使用Kerberos搭配NFS以獲得強大的安全性

ONTAP 9

NetApp
February 12, 2026

目錄

使用Kerberos搭配NFS以獲得強大的安全性

ONTAP NFS 對 Kerberos 的支持

Kerberos為用戶端/伺服器應用程式提供強大的安全驗證功能。驗證可驗證伺服器的使用者和處理程序身分。在支援VMware的環境中ONTAP 、Kerberos可在儲存虛擬機器（SVM）和NFS用戶端之間提供驗證。

在發揮作用的過程中、支援下列Kerberos功能：ONTAP

- Kerberos 5驗證搭配完整性檢查（krb5i）

  Krb5i使用Checksum來驗證用戶端與伺服器之間傳輸的每個NFS訊息完整性。這項功能在安全性方面非常實用（例如、確保資料未遭竄改）、也有助於確保資料完整性（例如、在不可靠的網路上使用NFS時、可防止資料毀損）。

- Kerberos 5驗證搭配隱私權檢查（krb5p）

  Krb5p使用Checksum加密用戶端與伺服器之間的所有流量。這更安全、也會產生更多負載。

- 128位元和256位元AES加密

  進階加密標準（AES）是一種加密演算法、用於保護電子資料安全。ONTAP 支援採用 128 位元金鑰（ AES-128 ）的 AES 、以及採用 256 位元金鑰（ AES-256 ）加密的 AES 、以提供更強大的安全性。

- SVM層級Kerberos領域組態

  SVM系統管理員現在可以在SVM層級建立Kerberos領域組態。這表示SVM管理員不再需要仰賴叢集管理員來進行Kerberos領域組態、也能在多租戶環境中建立個別的Kerberos領域組態。

使用 ONTAP NFS 設定 Kerberos 的要求

在系統上使用NFS設定Kerberos之前、您必須先確認網路和儲存環境中的某些項目已正確設定。

> 設定環境的步驟取決於您所使用的用戶端作業系統、網域控制器、Kerberos、DNS等版本和類型。記錄所有這些變數不在此文件範圍之內。如需詳細資訊、請參閱各元件的相關文件。
>
> 如需ONTAP 如何在使用Windows Server 2008 R2 Active Directory和Linux主機的環境中使用NFSv3和NFSv3設定支援功能的支援功能和Kerberos 5的詳細範例、請參閱技術報告4073。

應先設定下列項目：

網路環境需求

- Kerberos

  您必須使用金鑰發佈中心（Kdc）進行有效的Kerberos設定、例如Windows Active Directory型Kerberos

或MIT Kerberos。

NFS 伺服器必須使用 `nfs` 作為其機器主體的主要元件。

- 目錄服務

  您必須在環境中使用安全目錄服務、例如Active Directory或OpenLDAP、這類服務設定為使用LDAP over SSL/TLS。

- NTP

  您必須有執行NTP的工作時間伺服器。這是防止Kerberos驗證因時間偏移而失敗的必要步驟。

- 網域名稱解析（DNS）

  每個UNIX用戶端和每個SVM LIF都必須在Kdc的正向和反向對應區域下註冊適當的服務記錄（SRF）。所有參與者都必須透過DNS正確解析。

- 使用者帳戶

  每個用戶端都必須在Kerberos領域中擁有使用者帳戶。NFS伺服器必須使用「NFS」作為其機器主體的主要元件。

NFS 用戶端需求

- NFS

  每個用戶端都必須正確設定、才能使用NFSv3或NFSv4透過網路進行通訊。

  用戶端必須支援RFC1964和RFC2203。

- Kerberos

  每個用戶端都必須正確設定、才能使用Kerberos驗證、包括下列詳細資料：

  - 已啟用TGS通訊的加密。

    AES-256提供最強大的安全性。

  - 已啟用TGTT通訊最安全的加密類型。
  - Kerberos領域和網域已正確設定。
  - GSS 已啟用。

    使用機器認證時：

  - 請勿執行 `gssd` 使用 `-n` 參數。
  - 請勿執行 `kinit` 作為 root 使用者。

- 每個用戶端都必須使用最新且更新的作業系統版本。

  這可為使用Kerberos的AES加密提供最佳的相容性與可靠性。

- DNS

  每個用戶端都必須正確設定、才能使用DNS進行正確的名稱解析。

- NTP

  每個用戶端都必須與NTP伺服器同步。

- 主機與網域資訊

  每個用戶端 `/etc/hosts` 和 `/etc/resolv.conf` 檔案必須分別包含正確的主機名稱和 DNS 資訊。

- Keytab檔案

  每個用戶端都必須有來自於Kdc的Keytab檔案。領域必須以大寫字母顯示。加密類型必須為AES-256、才能獲得最強的安全性。

- 選用：為獲得最佳效能、用戶端可享有至少兩個網路介面：一個用於與區域網路通訊、另一個用於與儲存網路通訊。

儲存系統需求

- NFS授權

  儲存系統必須安裝有效的NFS授權。

- CIFS 授權

  CIFS授權為選用授權。只有在使用多重傳輸協定名稱對應時、才需要檢查Windows認證。在純UNIX的嚴格環境中、不需要這項功能。

- SVM

  您必須在系統上設定至少一個SVM。

- SVM上的DNS

  您必須在每個SVM上設定DNS。

- NFS 伺服器

  您必須在SVM上設定NFS。

- AES加密

  為了獲得最強大的安全性、您必須設定NFS伺服器、使其僅允許Kerberos使用AES-256加密。

- SMB 伺服器

  如果您執行的是多重傳輸協定環境、則必須在SVM上設定SMB。多重傳輸協定名稱對應需要SMB伺服器。

- 磁碟區

您必須有根磁碟區和至少一個設定供SVM使用的資料磁碟區。

- 根Volume

  SVM的根Volume必須具有下列組態：

名稱	設定
安全風格	UNIX
UID	root或ID 0
Gid	root或ID 0
UNIX權限	7777

  相較於根磁碟區、資料磁碟區可以有任一種安全樣式。

- UNIX 群組

  SVM必須設定下列UNIX群組：

群組名稱	群組**ID**
精靈	1.
根	0%
pcuser	65534（ONTAP 建立SVM時由SVM自動建立）

- UNIX 使用者

  SVM必須設定下列UNIX使用者：

使用者名稱	使用者**ID**	主要群組**ID**	留言
NFS	500	0%	GSS 初始化階段所需 NFS用戶端使用者的第一個使用者是使用者。
pcuser	65534	65534	NFS 和 CIFS 多重傳輸協定的使用需求 建立 SVM 時、由 ONTAP 自動建立並新增至 pcuser 群組。

使用者名稱	使用者ID	主要群組ID	留言
根	0%	0%	安裝所需

如果NFS用戶端使用者的SPN-UNIX名稱對應存在、則不需要NFS使用者。

- 匯出原則與規則

  您必須設定匯出原則、並針對根磁碟區、資料磁碟區和qtree設定必要的匯出規則。如果透過 Kerberos 存取 SVM 的所有磁碟區、您可以設定匯出規則選項 `-rorule`、 `-rwrule`和 `-superuser` 將根磁碟區移至 `krb5` 、 `krb5i`或 `krb5p`。

- Kerberos UNIX名稱對應

  如果您想讓NFS用戶端使用者的使用者具有root權限、您必須建立一個指向root的名稱對應。

相關資訊

"NetApp技術報告4073：安全統一化驗證"

"NetApp 互通性對照表工具"

"系統管理"

"邏輯儲存管理"

為 NFSv4 指定 ONTAP 使用者 ID 網域

若要指定使用者 ID 網域、您可以設定 `-v4-id-domain` 選項。

關於這項工作

根據預設ONTAP 、如果已設定NFSv4使用者ID對應、則使用NIS網域。如果未設定NIS網域、則會使用DNS網域。例如、如果您有多個使用者ID網域、則可能需要設定使用者ID網域。網域名稱必須符合網域控制器上的網域組態。NFSv3不需要此功能。

步驟

1. 輸入下列命令：

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

版權資訊

商標資訊