Hohe Sicherheit durch Kerberos mit NFS

ONTAP 9

NetApp
September 12, 2024

Inhalt

Hohe Sicherheit durch Kerberos mit NFS

ONTAP-Unterstützung für Kerberos

Kerberos bietet eine starke, sichere Authentifizierung für Client-/Server-Applikationen. Authentifizierung ermöglicht die Überprüfung von Benutzer- und Prozessidentitäten auf einem Server. In der ONTAP Umgebung bietet Kerberos die Authentifizierung zwischen Storage Virtual Machines (SVMs) und NFS-Clients.

In ONTAP 9 wird die folgende Kerberos-Funktion unterstützt:

- Kerberos 5-Authentifizierung mit Integritätsprüfung (krb5i)

  Krb5i verwendet Prüfsummen, um die Integrität jeder NFS-Nachricht, die zwischen Client und Server übertragen wurde, zu überprüfen. Dies ist sowohl aus Sicherheitsgründen (um sicherzustellen, dass Daten nicht manipuliert werden) als auch aus Gründen der Datenintegrität (zum Beispiel zur Vermeidung von Datenkorruption bei der Nutzung von NFS über unzuverlässige Netzwerke) nützlich.

- Kerberos 5-Authentifizierung mit Datenschutzprüfung (krb5p)

  Krb5p verwendet Prüfsummen, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln. Dies ist sicherer und führt zu einer höheren Belastung.

- 128-Bit- und 256-Bit-AES-Verschlüsselung

  Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus zur Sicherung elektronischer Daten. Für Kerberos unterstützt ONTAP AES mit 128-Bit-Schlüsseln (AES-128) und AES mit 256-Bit-Verschlüsselung (AES-256).

- Kerberos-Bereichskonfigurationen auf SVM-Ebene

  SVM-Administratoren können jetzt Kerberos-Bereichskonfigurationen auf SVM-Ebene erstellen. Das bedeutet, dass SVM-Administratoren sich bei der Konfiguration von Kerberos-Bereich nicht mehr auf den Cluster-Administrator verlassen müssen und in einer mandantenfähigen Umgebung einzelne Kerberos-Bereichskonfigurationen erstellen können.

Anforderungen für die Konfiguration von Kerberos mit NFS

Bevor Sie Kerberos mit NFS auf Ihrem System konfigurieren, müssen Sie sicherstellen, dass bestimmte Elemente in Ihrer Netzwerk- und Speicherumgebung ordnungsgemäß konfiguriert sind.

> Die Schritte zur Konfiguration Ihrer Umgebung hängen davon ab, welche Version und Art von Clientbetriebssystem, Domänencontroller, Kerberos, DNS usw. Sie verwenden. Die Dokumentation all dieser Variablen übersteigt den Rahmen dieses Dokuments. Weitere Informationen finden Sie in der entsprechenden Dokumentation zu den einzelnen Komponenten.
>
> Ein detailliertes Beispiel, wie man ONTAP und Kerberos 5 mit NFSv3 und NFSv4 in einer Umgebung mit Windows Server 2008 R2 Active Directory und Linux Hosts einrichtet, finden Sie im technischen Bericht 4073.

Die folgenden Elemente sollten zuerst konfiguriert werden:

Anforderungen an die Netzwerkumgebung

- Kerberos

  Sie müssen über ein funktioniertes Kerberos-Setup mit einem Key Distribution Center (KDC) verfügen, z. B. mit Windows Active Directory-basierten Kerberos oder mit Kerberos.

  NFS-Server müssen sie verwenden `nfs` Als Hauptkomponente ihres Maschinentrancheals.

- Verzeichnisdienst

  Sie müssen einen sicheren Verzeichnisdienst in Ihrer Umgebung verwenden, z. B. Active Directory oder OpenLDAP, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist.

- NTP

  Sie müssen über einen Arbeitszeitserver verfügen, auf dem NTP ausgeführt wird. Dies ist notwendig, um ein Versagen der Kerberos-Authentifizierung aufgrund von Zeitverzerrung zu verhindern.

- DNS (Domain Name Resolution)

  Jeder UNIX-Client und jede SVM-LIF müssen über einen entsprechenden Service-Datensatz (SRV) verfügen, der beim KDC unter „Forward and Reverse Lookup Zones“ registriert ist. Alle Teilnehmer müssen über DNS richtig lösbar sein.

- Benutzerkonten

  Jeder Client muss über ein Benutzerkonto im Kerberos-Bereich verfügen. NFS-Server müssen „`nfs`“ als primäre Komponente ihres Machine-Principal verwenden.

Anforderungen des NFS-Clients

- NFS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um mit NFSv3 oder NFSv4 über das Netzwerk zu kommunizieren.

  Die Clients müssen RFC1964 und RFC2203 unterstützen.

- Kerberos

  Jeder Client muss richtig konfiguriert sein, um Kerberos-Authentifizierung zu verwenden, einschließlich der

folgenden Details:

- Die Verschlüsselung für TGS-Kommunikation ist aktiviert.

  AES-256 für höchste Sicherheit.

- Der sicherste Verschlüsselungstyp für die TGT-Kommunikation ist aktiviert.
- Der Kerberos-Bereich und die Domäne sind korrekt konfiguriert.
- GSS ist aktiviert.

  Bei Verwendung von Geräteanmeldeinformationen:

- Nicht ausführen `gssd` Mit dem `-n` Parameter.
- Nicht ausführen `kinit` Als Root-Benutzer.

- Jeder Client muss die neueste und aktualisierte Betriebssystemversion verwenden.

  Dies bietet die beste Kompatibilität und Zuverlässigkeit für AES-Verschlüsselung mit Kerberos.

- DNS

  Jeder Client muss richtig konfiguriert sein, damit DNS für die richtige Namensauflösung verwendet wird.

- NTP

  Jeder Client muss mit dem NTP-Server synchronisiert werden.

- Host- und Domain-Informationen

  Jedem Kunden `/etc/hosts` Und `/etc/resolv.conf` Dateien müssen den richtigen Host-Namen bzw. die richtigen DNS-Informationen enthalten.

- Keytab-Dateien

  Jeder Client muss über eine Keytab-Datei aus dem KDC verfügen. Der Bereich muss in Großbuchstaben liegen. Der Verschlüsselungstyp muss AES-256 sein, um höchste Sicherheit zu gewährleisten.

- Optional: Für eine optimale Leistung profitieren Kunden von mindestens zwei Netzwerkschnittstellen: Eine für die Kommunikation mit dem lokalen Netzwerk und eine für die Kommunikation mit dem Speichernetzwerk.

Storage-Systemanforderungen

- NFS-Lizenz

  Auf dem Speichersystem muss eine gültige NFS-Lizenz installiert sein.

- CIFS-Lizenz

  Die CIFS-Lizenz ist optional. Sie ist nur zum Überprüfen der Windows-Anmeldeinformationen erforderlich, wenn die Multiprotokoll-Namenszuweisung verwendet wird. In einer strikten, ausschließlich auf UNIX ausgesetzten Umgebung ist dies nicht erforderlich.

- SVM

Auf dem System muss mindestens eine SVM konfiguriert sein.

- DNS auf der SVM

  Sie müssen DNS für jede SVM konfiguriert haben.

- NFS-Server

  Sie müssen NFS auf der SVM konfiguriert haben.

- AES-Verschlüsselung

  Für eine starke Sicherheit müssen Sie den NFS-Server so konfigurieren, dass nur AES-256-Verschlüsselung für Kerberos zugelassen ist.

- SMB Server

  Falls Sie eine Multi-Protokoll-Umgebung ausführen, müssen Sie SMB für die SVM konfiguriert haben. Der SMB-Server ist für die Multiprotokoll-Namenszuweisung erforderlich.

- Volumes

  Sie müssen über ein Root-Volume und mindestens ein Daten-Volume verfügen, das für die Verwendung durch die SVM konfiguriert ist.

- Root-Volume

  Das Root-Volume der SVM muss über folgende Konfiguration verfügen:

Name	Einstellung
Sicherheitsstil	UNIX
UID	Root oder ID 0
GID	Root oder ID 0
UNIX-Berechtigungen	777

  Im Gegensatz zum Root-Volume kann bei Daten-Volumes entweder der Sicherheitsstil genutzt werden.

- UNIX-Gruppen

  Die SVM muss über die folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0

Gruppenname	Gruppen-ID
Pcuser	65534 (wird automatisch von ONTAP beim Erstellen der SVM erstellt)

- UNIX-Benutzer

  Die SVM muss über die folgenden UNIX-Benutzer konfiguriert sein:

Benutzername	Benutzer-ID	ID der primären Gruppe	Kommentar
nfs	500	0	Erforderlich für GSS INIT-Phase Die erste Komponente des SPN-Client-Benutzers des NFS wird als Benutzer verwendet.
Pcuser	65534	65534	Erforderlich für NFS- und CIFS-Multi-Protokoll-Verwendung Wird bei der Erstellung der SVM automatisch von ONTAP erstellt und zur pcuser-Gruppe hinzugefügt.
Stamm	0	0	Zur Montage erforderlich

  Der nfs-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX Namenszuweisung für das SPN des NFS-Client-Benutzers besteht.

- Exportrichtlinien und Regeln

  Sie müssen Exportrichtlinien mit den erforderlichen Exportregeln für das Root-Medium und die Daten-Volumes und qtrees konfiguriert haben. Wenn über Kerberos auf alle Volumes der SVM zugegriffen wird, können Sie die Optionen für die Exportregel festlegen `-rorule`, `-rwrule`, und `-superuser` Für das Root-Volume zu `krb5` , `krb5i`, Oder `krb5p`.

- Kerberos-UNIX-Namenszuweisung

  Wenn der vom NFS-Client-Benutzer SPN identifizierte Benutzer über Root-Berechtigungen verfügen soll, müssen Sie eine Namenszuweisung zum Root erstellen.

Verwandte Informationen

"Technischer Bericht 4073 von NetApp: Sichere einheitliche Authentifizierung"

"NetApp Interoperabilitäts-Matrix-Tool"

"Systemadministration"

Geben Sie die Benutzer-ID-Domäne für NFSv4 an

Um die Benutzer-ID-Domäne anzugeben, können Sie die festlegen `-v4-id-domain` Option.

Über diese Aufgabe

Standardmäßig verwendet ONTAP die NIS-Domäne für die Zuordnung der NFSv4-Benutzer-ID, wenn eine festgelegt ist. Wenn keine NIS-Domäne festgelegt ist, wird die DNS-Domäne verwendet. Möglicherweise müssen Sie die Benutzer-ID-Domäne festlegen, wenn Sie beispielsweise mehrere Benutzer-ID-Domänen haben. Der Domänenname muss mit der Domänenkonfiguration auf dem Domänencontroller übereinstimmen. Es ist nicht für NFSv3 erforderlich.

Schritt

1. Geben Sie den folgenden Befehl ein:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```