이름 서비스 구성

ONTAP 9

NetApp
April 24, 2024

목차

이름 서비스 구성

ONTAP 네임 서비스 스위치 구성의 작동 방식

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

LDAP 개요

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 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.
  - '--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 "nsswitch 인증을 위한 LDAP 빠른 바인딩."
- 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".

LDAP 서명 및 봉인 개념

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.

LDAPS 개념

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 9.5-9.8에서 LDAPS는 포트 636에서만 활성화할 수 있습니다. 이렇게 하려면 '-use-ldaps-for-ad-ldap' 매개 변수를 'vserver cifs security modify' 명령과 함께 사용하십시오.
  - ONTAP 9.9.1부터 포트 636이 기본값으로 유지되지만 LDAPS는 모든 포트에서 활성화할 수 있습니다. 이렇게 하려면 '-ldaps-enabled' 매개 변수를 'true'로 설정하고 원하는 '-port' 매개 변수를 지정합니다. 자세한 내용은 'vserver services name-service ldap client create' man 페이지를 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.

LDAP RFC2307bis 지원을 활성화합니다

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

필요한 것

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 검색에 대한 구성 옵션입니다

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'	필요한 경우 모든 LDAP 검색다중 값에 대한 기본 DN을 입력할 수 있습니다(예: ONTAP 9.5 이상 릴리스에서 LDAP 조회 추적을 사용하는 경우).
``기본범위''	모든 LDAP 검색에 대한 기본 범위입니다
'-user-dn'	모든 LDAP 사용자의 기본 DNS 검색이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
'- 사용자 범위'	모든 LDAP 사용자 검색에 대한 기본 범위 이 매개 변수는 사용자 이름 매핑 검색에도 적용됩니다.
``그룹-dn''	모든 LDAP 그룹 검색에 대한 기본 DNS입니다
그룹-범위	모든 LDAP 그룹 검색에 대한 기본 범위입니다
'-넷그룹-dn'	모든 LDAP 넷그룹 검색에 대한 기본 DNS입니다
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.

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.

필요한 것

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.

   > ONTAP 9.2부터 -ldap-servers 필드가 -servers 필드를 대체합니다. 이 새 필드는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

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"

nsswitch 인증에 LDAP 고속 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."

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.

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'

   - 새 관리자 사용자는 를 참조하십시오 "LDAP 또는 NIS 계정 액세스를 설정합니다."

LDAP 통계를 표시합니다

ONTAP 9.2부터는 스토리지 시스템의 SVM(스토리지 가상 머신)에 대한 LDAP 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

필요한 것

- 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 예제는 객체 'ECD_EXTERNAL_SERVICE_OP'에 대한 성능 데이터를 보여 줍니다.

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance “vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1”

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```