Utilizza Kerberos con NFS per una sicurezza elevata

ONTAP 9

NetApp
April 24, 2024

Sommario

Utilizza Kerberos con NFS per una sicurezza elevata

Panoramica sull'utilizzo di Kerberos con NFS per una maggiore sicurezza

Se nel proprio ambiente viene utilizzato Kerberos per l'autenticazione avanzata, è necessario collaborare con l'amministratore Kerberos per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare la SVM come client Kerberos.

L'ambiente deve soddisfare le seguenti linee guida:

- Prima di configurare Kerberos per ONTAP, l'implementazione del sito deve seguire le Best practice per la configurazione del server e del client Kerberos.
- Se possibile, utilizzare NFSv4 o versioni successive se è richiesta l'autenticazione Kerberos.

  NFSv3 può essere utilizzato con Kerberos. Tuttavia, i benefici di sicurezza completi di Kerberos sono realizzati solo nelle implementazioni ONTAP di NFSv4 o versioni successive.

- Per promuovere l'accesso ridondante al server, è necessario attivare Kerberos su diversi file di dati LIF su più nodi del cluster utilizzando lo stesso SPN.
- Quando Kerberos è attivato su SVM, è necessario specificare uno dei seguenti metodi di sicurezza nelle regole di esportazione per volumi o qtree, a seconda della configurazione del client NFS.
  - `krb5` (Protocollo Kerberos v5)
  - `krb5i` (Protocollo Kerberos v5 con controllo dell'integrità mediante checksum)
  - `krb5p` (Protocollo Kerberos v5 con servizio di privacy)

Oltre al server e ai client Kerberos, è necessario configurare i seguenti servizi esterni affinché ONTAP supporti Kerberos:

- Servizio di directory

  È necessario utilizzare un servizio directory sicuro nel proprio ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS. Non utilizzare NIS, le cui richieste vengono inviate in testo non crittografato e quindi non sono sicure.

- 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.

Verificare le autorizzazioni per la configurazione Kerberos

Kerberos richiede l'impostazione di determinate autorizzazioni UNIX per il volume root SVM e per utenti e gruppi locali.

Fasi

1. Visualizzare le autorizzazioni pertinenti sul volume root SVM:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   Il volume root di SVM deve avere la seguente configurazione:

Nome…	Impostazione in corso…
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	755

   Se questi valori non vengono visualizzati, utilizzare `volume modify` per aggiornarli.

2. Visualizzare gli utenti UNIX locali:

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   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. L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.
root	0	0	Necessario per il montaggio.

   Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-user modify` per aggiornarli.

3. Visualizzare i gruppi UNIX locali:

   `vserver services name-service unix-group show -vserver vserver _name`

   La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0

   Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-group modify` per aggiornarli.

Creare una configurazione di autenticazione Kerberos NFS

Se si desidera che ONTAP acceda a server Kerberos esterni nel proprio ambiente, è necessario prima configurare SVM in modo che utilizzi un'area Kerberos esistente. A tale scopo, è necessario raccogliere i valori di configurazione per il server KDC Kerberos, quindi utilizzare `vserver nfs kerberos realm create` Per creare la configurazione dell'area di autenticazione Kerberos su una SVM.

Di cosa hai bisogno

L'amministratore del cluster deve aver configurato NTP sul sistema di storage, sul client e sul server KDC per evitare problemi di autenticazione. Le differenze di tempo tra un client e un server (disallineamento del clock) sono una causa comune di errori di autenticazione.

Fasi

1. Rivolgersi all'amministratore Kerberos per determinare i valori di configurazione appropriati da fornire con `vserver nfs kerberos realm create` comando.
2. Creare una configurazione di area di autenticazione Kerberos su SVM:

   `vserver nfs kerberos realm create -vserver vserver_name -realm realm_name {AD_KDC_server_values |AD_KDC_server_values} -comment "text"`

3. Verificare che la configurazione dell'area di autenticazione Kerberos sia stata creata correttamente:

   `vserver nfs kerberos realm show`

Esempi

Il seguente comando crea una configurazione del realm Kerberos NFS per SVM vs1 che utilizza un server Microsoft Active Directory come server KDC. L'area di autenticazione Kerberos è AUTH.EXAMPLE.COM. Il server Active Directory è denominato ad-1 e il suo indirizzo IP è 10.10.8.14. L'inclinazione dell'orologio consentita è di 300 secondi (impostazione predefinita). L'indirizzo IP del server KDC è 10.10.8.14 e il numero di porta è 88 (impostazione predefinita). "Microsoft Kerberos config" è il commento.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

Il seguente comando crea una configurazione di autenticazione Kerberos NFS per SVM vs1 che utilizza un KDC MIT. L'area di autenticazione Kerberos è SECURITY.EXAMPLE.COM. L'inclinazione dell'orologio consentita è di 300 secondi. L'indirizzo IP del server KDC è 10.10.9.1 e il numero di porta è 88. Il vendor di KDC è un altro a indicare un vendor UNIX. L'indirizzo IP del server amministrativo è 10.10.9.1 e il numero di porta è 749 (impostazione predefinita). L'indirizzo IP del server delle password è 10.10.9.1 e il numero di porta è 464 (impostazione predefinita). Il commento è "UNIX Kerberos config".

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurare i tipi di crittografia consentiti per NFS Kerberos

Per impostazione predefinita, ONTAP supporta i seguenti tipi di crittografia per NFS Kerberos: DES, 3DES, AES-128 e AES-256. È possibile configurare i tipi di crittografia consentiti per ogni SVM in modo che si adatti ai requisiti di sicurezza per il proprio ambiente specifico utilizzando `vserver nfs modify` con il `-permitted-enc-types` parametro.

A proposito di questa attività

Per una maggiore compatibilità con i client, ONTAP supporta sia la crittografia DES debole che la crittografia AES avanzata per impostazione predefinita. Ciò significa, ad esempio, che se si desidera aumentare la protezione e l'ambiente lo supporta, è possibile utilizzare questa procedura per disattivare DES e 3DES e richiedere ai client di utilizzare solo la crittografia AES.

Si consiglia di utilizzare la crittografia più efficace disponibile. Per ONTAP, cioè AES-256. Verificare con l'amministratore di KDC che questo livello di crittografia sia supportato nell'ambiente in uso.

- L'attivazione o la disattivazione completa di AES (sia AES-128 che AES-256) su SVM è un'interruzione perché distrugge il file DES principal/keytab originale, richiedendo quindi la disattivazione della configurazione Kerberos su tutti i LIF per SVM.

  Prima di apportare questa modifica, verificare che i client NFS non si basino sulla crittografia AES su SVM.

- L'attivazione o la disattivazione DI DES o 3DES non richiede modifiche alla configurazione Kerberos sui LIF.

Fase

1. Attivare o disattivare il tipo di crittografia consentito:

Se si desidera attivare o disattivare…	Attenersi alla procedura descritta di seguito…
DES o 3DES	a. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separare più tipi di crittografia con una virgola. b. Verificare che la modifica sia stata eseguita correttamente: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

AES-128 o AES-256	a. Identificare su quali SVM e LIF Kerberos sono attivati:
	`vserver nfs kerberos interface show`
	
	b. Disattiva Kerberos su tutti i LIF della SVM il cui tipo di crittografia Kerberos NFS consentiva di modificare:
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	Separare più tipi di crittografia con una virgola.
	
	d. Verificare che la modifica sia stata eseguita correttamente:
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. Riabilitare Kerberos su tutti i LIF su SVM:
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. Verificare che Kerberos sia attivato su tutti i LIF:
	`vserver nfs kerberos interface show`

Attivare Kerberos su una LIF dati

È possibile utilizzare `vserver nfs kerberos interface enable` Comando per abilitare Kerberos su una LIF dati. In questo modo, SVM può utilizzare i servizi di sicurezza Kerberos per NFS.

A proposito di questa attività

Se si utilizza un KDC Active Directory, i primi 15 caratteri di qualsiasi SPN utilizzato devono essere univoci tra le SVM all'interno di un'area di autenticazione o di un dominio.

Fasi

1. Creare la configurazione Kerberos NFS:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP richiede la chiave segreta per l'SPN del KDC per abilitare l'interfaccia Kerberos.

   Per i KDC Microsoft, viene contattato il KDC e vengono inviati un prompt di nome utente e password alla CLI per ottenere la chiave segreta. Se è necessario creare l'SPN in un'unità organizzativa diversa dell'area Kerberos, è possibile specificare l'opzione `-ou` parametro.

   Per i KDC non Microsoft, è possibile ottenere la chiave segreta utilizzando uno dei due metodi seguenti:

Se…	È inoltre necessario includere il seguente parametro con il comando…
Disporre delle credenziali di amministratore di KDC per recuperare la chiave direttamente dal KDC	`-admin-username` *`kdc_admin_username`*
Non si dispone delle credenziali di amministratore di KDC, ma di un file keytab del KDC contenente la chiave	`-keytab-uri` {ftp

2. Verificare che Kerberos sia stato attivato su LIF:

   `vserver nfs kerberos-config show`

3. Ripetere i passaggi 1 e 2 per attivare Kerberos su più LIF.

Esempio

Il seguente comando crea e verifica una configurazione Kerberos NFS per la SVM denominata vs1 sull'interfaccia logica ves03-d1, con l'SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM nell'OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```