Troubleshoot Tunnel Provisioning Issues

Problem

Require guidance on troubleshooting issues related to tunnel provisioning failures by examining server logs and adjusting logging levels.

Solution

Use server.log Command

Here are the steps to troubleshoot tunnel provisioning issues:

1. Login to the Cisco IoT FND server using the SSH command.
2. Navigate to the directory where your logs are stored using the cd command. For example: `/opt/fnd/logs` or `/opt/cgms/server/cgms/logs/`.
3. Run the `server.log` command to view the log files.

Use Cisco IoT FND GUI

1. Login to Cisco IoT FND.
2. From the Cisco IoT FND menubar, choose **ADMIN** > **Logging** > **Log Level Settings**.
3. Ensure that **Tunnel Provisioning** option is checked.
4. Choose the **Log Level** as **Debug**.

Identify Issues In Logs

Look for specific error messages in the logs. For example, a common issue is the **Tunnel provisioning request queue is full**. This error indicates that the request queue has reached its capacity and new requests are being dropped.

Understand the Queue Limitation

Until Cisco IoT FND Release 4.12.1, the tunnel provisioning queue size is limited to 12 requests. If the queue is full, additional requests are not processed.

Resolution

- Consider upgrading to a Cisco IoT FND version later than Cisco IoT FND Release 4.12. The queue size is increased.
- Try restarting Cisco IoT FND which might temporarily resolve the issue by clearing the queue.

Troubleshoot Zero Touch Deployment

Problem

Unable to find the process for Zero Touch Deployment (ZTD) related to tunnel provisioning in a network setup.

Solution

Here are the steps involved in ZTD for tunnel provisioning:

1. Register your device on Cisco IoT FND.
2. Ensure that the FAR is booted and connected to WAN.
3. Obtain the initial configuration settings.
4. Request a Local Device Identifier (LDevID) certificate from a Public Key Infrastructure (PKI) or Registration Authority (RA).
5. Communicate with the Tunnel Provisioning Service (TPS) to initiate tunnel setup.
6. Establish a FlexVPN tunnel to the HER.
7. The FAR contacts the Cisco IoT FND for device registration.
8. The configuration is sent from Cisco IoT FND to FAR.
9. The FAR is fully operational and registered in the Cisco IoT FND.

Here's an example tunnel provisioning log:

```
Received tunnel provisioning request from [IR1101-K9+FCW22520078]
Adding tunnel provisioning request to queue for FAR ID=
Provisioning tunnels on element [IR1101-K9+FCW22520078]
Retrieved current configuration of element [IR1101-K9+FCW22520078] before tunnel provisioning
Retrieved status of file [flash:/before-registration-config] on [IR1101-K9+FCW22520078].
File does not exist
Retrieved status of file [flash:/before-tunnel-config] on [IR1101-K9+FCW22520078]. File
does not exist.
```

```
Copied running-config of [IR1101-K9+FCW22520078] to [flash:/before-tunnel-config]
Opened a NETCONF session with element [HTABT-TGOT-DC-RT1] at [163.88.181.2]
Sending [show interfaces | include Description: | Encapsulation | address is | line protocol
 | packets input, | packets output, | Tunnel protection | Tunnel protocol| Tunnel source]
to element [HTABT-TGOT-DC-RT1]
Received response to [show interfaces | include Description: | Encapsulation | address is
| line protocol | packets input, | packets output, | Tunnel protection | Tunnel protocol|
Tunnel source] from element [HTABT-TGOT-DC-RT1]
Sending [show ip nhrp | include ^[0-9A-F]| Tunnel| NBMA] to element [HTABT-TGOT-DC-RT1]
Received response to [show ip nhrp | include ^[0-9A-F]| Tunnel| NBMA] from element
[HTABT-TGOT-DC-RT1]
Sending [show ipv6 nhrp | include ^[0-9A-F]| Tunnel| NBMA] to element [HTABT-TGOT-DC-RT1]
Received response to [show ipv6 nhrp | include ^[0-9A-F]| Tunnel| NBMA] from element
[HTABT-TGOT-DC-RT1]
Sending [show ipv6 interface | include address | protocol | subnet] to element
[HTABT-TGOT-DC-RT1]
Received response to [show ipv6 interface | include address | protocol | subnet] from element
 [HTABT-TGOT-DC-RT1]
Closed NETCONF session with element [HTABT-TGOT-DC-RT1]
Obtained current configuration of element [HTABT-TGOT-DC-RT1] before tunnel provisioning
Configured tunnels on [IR1101-K9+FCW22520078]
Retrieved current configuration of element [IR1101-K9+FCW22520078] after tunnel provisioning.
Processed tunnel template for element [ASR1001+93UA2TVWZAR]. Time to process [5 ms].
Configured element [IR1101-K9+FCW223700AG] to register with IoT-FND at
[https://10.48.43.229:9121/cgna/ios/registration]
```

Note

- If the router tunnel addition template is empty, Cisco IoT FND proceeds with the standard registration process.
- Cisco IoT FND establishes a rollback point to ensure that the the Cisco Connected Grid Router (CGR) can revert to a trusted configuration. This is crucial before attempting tunnel provisioning or further device configuration phases. During the process, different configuration files are generated to serve as trust points. These files enable FND to revert the CGR's configuration if there are trust issues or if specific updates are needed. The configuration files are stored in the CGR's flash memory.
- Establish a rollback point to support the provisioning of new tunnel configurations.

Troubleshoot Tunnel Provisioning DHCP Configuration Issue

Problem

Seeing a **Tunnel Provisioning Failure** event in the Cisco IoT FND logs.

Solution

You need to monitor the address allocation process using the following steps:

1. Check the Cisco IoT FND server.log file to determine if Cisco IoT FND is sending a DHCP request during tunnel provisioning.
2. Check the DHCP server.log file to determine if the DHCP request from Cisco IoT FND reached the DHCP server.

3. If the requests are not reaching the server. From the Cisco IoT FND menubar, choose **ADMIN** > **System Management** > **Provisioning Settings** and ensure that the DHCP **Server Address** is right.
4. Check for network problems between Cisco IoT FND server and the DHCP server.
5. Analyze the DHCP server log files to identify errors in the configuration and fix them.

Example

The Cisco Connected Grid Routers time out during Tunnel Provisioning and then rollback to before-tunnel-config repeatedly:

Error seen in server.log:

```
238471507: imcltcgnmsp01: Dec 13 2017 03:24:03.709 +0000: %CGMS-3-UNSPECIFIED:
%[ch=CiscoIosTunnelProvServlet$CiscoIosTunnelProvProcess][eid=CGR1240/K9+FTX2130G06C][ip=10.189.110.137][sev=ERROR][tid=IOS
 CGR Tunnel-892]: Tunnel provisioning request for element [CGR1240/K9+FTX2130G06C] failed
[com.cisco.cgms.dhcp.proxyclient.v4.TimeoutWaitingForOfferException: Timed out waiting for
 a DHCPOFFER message].
```

In the above error, you can see that the Cisco IoT FND server has sent a DHCPDISCOVER request and is waiting for a DHCPOFFER message from the DHCP server and it times out waiting.

Here are the DHCP logs:

```
Bluecat DHCP: Customer's DHCP
Dec 13 15:24:44 cltuofdhcp dhcpd: DHCPRELEASE of 10.190.140.110 from 00:00:00:00:00:00 via
 10.200.230.34 (found)
Dec 13 15:24:44 cltuofdhcp dhcpd: DHCPDISCOVER from 00:00:00:00:00:00 via 10.200.230.34
Dec 13 15:24:45 cltuofdhcp dhcpd: DHCPOFFER on 10.190.140.110 to 00:00:00:00:00:00 via
10.200.230.34
Dec 13 15:24:45 cltuofdhcp dhcpd: DHCPREQUEST for 10.190.140.110 (10.200.230.33) from
00:00:00:00:00:00 via 10.200.230.34
Dec 13 15:24:45 cltuofdhcp dhcpd: DHCPACK on 10.190.140.110 to 00:00:00:00:00:00 via
10.200.230.34
Dec 13 15:24:46 cltuofdhcp dhcpd: DHCPDISCOVER from 00:00:00:00:00:00 via 10.200.230.34:
network 10.190.192.0/18: no free leases
Dec 13 15:24:50 cltuofdhcp dhcpd: DHCPDISCOVER from 00:00:00:00:00:00 via 10.200.230.34:
network 10.190.192.0/18: no free leases
Dec 13 15:24:58 cltuofdhcp dhcpd: DHCPDISCOVER from 00:00:00:00:00:00 via 10.200.230.34:
network 10.190.192.0/18: no free leases
```

From the above logs, you can see that there is an issue which prevents IPs in the 10.190.192.0/18 scope from being allocated. DHCP configuration needs to be fixed in order for tunnel provisioning to work in this case.

Troubleshoot Incorrect CGNA Profile URL

Problem

Seeing an incorrect CGNA profile configuration URL error.

Solution

Verify if you've entered the URL in the right format. The right format of the CGNA profile configuration URL is https://<FND IP>:9120/cgna/ios/tunnel

Troubleshoot HER FlexVPN

Problem

Unable to configure the FlexVPN client on a Cisco Connected Grid Router (CGR).

Solution

Here are the instructions to configure the FlexVPN on a Cisco Connected Grid Router:

1. Access the Cisco Connected Grid Router's configuration using the SSH command.
2. Run `show running-config`, `show crypto ikev2 sa`, and `show cypto ipsec sa` to review the FlexVPN configuration.
3. Use `show interfaces` to check the status of the dynamically created tunnel interface.
4. Verify that the tunnel interface associated with FlexVPN is up and running.
5. Run `show logging` and review the logs for any errors or warnings related to FlexVPN.
6. Look for messages indicating issues in tunnel establishment or connectivity.
7. Use `show template` to review the applied templates and confirm if they match the intended configuration for FlexVPN.

   Verify that the HER FlexVPN configuration on the Cisco IOS Connected Grid Router is set up and operational. This ensures that the CGR can dynamically create tunnel endpoints and maintain secure communication with the HER.

Troubleshoot Profile Environment Variable

Problem

Need to verify that the correct profile is configured for the `ZTD_SCEP_CGNA_Profile` environment variable.

Solution

You'll need to check the Cisco Global Network Architecture (CGNA) profile settings on your device:

1. Login to the device using the SSH command.
2. Run `show cgna profile-all` and see all the configured CGNA profiles and check which one is active.
3. Look for `ZTD_SCEP_CGNA_Profile` environment variable ensuring it is set to the intended profile.
4. Confirm that the TCL script `tm_ztd_scep.tcl` has run without errors. This script is responsible for activating the correct CGNA profile.
5. Ensure that the LDevID certificate is correctly retrieved from the PKI, as this is necessary for the profile activation.
6. Check logs for any errors or warnings that might indicate problems with profile configuration or activation.

Debug FAR Devices Using Commands

Problem

Unable to debug FAR devices.

Solution

Here are the instructions to debug FAR devices using commands:

1. Login to Cisco IoT FND server as root using the SSH command.
2. Run the following commands to debug FAR devices:

   ```
   show crypto session
   debug crypto ikev2
   debug crypto ipsec
   ```

   You see the debugging logs for you to take action on.

Verify TPS and DNS Connectivity

Problem

How to ensure TPS and DNS connectivity?

Solution

Here are the steps to ensure TPS and DNS connectivity:

1. Ensure that the TPS service is running on Cisco IoT FND.
2. Review the TPS proxy logs located at: `/opt/cgms-tpsproxy/log/tpsproxy.log` to identify any issues.
3. If a Fully Qualified Domain Name (FQDN) is used, ensure the CGNA profile correctly resolves the TPS FQDN through the DNS.
4. Verify connectivity between the DNS and the FAR. Attempt to ping the TPS FQDN from the FAR to confirm connectivity.
5. Ensure the DNS records are correctly set up to resolve the TPS FQDN. This involves checking the DNS server for accurate entries.
6. Check the TPS FQDN configuration in the CGNA URL to ensure it is correctly set up and pointing to the intended server.

Verify Tunnel Configuration Information

Problem

Unable to verify the tunnel configuration information.

Solution

Here are the steps to verify the tunnel configuration information:

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Tunnel Provisioning** > **Router Tunnel Addition**.
2. You can see the entire router tunnel addition information in the tab.