NAS 파일 액세스 이해

ONTAP 9

NetApp
February 12, 2026

목차

NAS 파일 액세스 이해

네임스페이스 및 교차점

ONTAP NAS 네임스페이스 및 연결 지점에 대해 알아보세요

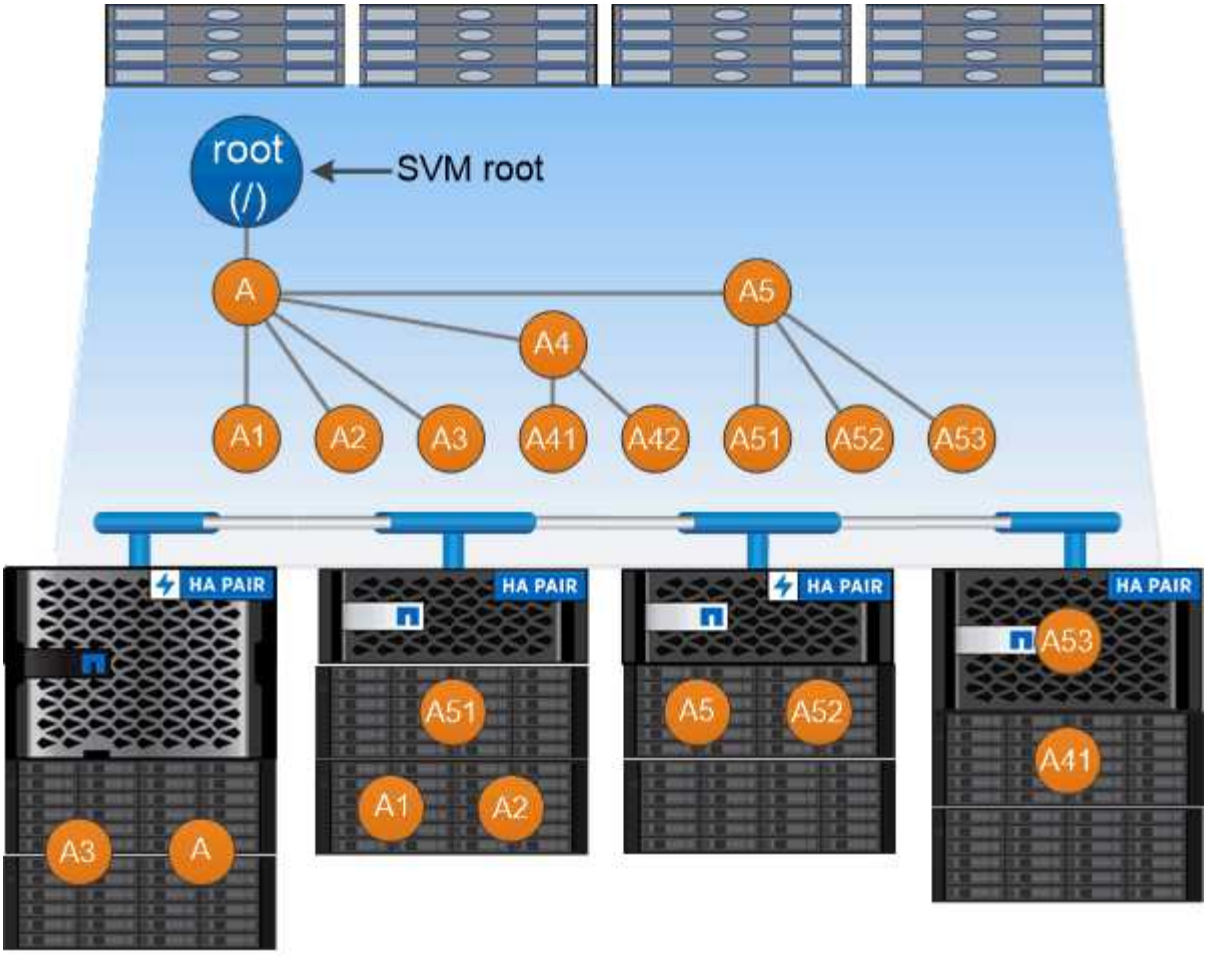
nas_namespace_는 단일 파일 시스템 계층을 생성하기 위해 _junction points_에 함께 결합된 볼륨의 논리적 그룹입니다. 권한이 충분한 클라이언트는 저장소에 있는 파일의 위치를 지정하지 않고 네임스페이스의 파일에 액세스할 수 있습니다. Junced 볼륨은 클러스터의 모든 위치에 상주할 수 있습니다.

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
```

ONTAP NAS 네임스페이스 아키텍처에 대해 알아보세요

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.

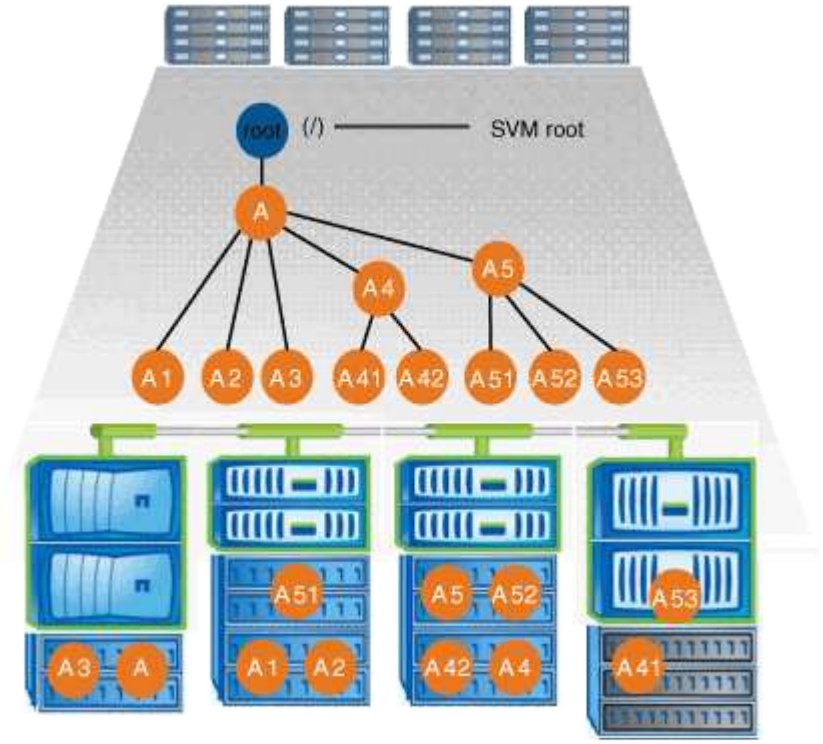
네임스페이스 맨 위에는 항상 루트 볼륨이 있으며, 이 볼륨은 슬래시(/)로 표시됩니다. 루트 아래의 네임스페이스 아키텍처는 세 가지 기본 범주로 분류됩니다.

- 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.

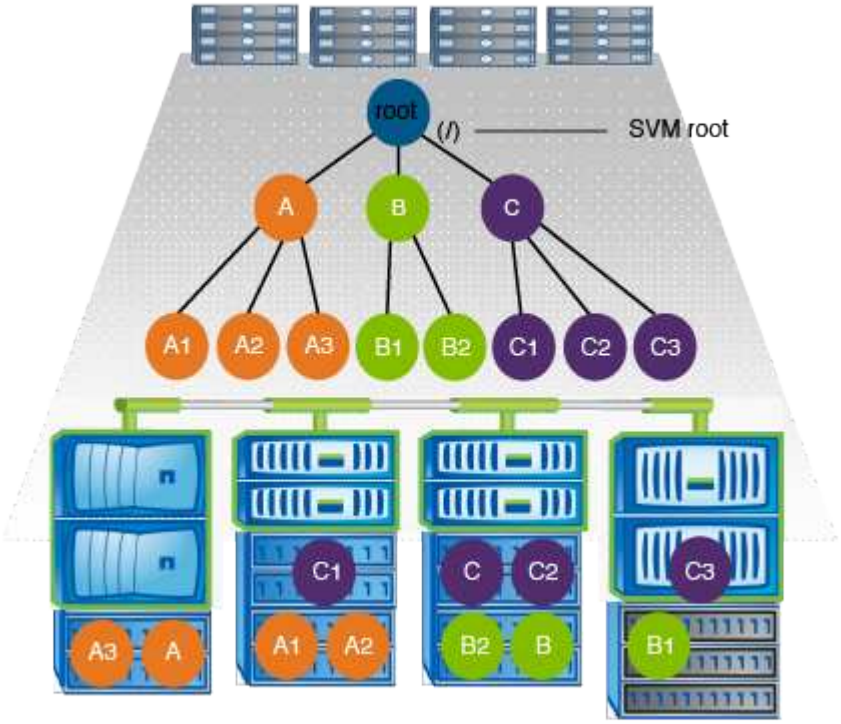


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 연결 구성은 "데이터"라는 디렉토리인 단일 삽입 지점 아래에 모든 볼륨이 접합되는 다음과 같은 구성으로 보일 수 있습니다.

```
                    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.



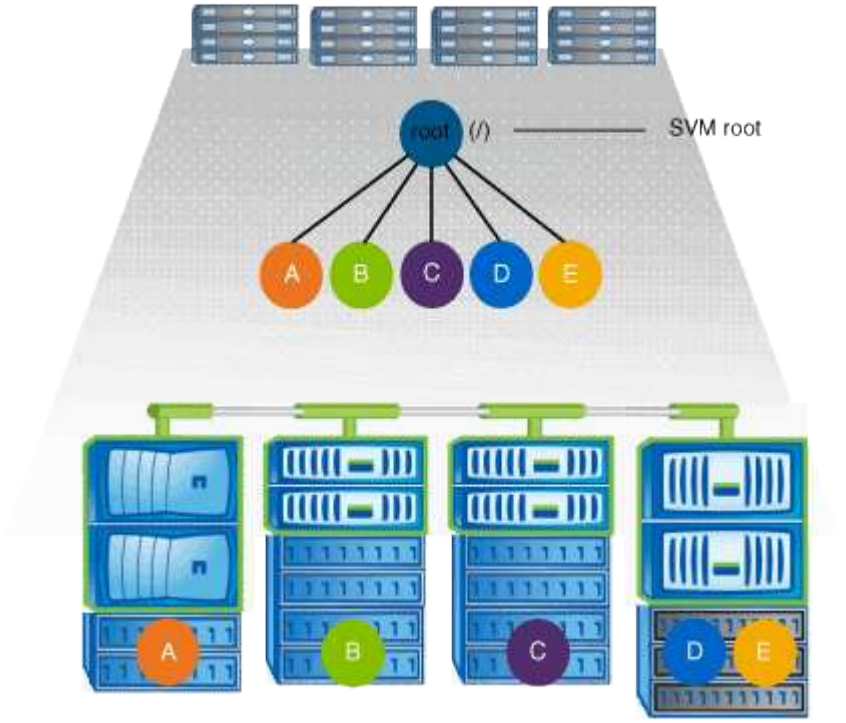
예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 SVM의 루트 볼륨에 세 개의 삽입 지점이 있는 다음과 같은 구성을 예로 들 수 있습니다. 두 개의 삽입 지점은 "다타"와 "프로젝트"라는 디렉토리입니다. 한 삽입 지점은 "audit"이라는 이름의 접합부입니다.

```
                    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       Junction    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

ONTAP NAS 파일 액세스 제어에 대해 알아보세요

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.

ONTAP NAS SVM에 대한 인증 기반 제한 사항에 대해 알아보세요**.**

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.

ONTAP NAS SVM에 대한 파일 기반 제한 사항에 대해 알아보세요**.**

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

NAS 클라이언트에 대한 ONTAP 인증에 대해 알아보세요

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.

ONTAP이 이름 서비스를 사용하는 방법을 알아보세요

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".

NFS 클라이언트에서 ONTAP SMB 파일 액세스 권한 부여

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.

ONTAP NFS 자격 증명 캐시 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.