차단된 클라이언트로 표시된 클라이언트를 확인할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client show` NFSv4 차단된 클라이언트 목록을 표시하는 명령입니다.

차단된 클라이언트 목록에서 클라이언트를 제거합니다

클라이언트별 임계값에 도달한 클라이언트는 연결이 끊어지고 블록 클라이언트 캐시에 추가됩니다. 관리자는 다음

명령을 사용하여 클라이언트를 블록 클라이언트 캐시에서 제거할 수 있습니다. 이렇게 하면 클라이언트가 ONTAP NFSv4 서버에 접속할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 차단된 클라이언트 캐시를 플러시하는 명령입니다.
2. 를 사용합니다 `vserver nfs storepool blocked-client show` 클라이언트가 블록 클라이언트 캐시에서 제거되었는지 확인하는 명령입니다.

예

이 예에서는 모든 노드에서 IP 주소 "10.2.1.1"이 플러시되는 차단된 클라이언트를 표시합니다.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

pNFS를 사용하거나 사용하지 않도록 설정합니다

pNFS는 NFS 클라이언트가 스토리지 장치에서 직접 및 병렬로 읽기/쓰기 작업을 수행할 수 있도록 지원하여 잠재적 병목 현상으로 NFS 서버를 우회함으로써 성능을 개선합니다. pNFS(parallel NFS)를 활성화 또는 비활성화하려면 '-v4.1-pNFS' 옵션을 수정합니다.

ONTAP 릴리즈가...	**pNFS** 기본값은...
9.8 이상	사용 안 함
9.7 이하	활성화됨

필요한 것

pNFS를 사용하려면 NFSv4.1 지원이 필요합니다.

pNFS를 활성화하려면 먼저 NFS 조회를 비활성화해야 합니다. 둘 다 동시에 활성화할 수는 없습니다.

SVM에서 Kerberos와 pNFS를 사용하는 경우 SVM의 모든 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
pNFS를 활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS enabled'
pNFS를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS disabled'

관련 정보

- NFS 트렁킹 개요

TCP 및 UDP를 통한 NFS 액세스를 제어합니다

TCP와 UDP를 통해 각각 '-TCP' 및 '-UDP' 매개 변수를 수정하여 SVM(스토리지 가상 시스템)에 대한 NFS 액세스를 설정하거나 해제할 수 있습니다. 따라서 NFS 클라이언트가 사용자 환경에서 TCP 또는 UDP를 통해 데이터에 액세스할 수 있는지 여부를 제어할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 NFS에만 적용됩니다. 보조 프로토콜에는 영향을 미치지 않습니다. 예를 들어, TCP를 통한 NFS가 해제되어 있는 경우 TCP를 통한 마운트 작업은 계속 성공합니다. TCP 또는 UDP 트래픽을 완전히 차단하려면 내보내기 정책 규칙을 사용할 수 있습니다.

> 명령 실패 오류를 방지하려면 NFS용 TCP를 해제하기 전에 SnapDiff RPC Server를 꺼야 합니다. 'vserver snapdiff -rpc -server off -vserver vserver name' 명령을 사용하여 TCP를 비활성화할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

NFS 액세스를 원하는 경우...	명령 입력...
TCP를 통해 활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp enabled'
TCP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp disabled'
UDP를 통해 활성화됩니다	'vserver nfs modify -vserver vserver_name -udp enabled'
UDP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -udp disabled'

예약되지 않은 포트에서 NFS 요청 제어

'-mount-rootonly' 옵션을 설정하여 예약되지 않은 포트에서 NFS 마운트 요청을 거부할 수 있습니다. 예약되지 않은 포트의 모든 NFS 요청을 거부하려면 '-nfs-rootonly' 옵션을 설정합니다.

이 작업에 대해

기본적으로 '-mount-rootonly' 옵션은 'enabled'입니다.

기본적으로 '-nfs-rootonly' 옵션은 '사용 안 함'입니다.

이러한 옵션은 NULL 프로시저에는 적용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
예약되지 않은 포트에서 NFS 마운트 요청을 허용합니다	'vserver nfs modify -vserver vserver_name -mount -rootonly disabled'
예약되지 않은 포트에서 NFS 마운트 요청을 거부합니다	'vserver nfs modify -vserver vserver_name -mount -rootonly enabled'
예약되지 않은 포트에서 모든 NFS 요청을 허용합니다	'vserver nfs modify -vserver vserver_name -nfs-rootonly disabled'
예약되지 않은 포트의 모든 NFS 요청을 거부합니다	'vserver nfs modify -vserver vserver_name -nfs-rootonly enabled'

알 수 없는 **UNIX** 사용자의 **NTFS** 볼륨 또는 **qtree**에 대한 **NFS** 액세스를 처리합니다

ONTAP가 NTFS 보안 스타일로 볼륨이나 qtree에 연결하려고 시도하는 UNIX 사용자를 식별할 수 없는 경우 사용자를 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 보다 엄격한 보안을 위해 이러한 사용자에 대한 액세스를 거부하거나 모든 사용자에 대한 최소 액세스 수준을 보장하도록 ONTAP를 기본 Windows 사용자에게 매핑하도록 구성할 수 있습니다.

필요한 것

이 옵션을 활성화하려면 기본 Windows 사용자를 구성해야 합니다.

이 작업에 대해

UNIX 사용자가 NTFS 보안 스타일로 볼륨이나 qtree에 액세스하려고 할 경우 ONTAP에서 NTFS 권한을 올바르게 평가할 수 있도록 UNIX 사용자를 Windows 사용자에게 먼저 매핑해야 합니다. 그러나 ONTAP가 구성된 사용자 정보 이름 서비스 소스에서 UNIX 사용자의 이름을 찾을 수 없는 경우 UNIX 사용자를 특정 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 다음과 같은 방법으로 이러한 알 수 없는 UNIX 사용자를 처리하는 방법을 결정할 수 있습니다.

- 알 수 없는 UNIX 사용자에 대한 액세스를 거부합니다.

  이렇게 하면 모든 UNIX 사용자가 NTFS 볼륨이나 qtree에 액세스할 수 있도록 명시적 매핑이 요구되므로 보안이 더욱 강화됩니다.

- 알 수 없는 UNIX 사용자를 기본 Windows 사용자로 매핑합니다.

  따라서 모든 사용자가 기본 Windows 사용자를 통해 NTFS 볼륨 또는 qtree에 대한 최소 액세스 수준을 얻을 수

있으므로 보안이 낮지만 편의성이 높아집니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

알 수 없는 UNIX 사용자에 대해 기본 Windows 사용자를 사용하려는 경우…	명령 입력…
활성화됨	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예약되지 않은 포트를 사용하여 **NFS** 내보내기를 마운트하는 클라이언트에 대한 고려 사항

'-mount-rootonly' 옵션은 사용자가 루트로 로그인한 경우에도 예약되지 않은 포트를 사용하여 NFS 내보내기를 마운트하는 클라이언트를 지원해야 하는 스토리지 시스템에서 해제되어야 합니다. 이러한 클라이언트에는 Hummingbird 클라이언트와 Solaris NFS/IPv6 클라이언트가 포함됩니다.

'-mount-rootonly' 옵션이 설정된 경우 ONTAP는 예약되지 않은 포트를 사용하는 NFS 클라이언트가 허용되지 않습니다. 즉, 번호가 1,023보다 큰 포트를 사용하여 NFS 내보내기를 마운트할 수 있습니다.

도메인을 확인하여 넷그룹에 대해 보다 엄격한 액세스 검사를 수행합니다

기본적으로 ONTAP는 넷그룹에 대한 클라이언트 액세스를 평가할 때 추가 검증을 수행합니다. 추가 검사를 통해 클라이언트 도메인이 SVM(스토리지 가상 머신)의 도메인 구성과 일치하는지 확인합니다. 그렇지 않으면 ONTAP는 클라이언트 액세스를 거부합니다.

이 작업에 대해

ONTAP에서 클라이언트 액세스에 대한 엑스포트 정책 규칙을 평가하고 엑스포트 정책 규칙에 넷그룹이 포함되어 있는 경우, ONTAP는 클라이언트의 IP 주소가 넷그룹에 속하는지 여부를 결정해야 합니다. 이를 위해 ONTAP는 DNS를 사용하여 클라이언트의 IP 주소를 호스트 이름으로 변환하고 FQDN(정규화된 도메인 이름)을 얻습니다.

넷그룹 파일에 호스트에 대한 짧은 이름만 나열되고 호스트에 대한 짧은 이름이 여러 도메인에 있는 경우 다른 도메인의 클라이언트가 이 검사 없이 액세스할 수 있습니다.

이를 방지하기 위해 ONTAP는 호스트의 DNS에서 반환된 도메인을 SVM용으로 구성된 DNS 도메인 이름 목록과 비교합니다. 일치하는 경우 액세스가 허용됩니다. 일치하지 않으면 액세스가 거부됩니다.

이 검증은 기본적으로 활성화되어 있습니다. 고급 권한 수준에서 사용할 수 있는 '-netgroup-dns-domain-search' 매개변수를 수정하여 이 매개 변수를 관리할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

넷그룹에 대한 도메인 확인을 원할 경우...	입력...
활성화됨	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search disabled'

3. 권한 수준을 admin으로 설정합니다.

   'Set-Privilege admin'입니다

NFSv3 서비스에 사용되는 포트를 수정합니다

스토리지 시스템의 NFS 서버에서는 마운트 데몬, Network Lock Manager 등의 서비스를 사용하여 특정 기본 네트워크 포트를 통해 NFS 클라이언트와 통신합니다. 대부분의 NFS 환경에서 기본 포트는 올바르게 작동하고 수정할 필요가 없지만, NFSv3 환경에서 다른 NFS 네트워크 포트를 사용하려는 경우에는 변경할 수 있습니다.

필요한 것

스토리지 시스템에서 NFS 포트를 변경하려면 모든 NFS 클라이언트가 시스템에 다시 연결해야 하므로 먼저 이 정보를 사용자에게 전달해야 합니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)에 대해 NFS 마운트 데몬, Network Lock Manager, Network Status Monitor, NFS 할당량 데몬 서비스에서 사용하는 포트를 설정할 수 있습니다. 포트 번호 변경은 TCP 및 UDP를 통해 데이터에 액세스하는 NFS 클라이언트에 영향을 줍니다.

NFSv4 및 NFSv4.1의 포트는 변경할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. NFS에 대한 액세스 해제:

   'vserver nfs modify -vserver vserver_name -access false'

3. 특정 NFS 서비스의 NFS 포트를 설정합니다.

   'vserver nfs modify -vserver vserver vserver_namenfs_port_parameterport_number'

NFS 포트 매개 변수입니다	설명	기본 포트입니다
'- mountd-port'입니다	NFS 마운트 데몬입니다	635
``NLM-PORT'	네트워크 잠금 관리자	4045
'-NSM-port'입니다	네트워크 상태 모니터	4046
``rquotad-port''	NFS 할당량 데몬입니다	4049

   기본 포트 이외에 허용되는 포트 번호 범위는 1024 ~ 65535입니다. 각 NFS 서비스는 고유한 포트를 사용해야 합니다.

4. NFS에 대한 액세스 설정:

   'vserver nfs modify -vserver vserver_name -access TRUE'

5. 'network connections listening show' 명령어를 이용하여 포트 번호 변화를 확인한다.
6. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 NFS 마운트 데몬 포트가 1113으로 설정됩니다.

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- --------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFS 서버 관리를 위한 명령입니다

NFS 서버를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
NFS 서버를 생성합니다	'vserver nfs create
NFS 서버를 표시합니다	'vserver nfs show'
NFS 서버를 수정합니다	'vserver nfs modify(가상 NFS 수정)'
NFS 서버를 삭제합니다	'vserver nfs delete

NFSv3 마운트 지점 아래에 있는 '.snapshot' 디렉토리를 숨깁니다 이 옵션을 사용하는 경우에도 '.snapshot' 디렉토리에 대한 명시적 액세스는 계속 허용됩니다.	'-v3-hide-snapshot' 옵션이 활성화된 'vserver nfs' 명령입니다

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

이름 서비스 문제를 해결합니다

클라이언트가 이름 서비스 문제로 인해 액세스 오류가 발생하는 경우, 'vserver services name-service getxxbyy' 명령 제품군을 사용하여 다양한 이름 서비스 조회를 수동으로 수행하고 조회에 대한 세부 정보와 결과를 확인하여 문제 해결에 도움이 될 수 있습니다.

이 작업에 대해

- 각 명령에 대해 다음을 지정할 수 있습니다.
  - 조회를 수행할 노드 또는 SVM(스토리지 가상 머신)의 이름입니다.

    이를 통해 특정 노드 또는 SVM에 대한 네임 서비스 조회를 테스트하여 잠재적 네임 서비스 구성 문제에 대한 검색 범위를 좁힐 수 있습니다.
  - 조회에 사용된 소스를 표시할지 여부를 나타냅니다.

    이를 통해 올바른 소스가 사용되었는지 확인할 수 있습니다.
- ONTAP는 구성된 이름 서비스 스위치 순서에 따라 조회를 수행하기 위한 서비스를 선택합니다.
- 이러한 명령은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

를 검색하려면…	명령 사용…
호스트 이름의 IP 주소입니다	'vserver services name-service getxxyy getaddrinfo''vserver services name-service getxxyy gethostbyname'(IPv4 주소만 해당)
그룹 ID별 그룹 구성원	'vserver services name-service getxxyy getgrbygid'
그룹 이름으로 그룹의 구성원	'vserver services name-service getxxyy getgrbyname'
사용자가 속한 그룹 목록입니다	'vserver services name-service getxxyy getgrlist'

IP 주소의 호스트 이름입니다	'vserver services name-service getxxbyyy GetNameInfo''vserver services name-service getxxyy gethostbyaddr'(IPv4 주소만)
사용자 이름별 사용자 정보	'vserver services name-service getxxbyyy getpwbyname' '-use-RBAC' 매개변수를 TRUE로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
사용자 ID별 사용자 정보	'vserver services name-service getxxbyyy getpwbyuid' '-use-RBAC' 매개 변수를 true로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyy netgrp'
Netgroup-by-host 검색을 사용하는 클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyyy netgrpbyhost'

다음 예에서는 acast1.eng.example.com 호스트의 IP 주소를 획득하여 SVM VS1 에 대한 DNS 조회 테스트를 보여줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

다음 예에서는 UID 501768을 가진 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 NIS 조회 테스트를 보여줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

다음 예제는 이름이 ldap1인 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 LDAP 조회 테스트를 보여줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

다음 예에서는 클라이언트 dnshost0이 넷그룹 lnetgroup136의 구성원인지 여부를 확인함으로써 SVM V1에 대한 넷그룹 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 수행한 테스트의 결과를 분석하고 필요한 조치를 취합니다.

만약...	다음을 확인하십시오.
호스트 이름 또는 IP 주소 조회에 실패했거나 잘못된 결과가 발생했습니다	DNS 구성
조회가 잘못된 소스를 쿼리했습니다	네임 서비스 스위치 구성
사용자 또는 그룹 조회에 실패했거나 잘못된 결과가 발생했습니다	• 네임 서비스 스위치 구성 • 소스 구성(로컬 파일, NIS 도메인, LDAP 클라이언트) • 네트워크 구성(예: LIF 및 라우트)
호스트 이름 조회가 실패했거나 시간이 초과되었으며 DNS 서버가 DNS 짧은 이름(예: host1)을 확인하지 않습니다.	최상위 도메인(TLD) 쿼리에 대한 DNS 구성 vserver services name-service dns modify 명령에 대한 `-is-tLD-query-enabled false ' 옵션을 사용하여 TLD 쿼리를 비활성화할 수 있습니다.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

네임 서비스 연결을 확인합니다

ONTAP 9.2부터는 DNS 및 LDAP 네임 서버가 ONTAP에 연결되어 있는지 확인할 수 있습니다. 이러한 명령은 admin 권한 수준에서 사용할 수 있습니다.

이 작업에 대해

이름 서비스 구성 검사기를 사용하여 필요에 따라 유효한 DNS 또는 LDAP 네임 서비스 구성을 확인할 수 있습니다. 이러한 검증 검사는 명령줄 또는 System Manager에서 시작할 수 있습니다.

DNS 구성의 경우 모든 서버가 테스트되고 유효한 구성으로 간주되려면 해당 구성이 제대로 작동되어야 합니다. LDAP 구성의 경우 서버가 가동되는 한 구성이 유효합니다. 'ip-config-validation' 필드가 true(기본값 false)가 아닌 경우 이름 서비스 명령은 구성 검사기를 적용합니다.

단계

1. 적절한 명령을 사용하여 네임 서비스 구성을 확인합니다. UI는 구성된 서버의 상태를 표시합니다.

확인하려면…	이 명령 사용…
DNS 구성 상태입니다	'vserver services name-service dns check'
LDAP 구성 상태입니다	'vserver services name-service ldap check'

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

구성된 서버 중 하나(name-servers/ldap-servers)에 연결할 수 있고 서비스를 제공하는 경우 구성 검증이 성공적으로 수행됩니다. 일부 서버에 연결할 수 없는 경우 경고가 표시됩니다.

이름 서비스 스위치 항목을 관리하는 명령입니다

이름 서비스 스위치 항목은 생성, 표시, 수정 및 삭제하여 관리할 수 있습니다.

원하는 작업	이 명령 사용…
이름 서비스 스위치 항목을 생성합니다	'vserver services name-service ns-switch create'
이름 서비스 스위치 항목을 표시합니다	'vserver services name-service ns-switch show'
이름 서비스 스위치 항목을 수정합니다	'vserver services name-service ns-switch modify'를 참조하십시오
이름 서비스 스위치 항목을 삭제합니다	'vserver services name-service ns-switch delete'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

이름 서비스 캐시를 관리하는 명령입니다

TTL(Time To Live) 값을 수정하여 이름 서비스 캐시를 관리할 수 있습니다. TTL 값은 이름 서비스 정보가 캐시에 지속되는 기간을 결정합니다.

TTL 값을 수정하려는 경우…	이 명령 사용…
Unix 사용자	'vserver services name-service cache unix-user settings
Unix 그룹	'vserver services name-service cache unix-group settings'
Unix 넷그룹	'vserver services name-service cache netgroups settings'(SVM 서비스 이름 서비스 캐시 넷그룹 설정)
호스트	'vserver services name-service cache hosts settings'(SVM 서비스 이름 서비스 캐시 호스트 설정)
그룹 구성원 자격	'vserver services name-service cache group-membership settings'

관련 정보

"ONTAP 9 명령"

이름 매핑을 관리하는 명령입니다

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
이름 매핑을 생성합니다	'vserver name-mapping create'
특정 위치에 이름 매핑을 삽입합니다	'vserver name-mapping insert'
이름 매핑을 표시합니다	'vserver name-mapping show'
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	'vserver name-mapping swap'
이름 매핑을 수정합니다	'vserver name-mapping modify'입니다
이름 매핑을 삭제합니다	'vserver name-mapping delete
올바른 이름 매핑을 확인합니다	'vserver security file-directory show-Effective-permissions-vserver vs1-win-user-name user1-path/-share-name SH1'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

로컬 **UNIX** 사용자를 관리하는 명령입니다

로컬 UNIX 사용자를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
로컬 UNIX 사용자를 생성합니다	'vserver services name-service unix-user create'를 참조하십시오
URI에서 로컬 UNIX 사용자를 로드합니다	'vserver services name-service unix-user load-from-Uri'
로컬 UNIX 사용자를 표시합니다	'vserver services name-service unix-user show'를 참조하십시오
로컬 UNIX 사용자를 수정합니다	'vserver services name-service unix-user modify'를 참조하십시오
로컬 UNIX 사용자를 삭제합니다	'vserver services name-service unix-user delete

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

로컬 **UNIX** 그룹을 관리하는 명령입니다

로컬 UNIX 그룹을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
로컬 UNIX 그룹을 생성합니다	'vserver services name-service unix-group create'를 참조하십시오
로컬 UNIX 그룹에 사용자를 추가합니다	'vserver services name-service unix-group adduser'
URI에서 로컬 UNIX 그룹을 로드합니다	가상 서버 서비스 이름 서비스 unix-group load-from-Uri
로컬 UNIX 그룹을 표시합니다	'vserver services name-service unix-group show'를 참조하십시오
로컬 UNIX 그룹을 수정합니다	'vserver services name-service unix-group modify'를 참조하십시오
로컬 UNIX 그룹에서 사용자를 삭제합니다	'vserver services name-service unix-group deluser'
로컬 UNIX 그룹을 삭제합니다	'vserver services name-service unix-group delete'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

로컬 **UNIX** 사용자, 그룹 및 그룹 구성원에 대한 제한

ONTAP는 클러스터의 최대 UNIX 사용자 및 그룹 수와 이러한 제한을 관리하는 명령에 대한 제한을 도입했습니다. 이러한 제한을 사용하면 관리자가 클러스터에 너무 많은 로컬 UNIX 사용자 및 그룹을 생성하지 못하도록 하여 성능 문제를 방지할 수 있습니다.

로컬 UNIX 사용자 그룹 및 그룹 구성원의 총 수에 대한 제한이 있습니다. 로컬 UNIX 사용자에게는 별도의 제한이 있습니다. 제한은 클러스터 전반에 적용됩니다. 이러한 각 새 제한은 미리 할당된 하드 제한까지 수정할 수 있는 기본값으로 설정됩니다.

데이터베이스	기본 제한	엄격한 제한
로컬 UNIX 사용자	32,768입니다	65,536
로컬 UNIX 그룹 및 그룹 구성원	32,768입니다	65,536

로컬 **UNIX** 사용자 및 그룹에 대한 제한을 관리합니다

로컬 UNIX 사용자 및 그룹에 대한 제한을 관리하기 위한 특정 ONTAP 명령이 있습니다. 클러스터 관리자는 이러한 명령을 사용하여 과도한 수의 로컬 UNIX 사용자 및 그룹과 관련된 것으로 여겨지는 클러스터의 성능 문제를 해결할 수 있습니다.

이 작업에 대해

이러한 명령은 클러스터 관리자가 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 사용...
로컬 UNIX 사용자 제한에 대한 정보를 표시합니다	'vserver services unix-user max-limit show'를 선택합니다
로컬 UNIX 그룹 제한에 대한 정보를 표시합니다	'vserver services unix-group max-limit show'를 선택합니다
로컬 UNIX 사용자 제한을 수정합니다	'vserver services unix-user max-limit modify'를 참조하십시오
로컬 UNIX 그룹 제한을 수정합니다	'vserver services unix-group max-limit modify'를 참조하십시오

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

로컬 넷그룹을 관리하기 위한 명령입니다

로컬 넷그룹을 URI에서 로드하고, 노드 간에 상태를 확인하고, 표시하고, 삭제하여 관리할 수 있습니다.

원하는 작업	명령 사용…
URI에서 넷그룹을 로드합니다	'vserver services name-service netgroup load'
전체 노드에서 넷그룹의 상태를 확인합니다	'vserver services name-service netgroup status' 고급 권한 수준에서 사용할 수 있습니다.
로컬 넷그룹을 표시합니다	'vserver services name-service netgroup file show'를 참조하십시오
로컬 넷그룹을 삭제합니다	'vserver services name-service 넷그룹 파일 삭제

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

NIS 도메인 구성을 관리하는 명령입니다

NIS 도메인 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
NIS 도메인 구성을 생성합니다	'vserver services name-service nis-domain create'를 참조하십시오
NIS 도메인 구성을 표시합니다	'vserver services name-service NIS-domain show'를 참조하십시오

NIS 도메인 구성의 바인딩 상태를 표시합니다	'vserver services name-service nis-domain show-bound'
NIS 통계를 표시합니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 표시-통계.
NIS 통계를 지웁니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 지우기-통계.
NIS 도메인 구성을 수정합니다	'vserver services name-service NIS-domain modify'를 참조하십시오
NIS 도메인 구성을 삭제합니다	'vserver services name-service nis-domain delete'
호스트 별 넷그룹 검색에 대한 캐싱을 설정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service NIS-domain netgroup-database config modify'입니다.

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

LDAP 클라이언트 구성을 관리하는 명령입니다

LDAP 클라이언트 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 구성을 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용…
LDAP 클라이언트 구성을 생성합니다	'vserver services name-service ldap client create'
LDAP 클라이언트 구성을 표시합니다	'vserver services name-service ldap client show'
LDAP 클라이언트 구성을 수정합니다	'vserver services name-service ldap client modify'를 참조하십시오
LDAP 클라이언트 바인딩 암호를 변경합니다	'vserver services name-service ldap client modify-bind-password'
LDAP 클라이언트 구성을 삭제합니다	'vserver services name-service ldap client delete'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

LDAP 구성을 관리하는 명령입니다

LDAP 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…

LDAP 구성을 생성합니다	'vserver services name-service ldap create'
LDAP 구성을 표시합니다	'vserver services name-service ldap show'
LDAP 구성을 수정합니다	'vserver services name-service ldap modify'를 참조하십시오
LDAP 구성을 삭제합니다	'vserver services name-service ldap delete'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

LDAP 클라이언트 스키마 템플릿을 관리하는 명령입니다

LDAP 클라이언트 스키마 템플릿을 관리하기 위한 특정 ONTAP 명령이 있습니다.

SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 스키마를 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용…
기존 LDAP 스키마 템플릿을 복사합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 복사'입니다.
LDAP 스키마 템플릿을 표시합니다	'vserver services name-service ldap client schema show'를 참조하십시오
LDAP 스키마 템플릿을 수정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 수정'입니다.
LDAP 스키마 템플릿을 삭제합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 삭제'입니다.

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

NFS Kerberos 인터페이스 구성을 관리하는 명령입니다

NFS Kerberos 인터페이스 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
LIF에서 NFS Kerberos를 사용하도록 설정합니다	'vserver NFS Kerberos interface enable'
NFS Kerberos 인터페이스 구성을 표시합니다	vserver nfs Kerberos interface show를 선택합니다

NFS Kerberos 인터페이스 구성을 수정합니다	가상 NFS Kerberos 인터페이스 수정
LIF에서 NFS Kerberos를 사용하지 않도록 설정합니다	'vserver NFS Kerberos interface disable'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

NFS Kerberos 영역 구성을 관리하는 명령입니다

NFS Kerberos 영역 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용**...**
NFS Kerberos 영역 구성을 생성합니다	'vserver NFS Kerberos 영역 생성'
NFS Kerberos 영역 구성을 표시합니다	가상 NFS Kerberos 영역 표시
NFS Kerberos 영역 구성을 수정합니다	가상 NFS Kerberos 영역 수정
NFS Kerberos 영역 구성을 삭제합니다	'vserver NFS Kerberos 영역 삭제'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

엑스포트 정책을 관리하는 명령입니다

내보내기 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
엑스포트 정책에 대한 정보를 표시합니다	vserver export-policy show를 참조하십시오
엑스포트 정책의 이름을 바꿉니다	'vserver export-policy rename'
엑스포트 정책을 복사합니다	'vserver export-policy copy'
엑스포트 정책을 삭제합니다	'vserver export-policy delete

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

내보내기 규칙을 관리하는 명령입니다

내보내기 규칙을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
엑스포트 규칙을 생성합니다	'vserver export-policy rule create'
내보내기 규칙에 대한 정보를 표시합니다	'vserver export-policy rule show'를 선택합니다
엑스포트 규칙을 수정합니다	'vserver export-policy rule modify'입니다
엑스포트 규칙을 삭제합니다	'vserver export-policy rule delete

서로 다른 클라이언트와 일치하는 동일한 내보내기 규칙을 여러 개 구성한 경우 내보내기 규칙을 관리할 때 해당 규칙을 동기화 상태로 유지해야 합니다.

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

NFS 자격 증명 캐시를 구성합니다

NFS 자격 증명 캐시 라이브 시간 수정 이유

ONTAP는 보다 빠른 액세스를 제공하고 성능을 향상시키기 위해 자격 증명 캐시를 사용하여 NFS 내보내기 액세스에 대한 사용자 인증에 필요한 정보를 저장합니다. 자격 증명 캐시에 정보가 저장되는 기간을 구성하여 사용자 환경에 맞게 정보를 사용자 지정할 수 있습니다.

NFS 자격 증명 캐시 TTL(Time-to-Live)을 수정하면 문제를 해결하는 데 도움이 되는 몇 가지 시나리오가 있습니다. 이러한 시나리오가 무엇인지, 그리고 이러한 수정 결과로 초래되는 결과를 이해해야 합니다.

이유

다음과 같은 경우 기본 TTL을 변경하십시오.

문제	구제 조치
사용자 환경의 네임 서버에서 ONTAP의 요청 로드가 높기 때문에 성능이 저하됩니다.	캐시된 양의 자격 증명과 음의 자격 증명에 대한 TTL을 늘려 ONTAP에서 이름 서버로 보내는 요청 수를 줄입니다.
이름 서버 관리자가 이전에 거부된 NFS 사용자에 대한 액세스를 허용하도록 변경되었습니다.	캐시된 음수 자격 증명에 대한 TTL을 줄여 NFS 사용자가 외부 이름 서버에서 새 자격 증명을 요청할 때까지 ONTAP를 기다려야 하는 시간을 줄임으로써 액세스 권한을 얻을 수 있습니다.
이름 서버 관리자가 이전에 허용된 NFS 사용자에 대한 액세스를 거부하도록 변경되었습니다.	캐시된 양의 자격 증명에 대한 TTL을 줄여 ONTAP가 외부 이름 서버에서 새 자격 증명을 요청하는 시간을 줄임으로써 NFS 사용자가 액세스를 거부하도록 합니다.

결과

양의 자격 증명과 음수 자격 증명을 캐시하기 위해 시간을 개별적으로 수정할 수 있습니다. 그러나 그렇게 할 때의 장단점을 모두 알아야 합니다.

만약...	장점은...	단점은...
양의 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되었지만 더 이상 허용되지 않았던 NFS 사용자에 대한 액세스를 거부하는 데 시간이 더 오래 걸립니다.
양의 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되었지만 이제는 그렇지 않은 NFS 사용자에 대한 액세스를 거부하는 데 걸리는 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.
부정적인 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 오래 걸립니다.
부정적인 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.

캐시된 **NFS** 사용자 자격 증명에 대한 라이브 시간 구성

SVM(스토리지 가상 시스템)의 NFS 서버를 수정하여 ONTAP에서 NFS 사용자에 대한 자격 증명을 내부 캐시(TTL(Time-to-Live)에 저장하는 시간을 구성할 수 있습니다. 따라서 네임 서버의 높은 부하나 NFS 사용자 액세스에 영향을 미치는 자격 증명의 변경과 관련된 특정 문제를 완화할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

캐싱된 TTL을 수정하려는 경우...	명령 사용...

양의 자격 증명	'vserver nfs modify -vserver vserver_name -cached -cred -positive -ttl time_to_live' TTL은 밀리초 단위로 측정됩니다. ONTAP 9.10.1 이상부터 기본값은 1시간(3,600,000밀리초)입니다. ONTAP 9.9.1 이하 버전의 경우 기본값은 24시간(86,400,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.
음수 자격 증명	'vserver nfs modify -vserver vserver_name -cached -cred -negative -tl time_to_live' TTL은 밀리초 단위로 측정됩니다. 기본값은 2시간(7,200,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

엑스포트 정책 캐시 관리

엑스포트 정책 캐시 플러시

ONTAP는 빠른 액세스를 위해 여러 엑스포트 정책 캐시를 사용하여 엑스포트 정책과 관련된 정보를 저장합니다. 내보내기 정책 캐시를 수동으로 플러싱하면('vserver export-policy cache flush') 오래된 정보가 제거되고 ONTAP가 적절한 외부 리소스에서 현재 정보를 검색하도록 합니다. 이렇게 하면 NFS 내보내기에 대한 클라이언트 액세스와 관련된 다양한 문제를 해결할 수 있습니다.

이 작업에 대해

다음과 같은 이유로 인해 엑스포트 정책 캐시 정보가 오래된 것일 수 있습니다.

- 정책 규칙을 내보내기 위한 최근 변경 사항
- 이름 서버의 호스트 이름 레코드에 대한 최근 변경 사항
- 이름 서버의 넷그룹 항목에 대한 최근 변경 사항
- 네트워크 중단 상태에서 복구되어 넷그룹이 완전히 로드되지 않았습니다

단계

1. 이름 서비스 캐시를 사용하지 않는 경우 다음 작업 중 하나를 고급 권한 모드에서 수행합니다.

플러시를 원하는 경우...	명령 입력...
모든 엑스포트 정책 캐시(Showmount 제외)	'vserver export-policy cache flush-vserver vserver_name'

플러시를 원하는 경우...	명령 입력...
엑스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access'는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache host'
넷그룹 캐시입니다	넷그룹의 처리는 리소스를 많이 소모하는 작업입니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

2. 이름 서비스 캐시가 활성화된 경우 다음 작업 중 하나를 수행합니다.

플러시를 원하는 경우...	명령 입력...
엑스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access'는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver services name-service cache hosts forward-lookup delete-all'
넷그룹 캐시입니다	SVM 서비스 이름-서비스 캐시 넷그룹 IP-넷그룹 삭제-모두 SVM 서비스 이름-서비스 캐시 넷그룹 구성원 삭제 -모두(All) 넷그룹 처리는 리소스를 많이 소모합니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

엑스포트 정책 넷그룹 큐 및 캐시를 표시합니다

ONTAP는 넷그룹 큐를 가져와 확인할 때 넷그룹 큐를 사용하고 넷그룹 캐시를 사용하여 결과 정보를 저장합니다. 엑스포트 정책 넷그룹 관련 문제를 해결할 때 'vserver export-policy netgroup queue show' 및 'vserver export-policy netgroup cache show' 명령을 사용하여 넷그룹 큐의 상태와 넷그룹 캐시의 내용을 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

엑스포트 정책 넷그룹을 표시하려면…	명령 입력…
대기열	'vserver export-policy netgroup queue show'를 선택합니다
캐시	'vserver export-policy netgroup cache show -vserver vserver_name'을 선택합니다

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

클라이언트 **IP** 주소가 넷그룹의 구성원인지 확인합니다

넷그룹과 관련된 NFS 클라이언트 액세스 문제를 해결할 때 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.

이 작업에 대해

넷그룹 구성원 자격을 확인하면 ONTAP가 클라이언트가 넷그룹의 구성원인지 여부를 확인할 수 있습니다. 또한 넷그룹 정보를 새로 고치는 동안 ONTAP 넷그룹 캐시가 임시 상태인지 여부를 알 수 있습니다. 이 정보는 클라이언트가 예기치 않게 액세스 권한을 부여받거나 거부되는 이유를 이해하는 데 도움이 될 수 있습니다.

단계

1. 클라이언트 IP 주소의 넷그룹 멤버쉽을 확인합니다. 'vserver export-policy netgroup check-membership-vserver vserver_name-netgroup netgroup_name-client-ip client_ip'

   명령을 실행하면 다음 결과가 반환될 수 있습니다.

   - 클라이언트가 넷그룹의 구성원입니다.

     역방향 조회 검사 또는 호스트 별 넷그룹 검색을 통해 확인되었습니다.

   - 클라이언트가 넷그룹의 구성원입니다.

     ONTAP 넷그룹 캐시에서 발견되었습니다.

   - 클라이언트가 넷그룹의 구성원이 아닙니다.
   - ONTAP가 현재 넷그룹 캐시를 새로 고치고 있기 때문에 클라이언트의 구성원을 확인할 수 없습니다.

     이 작업이 수행되지 않을 때까지 멤버 자격은 명시적으로 배제될 수 없습니다. 'vserver export-policy netgroup queue show' 명령을 사용하여 넷그룹의 로드를 모니터링하고 작업이 완료된 후 검사를 다시 시도하십시오.

예

다음 예에서는 IP 주소가 172.17.16.72인 클라이언트가 SVM VS1 에 있는 넷그룹 수은의 구성원인지 여부를 확인합니다.

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

액세스 캐시 성능을 최적화합니다

여러 매개 변수를 구성하여 액세스 캐시를 최적화하고 성능과 액세스 캐시에 저장된 정보의 현재 상태 간에 적절한 균형을 찾을 수 있습니다.

이 작업에 대해

액세스 캐시 새로 고침 기간을 구성할 때는 다음 사항을 염두에 두십시오.

- 값이 높을수록 액세스 캐시에서 항목이 더 오래 유지됩니다.

  ONTAP는 액세스 캐시 항목을 새로 고치는 데 리소스를 적게 사용하기 때문에 성능이 향상됩니다. 단점은 엑스포트 정책 규칙이 변경되고 액세스 캐시 항목이 오래되면 업데이트하는 데 시간이 오래 걸린다는 것입니다. 따라서 액세스를 받아야 하는 클라이언트가 거부되고 거부되어야 하는 클라이언트가 액세스할 수 있습니다.

- 값이 낮을수록 ONTAP에서 액세스 캐시 항목을 더 자주 새로 고칩니다.

  장점은 항목이 더 최신 항목이고 클라이언트가 올바르게 액세스 권한을 부여하거나 거부될 가능성이 더 높다는 점입니다. 단점은 ONTAP에서 액세스 캐시 항목을 새로 고치는 데 더 많은 리소스를 사용하기 때문에 성능이 저하된다는 것입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

수정 방법	입력...
양의 항목에 대한 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-positive timeout_value'
음수 항목의 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-negative timeout_value'
이전 항목의 제한 시간	'vserver export-policy access-cache config modify -all-vservers-ab하비스트-timeout_value'

3. 새 매개 변수 설정을 확인합니다.

   'vserver export-policy access-cache config show-all-vservers'

4. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

파일 잠금 관리

프로토콜 간 파일 잠금 정보

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 rm, rmdir, mv 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

ONTAP에서 읽기 전용 비트를 처리하는 방법

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP는 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우

ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.

- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

> 파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

공유 경로 구성 요소의 잠금 처리에 대한 **ONTAP**와 **Windows**의 차이점

Windows와 달리 ONTAP는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP는 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하기 위해 사용자 또는 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 하는 Windows ACL(액세스 제어 목록) 보안 설정을 적용할 수 있습니다.

에 대해 자세히 알아보십시오 "클라이언트가 액세스하는 동안 디렉토리의 이름을 변경하지 못하도록 하는 방법".

잠금에 대한 정보를 표시합니다

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

다음 예에서는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vserver locks 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: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   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: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
```

```
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              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
```

잠금 해제

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

'vserver lock break' 명령은 고급 권한 수준 이상에서만 사용할 수 있습니다. 명령에 대한 man 페이지에 자세한 정보가 포함되어 있습니다.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

   명령에 대한 man 페이지에 자세한 정보가 포함되어 있습니다.

2. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 다음 작업 중 하나를 수행합니다.

다음을 지정하여 잠금을 해제하려면…	명령 입력…

SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로	'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif'
잠금 ID입니다	'vserver lock break-lockid UUID

4. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

FPolicy를 먼저 읽고 첫 번째 쓰기 필터가 NFS에서 작동하는 방식

FPolicy가 읽기/쓰기 작업이 있는 외부 FPolicy 서버를 사용하여 모니터링되는 이벤트로 사용되는 경우 NFS 클라이언트에서 읽기/쓰기 요청의 트래픽이 많을 때 응답 시간이 오래 됩니다. NFS 클라이언트의 경우 FPolicy에서 첫 번째 읽기 및 첫 번째 쓰기 필터를 사용하므로 FPolicy 알림의 수가 줄어들고 성능이 향상됩니다.

NFS에서 클라이언트는 해당 핸들을 페치하여 파일에서 I/O를 수행합니다. 이 핸들은 서버와 클라이언트의 재부팅 후에도 유효합니다. 따라서 클라이언트는 핸들을 캐시하고 핸들을 다시 검색하지 않고 요청을 보낼 수 있습니다. 일반 세션에서 많은 읽기/쓰기 요청이 파일 서버로 전송됩니다. 이러한 모든 요청에 대해 알림이 생성되는 경우 다음과 같은 문제가 발생할 수 있습니다.

- 추가 알림 처리 및 응답 시간 증가로 인한 로드 증가
- 서버가 모든 알림의 영향을 받지 않더라도 FPolicy 서버에 많은 수의 알림이 전송됩니다.

클라이언트에서 특정 파일에 대한 첫 번째 읽기/쓰기 요청을 받으면 캐시 항목이 생성되고 읽기/쓰기 횟수가 증가합니다. 이 요청은 첫 번째 읽기/쓰기 작업으로 표시되며 FPolicy 이벤트가 생성됩니다. NFS 클라이언트에 대한 FPolicy 필터를 계획하고 생성하기 전에 FPolicy 필터 작동 방식에 대한 기본 사항을 이해해야 합니다.

- First-read: 첫 번째 읽기에 대한 클라이언트 읽기 요청을 필터링합니다.

  NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리되는 첫 번째 읽기 요청이 결정됩니다.

- First-write: 첫 번째 쓰기에 대한 클라이언트 쓰기 요청을 필터링합니다.

  NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리하는 첫 번째 쓰기 요청이 결정됩니다.

다음 옵션은 NFS 서버 데이터베이스에 추가됩니다.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

NFSv4.1 서버 구현 ID를 수정합니다

NFSv4.1 프로토콜에는 서버 도메인, 이름 및 날짜를 문서화하는 서버 구현 ID가 포함됩니다. 서버 구현 ID 기본값을 수정할 수 있습니다. 예를 들어, 사용 통계를 수집하거나 상호 운용성 문제를 해결하는 경우 기본값을 변경하면 유용합니다. 자세한 내용은 RFC 5661을 참조하십시오.

이 작업에 대해

세 옵션의 기본값은 다음과 같습니다.

옵션을 선택합니다	옵션 이름입니다	기본값
NFSv4.1 구현 ID 도메인	'-v4.1-구현도메인'	NetApp.com
NFSv4.1 구현 ID 이름	'-v4.1-구현명'	클러스터 버전 이름입니다
NFSv4.1 구현 ID 날짜	'-v4.1-구현일'	클러스터 버전 날짜입니다

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

NFSv4.1 구현 **ID**를 수정하려는 경우…	명령 입력…
도메인	'vserver nfs modify-v4.1-imImplementation-domain domain'
이름	'vserver nfs modify-v4.1-im구현-name 이름'
날짜	'vserver nfs modify-v4.1-dimImplementation-date date

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFSv4 ACL 관리

NFSv4 ACL 설정 이점

NFSv4 ACL을 설정하면 많은 이점이 있습니다.

NFSv4 ACL을 설정하면 다음과 같은 이점이 있습니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세밀하게 제어합니다
- NFS 보안 강화
- CIFS와의 상호 운용성 향상
- 사용자당 16개 그룹의 NFS 제한을 제거합니다

NFSv4 ACL의 작동 방식

NFSv4 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. ACL이 있는 디렉터리에 새 파일이나 하위 디렉터리가 만들어지면 새 파일 또는 하위 디렉터리는 적절한 상속 플래그로 태그가 지정된 ACL의 모든 ACE(ACL 항목)를 상속합니다.

NFSv4 요청의 결과로 파일이나 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되는지, 표준 UNIX 파일 액세스 권한만 포함되는지, 상위 디렉토리에 ACL이 있는지 여부에 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우 ACE에 적절한 상속 플래그가 지정된 경우 상위 디렉토리의 ACL에 있는 ACE는 새 파일 또는 디렉토리에 의해 상속됩니다.

> 상위 ACL은 '-v4.0-acl'이 'off'로 설정되어 있어도 상속된다.

- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여 표준 UNIX 파일 액세스 권한을 설정합니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 상속할 수 없는 ACL이 있는 경우 새 객체는 모드 비트로만 생성됩니다.

> vserver nfs나 vserver export-policy rule의 명령을 사용하여 '-chown-mode' 매개 변수를 '제한'으로 설정한 경우 NFSv4 ACL로 설정된 온디스크 사용 권한이 비루트 사용자가 파일 소유권을 변경할 수 있도록 허용하더라도 슈퍼유저만이 파일 소유권을 변경할 수 있습니다. 자세한 내용은 관련 man 페이지를 참조하십시오.

NFSv4 ACL 수정 설정 또는 해제

ONTAP가 ACL이 있는 파일 또는 디렉토리에 대해 'chmod' 명령을 수신하면 기본적으로 ACL이 유지되고 모드 비트 변경을 반영하도록 수정됩니다. 대신 ACL을 삭제하고자 하는 경우 동작을 변경하기 위해 '-v4-acl-preserve' 파라미터를 비활성화할 수 있습니다.

이 작업에 대해

통합 보안 스타일을 사용할 때 이 매개 변수는 클라이언트가 파일 또는 디렉터리에 대해 chmod, chgroup 또는 chown 명령을 보낼 때 NTFS 파일 권한을 보존할지 또는 삭제할지 여부도 지정합니다.

이 매개 변수의 기본값은 활성화되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다…
기존 NFSv4 ACL 보존 및 수정 설정(기본값)	'vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled'
모드 비트를 변경할 때 NFSv4 ACL을 보존하고 삭제합니다	'vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP에서 **NFSv4 ACL**을 사용하여 파일을 삭제할 수 있는지 여부를 확인하는 방법

파일을 삭제할 수 있는지 여부를 확인하기 위해 ONTAP에서는 파일의 삭제 비트와 포함하는 디렉토리의 delete_child 비트를 함께 사용합니다. 자세한 내용은 NFS 4.1 RFC 5661을 참조하십시오.

NFSv4 ACL을 설정하거나 해제합니다

NFSv4 ACL을 설정하거나 해제하려면 '-v4.0-acl' 및 '-v4.1-acl' 옵션을 수정할 수 있습니다. 이러한 옵션은 기본적으로 비활성화되어 있습니다.

이 작업에 대해

'-v4.0-acl' 또는 '-v4.1-acl' 옵션은 NFSv4 ACL의 설정 및 보기를 제어하지만 액세스 검사를 위해 이러한 ACL의 적용을 제어하지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
NFSv4.0 ACL을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl enabled'
NFSv4.0 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl disabled'
NFSv4.1 ACL을 활성화합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl enabled'

NFSv4.1 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl disabled'

NFSv4 ACL의 최대 **ACE** 제한을 수정합니다

매개 변수 '-v4-acl-max-aces'를 수정하여 각 NFSv4 ACL에 대해 허용되는 최대 ACE 수를 수정할 수 있습니다. 기본적으로 이 제한은 각 ACL에 대해 400개의 ACE로 설정됩니다. 이 제한을 늘리면 400개 이상의 ACE가 포함된 ACL을 사용하여 ONTAP를 실행하는 스토리지 시스템으로 데이터를 성공적으로 마이그레이션할 수 있습니다.

이 작업에 대해

이 제한을 늘리면 NFSv4 ACL을 사용하여 파일을 액세스하는 클라이언트의 성능에 영향을 줄 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. NFSv4 ACL의 최대 ACE 제한 수정:

   'vserver nfs modify -v4-acl-max-aces max_ace_limit'

   의 유효한 범위

   최대 에이스 한계는 192에서 1024로

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFSv4 파일 위임을 관리합니다

NFSv4 읽기 파일 위임을 설정하거나 해제합니다

NFSv4 읽기 파일 위임을 설정하거나 해제하려면 "-v4.0-read-delegation' 또는 '-v4.1-read-delegation' 옵션을 수정할 수 있습니다. 읽기 파일 위임을 사용하면 파일 열기 및 닫기와 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 읽기 파일 위임은 사용되지 않습니다.

읽기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 서버와 클라이언트에서 위임을 복구해야 한다는 단점이 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
NFSv4 읽기 파일 위임을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled'
NFSv4.1 읽기 파일 위임을 사용하도록 설정합니다	다음 명령을 입력합니다. + 'vserver NFS modify -vserver vserver_name -v4.1 -read -delegation enabled'
NFSv4 읽기 파일 위임을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled'
NFSv4.1 읽기 파일 위임을 사용하지 않도록 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled'

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

NFSv4 쓰기 파일 위임을 설정 또는 해제합니다

쓰기 파일 위임을 설정하거나 해제하려면 "-v4.0-write-delegation' 또는 '-v4.1-write-delegation' 옵션을 수정할 수 있습니다. 쓰기 파일 위임을 사용하면 파일 열기 및 닫기 외에도 파일 및 레코드 잠금과 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 쓰기 파일 위임은 사용되지 않습니다.

쓰기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 위임을 복구하려면 서버와 해당 클라이언트가 추가 작업을 수행해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
NFSv4 쓰기 파일 위임을 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v4.1 -write-delegation enabled' 명령을 입력합니다

원하는 작업	그러면...
NFSv4 쓰기 파일 위임을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled' 명령을 입력합니다

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

NFSv4 파일을 구성하고 잠금을 기록합니다

NFSv4 파일 및 레코드 잠금에 대해 설명합니다

NFSv4 클라이언트의 경우 ONTAP는 NFSv4 파일 잠금 메커니즘을 지원하여 임대 기반 모델에서 모든 파일 잠금의 상태를 유지합니다.

"NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"

NFSv4 잠금 임대 기간을 지정합니다

NFSv4 잠금 임대 기간(즉, ONTAP가 클라이언트에 잠금을 부여하는 기간)을 지정하려면 '-v4-lease-seconds' 옵션을 수정할 수 있습니다. 리스 기간이 짧을수록 서버 복구 속도가 빨라지며 리스 기간이 길면 매우 많은 양의 클라이언트를 처리하는 서버에 유용합니다.

이 작업에 대해

기본적으로 이 옵션은 30으로 설정되어 있습니다. 이 옵션의 최소값은 10입니다. 이 옵션의 최대값은 'locking.lease_seconds' 옵션으로 설정할 수 있는 locking grace 기간입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFSv4 잠금 유예 기간을 지정합니다

NFSv4 잠금 유예 기간(즉, 서버 복구 중에 클라이언트가 ONTAP에서 잠금 상태를 복구하려는 기간)을 지정하려면 "-v4-grace-seconds" 옵션을 수정할 수 있습니다.

이 작업에 대해

기본적으로 이 옵션은 45로 설정되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-grace-seconds_number_of_seconds _'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFSv4 참조 작동 방식

NFSv4 조회를 설정하면 ONTAP는 NFSv4 클라이언트에 ""intra-SVM" 조회를 제공합니다. SVM 내 의뢰는 NFSv4 요청을 수신하는 클러스터 노드가 SVM(스토리지 가상 머신)의 다른 논리 인터페이스(LIF)에 NFSv4 클라이언트를 참조하는 경우를 말합니다.

NFSv4 클라이언트는 해당 시점부터 타겟 LIF에서 조회 대상이 된 경로를 액세스해야 합니다. 원래 클러스터 노드는 SVM에 데이터 볼륨이 상주하는 클러스터 노드에 상주하는 LIF가 존재한다고 판단하여 클라이언트가 데이터에 더 빠르게 액세스하고 추가 클러스터 통신을 피할 수 있게 해줍니다.

NFSv4 조회를 설정하거나 해제합니다

'-v4-fsid-change' 및 '-v4.0-referral' 또는 '-v4.1-referral' 옵션을 활성화하여 스토리지 가상 시스템(SVM)에서 NFSv4 조회를 설정할 수 있습니다. NFSv4 조회를 설정하면 이 기능을 지원하는 NFSv4 클라이언트에 대한 데이터 액세스 속도가 빨라집니다.

필요한 것

NFS 조회를 설정하려면 먼저 parallel NFS를 해제해야 합니다. 동시에 둘 다 활성화할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
NFSv4 조회를 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled"vserver nfs modify -vserver vserver vserver_name -v4.0 -referral enabled'

NFSv4 조회를 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -referral disabled'
NFSv4.1 조회를 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled"vserver nfs modify -vserver vserver vserver_name -v4.1 -referral enabled'
NFSv4.1 조회를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -referral disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFS 통계를 표시합니다

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 NFS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tistics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NFS 객체를 식별합니다.

   '스타티틱스 카탈로그 객체 표시 - 객체 NFS *'

2. 자폐 시작 및 선택적 '자폐 중지' 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

예**: NFSv3** 성능 모니터링

다음 예제에는 NFSv3 프로토콜의 성능 데이터가 나와 있습니다.

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

다음 명령을 실행하면 성공한 읽기 및 쓰기 요청 수와 총 읽기 및 쓰기 요청 수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                             Value
    --------------------------- ---------------------------
    read_success                                        40042
    read_total                                          40042
    write_success                                     1492052
    write_total                                       1492052
```

관련 정보

"성능 모니터링 설정"

DNS 통계를 표시합니다

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 DNS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령어를 사용하여 데이터를 볼 수 있는 DNS 객체를 확인할 수 있다.

   '통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op *'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

DNS 통계 모니터링

다음 예에서는 DNS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

다음 명령을 실행하면 전송된 DNS 쿼리 수와 수신, 실패 또는 제한 시간이 초과된 DNS 쿼리 수를 비교하여 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

다음 명령을 실행하면 특정 서버의 DNS 쿼리에 대해 특정 오류가 수신된 횟수를 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

관련 정보

"성능 모니터링 설정"

NIS 통계를 표시합니다

스토리지 시스템에 SVM(스토리지 가상 머신)에 대한 NIS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NIS 객체를 식별합니다.

   '통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op *'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

NIS 통계 모니터링

다음 예에서는 NIS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

다음 명령을 실행하면 전송된 NIS 쿼리 수와 수신, 실패 또는 시간 초과 NIS 쿼리 수를 비교하여 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- ---------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

다음 명령을 실행하면 특정 서버의 NIS 쿼리에 대해 특정 오류가 수신된 횟수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- ---------------------------------
    count                                                           1
    error_string                                          YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

관련 정보

"성능 모니터링 설정"

VMware vStorage over NFS 지원

ONTAP는 NFS 환경에서 특정 VMware VAAI(vStorage APIs for Array Integration) 기능을 지원합니다.

지원되는 기능

지원되는 기능은 다음과 같습니다.

- 복사본 오프로드

  ESXi 호스트에서 호스트를 사용하지 않고 소스 및 대상 데이터 저장소 위치 간에 직접 VMDK(가상 머신 또는 가상 머신 디스크)를 복제할 수 있습니다. 이렇게 하면 ESXi 호스트 CPU 주기와 네트워크 대역폭이 절약됩니다. 복제 오프로드는 소스 볼륨이 스파스 상태인 경우 공간 효율성을 유지합니다.

- 공간 예약

  VMDK 파일용 공간을 예약하여 스토리지 공간을 보장합니다.

제한 사항

VMware vStorage over NFS에는 다음과 같은 제한 사항이 있습니다.

- 다음과 같은 경우 복사 오프로드 작업이 실패할 수 있습니다.

- 소스 또는 타겟 볼륨에서 웨이브다리미를 실행하는 동안 일시적으로 볼륨이 오프라인 상태가 되기 때문입니다
- 소스 또는 타겟 볼륨을 이동하는 동안
- 소스 또는 타겟 LIF를 이동하는 동안
- Takeover 또는 Giveback 작업을 수행하는 동안
- 스위치오버 또는 스위치백 작업을 수행하는 동안

- 다음 시나리오에서 파일 핸들 형식의 차이로 인해 서버 측 복제가 실패할 수 있습니다.

  Qtree를 내보낸 적이 없는 SVM으로 현재 또는 이전에 qtree를 내보낸 SVM에서 데이터를 복사하려고 합니다. 이러한 제한 사항을 해결하려면 대상 SVM에서 qtree를 하나 이상 내보낼 수 있습니다.

관련 정보

"Data ONTAP에서 지원하는 VAAI 오프로드 작업은 무엇입니까?"

VMware vStorage over NFS를 사용하거나 사용하지 않도록 설정합니다

"vserver NFS modify" 명령을 사용하여 SVM(스토리지 가상 머신)에서 VMware vStorage over NFS에 대한 지원을 설정하거나 해제할 수 있습니다.

이 작업에 대해

기본적으로 VMware vStorage over NFS에 대한 지원은 비활성화되어 있습니다.

단계

1. SVM에 대한 현재 vStorage 지원 상태 표시:

   'vserver nfs show -vserver vserver_name -instance'

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
VMware vStorage 지원을 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage enabled'
VMware vStorage 지원을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage disabled'

작업을 마친 후

이 기능을 사용하려면 먼저 VMware VAAI용 NFS 플러그인을 설치해야 합니다. 자세한 내용은 _VMware VAAI_용 NetApp NFS 플러그인 설치 를 참조하십시오.

관련 정보

"NetApp 설명서: VMware VAAI용 NetApp NFS 플러그인"

rquota 지원을 설정하거나 해제합니다

ONTAP는 원격 할당량 프로토콜 버전 1(rquota v1)을 지원합니다. rquota 프로토콜을 사용하면 NFS 클라이언트가 원격 시스템에서 사용자에 대한 할당량 정보를 얻을 수 있습니다. "vserver NFS modify" 명령을 사용하여 SVM(스토리지 가상 시스템)에서 rquota를 설정할 수 있습니다.

이 작업에 대해

기본적으로 rquota는 비활성화되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
SVM에 대해 rquota 지원을 설정합니다	'vserver nfs modify -vserver vserver_name -rquota enable'
SVM에 대한 rquota 지원을 비활성화합니다	'vserver nfs modify -vserver vserver_name -rquota disable'

할당량에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

TCP 전송 크기를 수정하여 NFSv3 및 NFSv4 성능 향상

TCP 최대 전송 크기를 수정하여 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 접속하는 NFSv3 및 NFSv4 클라이언트의 성능을 향상시킬 수 있습니다.

클라이언트가 지연 시간이 10밀리초 이상 인 WAN(Wide Area Network) 또는 MAN(Metro Area Network)과 같이 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 액세스하는 경우 TCP 최대 전송 크기를 수정하여 연결 성능을 향상시킬 수 있습니다. LAN(Local Area Network)과 같이 지연 시간이 짧은 네트워크에서 스토리지 시스템에 액세스하는 클라이언트는 이러한 매개 변수를 수정해도 거의 이점을 얻을 수 없습니다. 처리량 향상이 지연 시간에 미치는 영향을 상쇄하지 않는다면 이러한 매개 변수를 사용해서는 안 됩니다.

스토리지 환경에서 이러한 매개 변수를 수정하여 이점을 얻을 수 있는지 확인하려면 먼저 성능이 떨어지는 NFS 클라이언트에 대한 포괄적인 성능 평가를 수행해야 합니다. 낮은 성능이 클라이언트에 대한 과도한 라운드 트립 지연 및 작은 요청 때문인지 검토합니다. 이러한 조건에서는 클라이언트와 서버가 사용 가능한 대역폭을 완전히 사용할 수 없습니다. 왜냐하면 대부분의 듀티 사이클이 연결을 통해 전송되는 작은 요청과 응답을 대기하는 데 소비하기 때문입니다.

NFSv3 및 NFSv4 요청 크기를 늘리면 클라이언트 및 서버에서 사용 가능한 대역폭을 보다 효율적으로 사용하여 단위 시간당 더 많은 데이터를 이동할 수 있으므로 연결의 전반적인 효율성이 향상됩니다.

스토리지 시스템과 클라이언트 간의 구성은 달라질 수 있습니다. 스토리지 시스템과 클라이언트는 전송 작업에 대해 최대 1MB의 크기를 지원합니다. 그러나 스토리지 시스템이 1MB의 최대 전송 크기를 지원하도록 구성했지만 클라이언트가 64KB만 지원하는 경우 마운트 전송 크기는 64KB 이하로 제한됩니다.

이러한 매개변수를 수정하기 전에 대용량 응답을 조립하고 전송하는 데 필요한 기간 동안 스토리지 시스템에 메모리가 추가로 소비된다는 점을 염두에 두어야 합니다. 스토리지 시스템에 대한 대기 시간이 많을수록 추가 메모리 소비량이 증가합니다. 메모리 용량이 큰 스토리지 시스템은 이 변경으로 인해 거의 영향을 주지 않을 수 있습니다. 메모리 용량이

낮은 스토리지 시스템에서 눈에 띄는 성능 저하가 발생할 수 있습니다.

이 매개 변수를 사용하는 것은 클러스터의 여러 노드에서 데이터를 검색하는 기능에 달려 있습니다. 클러스터 네트워크의 지연으로 인해 전반적인 응답 시간이 길어질 수 있습니다. 이러한 매개 변수를 사용하면 전반적인 지연 시간이 증가하는 경향이 있습니다. 따라서 지연 시간에 민감한 워크로드에 부정적인 영향이 나타날 수 있습니다.

NFSv3 및 NFSv4 TCP 최대 전송 크기를 수정합니다

NFSv3 및 NFSv4.x 프로토콜을 사용하여 모든 TCP 연결에 대해 최대 전송 크기를 구성하려면 '-tcp-max-xfer-size' 옵션을 수정할 수 있습니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)별로 이러한 옵션을 개별적으로 수정할 수 있습니다.

ONTAP 9부터 v3-tcp-max-read-size와 v3-tcp-max-write-size 옵션은 더 이상 사용되지 않습니다. 대신 '-tcp-max-xfer-size' 옵션을 사용해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
NFSv3 또는 NFSv4 TCP 최대 전송 크기를 수정합니다	'vserver nfs modify -vserver vserver_name -tcp -max -xfer-size integer_max_xfer_size'

옵션을 선택합니다	범위	기본값
'-tcp-max-xfer-size'를 선택합니다	8192 ~ 1048576바이트	65536바이트

> 입력하는 최대 전송 크기는 4KB(4096바이트)의 배수여야 합니다. 제대로 정렬되지 않은 요청은 성능에 부정적인 영향을 줍니다.

3. 'vserver nfs show-fields tcp-max-xfer-size' 명령을 사용하여 변경 사항을 확인합니다.
4. 클라이언트가 정적 마운트를 사용하는 경우 새 매개 변수 크기를 마운트 해제하고 다시 마운트하여 적용합니다.

예

다음 명령을 실행하면 이름이 VS1인 SVM에서 NFSv3 및 NFSv4.x TCP 최대 전송 크기가 1048576바이트로 설정됩니다.

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

NFS 사용자에게 허용되는 그룹 ID 수를 구성합니다

기본적으로 ONTAP는 Kerberos(RPCSEC_GSS) 인증을 사용하여 NFS 사용자 자격 증명을 처리할 때 최대 32개의 그룹 ID를 지원합니다. AUTH_SYS 인증을 사용하는 경우 RFC 5531에 정의된 대로 기본 최대 그룹 ID 수는 16입니다. 기본 그룹 수보다 많은 그룹의 구성원인 사용자가 있는 경우 최대 1,024개까지 늘릴 수 있습니다.

이 작업에 대해

사용자의 자격 증명에 기본 그룹 ID 수보다 많은 수의 그룹 ID가 있는 경우 나머지 그룹 ID가 잘리고 스토리지 시스템에서 파일을 액세스하려고 할 때 오류가 발생할 수 있습니다. SVM당 최대 그룹 수를 환경의 최대 그룹을 나타내는 숫자로 설정해야 합니다.

다음 표는 세 가지 샘플 구성에서 최대 그룹 ID 수를 결정하는 "vserver NFS modify" 명령의 두 가지 매개 변수를 보여줍니다.

매개 변수	설정	결과 그룹 ID 제한
'-확장-그룹-제한' ``auth-sys-extended-groups''	32인치 '비활성화'입니다 기본 설정입니다.	RPCSEC_GSS:32 AUTH_SYS:16
'-확장-그룹-제한' ``auth-sys-extended-groups''	256입니다 '비활성화'입니다	RPCSEC_GSS:256 AUTH_SYS:16
'-확장-그룹-제한' ``auth-sys-extended-groups''	512 "활성화됨"	RPCSEC_GSS:512 AUTH_SYS:512

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

허용된 보조 그룹의 최대 수를 설정하려면…	명령 입력…
RPCSEC_GSS에만 해당하고 AUTH_SYS는 기본값 16으로 설정된 상태로 둡니다	'vserver nfs modify -vserver vserver_name -extended-groups-limit{32-1024} -auth-sys-extended -groups disabled'
RPCSEC_GSS 및 AUTH_SYS의 경우	'vserver nfs modify -vserver vserver_name -extended-groups-limit{32-1024} -auth-sys-extended -groups enabled'

3. '-extended-groups-limit' 값을 확인하고 AUTH_SYS가 확장된 그룹('vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups, extended-groups-limit')을 사용하고 있는지 확인합니다
4. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 예에서는 AUTH_SYS 인증에 대해 확장된 그룹을 활성화하고, AUTH_SYS 및 RPCSEC_GSS 인증에 대해 확장 그룹의 최대 수를 512로 설정합니다. 이러한 변경은 VS1 이라는 SVM에 액세스하는 클라이언트에만 적용됩니다.

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ----------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

NTFS 보안 스타일 데이터에 대한 루트 사용자 액세스를 제어합니다

NFS 클라이언트가 NTFS 보안 스타일 데이터에 액세스하고 NTFS 클라이언트가 NFS 보안 스타일 데이터에 액세스할 수 있도록 ONTAP를 구성할 수 있습니다. NFS 데이터 저장소에서 NTFS 보안 스타일을 사용하는 경우 루트 사용자가 액세스를 처리하는 방법을 결정하고 이에 따라 SVM(스토리지 가상 머신)을 구성해야 합니다.

이 작업에 대해

루트 사용자가 NTFS 보안 스타일 데이터에 액세스할 때 다음 두 가지 옵션이 있습니다.

- 다른 NFS 사용자와 마찬가지로 루트 사용자를 Windows 사용자에게 매핑하고 NTFS ACL에 따라 액세스를 관리합니다.
- NTFS ACL을 무시하고 루트에 대한 전체 액세스를 제공합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

루트 사용자가 다음을 수행할 수 있도록 하려면…	명령 입력…
Windows 사용자에게 매핑되어야 합니다	'vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled'
NT ACL 검사를 생략합니다	'vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled'

기본적으로 이 매개 변수는 사용되지 않습니다.

이 매개 변수가 설정되어 있지만 루트 사용자에 대한 이름 매핑이 없는 경우 ONTAP에서는 감사를 위해 기본 SMB 관리자 자격 증명을 사용합니다.

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

지원되는 **NFS** 버전 및 클라이언트

지원되는 **NFS** 버전 및 클라이언트의 개요

네트워크에서 NFS를 사용하려면 먼저 ONTAP가 지원하는 NFS 버전과 클라이언트를 알아야 합니다.

이 표에서는 ONTAP에서 주 및 부 NFS 프로토콜 버전이 기본적으로 지원되는 경우 설명합니다. 기본적으로 지원에서는 이 버전이 NFS 프로토콜을 지원하는 ONTAP의 최초 버전임을 표시하지 않습니다.

버전	기본적으로 사용됩니다
NFSv3	예
NFSv4.0	예, ONTAP 9.9.1부터 시작합니다
NFSv4.1	예, ONTAP 9.9.1부터 시작합니다
NFSv4.2	예, ONTAP 9.9.1부터 시작합니다
pNFS를 사용합니다	아니요

ONTAP가 지원하는 NFS 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

ONTAP에서 지원하는 NFSv4.0 기능

ONTAP는 SPKM3 및 LIPKEY 보안 메커니즘을 제외한 NFSv4.0의 모든 필수 기능을 지원합니다.

지원되는 NFSv4 기능은 다음과 같습니다.

- * 복합 *

  클라이언트가 단일 RPC(원격 프로시저 호출) 요청에서 여러 파일 작업을 요청할 수 있습니다.

- * 파일 위임 *

  서버가 읽기 및 쓰기 액세스를 위해 일부 유형의 클라이언트에 파일 제어를 위임할 수 있도록 합니다.

- * 의사 fs *

  NFSv4 서버에서 스토리지 시스템의 마운트 지점을 결정하는 데 사용됩니다. NFSv4에는 마운트 프로토콜이 없습니다.

- * 잠금 *

  임대 기반. NFSv4에는 별도의 NLM(Network Lock Manager) 또는 NSM(Network Status Monitor) 프로토콜이 없습니다.

NFSv4.0 프로토콜에 대한 자세한 내용은 RFC 3530을 참조하십시오.

NFSv4에 대한 ONTAP 지원의 제한사항

NFSv4에 대한 ONTAP 지원의 몇 가지 제한 사항에 대해 알고 있어야 합니다.

- 위임 기능은 모든 클라이언트 유형에서 지원되지 않습니다.
- ONTAP 9.4 및 이전 릴리즈에서는 UTF8 볼륨 이외의 볼륨에 ASCII가 아닌 문자가 있는 이름이 스토리지 시스템에서 거부됩니다.

  ONTAP 9.5 이상 릴리즈에서는 utf8mb4 언어 설정으로 생성하고 NFS v4를 사용하여 마운트된 볼륨이 더 이상 이 제한을 받지 않습니다.

- 모든 파일 핸들은 영구적이며, 서버는 휘발성 파일 핸들을 제공하지 않습니다.
- 마이그레이션 및 복제는 지원되지 않습니다.
- NFSv4 클라이언트는 읽기 전용 로드 공유 미러에서 지원되지 않습니다.

  ONTAP는 직접 읽기 및 쓰기 액세스를 위해 NFSv4 클라이언트를 로드 공유 미러 소스로 라우팅합니다.

- 명명된 특성은 지원되지 않습니다.
- 다음을 제외한 모든 권장 속성이 지원됩니다.
  - '보관'
  - '숨겨짐'

- 동질성
- 'mimetype'입니다
- 쿼터쿼터_AVAIL_HARD를 선택합니다
- 쿼터가용성 소프트
- quota_used
- '시스템'
- Time_backup을 선택합니다

> "quota *" 특성은 지원하지 않지만 ONTAP는 RQUOTA Side Band 프로토콜을 통해 사용자 및 그룹 할당량을 지원합니다.

NFSv4.1을 위한 ONTAP 지원

ONTAP 9.8부터는 NFSv4.1이 활성화된 경우 기본적으로 nconnect 기능을 사용할 수 있습니다.

이전 버전의 NFS 클라이언트 구축에서는 마운트와 단일 TCP 연결만 사용합니다. ONTAP에서 단일 TCP 연결은 IOPS 증가에 따라 병목 현상을 일으킬 수 있습니다. 그러나 nconnect 지원 클라이언트는 단일 NFS 마운트와 연결된 여러 개의 TCP 연결(최대 16개)을 가질 수 있습니다. 이러한 NFS 클라이언트는 라운드 로빈 방식으로 여러 TCP 연결에서 파일 작업을 멀티플렉싱하므로 사용 가능한 네트워크 대역폭에서 더 높은 처리량을 얻을 수 있습니다. nConnect는 NFSv3 및 NFSv4.1 마운트에 대해서만 권장됩니다.

nconnect가 클라이언트 버전에서 지원되는지 확인하려면 NFS 클라이언트 설명서를 참조하십시오.

NFSv4.1은 ONTAP 9.9.1 이상에서 기본적으로 활성화되어 있습니다. 이전 릴리즈에서는 SVM(스토리지 가상 머신)에서 NFS 서버를 생성할 때 '-v4.1' 옵션을 지정하고 이를 '사용'으로 설정하여 사용할 수 있습니다.

ONTAP는 NFSv4.1 디렉토리 및 파일 레벨 위임을 지원하지 않습니다.

NFSv4.2에 대한 ONTAP 지원

ONTAP 9.8부터 ONTAP는 NFSv4.2 사용 클라이언트에 대한 액세스를 허용하는 NFSv4.2 프로토콜을 지원합니다.

NFSv4.2는 ONTAP 9.9.1 이상에서 기본적으로 설정됩니다. ONTAP 9.8에서 을 지정하여 v4.2를 수동으로 활성화해야 합니다 `-v4.1` 옵션을 선택하고 로 설정합니다 `enabled` SVM(스토리지 가상 머신)에 NFS 서버를 생성할 때 또한 NFSv4.1을 활성화하면 클라이언트가 v4.2로 마운트된 상태에서 NFSv4.1 기능을 사용할 수 있습니다.

연속적인 ONTAP 릴리즈는 NFSv4.2 옵션 기능에 대한 지원을 확장합니다.

다음으로 시작...	NFSv4.2의 옵션 기능은 다음과 같습니다.
ONTAP 9.12.1	• NFS 확장 속성입니다 • Sparse 파일 • 공간 예약

다음으로 시작...	**NFSv4.2**의 옵션 기능은 다음과 같습니다.
ONTAP 9.9.1	MAC(Mandatory Access Control) 레이블 NFS

NFS v4.2 보안 레이블

ONTAP 9.9.1부터 NFS 보안 레이블을 활성화할 수 있습니다. 기본적으로 비활성화되어 있습니다.

NFS v4.2 보안 레이블에서 ONTAP NFS 서버는 MAC(Mandatory Access Control)를 인식하여 클라이언트가 전송한 sec_label 특성을 저장 및 검색합니다.

자세한 내용은 을 참조하십시오 "RFC 7240".

ONTAP 9.12.1부터는 NDMP 덤프 작업에 NFS v4.2 보안 레이블이 지원됩니다. 이전 릴리즈의 파일 또는 디렉터리에서 보안 레이블이 발견되면 덤프가 실패합니다.

단계

1. 권한 설정을 고급으로 변경합니다.

```
set -privilege advanced
```

2. 보안 레이블 활성화:

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

NFS 확장 속성입니다

ONTAP 9.12.1부터 NFS 확장 특성(xattrs)이 기본적으로 사용하도록 설정됩니다.

확장 특성은 에 의해 정의된 표준 NFS 속성입니다 "RFC 8276" 최신 NFS 클라이언트에서 사용하도록 설정됩니다. 사용자 정의 메타데이터를 파일 시스템 객체에 연결하는 데 사용할 수 있으며 고급 보안 구축에 관심이 있습니다.

NFS 확장 속성은 현재 NDMP 덤프 작업에 지원되지 않습니다. 파일 또는 디렉토리에서 확장 속성이 발견되면 덤프는 진행되지만 해당 파일 또는 디렉토리의 확장 속성은 백업하지 않습니다.

확장 속성을 비활성화해야 하는 경우 를 사용하십시오 `vserver nfs modify -v4.2-xattrs disabled` 명령.

ONTAP은 병렬 NFS를 지원합니다

ONTAP는 pNFS(parallel NFS)를 지원합니다. pNFS 프로토콜은 클라이언트가 클러스터의 여러 노드에 분산된 파일 세트에 직접 액세스할 수 있도록 함으로써 성능을 개선합니다. 클라이언트가 볼륨에 대한 최적의 경로를 찾는 데 도움이 됩니다.

하드 마운트 사용

장착 문제를 해결할 때 올바른 장착 유형을 사용하고 있는지 확인해야 합니다. NFS는 소프트

마운트와 하드 마운트의 두 가지 마운트 유형을 지원합니다. 안정성을 위해 하드 마운트만 사용해야 합니다.

소프트 마운트를 사용하면 안 됩니다. 특히, NFS 시간 제한이 자주 발생할 가능성이 있습니다. 이러한 시간 초과로 인해 경합 상태가 발생하여 데이터가 손상될 수 있습니다.

NFS 및 SMB 파일 및 디렉토리 명명 종속성

NFS 및 SMB 파일 및 디렉토리 이름 지정 종속성 개요

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

문자 파일 또는 디렉터리 이름에 사용할 수 있습니다

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대/소문자를 구분하십시오

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testdir 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
  - SMB 클라이언트에서는 testdir과 testDI~1이 표시됩니다.
  - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDI~1' 디렉토리 이름을 생성한다.

이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 text.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
  - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
  - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.

> Vserver CIFS 문자 매핑 명령을 사용하여 문자 매핑을 생성한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조회가 발생할 수 있습니다. 즉, 파일 이름 조회는 문자 매핑이 작성되었고 파일 이름이 해당 문자 매핑을 사용하는 경우에만 대/소문자를 구분합니다.

ONTAP에서 파일 및 디렉터리 이름을 만드는 방법

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉토리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉토리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3 형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉토리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

  비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications_new.html'이라는 다른 파일을 만들 경우 'specifications_new.html'의 8.3 형식은 'specif~2.htm'입니다.

ONTAP에서 멀티바이트 파일, 디렉토리 및 qtree 이름을 처리하는 방식

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 _utf8mb4_language 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

- 다음 방법 중 하나로 새 볼륨을 만들어야 합니다.
- 볼륨 '-language' 옵션을 명시적으로 설정하기:

  '볼륨 생성 - 언어 utf8mb4{…}'

- 옵션으로 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션 상속:

  ``vserver[create|modify] -language utf8mb4{…}''volume create{…}'

- ONTAP 9.6 이하 버전을 사용하는 경우 utf8mb4 지원을 위해 기존 볼륨을 수정할 수 없으며 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

  ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 을 참조하십시오 "ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?".

를 누릅니다
utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

를 누릅니다

> 4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

  ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

  이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

유니코드 문자는 qtree 이름에 사용할 수 있습니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.
- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.

> ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

볼륨에서 **SMB** 파일 이름 변환에 대한 문자 매핑을 구성합니다

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 "":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

  각 접합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르지 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

  예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 ""a-b""라는 파일에 액세스하려는 Windows 클라이언트의 요청이 ""a:b""(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대/소문자를 구분하지 않습니다.
- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

단계

1. 문자 매핑 구성:

   'vserver cifs character-mapping create-vserver vserver_name-volume volume_name-mapping mapping_text,...'

매핑은 "":"로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C.

콜론으로 구분된 각 mapping_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

- 소스 매핑

  다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

유니코드 문자입니다	인쇄된 문자	설명
0x01-0x19	해당 없음	인쇄할 수 없는 제어 문자입니다
0x5C	\	백슬래시
0x3A	:	결장
0x2A	*	별표
0x3F	?	물음표
0x22	"	인용 부호가 있습니다
0x3C	를 누릅니다	보다 작음
0x3E	를 누릅니다	보다 큼
0x7C		
세로선	0xB1	±

- 타겟 매핑

  U+E0000…U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.

예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMB 파일 이름 변환에 대한 문자 매핑을 관리하는 명령입니다

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

원하는 작업	이 명령 사용…
새 파일 문자 매핑을 만듭니다	'vserver cifs character-mapping create'
파일 문자 매핑에 대한 정보를 표시합니다	'vserver cifs character-mapping show'
기존 파일 문자 매핑을 수정합니다	'vserver cifs character-mapping modify'를 참조하십시오
파일 문자 매핑을 삭제합니다	'vserver cifs character-mapping delete

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.