Configure TLS-Enabled NDDB 3.10.4 Controller in Centralized Standalone Mode Using Backup

Contents

Introduction

This document describes the procedure to rebuild a TLS-enabled Nexus Dashboard Data Broker (NDDB) v3.10.4 in Standalone Mode using a backup.

Prerequisites

Requirements

Before initiating the controller rebuild process, ensure these components are prepared and accessible:

- Virtual Machine Environment: A newly provisioned 64-bit Linux virtual machine meeting the minimum system requirements.
- Software Package: The official NDDB Controller installation media.
- System Backup: The most recent system backup file.
- Security Certificates: The specific tlsTrustStore and tlsKeyStore files associated with the controller to ensure secure communication.

Components Used

The information in this document is based on these software and hardware versions:

- Hardware: Cisco UCS C240 M7SX Rack Server
- Cisco Integrated Management Controller (CIMC) version: 4.3.6(250053)
- Virtualization/Operating System: Red Hat Enterprise Linux (RHEL) 9.5 (64-bit)
- Virtual Machine (VM) Operating system: Red Hat Enterprise Linux (RHEL) 9.5 (64-bit)

- Application: NDDB Controller 3.10.4 (Link)
- Access Method: Keyboard, Video, Mouse (KVM) for virtual media mapping
- File Transfer Utility: WinSCP (Windows Secure Copy).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Backup Procedure

This procedure is recommended for operations teams managing the NDDB Fabric to establish a routine for archiving critical controller data. It is essential to periodically export the system backup, along with the tlsTrustStore and tlsKeyStore files, from the active controller to ensure business continuity.

Note: Adhere to the Backup Strategy as per your organization for periodic backups, ensuring they are accessible before starting the rebuild process.

Step 1. Log in to the existing NDDB GUI instance using https://IP_address:8443/

Step 2. Navigate to the **Administration > Backup/ Restore** tab.

Step 3. Click **Backup Locally** to download the configuration as a zip file.

Step 4. Connect to 64-Bit Provisioned Linux VM using WINSCP, Navigate to the <path>/ndb/configuration folder and copy the tlsTrustStore and tlsKeyStore files to your local machine.

Rebuild Procedure

Caution: VM and Network Configuration: Before provisioning the new 64-bit Linux VM, ensure the original controller instance is fully powered off to prevent network or configuration conflicts. Once the original instance is offline, configure the new VM with the same IP address as the original.

Step 1. SSH to New Linux VM and run these commands to make directory to install NDDB controller.

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

Note: Note: change with user that is created while redeploying Linux VM.

Step 2. Download NDDB Controller Installation file from this link (Cisco Nexus Data Broker Software for centralized deployment) and using WinSCP, copy it to the CiscoNDDB folder (/home/<user>/Desktop/CiscoNDDB) created in **Step 1.** Also, copy the backup configuration file, the tlsTrustStore and tlsKeyStore files which are backed up. (using the periodic backup procedure)

Step 3. Once all the files are copied to CiscoNDDB directory. Navigate to the CiscoNDDB directory and run these command to install the CiscoNDDB Software.

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

Step 4. Copy the tlsTrustStore and tlsKeyStore files to /ndb/configuration folder:

```
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
```

Step 5. Start the NDDB instance again using these commands:

<#root>

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

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

Step 6 SSH to *Controller Server IP and* Navigate to path:

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

run,

<#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>
```

Note:

1. Since this is new controller deployment and no password has been set till now. The default password is **admin**.

2. Replace **ip-address_localhost*** with Controller server IP.

3. Ensure the tlsKeyStore and tlsTrustStore files and their corresponding passwords are prepared before proceeding. If these are missing, please refer to the documentation titled Generating TLS 3rd Party Certification Between NDB Server and NDB Switch for NXAPI to regenerate the necessary certificates using your original .cer and .key files.

Step 7. Log in to the new instance of the NDDB GUI using https://IP_address:8443/.

Step 8. Navigate to the **Administration** > **Backup/ Restore** tab.

Step 9. Click Restore Locally to upload the Backup configuration file which copied earlier in **Step 2**

Select the **Restore** check-box if you want Nexus Dashboard Data Broker to re-configure the configurations of the device, from the uploaded backup after NDDB is restarted. These are reconfigured:

- Global Configurations
- Port Configurations
- UDF
- Connections

Note:

---

1. The **Restore** checkbox is compatible exclusively with backup files generated from NDB Release 3.8 or later. Be aware that enabling this option triggers a full switch reprogramming; the duration of this process depends on the fabric size and the total number of policies. To prevent extended downtime, avoid using this checkbox for large NDDB Fabrics (exceeding 20 switches).

2. Upon successful configuration upload, a success message is visible on the GUI.

Step 10. Navigate to NDDB GUI> Devices > NDB Switches. Check the **NDDB Switches status is GREEN**. In case, it is red and **Check the Box for both switches**, click on **Action > Reconnect** and wait for 5 minutes.

If the status remains red after the 5-minute wait period, select the affected switches again and navigate to **Action > Rediscover**.

Warning: **Rediscover** triggers a policy push and can cause brief service impact. Only perform this action if the switch status is red.

Related Information

- Cisco Nexus Dashboard Data Broker Configuration Guide, Release 3.10.4