Installing and Configuring the CGDS Monitor

This chapter provides instructions on how to install and configure the CGDS Monitor on a server platform that is validated or certified by Cisco.

- About the Server and CGDS Monitor, page 2-1
- Installing and Configuring the CGDS Monitor, page 2-1
- Configuring the Network in the CGDS Server, page 2-4
- Configuring the Property File, page 2-6
- Accessing the CGDS Monitor, page 2-8

About the Server and CGDS Monitor

The CGDS application is tested and validated to work on either of the following servers:

- UCS C220 Non-Hardened Substation Server
- Advantech UNO-4683 Hardened Substation Server

The construction of the hardened server is optimized for harsh operating environments that are likely to exist within an electrical substation. The server is certified to be both IEEE 1613 and IEC 61850 compliant.

Run an ISO image taken from the CGDS CD on a bare UCS or Advantech box to configure the server for the CGDS Substation Workbench and install the CGDS Monitor.

The key features of the CGDS Monitor include:

- Discovery of switches and routers (including non-Cisco devices) and IEDs using the DNP, GOOSE, and SNMP protocols.
- Performance monitoring includes traffic Analysis and latency.
- Generic Object Oriented Substation Events (GOOSE) event analysis for the IED messages.
- Events and alarms.

The Substation Workbench provides the ability to monitor the GOOSE capture, performance monitoring, and sending alerts to the CGDS Monitor when abnormalities occur.

Installing and Configuring the CGDS Monitor

Install the CGDS Monitor on the UCS C220 M3 server from the CGDS Linux CD.

Send documentation feedback to cgds-docfeedback@cisco.com

- Verifying the Installation Media, page 2-2
- Prerequisites, page 2-2
- Installing the CGDS Monitor, page 2-3
- Configuring the Network in the CGDS Server, page 2-4
- Accessing the CGDS Monitor, page 2-8

Verifying the Installation Media

The hash code is used to validate the CGDS CD. The hash code is published with the CD. Verify whether the actual hash code matches with the hash code in the CD by entering the following command in the boot prompt:

```
linux mediacheck
```

If the hash code does not match, contact the Cisco representative for replacing the CD.

Prerequisites

Gather the information as specified in the "Collecting Required Information" section on page 1-1 before you start your installation.

The prerequisites for installing the CGDS Monitor are as follows:

1. Ensure that a virtual drive is created. For more information on how to create a virtual drive, see the "Creating a Virtual Drive" section on page 2-2.
2. Ensure that a copy of the CGDS ISO image is taken from the CGDS CD to the local machine.
3. Ensure that the Cisco Integrated Management Controller (CIMC) is upgraded to the latest version.

Creating a Virtual Drive

To create a virtual drive, perform the following steps:

Step 1 If the hard drive is a SATA, it is directly connected to the BIOS and can be configured using the booting menu.

Step 2 If the hard drive is a SAS, it needs to be configured through RAID.

To configure the hard drive through RAID, do the following:

a. Create an array.
b. Create a disk.
c. Select the disk as a bootable device.
d. Activate the disk.

Send documentation feedback to cgds-docfeedback@cisco.com

Installing the CGDS Monitor

To install the CGDS Monitor, perform the following steps:

Step 1 Log in to the CIMC.

Step 2 Insert the CGDS CD in your computer.

Step 3 Change the boot order to boot the system from the CDROM.

To change the boot order, do the following:

a. In the Server pane, click **BIOS**.
b. In the Actions area, click **Configure Boot Order**.
c. Click **OK**.
d. The Configure Boot Order page appears.
e. Click **CDROM**.
f. Click **Up**.
g. Click **Apply**.

Step 4 In the Actions area, click the **Launch KVM Console** link.

Step 5 In the KVM Console, click **Virtual Media**.

The Initializing connection dialog box appears.

Step 6 Click **Cancel**.

Step 7 Click **Add Image**.

Step 8 Navigate to the location where you have saved the copy of the CGDS ISO image on your local machine, and select the ISO image.

Step 9 Select the **Mapped** check box.

The ISO image is loaded on to the virtual media.

Step 10 From the Macros menu, choose **Ctrl-Alt-Del**.

The system restarts and boots from the CGDS installation CD.

Step 11 In the boot prompt, enter **Install** and press **Enter**.

The installation process is started. The KVM tab displays the progress of the installation process. Once the installation is done, the system automatically reboots.

Step 12 When rebooting, in the CIMC, change the boot order to boot the system from the HDD.

To change the boot order, do the following:

a. In the Server pane, click **BIOS**.
b. In the Actions area, click **Configure Boot Order**.
c. Click **OK**.
d. The Configure Boot Order page appears.
e. Click **HDD**.
f. Click **Up**.
g. Click **Apply**.

Once the installation is done, the system prompts to enter the CGDS credentials.

Send documentation feedback to cgds-docfeedback@cisco.com

Step 13 Enter the CGDS credentials that are provided with the ISO image.

The system prompts you to change the default password.

Step 14 Enter the current password.

```
Enter current password:
```

Step 15 Enter the new password and re-enter the password in the appropriate prompts.

```
Enter new password:
Re-type new password:
```

The Main menu appears.

Step 16 Enter one of the following alphabets and press **Enter** to choose a menu option for configuration:

- a—System Settings
- b—System Accounts
- c—Services Control
- d—Troubleshooting
- e—CGDS Administration
- X—Exit

Step 17 Enter X and press **Enter** to exit the Main menu.

Configuring the Network in the CGDS Server

To configure the network or application after installation, perform the following steps:

Step 1 Log in to the CIMC.

Step 2 In the Actions area, click the **Launch KVM Console** link.

The KVM Console appears.

Step 3 Enter the user name and password in the following prompts:

```
cgds login:
Password:
```

The Main menu appears with the following menu options:

  - a—System Settings
  - b—System Accounts
  - c—Services Control
  - d—Troubleshooting
  - e—CGDS Administration
  - X—Exit

Step 4 Enter **e** and press **Enter**.

The CGDS Administration page appears with the following menu options:

  - a—Configure Bridge Network

Send documentation feedback to cgds-docfeedback@cisco.com

- b—Show Bridge
- c—Install NAM
- d—NAM Console
- e—Show VMs
- R or < or ,—Return to prior menu

Step 5 Enter **a** and press **Enter**.

The content of the ifcfg-bridge0 file is displayed.

Step 6 Enter the following details:

- IPADDR=<*IP_address*>
- NETMASK=<*Netmask*>
- GATEWAY=<*Gateway_address*>
- DELAY=<*Delay*>

Step 7 Enter **:wq** and press **Enter** to save the file.

The system displays the following message after saving the file:

```
Press any key to return to the main menu.
```

When you press any key, the system displays the CGDS Administration menu.

Step 8 Enter **R** or **<** or **,** and press **Enter** to return to the prior menu.

The main menu appears.

After configuring the network address, restart the system by executing Step 9 through Step 13.

Step 9 Enter **c** and press **Enter**.

Step 10 The Service Control page appears with the following menu options:

- a—Networking
- R or < or ,—Return to prior menu

Step 11 Enter **a** and press **Enter**.

Step 12 The Networking page appears with the following menu options:

- a—Restart Networking
- R or < or ,—Return to prior menu

Step 13 Enter **a** and press **Enter** to restart the system.

Once the system is restarted, the system displays the following message:

```
Press any key to return to the main menu.
```

The set network configuration is applied to the system.

Step 14 In the main menu, enter **e** and press **Enter**.

The CGDS Administration page appears with the following menu options:

- a—Configure Bridge Network
- b—Show Bridge
- c—Install NAM
- d—NAM Console

Send documentation feedback to cgds-docfeedback@cisco.com

- e—Show VMs
- R or < or ,—Return to prior menu

Step 15 Enter **d** and press **Enter**.

The NAM console appears.

Step 16 To set the IP address for the NAM console, enter the following commands:

```
#ip address <ip_address> <subnet_mask>
#ip gateway <gateway_address>
#ip http server enable
```

The system prompts you to enter the NAM credentials.

Step 17 Enter the username as **admin** and the password as **ciscocisco**.

Note If the credentials of the NAM are changed, update the credentials in the discovery.config file that is available in the webwsma_2.war file.

Step 18 Enter **Exit** and press **Enter**.

The system logs out of the NAM console.

Step 19 Press **Ctrl+]**.

The system displays the following message:

```
Press any key to return to the main menu.
```

When you press any key, the system displays the main menu.

Configuring the Property File

You can configure the property file in one of the following situations:

- During a fresh installation of the CGDS.
- Whenever the CGDS server IP address or the NAM IP address is updated.
- After applying patches to the CGDS.

The prerequisites for configuring the property file are as follows:

1. Ensure that the network configuration is completed in the CGDS server. For more information on the network configuration, see the "Configuring the Network in the CGDS Server" section on page 2-4.
2. Ensure that the following details are updated in the config.sh file:
   - The IP address of the NAM console.
   - The port number of the Tomcat server.

To configure the property file, perform the following steps:

Step 1 Log in to the Putty tool.

Step 2 Navigate to the config.sh file that is located in the following path:

Send documentation feedback to cgds-docfeedback@cisco.com

/opt/cisco/cgds/bin

Step 3 Run the following command:

```
./config.sh
```

Step 4 Navigate to the ssl.conf file that is located in the following path:

/etc/httpd/conf.d

Step 5 Replace the port numbers from 8085 to 8080.

Step 6 Restart the httpd service.

Step 7 Stop the Tomcat service.

Step 8 Navigate to the following path:

/opt/cisco/apache/tomcat/webapps/CGDS/WEB-INF/classes

Step 9 Open the Config.properties file in edit mode.

Step 10 Update the lines as follows:

- iepLoginService = http://{CGDS_SERVER_IP}:8283/services/iep/logout—Replace this line with the following line:**iepLogoutService = http://{CGDS_SERVER_IP}:8283/services/iep/logout**
- identityService = https://{CGDS_SERVER_IP}:9449/carbon/userstore/index.jsp?region=region1&item=userstores_menu

Step 11 Start the Tomcat service.

Step 12 Untar the CGDS.war file, and copy the axis2.xml file from CGDSWAR_Exploded locations/esb to /opt/cisco/wso2/wso2esb/repository/conf/axis2/.

Step 13 Open the carbon.xml file that is located in the /opt/cisco/wso2/wso2esb/repository/conf/ path in edit mode.

Step 14 Update the lines as follows:

- <!--HostName>www.wso2.org</HostName-->—Replace this line with the following line: **<HostName>CGDS_SERVER_IP</HostName>**
- <ServerURL>local:/${carbon.context}/services/</ServerURL>—Comment the line as follows: **<!--<ServerURL>local:/${carbon.context}/services/</ServerURL-->**
- <!--<ServerURL>https://${carbon.local.ip}:${carbon.management.port}${carbon.context}/services/</ServerURL> -->—Replace this line with the following line: **<ServerURL>https://CGDS_SERVER_IP:${carbon.management.port}${carbon.context}/services/</ServerURL>**

Step 15 Open the carbon.xml file that is located in the /opt/cisco/wso2/wso2is/repository/conf/ path in edit mode

- <HostName>localhost</HostName>—Replace this line with the following line: **<HostName> CGDS_SERVER_IP </HostName>**
- <ServerURL>local:/${carbon.context}/services/</ServerURL>—Comment the line as follows: **<!--<ServerURL>local:/${carbon.context}/services/</ServerURL -->**
- <!--<ServerURL>https://${carbon.local.ip}:${carbon.management.port}${carbon.context}/services/</ServerURL> -->—Replace this line with the following line: **<ServerURL>https://CGDS_SERVER_IP:${carbon.management.port}${carbon.context}/services/</ServerURL>**

Step 16 Restart the wso2esb and wso2is services.

Send documentation feedback to cgds-docfeedback@cisco.com

The properties that are required for the CGDS server are configured.

Accessing the CGDS Monitor

Once the installation is complete, you can use the CGDS Monitor to perform network analysis on the substation data.

You can access the CGDS Monitor from any system in the substation network. The URL format to access the CGDS Monitor is as follows:

https://<*CGDS_Server_IP_Address*>/CGDS