Utilizzo di Kerberos con NFS per una maggiore sicurezza

ONTAP 9

NetApp
April 24, 2024

Sommario

Utilizzo di Kerberos con NFS per una maggiore sicurezza

Supporto ONTAP per Kerberos

Kerberos offre un'autenticazione sicura e sicura per le applicazioni client/server. L'autenticazione consente di verificare le identità di utenti e processi di un server. Nell'ambiente ONTAP, Kerberos fornisce l'autenticazione tra le macchine virtuali di storage (SVM) e i client NFS.

In ONTAP 9, sono supportate le seguenti funzionalità Kerberos:

- Autenticazione Kerberos 5 con controllo dell'integrità (krb5i)

  Krb5i utilizza checksum per verificare l'integrità di ogni messaggio NFS trasferito tra client e server. Ciò è utile sia per motivi di sicurezza (ad esempio, per garantire che i dati non siano stati manomessi) che per motivi di integrità dei dati (ad esempio, per prevenire la corruzione dei dati quando si utilizza NFS su reti non affidabili).

- Autenticazione Kerberos 5 con controllo della privacy (krb5p)

  Krb5p utilizza checksum per crittografare tutto il traffico tra il client e il server. Questo è più sicuro e comporta un carico maggiore.

- Crittografia AES a 128 e 256 bit

  Advanced Encryption Standard (AES) è un algoritmo di crittografia per la protezione dei dati elettronici. ONTAP supporta AES con chiavi a 128 bit (AES-128) e AES con chiavi a 256 bit (AES-256) per Kerberos per una maggiore protezione.

- Configurazioni di area di autenticazione Kerberos a livello di SVM

  Gli amministratori di SVM possono ora creare configurazioni di area di autenticazione Kerberos a livello di SVM. Ciò significa che gli amministratori di SVM non devono più affidarsi all'amministratore del cluster per la configurazione dell'area di autenticazione Kerberos e possono creare singole configurazioni dell'area di autenticazione Kerberos in un ambiente multi-tenancy.

Requisiti per la configurazione di Kerberos con NFS

Prima di configurare Kerberos con NFS sul sistema, è necessario verificare che alcuni elementi dell'ambiente di rete e di storage siano configurati correttamente.

> La procedura per configurare l'ambiente dipende dalla versione e dal tipo di sistema operativo client, controller di dominio, Kerberos, DNS e così via. che stai utilizzando. La documentazione di tutte queste variabili non rientra nell'ambito di questo documento. Per ulteriori informazioni, consultare la documentazione relativa a ciascun componente.
>
> Per un esempio dettagliato di come configurare ONTAP e Kerberos 5 con NFSv3 e NFSv4 in un ambiente che utilizza Active Directory di Windows Server 2008 R2 e host Linux, consultare il report tecnico 4073.

È necessario configurare prima i seguenti elementi:

Requisiti dell'ambiente di rete

- Kerberos

  È necessario disporre di una configurazione Kerberos funzionante con un centro di distribuzione delle chiavi (KDC), ad esempio Kerberos basato su Windows Active Directory o MIT Kerberos.

  I server NFS devono utilizzare `nfs` come componente principale del computer.

- Servizio di directory

  È necessario utilizzare un servizio directory sicuro nell'ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS.

- NTP

  È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

  Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolutibili correttamente tramite DNS.

- Account utente

  Ogni client deve disporre di un account utente nell'area Kerberos. I server NFS devono utilizzare "nfs" come componente principale del computer.

Requisiti del client NFS

- NFS

  Ciascun client deve essere configurato correttamente per comunicare in rete utilizzando NFSv3 o NFSv4.

  I client devono supportare RFC1964 e RFC2203.

- Kerberos

  Ciascun client deve essere configurato correttamente per utilizzare l'autenticazione Kerberos, inclusi i seguenti dettagli:

  - La crittografia per la comunicazione TGS è attivata.

    AES-256 per la massima sicurezza.

  - Il tipo di crittografia più sicuro per la comunicazione TGT è attivato.
  - Il dominio e l'area di autenticazione Kerberos sono configurati correttamente.
  - Il GSS è attivato.

    Quando si utilizzano le credenziali del computer:

    - Non eseguire `gssd` con `-n` parametro.
    - Non eseguire `kinit` come utente root.
- Ogni client deve utilizzare la versione più recente e aggiornata del sistema operativo.

  In questo modo si ottiene la migliore compatibilità e affidabilità per la crittografia AES con Kerberos.

- DNS

  Ciascun client deve essere configurato correttamente per utilizzare il DNS per la corretta risoluzione dei nomi.

- NTP

  Ciascun client deve essere sincronizzato con il server NTP.

- Informazioni su host e dominio

  Di ogni client `/etc/hosts` e. `/etc/resolv.conf` I file devono contenere rispettivamente il nome host e le informazioni DNS corretti.

- File keytab

  Ogni client deve avere un file keytab dal KDC. L'area di autenticazione deve essere in lettere maiuscole. Il tipo di crittografia deve essere AES-256 per garantire la massima sicurezza.

- Opzionale: Per ottenere le migliori performance, i client traggono vantaggio dalla presenza di almeno due interfacce di rete: Una per la comunicazione con la rete locale e una per la comunicazione con la rete di storage.

Requisiti di sistema per lo storage

- Licenza NFS

  Il sistema storage deve avere una licenza NFS valida installata.

- Licenza CIFS

  La licenza CIFS è opzionale. È necessario solo per il controllo delle credenziali Windows quando si utilizza la mappatura dei nomi multiprotocollo. Non è richiesto in un ambiente UNIX-only rigoroso.

- SVM

  È necessario configurare almeno una SVM sul sistema.

- DNS su SVM

  È necessario aver configurato il DNS su ogni SVM.

- Server NFS

  È necessario aver configurato NFS su SVM.

- Crittografia AES

Per una maggiore sicurezza, è necessario configurare il server NFS in modo che consenta solo la crittografia AES-256 per Kerberos.

- Server SMB

  Se si utilizza un ambiente multiprotocollo, è necessario aver configurato SMB su SVM. Il server SMB è necessario per la mappatura dei nomi multiprotocollo.

- Volumi

  È necessario disporre di un volume root e di almeno un volume di dati configurati per l'utilizzo da parte di SVM.

- Volume root

  Il volume root di SVM deve avere la seguente configurazione:

Nome	Impostazione
Stile di sicurezza	UNIX
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	777

  A differenza del volume root, i volumi di dati possono avere uno stile di sicurezza.

- Gruppi UNIX

  La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0
pcuser	65534 (creato automaticamente da ONTAP quando si crea la SVM)

- Utenti UNIX

  La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	Necessario per la fase DI INIT GSS Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.
pcuser	65534	65534	Necessario per l'utilizzo multiprotocollo NFS e CIFS Creato e aggiunto automaticamente al gruppo pcuser da ONTAP quando si crea la SVM.
root	0	0	Necessario per il montaggio

L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.

- Policy e regole di esportazione

  È necessario aver configurato i criteri di esportazione con le regole di esportazione necessarie per i volumi root e dati e qtree. Se si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e. `-superuser` per il volume root a. `krb5` , `krb5i`, o. `krb5p`.

- Mappatura dei nomi Kerberos-UNIX

  Se si desidera che l'utente identificato dall'utente client NFS SPN disponga delle autorizzazioni root, è necessario creare una mappatura dei nomi nella directory root.

Informazioni correlate

"Report tecnico di NetApp 4073: Autenticazione unificata sicura"

"Tool di matrice di interoperabilità NetApp"

"Amministrazione del sistema"

"Gestione dello storage logico"

Specificare il dominio ID utente per NFSv4

Per specificare il dominio ID utente, è possibile impostare `-v4-id-domain` opzione.

A proposito di questa attività

Per impostazione predefinita, ONTAP utilizza il dominio NIS per il mapping dell'ID utente NFSv4, se impostato. Se non viene impostato un dominio NIS, viene utilizzato il dominio DNS. Potrebbe essere necessario impostare il dominio ID utente se, ad esempio, si dispone di più domini ID utente. Il nome di dominio deve corrispondere alla configurazione del dominio sul controller di dominio. Non è richiesto per NFSv3.

Fase

1. Immettere il seguente comando:

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