내보내기 정책을 사용하여 SMB 액세스를 보호합니다

ONTAP 9

NetApp
April 24, 2024

목차

내보내기 정책을 사용하여 SMB 액세스를 보호합니다

SMB 액세스에 엑스포트 정책을 사용하는 방법

SMB 서버에서 SMB 액세스에 대한 엑스포트 정책을 사용하는 경우, SMB 클라이언트에서 SVM 볼륨에 대한 액세스를 제어할 때 엑스포트 정책이 사용됩니다. 데이터에 액세스하려면 SMB 액세스를 허용하는 엑스포트 정책을 생성한 다음, SMB 공유를 포함하는 볼륨과 정책을 연결할 수 있습니다.

내보내기 정책에는 데이터에 대한 액세스가 허용되는 클라이언트와 읽기 전용 및 읽기-쓰기 액세스에 지원되는 인증 프로토콜을 지정하는 하나 이상의 규칙이 적용됩니다. 모든 클라이언트, 클라이언트 서브넷 또는 특정 클라이언트에 대한 SMB 액세스를 허용하고 Kerberos 인증, NTLM 인증 또는 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 결정할 때 Kerberos 및 NTLM 인증을 사용하여 인증을 허용하도록 내보내기 정책을 구성할 수 있습니다.

내보내기 정책에 적용된 모든 내보내기 규칙을 처리한 후 ONTAP는 클라이언트에 액세스 권한이 부여되었는지 여부와 허용되는 액세스 수준을 결정할 수 있습니다. 내보내기 규칙은 Windows 사용자 및 그룹이 아니라 클라이언트 컴퓨터에 적용됩니다. 내보내기 규칙은 Windows 사용자 및 그룹 기반 인증 및 권한 부여를 대체하지 않습니다. 내보내기 규칙은 공유 및 파일 액세스 권한 외에도 액세스 보안의 또 다른 계층을 제공합니다.

볼륨에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨에 정확히 하나의 엑스포트 정책을 연결합니다. 각 SVM에는 여러 엑스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨이 있는 SVM에 대해 다음을 수행할 수 있습니다.

- SVM의 각 볼륨에 서로 다른 엑스포트 정책을 지정하여 개별 클라이언트 액세스 제어를 SVM의 각 볼륨에 할당
- 각 볼륨에 대해 새로운 엑스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨에 동일한 엑스포트 정책을 할당합니다.

각 SVM에는 규칙이 없는 "기본값"이라는 엑스포트 정책이 하나 이상 있습니다. 이 엑스포트 정책을 삭제할 수는 없지만 이름을 바꾸거나 수정할 수는 있습니다. 기본적으로 SVM의 각 볼륨은 기본 엑스포트 정책과 연결됩니다. SVM에서 SMB 액세스에 대한 엑스포트 정책을 사용하지 않도록 설정한 경우, "기본값" 엑스포트 정책은 SMB 액세스에 영향을 미치지 않습니다.

NFS 및 SMB 호스트 모두에 대한 액세스를 제공하는 규칙을 구성하고 이 규칙을 엑스포트 정책에 연결할 수 있습니다. 그런 다음, NFS 및 SMB 호스트 모두에 액세스해야 하는 데이터가 포함된 볼륨에 연결할 수 있습니다. 또는 SMB 클라이언트만 액세스해야 하는 일부 볼륨이 있는 경우, SMB 프로토콜을 사용해서만 액세스를 허용하고 읽기 전용 및 쓰기 액세스에 Kerberos 또는 NTLM(또는 둘 다)만 사용하는 규칙을 사용하여 엑스포트 정책을 구성할 수 있습니다. 그러면 엑스포트 정책이 SMB 액세스만 원하는 볼륨에 연결됩니다.

SMB에 대한 엑스포트 정책이 설정되어 있고 클라이언트가 해당 엑스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우, 요청이 실패하고 권한 거부 메시지가 표시됩니다. 클라이언트가 볼륨의 엑스포트 정책에 있는 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다. 공유 및 파일 권한이 액세스를 허용하는 경우에도 마찬가지입니다. 즉, SMB 공유가 포함된 볼륨에서 다음을 최소한으로 허용하도록 엑스포트 정책을 구성해야 합니다.

- 모든 클라이언트 또는 적절한 클라이언트 하위 집합에 대한 액세스를 허용합니다
- SMB를 통한 액세스를 허용합니다
- Kerberos 또는 NTLM 인증(또는 둘 다)을 사용하여 적절한 읽기 전용 및 쓰기 액세스 허용

에 대해 자세히 알아보십시오 "엑스포트 정책 구성 및 관리".

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.

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.

SMB를 통한 액세스를 제한하거나 허용하는 엑스포트 정책 규칙의 예

이 예에서는 SMB 액세스에 대한 엑스포트 정책이 설정된 SVM에서 SMB를 통한 액세스를 제한 또는 허용하는 엑스포트 정책 규칙을 생성하는 방법을 보여줍니다.

SMB 액세스에 대한 엑스포트 정책은 기본적으로 비활성화되어 있습니다. SMB 액세스에 대한 엑스포트 정책을 설정한 경우에만 SMB 액세스를 제한하거나 허용하는 엑스포트 정책 규칙을 구성해야 합니다.

SMB 액세스에 대한 엑스포트 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: cifs1
- 색인 번호: 1
- 클라이언트 일치: 192.168.1.0/24 네트워크의 클라이언트만 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM 또는 Kerberos 인증을 사용하는 클라이언트에 대한 액세스
- 읽기-쓰기 액세스: Kerberos 인증을 사용하는 클라이언트에 대한 액세스

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB 및 NFS 액세스에 대한 엑스포트 규칙

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: cifsnfs1
- 색인 번호: 2
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 및 NFS 액세스
- 읽기 전용 액세스: 모든 클라이언트에 대해
- 읽기-쓰기 액세스: Kerberos(NFS 및 SMB) 또는 NTLM 인증(SMB)을 사용하는 클라이언트에 대한 액세스
- UNIX 사용자 ID 0(영)에 대한 매핑: 사용자 ID 65534에 매핑됨(일반적으로 사용자 이름에 매핑되지 않음)
- SUID 및 SGID 액세스: 허용

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM을 사용한 SMB 액세스에 대한 내보내기 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: ntlm1
- 색인 번호: 1
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다
- 읽기-쓰기 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다

> NTLM 전용 액세스에 대해 읽기 전용 옵션 또는 읽기/쓰기 옵션을 구성하는 경우 클라이언트 일치 옵션에서 IP 주소 기반 항목을 사용해야 합니다. 그렇지 않으면 "액세스 거부" 오류가 발생합니다. 이는 ONTAP가 호스트 이름을 사용하여 클라이언트의 액세스 권한을 확인할 때 Kerberos SPN(서비스 사용자 이름)을 사용하기 때문입니다. NTLM 인증은 SPN 이름을 지원하지 않습니다.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제합니다

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수

있습니다. 내보내기 정책을 사용하여 리소스에 대한 SMB 액세스를 제어하는 것은 선택 사항입니다.

시작하기 전에

다음은 SMB에 대한 엑스포트 정책을 설정하기 위한 요구 사항입니다.

- 클라이언트에 대한 내보내기 규칙을 만들기 전에 클라이언트가 DNS에 ""PTR"" 레코드를 가지고 있어야 합니다.
- SVM이 NFS 클라이언트에 대한 액세스를 제공하고 NFS 액세스에 사용할 호스트 이름이 CIFS 서버 이름과 다른 경우 호스트 이름에 대한 ""a" 및 ""PTR"" 레코드 세트가 추가로 필요합니다.

이 작업에 대해

SVM에서 새 CIFS 서버를 설정할 때 SMB 액세스에 대한 엑스포트 정책을 사용하는 것은 기본적으로 해제되어 있습니다. 인증 프로토콜 또는 클라이언트 IP 주소 또는 호스트 이름을 기반으로 액세스를 제어하려는 경우 SMB 액세스에 대한 엑스포트 정책을 설정할 수 있습니다. 언제든지 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 엑스포트 정책 활성화 또는 비활성화:
   - 내보내기 정책 활성화: 'vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled true'
   - 엑스포트 정책 비활성화: 'vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled false
3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 엑스포트 정책을 사용하여 SVM VS1 기반 리소스에 대한 SMB 클라이언트 액세스를 제어할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

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