Configurare il controller NDDB 3.10.4 abilitato per TLS in modalità standalone centralizzata utilizzando il backup

Sommario

Introduzione

In questo documento viene descritta la procedura per ricostruire Nexus Dashboard Data Broker (NDDB) v3.10.4 abilitato per TLS in modalità standalone utilizzando un backup.

Prerequisiti

Requisiti

Prima di avviare il processo di ricostruzione del controller, verificare che i seguenti componenti siano preparati e accessibili:

- Ambiente macchina virtuale: Una macchina virtuale Linux a 64 bit con provisioning di recente in grado di soddisfare i requisiti minimi di sistema.
- Pacchetto software: Il supporto di installazione ufficiale del controller NDDB.
- Backup sistema: il file di backup del sistema più recente.
- Certificati di protezione: i file specifici tlsTrustStore e tlsKeyStore associati al controller per garantire comunicazioni protette.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Hardware: Server rack Cisco UCS C240 M7SX
- Versione Cisco Integrated Management Controller (CIMC): 4.3.6(250053)
- Virtualizzazione/sistema operativo: Red Hat Enterprise Linux (RHEL) 9.5 (64 bit)
- Sistema operativo Virtual Machine (VM): Red Hat Enterprise Linux (RHEL) 9.5 (64 bit)
- Applicazione: NDDB Controller 3.10.4 (Link)
- Metodo di accesso: Tastiera, video, mouse (KVM) per la mappatura dei supporti virtuali
- Utilità di trasferimento file: WinSCP (Windows Secure Copy).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura di backup

Questa procedura è consigliata ai team operativi che gestiscono l'infrastruttura NDDB per stabilire una routine di archiviazione dei dati critici del controller. È essenziale esportare periodicamente il backup del sistema, insieme ai file tlsTrustStore e tlsKeyStore, dal controller attivo per garantire la continuità aziendale.

Nota: Rispettare la strategia di backup definita dall'organizzazione per i backup periodici, assicurandosi che siano accessibili prima di avviare il processo di ricostruzione.

Passaggio 1. Accedere all'istanza GUI NDDB esistente utilizzando https://IP_address:8443/

Passaggio 2. Passare alla scheda Amministrazione > Backup/Ripristino.

Passaggio 3. Fare clic su Backup locale per scaricare la configurazione come file zip.

Passaggio 4. Connettersi alla VM Linux a 64 bit con provisioning tramite WINSCP, passare alla cartella <path>/ndb/configuration e copiare i file tlsTrustStore e tlsKeyStore nel computer locale.

Procedura di ricostruzione

⚠ Attenzione: Configurazione rete e VM: Prima di eseguire il provisioning della nuova VM Linux a 64 bit, verificare che l'istanza del controller originale sia completamente spenta per evitare conflitti di rete o di configurazione. Una volta che l'istanza originale è offline, configurare la nuova VM con lo stesso indirizzo IP dell'originale.

Passaggio 1. SSH su nuova VM Linux ed eseguire questi comandi per creare una directory in cui installare il controller NDDB.

```
mkdir /home/<user>/Desktop/CiscoNDDB
```

✎ Nota: Nota: cambia con l'utente creato durante la ridistribuzione della VM Linux.

Passaggio 2. Scaricare il file di installazione di NDDB Controller da questo collegamento (Cisco Nexus Data Broker Software per la distribuzione centralizzata) e utilizzare WinSCP, copiarlo nella cartella CiscoNDDB (/home/<user>/Desktop/CiscoNDDB) creata nel passaggio 1. Inoltre, copiare il file di configurazione del backup, i file tlsTrustStore e tlsKeyStore di cui viene eseguito il backup. (utilizzando la procedura di backup periodico)

Passaggio 3. Dopo aver copiato tutti i file nella directory CiscoNDDB. Passare alla directory CiscoNDDB ed eseguire questi comandi per installare il software CiscoNDDB.

```
cd /home/<user>/Desktop/CiscoNDDB
unzip ndb1000-sw-app-k9-3.10.4.zip
```

Passaggio 4. Copiare i file tlsTrustStore e tlsKeyStore nella cartella /ndb/configuration:

```
cp /home/<user>/Desktop/CiscoNDDB/tlsTrustStore /home/<user>/Desktop/CiscoNDDB/ndb/configuration/tl
cp /home/<user>/Desktop/CiscoNDDB/tlsKeyStore /home/<user>/Desktop/CiscoNDDB/ndb/configuration/tlsK
```

Passaggio 5. Avviare di nuovo l'istanza NDDB utilizzando i seguenti comandi:

<#root>

```
cd /home/<user>/Desktop/CiscoNDDB/ndb/
```

```
./runndb.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore
```

6. SSH sull'IP del server dei controller e passare al percorso:

```
cd /home/<user>/Desktop/CiscoNDDB/ndb/bin
```

lanciare,

<#root>

```
./ndb config-keystore-passwords --user admin --password admin --url https://
```

ip-address_localhost*

```
:8443 --verbose --prompt --keystore-password
```

keystore_password

```
 --truststore-password
```

truststore_password

```
Please enter your password:  <enter the NDB GUI Default password>
```

Nota:

1. Poiché si tratta di una nuova distribuzione del controller, fino ad ora non è stata impostata alcuna password. La password predefinita è admin.

2. Sostituire ip-address_localhost* con l'indirizzo IP del server controller.

3. Prima di procedere, verificare che i file tlsKeyStore e tlsTrustStore e le password corrispondenti siano stati preparati. Se mancano, fare riferimento alla documentazione Generating TLS 3rd Party Certification Between NDB Server and NDB Switch for NXAPI per rigenerare i certificati necessari utilizzando i file originali con estensione cer e key.

Passaggio 7. Accedere alla nuova istanza dell'interfaccia utente di NDDB utilizzando https://IP_address:8443/.

Passaggio 8. Passare alla scheda Amministrazione > Backup/Ripristino.

Passaggio 9. Fare clic su Ripristina localmente per caricare il file di configurazione di backup copiato in precedenza nel Passaggio 2

Selezionare la casella di controllo Ripristina se si desidera che Nexus Dashboard Data Broker riconfiguri le configurazioni del dispositivo dal backup caricato dopo il riavvio di NDDB. Questi elementi vengono riconfigurati:

· Configurazioni globali

· Configurazioni delle porte

· UDF

· Connessioni

Nota:

1. La casella di controllo Ripristina è compatibile esclusivamente con i file di backup generati da NDB release 3.8 o successive. Tenere presente che l'attivazione di questa opzione comporta la riprogrammazione completa dello switch; la durata di questo processo dipende dalle dimensioni dell'infrastruttura e dal numero totale di criteri. Per evitare tempi di inattività prolungati, evitare di utilizzare questa casella di controllo per i fabric NDDB di grandi dimensioni (oltre 20 switch).

2. Una volta completata la configurazione, viene visualizzato un messaggio di riuscita sulla GUI.

Passaggio 10. Passare a NDDB GUI> Dispositivi > Switch NDB. Verificare che lo stato degli switch NDDB sia GREEN. Se il colore è rosso e selezionare la casella per entrambi gli switch, fare clic su Azione > Riconnetti e attendere 5 minuti.

Se lo stato rimane rosso dopo il periodo di attesa di 5 minuti, selezionare di nuovo gli switch interessati e selezionare Azione > Nuova ricerca.

Avviso: Il rediscover attiva un push delle policy e può causare un breve impatto sul servizio. Eseguire questa azione solo se lo stato dello switch è rosso.

Informazioni correlate

- Guida alla configurazione di Cisco Nexus Dashboard Data Broker, versione 3.10.4

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).