강력한 보안을 위해 **NFS**와 **Kerberos** 사용

ONTAP 9

NetApp
April 24, 2024

목차

강력한 보안을 위해 NFS와 Kerberos 사용

Kerberos에 대한 ONTAP 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.

NFS로 Kerberos 구성 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.
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"

NFSv4의 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'