NFS를 사용하여 파일 액세스를 설정합니다

ONTAP 9

NetApp
February 14, 2026

목차

NFS를 사용하여 파일 액세스를 설정합니다

ONTAP SVM에서 NFS 파일 액세스 설정에 대해 알아보세요

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

내보내기 정책이 ONTAP NFS 볼륨 또는 Qtree에 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.

ONTAP NFS SVM에 대한 기본 내보내기 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.

ONTAP NFS 내보내기 규칙 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.

나열되지 않은 보안 유형을 사용하는 **NFS** 클라이언트에 대한 **ONTAP SVM** 액세스 관리

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.
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

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. `-rwrule any` 매개변수:

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.

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. `-rwrule none` 매개변수:

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.

ONTAP 보안 유형이 NFS 클라이언트 액세스 수준을 결정하는 방식

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.

ONTAP NFS 슈퍼유저 액세스 요청 관리에 대해 알아보세요

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.
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.

ONTAP NFS 내보내기 정책 캐시에 대해 알아보세요

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

캐시 이름입니다	저장된 정보의 유형입니다
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.

ONTAP NFS 액세스 캐시에 대해 알아보세요

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.

ONTAP NFS 액세스 캐시 매개변수에 대해 알아보세요

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.

ONTAP NFS qtree에서 내보내기 정책 제거

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 대한 ONTAP NFS qtree ID 검증

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

ONTAP NFS FlexVol 볼륨에 대한 정책 제한 및 중첩된 연결 내보내기

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 NFS와 Kerberos 사용

Kerberos에 대한 ONTAP NFS 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.

ONTAP NFS를 사용하여 Kerberos를 구성하기 위한 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 클라이언트 요구 사항

- 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.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다	설명
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"

NFSv4에 대한 **ONTAP** 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 NFS 이름 서비스 스위치 구성에 대해 자세히 알아보십시오

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
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

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
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

ONTAP NFS SVM용 LDAP에 대해 알아보세요

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 이상에서는 LDAP 서버에서 TLS 또는 SSL을 활성화해야 합니다. ONTAP 9.4~9.0에서는 SSL이 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 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다."
- 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".

ONTAP NFS SVM에 대한 **LDAP** 서명 및 봉인에 대해 알아보세요**.**

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.

ONTAP NFS SVM용 **LDAPS**에 대해 알아보세요

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 9.8-9.5에서는 LDAPS를 포트 636에서만 활성화할 수 있습니다. 그렇게 하려면 다음을 사용하세요. `-use-ldaps-for-ad-ldap` 매개변수를 사용하여 `vserver cifs security modify` 명령.
  - ONTAP 9.9.1부터 포트 636이 기본값으로 유지되지만 LDAPS는 모든 포트에서 활성화할 수 있습니다. 이렇게 하려면 `-ldaps-enabled` 매개 변수를 로 `true` 설정하고 원하는 `-port` 매개 변수를 지정합니다. 에 대한 자세한 내용은 `vserver services name-service ldap client create` "ONTAP 명령 참조입니다"을 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.

ONTAP NFS SVM에 대한 **LDAP RFC2307bis** 지원 활성화

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

시작하기 전에

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 검색을 위한 **ONTAP NFS** 구성 옵션

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 매개 변수가 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'	모든 LDAP 검색에 대한 기본 DN입니다. 필요한 경우 여러 값을 입력할 수 있습니다(예: ONTAP 9.5 이상 릴리스에서 LDAP 참조 추적이 활성화된 경우).
``기본범위''	모든 LDAP 검색에 대한 기본 범위입니다.
'-user-dn'	모든 LDAP 사용자 검색에 대한 기본 DN입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
'- 사용자 범위'	모든 LDAP 사용자 검색의 기본 범위입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
``그룹-dn''	모든 LDAP 그룹 검색에 대한 기본 DN입니다.
그룹-범위	모든 LDAP 그룹 검색에 대한 기본 범위입니다.
'-넷그룹-dn'	모든 LDAP 넷그룹 검색에 대한 기본 DN입니다.
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.

사용자 지정 **LDAP** 검색 필터

LDAP 구성 옵션 매개 변수를 사용하여 사용자 지정 검색 필터를 생성할 수 있습니다. `-group-membership-filter`매개 변수는 LDAP 서버에서 그룹 구성원 자격을 조회할 때 사용할 검색 필터를 지정합니다.

유효한 필터의 예는 다음과 같습니다.

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

에 대해 자세히 "ONTAP에서 LDAP를 구성하는 방법"알아보십시오.

ONTAP NFS SVM에 대한 **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.

시작하기 전에

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.

> 그만큼 `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-ldap-servers` LDAP 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

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"

ONTAP NFS SVM에 대한 **nsswitch** 인증을 위해 **LDAP** 빠른 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."

시작하기 전에

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.
- 빠른 바인딩이 성공하려면 관리자의 UID 번호와 GID 번호가 입력되어 있고 조회 가능해야 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'

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   ◦ 새 관리자는 를 참조하십시오"LDAP 또는 NIS ONTAP 계정 액세스를 설정합니다".

ONTAP NFS SVM에 대한 **LDAP** 통계 표시

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

시작하기 전에

- 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 예제에서는 카운터에 대해 * smpl_1 * 이라는 샘플의 통계를 표시합니다. avg_processor_busy 및 cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

관련 정보

- "통계에 따르면"
- "통계 시작"
- "통계 중지"

이름 매핑을 구성합니다

ONTAP NAS SVM에 대한 이름 매핑 구성에 대해 알아보세요**.**

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.

ONTAP NAS SVM에 대한 이름 매핑에 대해 알아보세요

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.

ONTAP NAS SVM에서 UNIX-Windows 사용자 이름 매핑을 위한 다중 도메인 검색

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.
*	* {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.

ONTAP NAS SVM에 대한 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.

ONTAP NAS SVM에 대한 이름 매핑 만들기

'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 이 문을 사용하여 null 대체 문자열(공백 문자)을 사용하여 사용자에 대한 매핑을 명시적으로 거부할 `" "` 수도 `-replacement` 있습니다. 에 대한 자세한 내용은 `vserver name-mapping create` link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["ONTAP 명령 참조입니다"^]을 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
```

ONTAP NAS SVM의 기본 사용자 구성

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

NFS 이름 매핑을 관리하기 위한 ONTAP 명령

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`
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`

에 대한 자세한 내용은 `vserver name-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SVM에 대한 Windows NFS 클라이언트의 액세스 활성화

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:\"

ONTAP SVM에 대한 NFS 클라이언트에서 내보내기 표시 활성화

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 사용하면 기본적으로 NFS 클라이언트가 내보내기 목록을 볼 수 있습니다. 이전 릴리즈에서는 `showmount` 명령의 옵션을 `vserver nfs modify` 명시적으로 설정해야 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/unix1   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```