내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

ONTAP 9

NetApp
April 24, 2024

목차

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.
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.
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 ID를 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'

Qtree ID 검증을 원하는 경우…	다음 명령을 입력합니다…
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.