

使用备份在集中式独立模式下配置启用TLS的 NDDB 3.10.4控制器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[备份过程](#)

[重建过程](#)

[相关信息](#)

简介

本文档介绍使用备份在独立模式下重建启用TLS的Nexus控制面板数据代理(NDDB)v3.10.4的过程。

先决条件

要求

在启动控制器重建过程之前，请确保这些组件已准备就绪且可以访问：

- 虚拟机环境：新调配的64位Linux虚拟机符合最低系统要求。
- 软件包：官方NDDB控制器安装介质。
- 系统备份：最新的系统备份文件。
- 安全证书：与控制器关联的特定tlsTrustStore和tlsKeyStore文件，以确保安全通信。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Hardware: Cisco UCS C240 M7SX机架式服务器
- 思科集成管理控制器(CIMC)版本：4.3.6(250053)
- 虚拟化/操作系统：Red Hat Enterprise Linux(RHEL)9.5 (64位)
- 虚拟机(VM)操作系统：Red Hat Enterprise Linux(RHEL)9.5 (64位)

- 应用：NDDDB控制器3.10.4([链路](#))
- 接入方法:用于虚拟媒体映射的键盘、视频、鼠标(KVM)
- 文件传输实用程序：WinSCP(Windows Secure Copy)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

备份过程

建议对管理NDDDB交换矩阵的运营团队执行此过程，以建立用于存档关键控制器数据的例程。从活动控制器定期导出系统备份以及tlsTrustStore和tlsKeyStore文件对于确保业务连续性至关重要。



注意：根据您的组织，遵循备份策略进行定期备份，确保在开始重建过程之前可以访问这些备份。

步骤1.使用https://IP_address:8443/登录到现有的NDDDB GUI实例

第2步：导航到Administration > Backup/Restore选项卡。

步骤3.点击本地备份(Backup Locally)将配置下载为zip文件。

步骤4.使用WINSOCP连接到64位调配的Linux虚拟机，导航到<path>/ndb/configuration文件夹，并将tlsTrustStore和tlsKeyStore文件复制到本地计算机。

重建过程



警告：虚拟机和网络配置：在调配新的64位Linux VM之前，请确保原始控制器实例已完全断电，以防止网络或配置冲突。原始实例离线后，使用与原始实例相同的IP地址配置新VM。

步骤1.通过SSH连接到新的Linux虚拟机，并运行这些命令以创建目录来安装NDDDB控制器。

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



注意：注意：使用重新部署Linux VM时创建的用户进行更改。

Step 2. 从该链接下载NDDDB控制器安装文件(用于集中部署的[Cisco Nexus数据代理软件](#))并使用WinSCP，将其复制到第1步中创建的CiscoNDDDB文件夹(/home/<user>/Desktop/CiscoNDDDB)。此外，复制备份配置文件、tlsTrustStore和tlsKeyStore文件。(使用定期备份过程)

步骤3.将所有文件复制到CiscoNDDDB目录之后。导航到CiscoNDDDB目录并运行以下命令以安装CiscoNDDDB软件。

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

步骤4.将tlsTrustStore和tlsKeyStore文件复制到/ndb/configuration文件夹中：

```
cp /home/<user>/Desktop/CiscoNDDDB/tlsTrustStore /home/<user>/Desktop/CiscoNDDDB/ndb/configuration/tlsTrustStore
cp /home/<user>/Desktop/CiscoNDDDB/tlsKeyStore /home/<user>/Desktop/CiscoNDDDB/ndb/configuration/tlsKeyStore
```

步骤5.使用以下命令再次启动NDDDB实例：

<#root>

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

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

第6步SSH到控制器服务器IP并导航到路径：

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

运行，

<#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>



注意：

1. 由于这是新的控制器部署，并且直到现在才设置密码。默认密码是 admin。
2. 将 *ip-address_localhost** 替换为控制器服务器 IP。
3. 确保在继续之前已准备 `tlsKeyStore` 和 `tlsTrustStore` 文件及其相应的密码。如果缺少这些证书，请参阅标题为 [在NDB服务器和NDB交换机之间为NXAPI生成TLS第三方认证](#) 的文档，以使用原始 `.cer` 和 `.key` 文件重新生成必要的证书。

步骤7. 使用 `https://IP_address:8443/` 登录到 NDDB GUI 的新实例。

第8步：导航到 Administration > Backup/ Restore 选项卡。

步骤9. 单击本地还原 (Restore Locally)，上传之前在步骤2中复制的备份配置文件

如果希望 Nexus 控制面板数据代理在 NDDB 重新启动后从上传的备份中重新配置设备的配置，请选择 Restore 复选框。这些配置已重新配置：

· 全局配置

· 端口配置

· UDF

· 连接



注意：

1. Restore复选框仅与从NDB 3.8版或更高版本生成的备份文件兼容。请注意，启用此选项会触发完整的交换机重新编程；此过程的持续时间取决于交换矩阵大小和策略总数。要防止长时间停机，请避免使用大型NDDDB交换矩阵（超过20台交换机）的此复选框。

2.成功上传配置后，GUI上会显示成功消息。

步骤10.导航到NDDDB GUI> Devices > NDB Switches。检查NDDDB Switches status is GREEN。如果其为红色且选中两台交换机的Box，请点击Action > Reconnect，并等待5分钟。

如果在5分钟等待时间后状态保持红色，请再次选择受影响的交换机，然后导航到操作>重新发现。



警告：重新发现会触发策略推送，并可能导致短暂的服务影响。仅当交换机状态为红色时才执行此操作。

相关信息

- [Cisco Nexus控制面板数据代理配置指南，版本3.10.4](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。