CX Cloud Agent FAQ and Troubleshooting Guide

Contents

Introduction

This document includes frequently asked questions and troubleshooting scenarios that users may encounter while working with the CX Cloud Agent.

Deployment

Q. Is URL redirection to cloudfront.net an expected behaviour when connecting to CX Cloud backend domain?

A. Yes, for some specific deployment scenarios the redirection to cloudfront.net is expected. Ounbound access should be allowed with redirection enabled on port 443 for these FQDN’s.

Q. With the "Re-install" option, can the user deploy the new CX Cloud Agent with a new IP Address?

A. Yes

Q. What file formats are available for installation?

A. OVA and VHD

Q. On which environment can the installable be deployed?

A. For OVA

- VMWare ESXi version 5.5 or later
- Oracle Virtual Box 5.2.30 or later

For VHD

- Windows Hypervisor 2012 to 2016

Q. Can CX Cloud Agent detect an IP address in a DHCP environment?

A. Yes, the IP address assignment during IP configuration is detected. However, the IP address change expected for the CX Cloud Agent in the future is not supported. It is recommended that customers reserve the IP for the CX Cloud Agent in their DHCP environment.

Q. Does CX Cloud Agent support both IPv4 and IPv6 configuration?

A. No, only IPV4 is supported.

Q. During IP configuration, is IP address validated?

A. Yes, IP address syntax and duplicate IP address assignment are validated.

Q. How long does it take for OVA deployment and IP configuration?

A.The OVA deployment depends on the speed of the network copying the data. IP configuration takes approximately 8-10 minutes including Kubernetes and container creations.

Q. Are there any limitations with respect to any hardware types?

A. The host machine on which OVA is deployed must meet the requirements provided as part of the CX portal setup. The CX Cloud Agent is tested with VMware/Virtual box running on a hardware with Intel Xeon E5 processors with vCPU to CPU ratio set at 2:1. If a less powerful processor CPU or larger ratio is used, the performance can degrade.

Q. Can the pairing code be generated anytime?

A. No, the pairing code can only be generated when the CX Cloud Agent is not registered.

Q. What are the bandwidth requirements between Cisco Catalyst Centers (for upto 10 clusters or 20 non-clusters) and CX Cloud Agent?

A.Bandwidth is not a constraint when the CX Cloud Agent and Cisco Catalyst Center are in the same LAN/WAN network in the customer environment. The minimum required network bandwidth is 2.7Mbit/sec for inventory collections of 5000 devices +13000 Access Points for an Agent to Cisco Catalyst Center connection. If syslogs are collected for Level 2 insights, the minimum required bandwidth is 3.5 Mbits/sec covers for 5000 devices +13000 Access Points for inventory, 5000 devices syslogs and 2000 devices for scans - all run in parallel from CX Cloud Agent..

Q. How the Agent syslogs can be accessed for monitoring the CX Cloud Agent Virtual Machine (VM)?

A. Syslogs for Agent VM can be accessed from the local VM login using the following two paths:

/var/log/syslog.1 (accessed via cxcadmin and cxcroot logins)

/var/log/syslog (accessed using root)

Releases and Patches

Q. What are the different kinds of versions listed for the upgrade of CX Cloud Agent?

A. Shown here are the set of the released versions of CX Cloud Agent that are listed:

- A.x.0 (where x is the latest production major feature release, example:1.3.0)
- A.x.y (where A.x.0 is mandatory and incremental upgrade to be initiated, x is the latest production major feature release, and y is the latest upgrade patch that is live, example: 1.3.1)
- A.x.y-z (where A.x.0 is mandatory and incremental upgrade to be initiated, x is the latest production major feature release, and y is the latest upgrade patch that is live, and z is the spot-patch that is an instant fix for a very short span of time, example: 1.3.1-1)

where A is a long-term release spread across 3-5 years.

Q. Where to find the latest released CX Cloud Agent version and how to upgrade the existing CX Cloud Agent?

A. To locate and upgrade to the latest CX Cloud Agent:

1. Log into the CX Cloud portal and navigate to the **Admin Center**. The **Data Sources** window opens**.**
2. Select **CX Cloud Agent** to open the detail view and click the **Software** tab**.**
3. Make a selection from the **Choose a software version to upgrade to** drop-down list and click **Install Update**.

Authentication and Proxy configuration

Q. What is the default user for the CX Cloud Agent Application?

A. cxcadmin.

Q. How is the password set for the default user?

A. Passwords are set during network configuration.

Q. Is there an option available to reset the password after Day-0?

A. No specific option is provided by the CX Cloud Agent to reset the password, but you can use the Linux commands to reset the password for cxcadmin.

Q. What are the password policies to configure CX Cloud Agent?

A. Password policies are:

- Maximum age (length) set to 90 days
- Minimum age (length) set to 8 days
- Maximum length 127 characters
- At least one upper case and one lower case character must be included
- Must contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/)
- The following characters are not permitted
    - Special 8-bit characters (e.g., ¬£, √Å √´, √¥, √ë, ¬ø, √ü)
    - Spaces
- Must not be the last 10 recently used passwords
- Must not contain regular expression
- Must not contain the followng words or derivatives: cisco, sanjose, and sanfran

Q. How do I confirm Secure Shell (SSH) reachability to a device from CX Cloud Agent?

A. To confirm SSH reachability:

1. Log in as cxcroot user.
2. Execute the following comand to enable the SSH port in Iptables:

```
Iptables -A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

3. Execute the following command to confirm SSH reachability:

```
ssh user@ip-address:port
```

To disable the SSH ports enabled above in the CX Cloud Agent:

1. Execute the following command to obtain the line number of the SSH port enabled in the iptables:

```
iptables -L OUTPUT --line-number | grep dpt | grep ssh | awk '{print $1}'
```

2. Execute the following command to delete the obtained line number:

```
iptables -L OUTPUT <Line number>
```

Q. How do I confirm SNMP reachability to a device from CX Cloud Agent?

A. To confirm SNMP reachability:

1. Log in as cxcroot user.
2. Execute the following comand to enable the SNMP ports in the Iptables:

```
iptables -A OUTPUT -p udp -m udp --dport 161 -j ACCEPT
```

```
iptables -A OUTPUT -p udp -m udp --dport 161 -j ACCEPT
```

3. Execute the following snmpwalk/snmpget command to confirm SNMP reachability :

```
snmpwalk -v2c -c cisco IPADDRESS
```

To disable the SNMP ports enabled above in the CX Cloud Agent:

1. Execute the following command to obtain the line numbers of the enabled SNMP ports (two line numbers are generated as a response):

```
iptables -L OUTPUT --line-number | grep dpt | grep ssh | awk '{print $1}'
```

2. Execute the following command to delete the line numbers (in descending order):

```
iptables -L OUTPUT <Line number2 Number>
```

```
iptables -L OUTPUT <Line number1 Number>
```

Q. How do I set the Grub password?

A. To set the Grub password:

1. Run .ssh as cxcroot and provide the token [contact the Support Team to obtain the cxcroot token].
2. Execute sudo su, to provide the same token.
3. Execute the *grub-mkpasswd-pbkdf2* command and set the Grub password. Hash of the provided password will be printed, copy the content.
4. vi to the file /etc/grub.d/00_header**.**
5. Navigate to the end of file and replace the hash output followed by the content password_pbkdf2 root ***** with the obtained hash for the password obtained in step 3.
6. Save the file with the command :wq!.
7. Execute the *update-grub* command.

Q. What is the expiration period for the cxcadmin password?

A. The password expires in 90 days.

Q. Does the system disable the account after consecutive unsuccessful login attempts?

A. Yes, the account is disabled after five (5) consecutive unsuccessful attempts. The lockout period is 30 minutes.

Q. How do I generate a passphrase?

A. To generate a passphrase:

1. Run .ssh and log in as cxcadmin user.
2. Execute the *remoteaccount cleanup -f* command.
3. Execute the *remoteaccount create* command.

Q. Does the proxy host support both hostname and IP?

A. Yes, but to use hostname, user must provide the Domain Name Server (DNS) IP during network configuration.

Secure Shell SSH

Q. What ciphers are supported by ssh shell?

A. The following ciphers are supported:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

Q. How do I log in to the console?

A. To log in:

1. Log in as cxcadmin user
2. Provide the cxcadmin password

Q. Are SSH logins logged?

A. Yes, they are logged as part of the "*var/logs/audit/audit.log*". file

Q. What is the idle session timeout?

A. SSH session timeout occurs if the CX Cloud Agent is idle for five (5) minutes.

Ports and Services

Q. What ports are kept open on the CX Cloud Agent?

A. These following ports are available:

- **Outbound port**: The deployed CX Cloud Agent can connect to the Cisco backend as indicated in the table on HTTPS port 443 or via a proxy to send data to Cisco as indicated in the table below. The deployed CX Cloud Agent can connect to Cisco Catalyst Center on HTTPS port 443.

AMERICAS	**EMEA**	**APJC**
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com

agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Note: In addition to the listed domains, when EMEA or APJC customers reinstall the CX Cloud Agent, the agent.us.csco.cloud domain must be allowed in the customer firewall.
The agent.us.csco.cloud domain is no longer required after successful reinstallation.

Note: Ensure that return traffic must be allowed on port 443.

- Inbound port: For local management of the CX Cloud Agent, 514(Syslog) and 22 (ssh) must be accessible. Customers must allow port 443 in their firewall to receive data from CX Cloud.

CX Cloud Agent Connection with Cisco Catalyst Center and Other Assets

Q. What is the purpose and relationship of Cisco Catalyst Center with CX Cloud Agent?

A. Cisco Catalyst Center is the Cloud Agent that manages the customer premise network devices. CX Cloud Agent collects device inventory information from the configured Cisco Catalyst Center and uploads the inventory information available in the **Asset View** of CX Cloud.

Q. Where can users provide Cisco Catalyst Center details on the CX Cloud Agent?

A. During the Day 0 - CX Cloud Agent setup, users can add the Cisco Catalyst Center details from the CX Cloud portal. During Day N operations, users can add additional Cisco Catalyst Centers from Admin Settings > Data Source.

Q. How many Cisco Catalyst Centers can be added?

A. Ten (10) Cisco Catalyst Center clusters or 20 Cisco Catalyst Center non-clusters can be added.

Q. How do I remove a connected Cisco Catalyst Center from CX Cloud Agent?

A. To remove a connected Cisco Catalyst Center from CX Cloud Agent, contact the Technical Assistance Center (TAC) to open a support case from the CX Cloud portal.

Q. What role can the Cisco Catalyst Center user have?

A. The user role can be either **admin** or **observer**.

Q. How are modifications reflected in CX Cloud Agent due to changes in connected Cisco Catalyst Center credentials?

A. Execute the *cxcli agent modifyController* command from the CX Cloud Agent console:

Contact support for any issues during Cisco Catalyst Center credentials update.

Q. How are the Cisco Catalyst Center and seed file asset details stored in CX Cloud Agent?

A. All data including credentials of CX Cloud Agent connected controllers (e.g., Cisco Catalyst Center) and directly connected assets (e.g., via seed file, IP range), are encrypted using AES-256 and stored in the CX Cloud Agent database which is protected with a secured user ID and password.

Q. Are there any limitations for entering IP ranges when adding other assets?

A. Yes, the CX Cloud Agent is unable to handle discovery operations for larger subnet IP ranges. Cisco recommends using minimized subnet ranges limited to 10,000 IP addresses.

Q. Can a public subnet be used for the CX Cloud Agent v2.4 deployment for the cluster and service custom subnet?

A. Cisco does not recommend using a public IP subnet for the following reasons:

- **Security Risks**: Public IP address expose cluster and services to the internet, increasing the risk of unauthorized access, attacks, and potential data breaches.
- **IP Address Conflicts**: Using public IP subnets can lead to IP conflicts, especially if the same IP addresses are assigned elsewhere on the internet, leading to connectivity issues and unexpected behavior.
- **Complexity in Network Configuration**: Managing network policies, firewall rules, and routing becomes more complex when dealing with public IP addresses. This can lead to misconfigurations and increased maintenance overhead.

A public IP subnet can be used if it is solely assigned to a customer organization and set up over the customer network.

Q. How frequently can the rediscovery operation be initiated?

A. The rediscovery operation should only be performed if there is a change in the customer network (e.g., after devices are added or deleted within the network).

Q. What is the workflow workflow for adding “Other Assets as a Data Source” when uploading a seed file?

A. The workflow is as follows:

1. Upload the seed file into CX Cloud.
2. The seed file is temporarily stored in the Cisco Cloud AWS S3 bucket (with SSE encryption enabled).
3. The seed file is pushed to the CX Cloud Agent and the seed file is deleted from the S3 bucket
4. The CX Cloud Agent processes the seed file entries and encrypts the credentials using a AES 256 key (this key is unique for each CX Cloud Agent). These encrypted credentials are stored in the CX Cloud Agent database.
5. The seed file is deleted from the CX Cloud Agent once the seed file entries are processed.

Q. What kind of encryption is used while accessing the Cisco Catalyst Center API from CX Cloud Agent?

A. HTTPS over TLS 1.2 is used for the communication between Cisco Catalyst Center and CX Cloud Agent.

Q. What operations are performed by CX Cloud Agent on the integrated Cisco Catalyst Center Cloud Agent?

A. CX Cloud Agent collects data from the Cisco Catalyst Center about network devices and uses the Cisco Catalyst Center command runner interface to talk to end devices and execute CLI commands (show command). No config change commands are executed.

Q. What default data is collected from Cisco Catalyst Center and uploaded to the backend?

A.

- Network Entity
- Modules
- Show version
- Config
- Device image information
- Tags

Q. What additional data is collected from Cisco Catalyst Center and uploaded to Cisco backend?

A. Refer to this document for more information.

Q. How is inventory data uploaded to the backend?

A. CX Cloud Agent uploads the inventory data via TLS 1.2 protocol to Cisco backend server.

Q. What is the inventory upload frequency?

A. Collection is triggered as per the user-defined schedule and is uploaded to the Cisco backend.

Q. Can the user re-schedule inventory?

A. Yes, an option is available from **Admin Center > Data Sources** to modify the schedule information.

Q. When does the connection timeout occur between Cisco Catalyst Center and Cloud Agent?

A. Timeouts are categorized as follows:

- For initial connection, timeout is a maximum of 300 seconds. If connection is not established between Cisco Catalyst Center and Cloud Agent within a maximum of five (5) minutes, then the connection terminates.
- For recurring, typical, or updates: response timeout is 1800 seconds. If the response is not received or not able to read within 30 minutes, the connection terminates.

CX Cloud Agent Used Diagnostic Scan

Q. What scan commands are executed on the device?

A. Commands that need to be executed on the device for the scan are dynamically determined during the scanning process. The set of commands can change over time, even for the same device (and not in control of Diagnostic Scan).

Q. Where are the scan results stored and profiled?

A. The scanned results are stored and profiled in the Cisco backend.

Q. Are the duplicates (by hostname or IP) in Cisco Catalyst Center, added to the Diagnostic Scan when Cisco Catalyst Center source is plugged in?

A. No, duplicates are filtered such that only the unique devices are extracted.

Q. What happens when one of the command scans fails?

A. The device scan completely stops and is marked as unsuccessful.

Q. What happens when multiple scans overlap?

A. Executing multiple diagnostic scans simultaneously can slow the scanning process and potentially result in scan failures. Cisco recommends scheduling diagnostic scans or initiating on-demand scans at least 6-7 hours apart from inventory collection schedules so they do not overlap.

CX Cloud Agent System Logs

Q. What health information is sent to the CX Cloud portal?

A. Application logs, Pod status, Cisco Catalyst Center details, audit logs, system details, and hardware details.

Q. What system details and hardware details are collected?

A. Sample output:

```
system_details":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"operatingSystem":"linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_utilization":"12.5%",
"total_memory":"16007MB",
"free_memory":"9994MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}
```

Q. How is health data sent to the backend?

A. With CX Cloud Agent, the health service (servicability) streams the data to the Cisco backend.

Q. What is the CX Cloud Agent's health data log retention policy in the backend?

A. The CX Cloud Agent's health data log retention policy in the backend is 120 days.

Q. What types of uploads are available?

A.

1. Inventory upload
2. Syslog upload
3. Agent Health upload, including of the health upload
   1. Services health – Every five (5) minutes
   2. Podlog – Every one (1) hour
   3. Audit log – Every one (1) hour

Troubleshooting

Issue: Not able to access the configured IP.

Solution: Execute ssh using configured IP. If connection times out, the possible reason is IP misconfiguration. In this case, reinstall by configuring a valid IP. This can be done through the portal with the reinstall option provided in the Admin Centerpage.

Issue: How do I verify that services are up and running after registration?

Solution: Follow the steps below to confirm that pods are up and running:

1. ssh to the configured IP as cxcadmin
2. Provide the password
3. Execute the *kubectl get pods* command

Pods can be in any state (Running, Initializing, or Container creating). After 20 minutes, the pods must be in Running state.

If state is **is not running** or **Pod Initializing**, check the pod description with the *kubectl describe pod <podname>* command.

The output will have information on the pod status.

Issue: How to verify whether SSL Interceptor is disabled at customer Proxy?
Solution: Execute the curl command shown here to verify the server certificate section. The response has the certificate details of concsoweb server.

curl -v --header 'Authorization: Basic xxxxxx' https://concsoweb-prd.cisco.com/

```
* Server certificate:

*  subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

*  start date: Feb 16 11:55:11 2021 GMT

*  expire date: Feb 16 12:05:00 2022 GMT

*  subjectAltName: host "concsoweb-prd.cisco.com" matched cert's "concsoweb-prd.cisco.com"

*  issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL CA G3

*  SSL certificate verify ok.

> GET / HTTP/1.1
```

Issue: kubectl commands failed and shows the error as “The connection to the server X.X.X.X:6443 was refused - did you specify the right host or port”
Solution:

- Verify for resource availability. [example: CPU, Memory].
- Wait for the Kubernetes service to start.

Issue: How to get the details of collection failure for a command/device?

Solution:

- Execute *kubectl get pods* and get the collection pod name.
- Execute *kubectl logs <collectionPodName>* to get the command/device specific details.

Issue: kubectl command not working with error "[authentication.go:64] Unable to authenticate the request due to an error: [x509: certificate has expired or is not yet valid, x509: certificate has expired or is not yet valid]"

Solution:Run the commands shown here as *cxcroot* user

```
rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl --insecure-skip-tls-verify=true delete secret -n kube-system k3s-serving
systemctl restart k3s
```

Collection Failure Responses

Collection failure cause can be any constraints or issues seen with the added controller or devices present in the controller.

The table shown here has the error snippet for use cases seen under the Collection microservice during the collection process.

Use Case	**Log Snippet in Collection Microservice**

If the requested device is not found in Cisco Catalyst Center	{
	  "command": "show version",
	  "status": "Failed",

Use Case	**Log Snippet in Collection Microservice**
	"commandResponse": "", "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a " }

If the requested device is not reachable from Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host "
	}

If the requested device is not reachable from Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection timed out: /X.X.X.X:22"
	}

If the requested command is not available in the device	{
	"command": "show run-config",
	"status": "Success",
	"commandResponse": " Error occured while executing command : show run-config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#",
	"errorMessage": ""
	}

If the requested device does not have SSHv2 and Cisco Catalyst Center tries to connect the device with SSHv2	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nSSH2 channel closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."
	}

If command is disabled in Collection microservice	{ "command": "config paging disable", "status": "Command_Disabled",

Use Case	**Log Snippet in Collection Microservice**
	"commandResponse": "Command collection is disabled", "errorMessage": "" }

If the Command Runner Task failed and task URL is not returned by Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s. Task URL is empty."
	}

If the Command Runner Task failed to get created in Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. No task details."
	}

If the Collection microservice is not receiving a response for a Command Runner request from Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s."
	}

If Cisco Catalyst Center is not completing the task within the configured timeout (5 mins per command in Collection microservice)	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. The command runner task failed for device %s, RequestURL: %s. No progress details."
	}

If the Command Runner Task failed and the file ID is empty for the submitted task by Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. File id is empty."
	}

If the Command Runner Task failed and	{

Use Case	Log Snippet in Collection Microservice
the file ID tag is not returned by Cisco Catalyst Center	"command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: %s. No file id details." }

If the device is not eligible for command runner execution	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Requested devices are not in inventory,try with other devices available in inventory"
	}

If the command runner is disabled for the user	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Role does not have valid permissions to access the API\"}\n"
	}

Diagnostic Scan Failure Responses

Scan failures and the causes can be from any of the listed components.

When users initiate a scan from the portal, occasionally it results as “failed: Internal server error”.

The cause for the issue is one of the listed components

- Control Point
- Network Data Gateway
- Connector
- Diagnostic Scan
- CX Cloud Agent Microservice [devicemanager, collection]
- Cisco Catalyst Center
- APIX
- Mashery
- Ping Access
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

To see the logs:

1. Log into the CX Cloud Agent console.
2. Execute *kubectl get pods*.

3. Obtain the pod name of collection, connector, and servicability.
4. To verify the collection, connector, and servicability microservice logs.

- Execute *kubectl logs <collectionpodname>*
- Execute *kubectl logs <connector>*
- Execute *kubectl logs <servicability>*

The table below displays the error snippet seen under the Collection microservice and servicability microservice logs that occurs due to the issues/constraints with the components.

Use case	**Log Snippet in Collection Microservice**

The device can be reachable and supported, but the commands to execute on that device are block-listed on the Collection microservice	{
	  "command": "config paging disable",
	  "status": "Command_Disabled",
	  "commandResponse": "Command collection is disabled",
	}

If the device for a scan is not available. Occurs in a scenario, when there is a sync issue between the components such as portal, diagnostic scan, CX component, and the Cisco Catalyst Center	No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a
If the device that is attempted for scan is busy, (in a scenario) where the same device is been part of other job and no parallel requests are handled from Cisco Catalyst Center for the device	All requested devices are already being queried by command runner in another session. Please try other devices
If the device is not supported for scan	Requested devices are not in inventory, try with other devices available in inventory
If the device attempted for scan is unreachable	"Error occurred while executing command: show udi\nError connecting to device [Host: x.x.x.x:22] No route to host : No route to host

If Cisco Catalyst Center is not reachable from Cloud Agent or Collection microservice of the Cloud Agent is not receiving response for a Command Runner request from Cisco Catalyst Center	{
	  "command": "show version",
	  "status": "Failed",
	  "commandResponse": "",
	  "errorMessage": "The command runner task failed for device %s, RequestURL: %s."
	}

Use Case	**Log Snippet in Control Point Agent Microservice**
If the scan request has schedule details missing	Failed to execute request {"message":"23502: null value in column \"schedule\" violates not-null constraint"}
If the scan request has device details missing	Failed to create scan policy. No valid devices in the request
If the connection between the CPA and connectivity is down	Failed to execute request
If the requested device for scan is not available in Diagnostic Scans	Failed to submit the request to scan. Reason = {\"message\":\"Device with Hostname=x.x.x.x' was not found\"}