이름 서비스 구성
ONTAP 9

NetApp
February 12, 2026

목차

이름 서비스 구성

ONTAP NFS 이름 서비스에 대해 알아보세요

스토리지 시스템의 구성에 따라 ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회해야 합니다. 이 정보를 얻으려면 ONTAP가 로컬 또는 외부 이름 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

클라이언트 인증 중에 NIS 또는 LDAP와 같은 이름 서비스를 사용하여 이름 조회를 용이하게 해야 합니다. 특히 NFSv4 이상을 구축할 때 보안을 강화하기 위해 가능하면 LDAP를 사용하는 것이 좋습니다. 또한 외부 이름 서버를 사용할 수 없는 경우 로컬 사용자 및 그룹을 구성해야 합니다.

이름 서비스 정보는 모든 소스에서 동기화되어야 합니다.

ONTAP NFS 이름 서비스 스위치 테이블 구성

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에 적용할 수 있는 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑에 사용할 이름 서비스를 결정해야 합니다.

넷그룹을 사용할 계획이라면 RFC 5952에 지정된 대로 넷그룹에 지정된 모든 IPv6 주소를 단축하고 압축해야 합니다.

이 작업에 대해

사용하지 않는 정보 소스는 포함하지 마십시오. 예를 들어 NIS가 사용자 환경에서 사용되지 않는 경우 '-Sources NIS' 옵션을 지정하지 마십시오.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

   'vserver services name-service ns-switch create-vserver_vserver_name_-database_database_name_-sources_source_names_'

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

   'vserver services name-service ns-switch show -vserver_vserver_name_'

   수정하려면 'vserver services name-service ns-switch modify' 또는 'vserver services name-service ns-switch delete' 명령을 사용해야 합니다.

예

다음 예에서는 SVM VS1 에서 로컬 넷그룹 파일을 사용할 수 있도록 이름 서비스 스위치 테이블에 새 항목을 생성하고 외부 NIS 서버에서 넷그룹 정보를 순서대로 찾습니다.

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

작업을 마친 후

- 데이터 액세스를 제공하려면 SVM에 지정한 이름 서비스를 구성해야 합니다.
- SVM에 대한 네임 서비스를 삭제할 경우 네임 서비스 스위치 테이블에서 해당 서비스를 제거해야 합니다.

  이름 서비스 스위치 테이블에서 이름 서비스를 삭제하지 않으면 스토리지 시스템에 대한 클라이언트 액세스가 예상대로 작동하지 않을 수 있습니다.

로컬 **UNIX** 사용자 및 그룹을 구성합니다

ONTAP NFS SVM에 대한 로컬 **UNIX** 사용자 및 그룹에 대해 알아보세요**.**

SVM에서 로컬 UNIX 사용자 및 그룹을 사용하여 인증 및 이름 매핑을 수행할 수 있습니다. UNIX 사용자 및 그룹을 수동으로 만들거나 UNIX 사용자 또는 그룹이 포함된 파일을 URI(Uniform Resource Identifier)에서 로드할 수 있습니다.

클러스터에 결합된 로컬 UNIX 사용자 그룹 및 그룹 구성원의 기본 최대 제한은 32,768입니다. 클러스터 관리자가 이 제한을 수정할 수 있습니다.

ONTAP NFS SVM에서 로컬 **UNIX** 사용자 생성

'vserver services name-service unix-user create' 명령을 사용하여 로컬 UNIX 사용자를 생성할 수 있습니다. 로컬 UNIX 사용자는 이름 매핑 처리에 사용되는 UNIX 이름 서비스 옵션으로 SVM에서 생성하는 UNIX 사용자입니다.

단계

1. 로컬 UNIX 사용자 생성:

   'vserver services name-service unix-user create-vserver_vserver_name_-user_user_name_-id_integer_-primary-gid_integer_-full-name_full_name_'

   '-user_user_name_'은(는) 사용자 이름을 지정합니다. 사용자 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 사용자가 지정하는 사용자 ID를 지정합니다.

   기본 그룹 ID는 -primary-gid_integer_ 로 지정합니다. 그러면 사용자가 기본 그룹에 추가됩니다. 사용자를 생성한 후 원하는 추가 그룹에 사용자를 수동으로 추가할 수 있습니다.

예

다음 명령을 실행하면 이름이 johnm인 로컬 UNIX 사용자가 이름이 vs1 인 SVM에 생성됩니다. 사용자는 ID 123 및 기본 그룹 ID 100을 가지고 있습니다.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

ONTAP NFS SVM에 로컬 UNIX 사용자 목록 로드

SVM에서 개별 로컬 UNIX 사용자를 수동으로 생성하는 대신 로컬 UNIX 사용자 목록을 URI(Uniform Resource Identifier)에서 SVM으로 로드하여 작업을 단순화할 수 있습니다('vserver services name-service unix-user load-from-Uri').

단계

1. 로드할 로컬 UNIX 사용자 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/passwd' 형식의 사용자 정보를 포함해야 합니다.

   '*user_name:password:user_ID:group_ID:full_name*'

   명령에서는 '*PASSWORD*' 필드 값과 '*FULL_NAME*' 필드 뒤에 있는 필드 값('*HOME_DIRECTORY*' 및 '*shell*')이 삭제됩니다.

   지원되는 최대 파일 크기는 2.5MB입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 포함되어 있으면 목록을 로드하지 못하고 오류 메시지가 표시됩니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 사용자 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-user load-from-Uri-vserver_vserver_name_-Uri{ftp|http|ftps|https}://*Uri* -overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/passwd` 에서 이름이 VS1 인 SVM으로 로컬 UNIX 사용자 목록이 로드됩니다. SVM의 기존 사용자는 URI의 정보로 덮어써지지 않습니다.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ONTAP NFS SVM에 로컬 UNIX 그룹 생성

"vserver services name-service unix-group create" 명령을 사용하여 SVM에 로컬인 UNIX 그룹을 생성할 수 있습니다. 로컬 UNIX 그룹은 로컬 UNIX 사용자와 함께 사용됩니다.

단계

1. 로컬 UNIX 그룹 생성:

   'vserver services name-service unix-group create-vserver_vserver_name_-name_group_name_-id_integer_'

   `-name_group_name_'은 그룹 이름을 지정합니다. 그룹 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 지정하는 그룹 ID를 지정합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 eng인 로컬 그룹이 생성됩니다. 그룹에 ID 101이 있습니다.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

ONTAP NFS SVM의 로컬 UNIX 그룹에 사용자 추가

'vserver services name-service unix-group adduser' 명령을 사용하여 SVM에 로컬인 보조 UNIX 그룹에 사용자를 추가할 수 있습니다.

단계

1. 로컬 UNIX 그룹에 사용자 추가:

'vserver services name-service unix-group adduser-vserver_vserver_name_-name_group_name_-username_user_name_'

'-name"*group_name*'은 사용자의 기본 그룹 외에도 사용자를 추가할 UNIX 그룹의 이름을 지정합니다.

예

다음 명령을 실행하면 이름이 max인 사용자가 이름이 eng인 로컬 UNIX 그룹에 이름이 vs1 인 SVM에 추가됩니다.

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

ONTAP NFS SVM의 URI에서 로컬 UNIX 그룹 로드

개별 로컬 UNIX 그룹을 수동으로 생성하는 대신 'vserver services name-service unix-group load-from-Uri' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 로컬 UNIX

그룹 목록을 로드할 수 있습니다.

단계

1. 로드할 로컬 UNIX 그룹 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/group' 형식의 그룹 정보를 포함해야 합니다.

   '*group_name:password:group_ID:comma_separated_list_of_users*'

   이 명령어는 '*PASSWORD*' 필드의 값을 삭제한다.

   지원되는 최대 파일 크기는 1MB입니다.

   그룹 파일에서 각 줄의 최대 길이는 32,768자입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 없어야 합니다. 그렇지 않으면 목록을 로드하지 못합니다. SVM에 이미 있는 항목이 있으면 "-overwrite" 매개 변수를 "true"로 설정하여 모든 기존 항목을 새 파일로 덮어쓰거나 새 파일에 기존 항목을 복제하는 항목이 없는지 확인해야 합니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 그룹 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-group load-from-Uri-vserver_vserver_name_-Uri{ftp|http|FTPS|https}://*Uri*-overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다. 이 매개 변수를 "true"로 지정하면 ONTAP는 지정된 SVM의 기존 로컬 UNIX 그룹 데이터베이스 전체를 로드하는 파일의 항목으로 바꿉니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/group` 에서 VS1 이라는 SVM으로 로컬 UNIX 그룹 목록이 로드됩니다. SVM의 기존 그룹은 URI의 정보로 덮어써지지 않습니다.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

넷그룹으로 작업합니다

ONTAP NFS SVM의 넷그룹에 대해 알아보세요

사용자 인증 및 내보내기 정책 규칙의 클라이언트와 일치시키기 위해 넷그룹을 사용할 수 있습니다. 외부 이름 서버(LDAP 또는 NIS)에서 넷그룹에 대한 액세스를 제공하거나, 'vserver services name-service netgroup load' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다.

시작하기 전에

넷그룹을 사용하기 전에 다음 조건이 충족되는지 확인해야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹의 모든 호스트는 순방향 및 역방향 DNS 조회를 일관되게 제공하기 위해 정방향(A) 및 역방향(PTR) DNS 레코드를 모두 포함해야 합니다.

  또한 클라이언트의 IP 주소에 PTR 레코드가 여러 개 있는 경우 이러한 모든 호스트 이름은 넷그룹의 구성원이어야 하며 해당 레코드가 있어야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹에 있는 모든 호스트의 이름은 철자가 올바르고 올바른 대소문자를 사용해야 합니다. 넷그룹에서 사용되는 호스트 이름의 대/소문자 불일치로 인해 내보내기 검사 실패와 같은 예기치 않은 동작이 발생할 수 있습니다.
- 넷그룹에 지정된 모든 IPv6 주소는 RFC 5952에 지정된 대로 단축되고 압축되어야 합니다.

  예를 들어 2011:hu9:0:0:0:0:3:1은 2011:hu9:3:1로 단축되어야 합니다.

이 작업에 대해

넷그룹으로 작업하는 경우 다음 작업을 수행할 수 있습니다.

- 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.
- 'vserver services name-service getxxbyy netgrp' 명령을 사용하여 클라이언트가 넷그룹에 속하는지 확인할 수 있습니다.

  조회를 수행하는 기본 서비스는 구성된 이름 서비스 스위치 순서에 따라 선택됩니다.

ONTAP NFS SVM의 URI에서 넷그룹 로드

내보내기 정책 규칙에서 클라이언트를 일치시키는 데 사용할 수 있는 방법 중 하나는 netgroup에 나열된 호스트를 사용하는 것입니다. 외부 이름 서버에 저장된 넷그룹을 사용하는 대신 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다('vserver services name-service netgroup load').

시작하기 전에

넷그룹 파일은 SVM에 로드되기 전에 다음 요구 사항을 충족해야 합니다.

- 파일은 NIS를 채우는 데 사용되는 것과 동일한 적절한 넷그룹 텍스트 파일 형식을 사용해야 합니다.

  ONTAP는 넷그룹 텍스트 파일 형식을 로드하기 전에 검사합니다. 파일에 오류가 있으면 로드되지 않고 파일에서 수행해야 하는 수정 사항을 나타내는 메시지가 표시됩니다. 오류를 해결한 후 Netgroup 파일을 지정된 SVM에 다시 로드할 수 있습니다.

- 넷그룹 파일의 호스트 이름에 있는 모든 영문자는 소문자여야 합니다.
- 지원되는 최대 파일 크기는 5MB입니다.
- 네스팅 넷그룹에 대해 지원되는 최대 수준은 1000입니다.
- 넷그룹 파일에 호스트 이름을 정의할 때는 운영 DNS 호스트 이름만 사용할 수 있습니다.

  내보내기 액세스 문제를 방지하려면 DNS CNAME 또는 라운드 로빈 레코드를 사용하여 호스트 이름을 정의하면 안 됩니다.

- 넷그룹 파일에서 3중 그룹의 사용자 및 도메인 부분은 ONTAP에서 지원하지 않으므로 비워 두어야 합니다.

  호스트/IP 부분만 지원됩니다.

이 작업에 대해

ONTAP는 로컬 넷그룹 파일에 대한 호스트 별 검색을 지원합니다. 넷그룹 파일을 로드하면 ONTAP에서 자동으로 netgroup.byhost 맵을 생성하여 넷그룹 기준 호스트 검색을 설정합니다. 이렇게 하면 내보내기 정책 규칙을 처리하여 클라이언트 액세스를 평가할 때 로컬 넷그룹 검색 속도를 크게 높일 수 있습니다.

단계

1. URI를 통해 넷그룹을 SVM에 로드:

   'vserver services name-service netgroup load-vserver_vserver_name_-source{ftp|http|FTPS|https}://*Uri*'

   넷그룹 파일을 로드하고 넷그룹을 생성합니다. byhost 맵은 몇 분 정도 걸릴 수 있습니다.

   넷그룹을 업데이트하려면 파일을 편집하고 업데이트된 넷그룹 파일을 SVM에 로드할 수 있습니다.

예

다음 명령을 실행하면 HTTP URL 'http://intranet/downloads/corp-netgroup`: 에서 이름이 VS1 인 SVM에 넷그룹 정의가 로드됩니다

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM 넷그룹 정의 확인

SVM에 넷그룹을 로드한 후 'vserver services name-service netgroup status' 명령을 사용하여 넷그룹 정의의 상태를 확인할 수 있습니다. 이렇게 하면 SVM을 백업하는 모든 노드에서 넷그룹 정의가 일관되는지 확인할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 넷그룹 정의의 상태를 확인합니다.

'vserver services name-service netgroup status'

자세한 보기에 추가 정보를 표시할 수 있습니다.

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예

권한 수준을 설정한 후 다음 명령을 실행하면 모든 SVM에 대한 넷그룹 상태가 표시됩니다.

```
vs1::> set -privilege advanced

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

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

ONTAP NFS SVM에 대한 NIS 도메인 구성 생성

사용자 환경에서 NIS(Network Information Service)를 사용하여 이름 서비스를 제공하는 경우 'vserver services name-service NIS-domain create' 명령을 사용하여 SVM에 대한 NIS 도메인 구성을 생성해야 합니다.

시작하기 전에

SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 NIS 서버를 사용할 수 있고 연결할 수 있어야 합니다.

NIS를 사용하여 디렉터리 검색을 수행할 경우 NIS 서버의 맵에는 각 항목에 대해 1,024자를 초과할 수 없습니다. 이 제한을 준수하지 않는 NIS 서버를 지정하지 마십시오. 그렇지 않으면 NIS 항목에 종속된 클라이언트 액세스가 실패할 수 있습니다.

이 작업에 대해

NIS 데이터베이스에 netgroup.byhost 맵이 포함되어 있으면 ONTAP에서 이를 사용하여 더 빨리 검색할 수 있습니다. 클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다. ONTAP 9.7부터 NIS 넷그룹.byhost 항목은 vserver services name-service NIS-domain netgroup-database 명령을 사용하여 캐싱될 수 있습니다.

호스트 이름 확인에 NIS를 사용하는 것은 지원되지 않습니다.

단계

1. NIS 도메인 구성 생성:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   NIS 서버는 최대 10개까지 지정할 수 있습니다.

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

2. 도메인이 생성되었는지 확인합니다.

   'vserver services name-service NIS-domain show'를 참조하십시오

예

다음 명령을 실행하면 NIS 도메인용 NIS 도메인 구성이 생성됩니다. SVM은 IP 주소의 NIS `nisdomain` 서버로 이름이 `vs1` 지정됩니다. `192.0.2.180`

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP를 사용합니다

ONTAP NFS SVM에서 LDAP 이름 서비스 사용에 대해 알아보세요

환경에서 LDAP를 네임 서비스로 사용하는 경우 LDAP 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 LDAP 클라이언트로 설정해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. 이름 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 활성화하려면 LDAP 클라이언트 modify 명령에 '-try-channel-binding' 매개 변수를 사용합니다.

자세한 내용은 을 참조하십시오"Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

- 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.
  - 도메인 암호는 -bind-as-cifs-server가 true로 설정된 경우 인증하기 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)

- 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.

를 참조하십시오

- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"
- "ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다"

ONTAP NFS SVM에 대한 새 LDAP 클라이언트 스키마 생성

사용자 환경의 LDAP 스키마가 ONTAP 기본값과 다른 경우 LDAP 클라이언트 구성을 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2012 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

기본값이 아닌 LDAP 스키마를 사용해야 하는 경우 LDAP 클라이언트 구성을 생성하기 전에 만들어야 합니다. 새 스키마를 만들기 전에 LDAP 관리자에게 문의하십시오.

ONTAP에서 제공하는 기본 LDAP 스키마는 수정할 수 없습니다. 새 스키마를 만들려면 복사본을 만든 다음 복사본을 적절하게 수정합니다.

단계

1. 기존 LDAP 클라이언트 스키마 템플릿을 표시하여 복사할 템플릿을 식별합니다.

   'vserver services name-service ldap client schema show'를 참조하십시오

2. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 기존 LDAP 클라이언트 스키마의 복사본을 만듭니다.

   'vserver services name-service LDAP 클라이언트 스키마 복사 - vserver_vserver_name_-schema_existing_schema_name_-new-schema-name_new_schema_name_'

4. 새 스키마를 수정하고 사용자 환경에 맞게 사용자 지정합니다.

   'vserver services name-service LDAP 클라이언트 스키마 수정

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성

ONTAP가 사용자 환경의 외부 LDAP 또는 Active Directory 서비스에 액세스하도록 하려면 먼저 스토리지 시스템에서 LDAP 클라이언트를 설정해야 합니다.

시작하기 전에

Active Directory 도메인 확인됨 목록의 처음 세 개 서버 중 하나가 작동 중이고 데이터를 제공하고 있어야 합니다. 그렇지 않으면 이 작업이 실패합니다.

여러 대의 서버가 있으며 그 중 어느 시점에서든 3대 이상의 서버가 다운됩니다.

단계

1. "vserver services name-service ldap client create" 명령에 대한 적절한 구성 값을 확인하려면 LDAP 관리자에게 문의하십시오.

   a. LDAP 서버에 대한 도메인 기반 또는 주소 기반 연결을 지정합니다.

      AD-DOMAIN과 -SERS 옵션은 상호 배타적입니다.

      - Active Directory 도메인에서 LDAP 서버 검색을 설정하려면 '-ad-domain' 옵션을 사용합니다.
        - 를 사용할 수 있습니다 `-restrict-discovery-to-site` LDAP 서버 검색을 지정된 도메인의 CIFS 기본 사이트로 제한하는 옵션입니다. 이 옵션을 사용하는 경우 에서 CIFS 기본 사이트도 지정해야 합니다 `-default-site`.
      - '-preferred-ad-servers' 옵션을 사용하여 쉼표로 구분된 목록에서 IP 주소로 하나 이상의 기본 Active Directory 서버를 지정할 수 있습니다. 클라이언트를 생성한 후 'vserver services name-service ldap client modify' 명령을 사용하여 이 목록을 수정할 수 있습니다.
      - 를 사용합니다 `-servers` 쉼표로 구분된 목록의 IP 주소로 하나 이상의 LDAP 서버(Active Directory 또는 UNIX)를 지정하는 옵션입니다.

        은 더 이상 사용되지 않습니다. `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드. 이 필드에는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

   b. 기본 또는 사용자 지정 LDAP 스키마를 지정합니다.

      대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 읽기 전용 스키마를 사용할 수 있습니다. 그렇지 않으면 기본 스키마를 사용하는 것이 좋습니다. 이 경우 기본 스키마(읽기 전용)를 복사한 다음 복사본을 수정하여 고유한 스키마를 만들 수 있습니다.

      기본 스키마:

      - MS-AD-BIS

        RFC-2307bis를 기반으로 하는 이 방식은 대부분의 표준 Windows 2012 이상 LDAP 구축에 선호되는 LDAP 스키마입니다.

- AD-IDMU

  UNIX용 Active Directory ID 관리를 기반으로 하는 이 스키마는 대부분의 Windows 2008, Windows 2012 이상 AD 서버에 적합합니다.

- AD-SFU

  UNIX용 Active Directory 서비스를 기반으로 하는 이 스키마는 대부분의 Windows 2003 및 이전 AD 서버에 적합합니다.

- RFC-2307

  RFC-2307(*LDAP*를 네트워크 정보 서비스로 사용하는 접근 방식)에 따라 이 스키마는 대부분의 UNIX AD 서버에 적합합니다.

c. 바인딩 값을 선택합니다.

- '-min-bind-level{anonymous|simple|sasl}'은 최소 bind authentication level을 지정한다.

  기본값은 ' * anonymous * '입니다.

- '-bind-dn_ldap_DN_'은 바인딩 사용자를 지정합니다.

  Active Directory 서버의 경우 계정(domain\user) 또는 보안 주체(user@domain.com) 양식에서 사용자를 지정해야 합니다. 그렇지 않으면 고유 이름(CN=user, DC=domain, DC=com) 형식으로 사용자를 지정해야 합니다.

- '-BIND-PASSWORD_PASSWORD_'는 바인딩 암호를 지정합니다.

d. 필요한 경우 세션 보안 옵션을 선택합니다.

LDAP 서버에서 필요한 경우 LDAP 서명 및 봉인 또는 TLS를 통한 LDAP를 활성화할 수 있습니다.

- '--세션-보안{none|sign|seal}'

  서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

  또한 서명과 봉인 바인딩이 실패할 경우 바인딩 인증을 ' * anonymous * ' 또는 ' * simple * '로 되돌리지 않으려면 '-min-bind-level' {'s ASL'}을 설정해야 합니다.

- '-use-start-tls'{'true'|'false'}

  '* true*'로 설정되어 있고 LDAP 서버가 이를 지원하는 경우 LDAP 클라이언트는 서버에 암호화된 TLS 연결을 사용합니다. 기본값은 ' * FALSE * '입니다. 이 옵션을 사용하려면 LDAP 서버의 자체 서명된 루트 CA 인증서를 설치해야 합니다.

> ⓘ 스토리지 VM에 도메인에 추가된 SMB 서버가 있고 LDAP 서버가 SMB 서버의 홈 도메인의 도메인 컨트롤러 중 하나인 경우 을 수정할 수 있습니다 `-session-security-for-ad-ldap` 옵션을 선택합니다 `vserver cifs security modify` 명령.

e. 포트, 쿼리 및 기준 값을 선택합니다.

기본값을 사용하는 것이 좋지만 LDAP 관리자에게 해당 값이 사용자 환경에 적합한지 확인해야 합니다.

- '-port_port_'는 LDAP 서버 포트를 지정합니다.

  기본값은 389입니다.

Start TLS를 사용하여 LDAP 연결을 보호하려면 기본 포트 389를 사용해야 합니다. 시작 TLS는 LDAP 기본 포트 389를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다. 포트를 변경하면 Start TLS가 실패합니다.

- '-query-timeout_integer_'는 쿼리 시간 제한(초)을 지정합니다.

  허용 범위는 1 ~ 10초입니다. 기본값은 3초입니다.

- `-base-dn_ldap_dn_'은 기본 DN을 지정합니다.

  필요한 경우 여러 값을 입력할 수 있습니다(예: LDAP 조회 추적을 사용하는 경우). 기본값은 ""(root)입니다.

- '-base-scope'{'base'|'onelel'|'ubtree'}는 기본 검색 범위를 지정합니다.

  기본값은 'Subtree'입니다.

- '-referral-enabled'{'true'|'false'}는 LDAP 조회 추적 활성화 여부를 지정합니다.

  ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에 반환되어 원하는 레코드가 참조된 LDAP 서버에 있음을 나타내는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있습니다. 기본값은 ' * FALSE * '입니다.

참조된 LDAP 서버에 있는 레코드를 검색하려면 LDAP 클라이언트 구성의 일부로 참조된 레코드의 기본 dn을 기본 dn에 추가해야 합니다.

2. 스토리지 VM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

   LDAP 클라이언트 구성을 생성할 때 스토리지 VM 이름을 제공해야 합니다.

3. LDAP 클라이언트 구성이 성공적으로 생성되었는지 확인합니다.

   'vserver services name-service ldap client show-client-config client_config_name'

예

다음 명령을 실행하면 스토리지 VM VS1이 LDAP용 Active Directory 서버와 함께 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

다음 명령을 실행하면 스토리지 VM VS1이 Active Directory 서버와 작동하여 서명과 봉인이 필요한 LDAP에 대해 ldap1이라는 새 LDAP 클라이언트 구성이 생성되고 LDAP 서버 검색이 지정된 도메인의 특정 사이트로 제한됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

다음 명령을 실행하면 스토리지 VM VS1이 LDAP 조회 추적이 필요한 LDAP용 Active Directory 서버와 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

다음 명령을 실행하면 기본 DN을 지정하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

다음 명령을 실행하면 조회 추적을 활성화하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

ONTAP NFS SVM과 LDAP 클라이언트 구성 연결

SVM에서 LDAP를 활성화하려면 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결해야 합니다.

시작하기 전에

- LDAP 도메인은 네트워크 내에 이미 존재해야 하며 SVM이 있는 클러스터에서 액세스할 수 있어야 합니다.
- SVM에 LDAP 클라이언트 구성이 있어야 합니다.

단계

1. SVM에서 LDAP 지원:

   'vserver services name-service LDAP create-vserver_vserver_name_-client-config_client_config_name_'

   > 그만큼 `vserver services name-service ldap create` 명령은 자동 구성 검증을 수행하고 ONTAP 이름 서버에 접속할 수 없는 경우 오류 메시지를 보고합니다.

   다음 명령을 실행하면 "VS1" SVM에서 LDAP를 활성화하고 "ldap1" LDAP 클라이언트 구성을 사용하도록 구성합니다.

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령은 SVM VS1 에서 LDAP 서버의 유효성을 검사합니다.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                    |
   | Client Configuration Name: c1                                   |
   | LDAP Status: up                                                 |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                                  |
   ```

ONTAP NFS SVM에 대한 LDAP 소스 확인

SVM을 위한 네임 서비스 스위치 테이블에 네임 서비스에 대한 LDAP 소스가 올바르게 나열되어 있는지 확인해야 합니다.

단계

1. 현재 이름 서비스 스위치 테이블 내용을 표시합니다.

   'vserver services name-service ns-switch show -vserver_svm_name_'

다음 명령을 실행하면 SVM My_SVM의 결과가 표시됩니다.

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

이름 매핑 정보를 검색할 소스 및 순서를 지정합니다. UNIX 전용 환경에서는 이 항목이 필요하지 않습니다. 이름 매핑은 UNIX와 Windows를 모두 사용하는 혼합 환경에서만 필요합니다.

2. 필요에 따라 ns-switch 항목을 업데이트합니다.

ns-switch 항목을 업데이트하려면...	명령 입력...
사용자 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database passwd -sources ldap, files'
그룹 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database group-sources ldap, files'
넷그룹 정보입니다	'vserver services name-service ns-switch modify -vserver_vserver_name_-database 넷그룹 - 소스 LDAP, 파일