CCE Serviceability and Monitoring using AppDynamics

Overview

For Cisco Contact Center Enterprise solution, it is important to have continuous and seamless monitoring of the deployed solution, and automated alerting when anomalies are detected. AppDynamics provides a solution for application and platform performance monitoring that helps to achieve the following:

- Platform, application, and end user monitoring (EUM) through dashboards and metrics
- Automated alerting mechanism in case of anomaly detection

For ordering and setting up AppDynamics SAAS controller, License key, and Beacon URL please contact appd_ucce_sales@cisco.com

Note **For AppDynamics, CCE supports SaaS and On-Prem controller (version 21.4.10-24683) over secure connection only.**

Supported Applications

All CCE solution components are supported except ECE, Customer Collaboration Platform (CCP), and Cloud Connect server. Here is a table depicting what is instrumented in each component and monitored:

Sl No	Component Name	Machine Agent (Server Visibility)	.Net Agent (For Windows Perfmon Integration)	JVM App Agents
1	Finesse **Note** End-user monitoring is supported for Finesse.	✓	Not Applicable	• Finesse-Desktop
2	CUIC	✓	Not Applicable	CUIC-Reporting
3	LiveData	✓	Not Applicable	• LiveData-ActiveMQ • LiveData-SocketIO
4	IdS	✓	Not Applicable	IdS Tomcat
5	VVB	✓	Not Applicable	• Speech-Server • VVB-Engine
6	CVP OAMP	✓	Not Applicable	OAMP
7	CVP ReportingServer	✓	Not Applicable	• ReportingServer • WebServicesManager
8	CVP Call/VXMLServer	✓	Not Applicable	• CallServer • VXMLServer • WebServicesManager
9	Router	✓	✓	Not Applicable
10	Logger	✓	✓	Not Applicable
11	PG	✓	✓	CCEJGW
12	AW-HDS	✓	✓	CCEAdmin
13	AW-HDS-DDS	✓	✓	CCEAdmin

Note

- CCESERVERAGENT JVM is an extension of machine agent for ICM nodes. Each ICM node will have one CCESERVERAGENT instance mapped to it.
- CCESERVERAGENT is not used for application performance monitoring. It is used only for mapping the windows server to the application in AppDynamics controller.
- LiveData-Worker JVM App Agent is disabled by default. You can enable it using the **set live-data appd-monitoring enable** CLI. For more information on the CLI, see the *Live Data CLI Commands* section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

Prerequisites

Application Group and Agent Licenses

Before the applications can be configured for performance monitoring, ensure that an AppDynamics application group is created and the required number of agent licenses are procured and allocated. An access key is generated for the application group. This access key is required later during the configuration procedure.

For details on how to acquire agent licenses, please contact appd_ucce_sales@cisco.com and for details on application group, access keys etc., see the documentation on AppDynamics at: https://docs.appdynamics.com/display/PRO45/AppDynamics+Essentials.

Note For end user monitoring on Finesse, you must procure AppDynamics ENUM license.

Cloud Connect

The CLI commands described in this chapter must be run from the Cloud Connect server. The nodes on which performance monitoring has to be enabled must be part of the Cloud Connect server orchestration inventory.

For installing and configuring Cloud Connect, refer to the *Install Cloud Connect* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

If Cloud Connect is on 12.6(2) and the target Windows and VOS nodes are on 12.6(1) during stagewise upgrade, ensure below ESs and COP are applied in respective 12.6(1) target nodes:

Component	ES/COP
Unified ICM	ES67
Unified CVP	ES19

Component	ES/COP
Finesse	ucos.appDynamicsProxyUpdate.1261.cop.sgn ucos.appDynamicsProxyUpdate.1261_rollback.cop.sgn
Cisco Unified Intelligence Center	
Live Data	
Cisco Identity Service	
Cisco Virtualized Voice Browser	

AppDynamics performance monitoring are supported in the following deployment types:

- UCCE-2000-Agents
- UCCE-4000-Agents
- UCCE-12000-Agents
- UCCE-24000-Agents
- PCCE-2000-Agents
- PCCE-4000-Agents
- PCCE-12000-Agents

Note The UCCE-12000-Agents, UCCE-24000-Agents, and PCCE-12000-Agents deployment types are supported only for AppDynamics performance monitoring and not for orchestration.

For information about how to onboard nodes to Cloud Connect server, refer to the **Orchestration Deployment Task Flow** section in the *Unified CCE or Packaged CCE Install and Upgrade Guide*.

CCE Solution Components

The CCE solution components existing in domain should have a unique FQDN. The components existing in a workgroup should have a unique hostname to register with AppDynamics controller for performance monitoring.

Performance Monitoring

In order to monitor the performance of CCE applications, platforms, and end-user-facing application such as Finesse desktop using AppDynamics, an administrator must configure and enable performance monitoring on target node.

Note Parallel execution of same or different CLI for AppDynamics on Cloud Connect server is not allowed.

Note If Cloud Connect is on 12.6(2), you can enable or check the status of performance monitoring or test the connection with AppDynamics controller only after upgrading the target node to 12.6(2). However, you can disable performance monitoring if the target node is on 12.6(1).

Note Before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.

Enable Performance Monitoring

To enable performance monitoring on Windows or VOS nodes, run the **utils app-monitoring enable** command. You can select a single node or a group of nodes from either Cloud Connect publisher or subscriber to enable performance monitoring. Ensure that the number of selected nodes doesn't exceed 10. Provide the details for configuring these nodes for monitoring. Deployment Name configured in Orchestration inventory is used as the application name in AppDynamics. For more information, see the **Add Deployment Type and Deployment Name** section in the Orchestration chapter of *Unified CCE or Packaged CCE Install and Upgrade Guide*.

Performance monitoring is enabled only after restarting the target node. If you choose not to restart the servers immediately, manually restart them later for the changes to take effect.

All the supported AppDynamics agents on the target nodes are enabled for monitoring; the administrator can't control the enable or disable of a specific AppDynamics agent on the target node.

Note You can also use this command to update any existing configuration details on selected nodes.

Command	**utils app-monitoring enable**
Description	This command enables performance monitoring on selected nodes.

Expected Inputs	

Select the node on which you need to enable performance monitoring and provide the following information:

Note You can select a single node or a group of nodes from either Cloud Connect publisher or subscriber to enable performance monitoring. Ensure that the number of selected nodes doesn't exceed 10.

- Controller Host: The hostname/URL of the AppDyanmics Controller. Agents may connect directly to the Controller or through a proxy.
- Controller Port: The port on which the AppDynamics Controller listens for agent traffic.
- Account Name: The name of the account listed in the AppDynamics Controller A single tenant Controller has two accounts: a default account name and an internal system account. For most connections, use the default account name.
- Account Access Key: A unique key associated with the AppDynamics Controller account. This is used as the API token by agents to authenticate/authorize themselves with the Controller.
- Beacon URL: The service endpoint where Javascript agents will connect for sending the end user monitoring metrics.
- Beacon Access Key: The access key used by Javascript agents for authenticating or authorizing themselves with the Beacon server. This is different from the Account Access Key mentioned above.
- Proxy Host: Proxy server IP/hostname via which the AppDynamics controller is connected.
- Proxy Port: Proxy port for connecting to the proxy server.
- Username: Username of the AppDynamics controller account.
- Password: Password of the AppDynamics controller account.

Note Username and Password are used for enabling Windows Event monitoring on ICM nodes. The administrator has an option to confirm on whether AppDynamics Windows event monitoring must be enabled or not, when the ICM node is selected for enabling AppDynamics. The Username and Password will be requested only when the administrator confirms to enable Windows Event Monitoring on ICM nodes.

Note Proxy Host and Proxy Port will be requested only when the administrator confirms to use proxy for application monitoring. Using proxy for application monitoring is optional.

	Note Beacon URL and Beacon Access Key used for end-user monitoring are applicable only for Finesse node. For more information on how to generate a Beacon Access Key, refer to the **Generate a Beacon Access Key** section below: Confirm to proceed, and select the option to restart.
Expected Outcome	Performance monitoring is configured for all the selected nodes and enabled if restart option is selected as "Yes". Windows Event Monitoring is enabled for ICM nodes based on administrator's confirmation. Proxy is configured for application monitoring based on administrator's confirmation to use proxy for application monitoring.

Note Application monitoring configuration on Unified ICM and Unified CVP will be removed as part of Unified ICM 12.6(2) or Unified CVP 12.6(2) uninstall only when you upgrade from 12.5(x). If application monitoring is already enabled and if you want to uninstall and reinstall Unified ICM 12.6(2) or Unified CVP 12.6(2) software, after the reinstallation, reconfigure application performance monitoring using the **utils app-monitoring enable** CLI.

Note If performance monitoring is already enabled, and if you want to add or delete the component in Unified ICM, then follow the below steps to update the performance counters for monitoring.

- Disable application performance monitoring using the **utils app-monitoring disable** command.
- Add or delete the component in the Unified ICM.
- Enable application performance monitoring using the **utils app-monitoring enable** command.

When application performance monitoring is enabled, the system specific and CCE-specific performance counters are enabled by default. You can add more counters for deployment by editing the **.NET Agent config file**. Refer to https://docs.appdynamics.com/display/PRO21/Configure+the+.NET+Agent. If you are adding more counters, ensure that you don't exceed 200 counters on a virtual machine. Manually added counters will be reset to the default value if you disable or enable application performance monitoring. The counters added to the monitoring list includes all the installed CCE services including the disabled services. Hence, delete the disabled CCE services from the server if they are not required.

Note Performance monitoring starts on VOS components approximately 15 to 20 minutes after reboot. During this period, performance monitoring status for the target node in **utils app-monitoring status** CLI will be shown as `Disabled.`

Generate Beacon Access Key

Perform the following steps to generate the Beacon Access Key:

1. Log in to AppDynamics controller.
2. Click **User Experience** tab.
3. Click **Add App** in Browser Apps tab.
4. Select Create an application using the Getting Started Wizard, and press **OK**. The Set Browser Application section appears.
5. Enter the application name in the Set Browser Application section. Click **Continue**. The Beacon Access Key will be generated.
6. The Send and Verify a Test Page operation will be initated, and it might take up to two minutes to complete. Once the activity is completed, the message, `Beacon Sent and Data Received & Page Created` is displayed with a tick mark.
7. Then, the message, `You have successfully verified the configuration` is displayed with a tick mark in the Instrument your own web pages section. Click **Continue**, and click **Save** in the next page.
8. Click on the **User Experience** tab to verify if the browser application has been created with the newly generated Beacon access key.

Update Performance Monitoring Configuration

To update the configuration details for performance monitoring, run the **app-monitoring enable** command. You must restart the servers for the changes to take effect. For details on the command, see Enable Performance Monitoring, on page 5.

Disable Performance Monitoring

To disable performance monitoring on Windows and VOS nodes, run the **app-monitoring disable** command. Performance monitoring will be disabled after restart of target node. The configurations will, however, be retained. Administrator will not be allowed to disable any specific AppDynamics agent on the target node. All supported AppDynamics agents will be disabled by default.

Command	**utils app-monitoring disable**
Description	This command is used to disable performance monitoring on selected nodes.
Expected Inputs	Select the node on which performance monitoring needs to be disabled. Confirm to proceed.
Expected Outcome	Performance monitoring is disabled for all the selected nodes.

Note If the Cloud Connect is on 12.6(2), you can enable or disable AppDynamics only after upgrading the target node to 12.6(2).

Check Status of Performance Monitoring

To check whether performance monitoring is enabled, disabled, or just configured but not enabled, on selected Windows or VOS nodes, run the **utils app-monitoring status** command.

Command	**utils app-monitoring status**
Description	This command is used to check if performance monitoring is enabled on selected nodes. This command also shows the following: • Proxy enabled status • Windows Event monitoring enabled status for ICM nodes
Expected Inputs	Select the node for which you want to check the status, and confirm to proceed.
Expected Outcome	Shows whether the configuration details for performance monitoring is enabled, disabled, or updated for the selected nodes: • If an update is made to the existing configuration and the node is restarted, then the status shows the updated configuration as current configuration used by AppDynamics performance monitoring. • If an update is made to the existing configuration and the node is not restarted, then the status shows both the current configuration used by AppDynamics performance monitoring as well as the to-be-applied configuration which will be applied post restart.

Test Connection with AppDynamics Controller

To test whether the configured Windows and VOS nodes are able to connect to the AppDynamics controller, run the **utils app-monitoring test-connection** command.

Command	**utils app-monitoring test-connection**
Description	This command is used to test the connectivity of selected Windows or VOS nodes to the AppDynamics controller.
Expected Inputs	Select the nodes for which you want to test the connectivity status.
Expected Outcome	Shows whether the selected nodes are able to connect to the AppDynamics controller.

Configure Thresholds and Alerts for Monitoring

We recommend using the templates delivered for configuring threshold and alerts on the AppDynamics controller.

- The Cisco-delivered templates can be imported on the application. For details on managing templates, see https://docs.appdynamics.com/display/PRO21/Configure+and+Manage+Alerting+Templates. For

downloading template, see https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(1)

- Once the template is imported, you have to replace the default email address (support@cisco.com) with a valid email address for alert notification.
- Adding at least one valid email address is mandatory. However, you can add multiple email addresses.
- Threshold for alerts is enabled by default as part of Cisco-delivered template.

Note You can also view, create, overwrite, delete, export, apply and disable the template on the application. For details on managing templates, see https://docs.appdynamics.com/display/PRO21/Configure+and+Manage+Alerting+Templates.

Configure JMX Monitoring and Alerting Templates for Finesse Desktop

We recommend using the following templates to configure JMX Monitoring for Finesse Desktop.

- Finesse_JMX_Metrics_Configuration.xml
- Finesse_JMX_Metrics_AlertingTemplate.json

Follow these steps to import the templates to the respective application:

1. Navigate to the respective application on the AppDynamics controller.
2. Select Tiers & Nodes section menu.
3. From the **Finesse-Desktop** tier, select the Finesse node.
4. Select the **JMX** tab.
5. Click the **Configure JMX Metrics** icon.
6. Click the **Import** icon.
7. Click the **Choose File** button.
8. Select the **Finesse_JMX_Metrics_Configuration.xml** file.
9. Click the **Import** button. The **FinesseMetrics List** is displayed if the import succeeds.
10. Import **Finesse_JMX_Metrics_AlertingTemplate.json**. See Configure Thresholds and Alerts for Monitoring, on page 10 for more information on importing the alerting template.

Dashboards

Dashboards are used to display the health of the system in a graphical manner on the AppDynamics controller. Data such as CPU and memory usage are collected from the system at platform level. Data such as health status of Java agents and .NET agents are collected from the system at application level. Administrators can

build custom dashboards with various widgets to visualize the data from individual systems as well as all the systems in the deployment. These dashboards can be imported or exported when deploying new CCE tenants.

For more information on Dashboards, see https://docs.appdynamics.com/display/PRO45/Dashboards+and+Reports.

Create Dashboards Using Templates

Administrators can create new dashboards or edit the dashboard template (JSON file) provided by us. This edited template file can then be imported to the AppDynamics Controller via the **Dashboards & Reports** tab.

For downloading template, see https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(2).

Edit the following strings in the template:

- "name" - Provide an appropriate name, which is displayed as the dashboard name in the Controller. For example, "Arihant - 2K Dashboard".
- "applicationName" - Update this with the corresponding application name for which you want to create a dashboard.

Note If WidgetName is "EventListWidget", then don't change the "applicationName".

- "entityName" - Set the name of the system that is monitored.
  - If the "entityType" is set to "APPLICATION_COMPONENT_NODE", update this string with the corresponding AW component node name. For example, "UCCEAWHDS121A".

Once the template file is edited and imported, the dashboard will display the performance and health status of the system.

Note

- If the "entityType" is set to "APPLICATION_COMPONENT", then do not make any changes to the "entityName".
- If the "entityType" is set to "BUSINESS_TRANSACTION", do not make any changes to the "scopingEntityName".
- There are no changes required in these cases as the type of entity is a tier-name, which is common to all the nodes in an application.

End User Monitoring

End user monitoring is available for the Finesse desktop application. It provides various browser-based metrics, such as the most frequently used browser, the most commonly used browser version, etc. It can provide geographical location of a Finesse agent desktop. The AppDynamics agents in the browser sends the metrics

to the AppDynamics Controller. You can view these metrics in the **User Experience** tab of the AppDynamics Controller application.

When you run the **app-monitoring enable** command to enable performance monitoring for Finesse, end user monitoring is also enabled. There is no additional step required. The Beacon URL and the Beacon Access Key that you provided when running the command are saved in the Finesse server. The network connectivity between the Finesse Agent desktop browser and the Beacon host, however, must be available. The Beacon host must be on the allowed list in the proxy server.

For more information, see https://docs.appdynamics.com/display/PRO45/End+User+Monitoring.

View Metrics

Once the monitoring is enabled on the VOS and Windows nodes, the AppDynamics agents start sending out performance metrics to the AppDynamics controller. These monitored metrics, also known as counters, are shipped from the Windows machines as performance counters, and from the respective JVMs of the VOS machines as JMX counters. These metrics can be viewed on the AppDynamics Controller interface and later utilized for setting thresholds, alerts, etc.

JMX Counter Thresholds

Cisco Finesse provides important JMX counters with associated threshold values that can be used to monitor the health of Finesse. The following tables list the JMX counters with corresponding threshold values at the login phase and steady phase.

Note The JMX counter IntervalLoginOperations with the JMX object name com.cisco.ccbu:category=LoginStats,component0=LoginStats-webservices will be used to determine the total number of logins.

If the number of logins that happened in the last 15 seconds is greater than 5, then it is login phase. Else it is steady phase. Respective threshold will be used dynamically based on the number of logins.

Table 1: JMX Counters on Tomcat Processes (Port 12399) - Login Phase Thresholds

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	400
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	500
currentThreadCount	The number of threads the thread pool currently has (both busy and free).	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	120

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
currentThreadsBusy	The number of threads currently processing requests.	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	100
RequestLongestTime	The maximum amount of time taken to complete an API request, in milliseconds.	com.cisco.ccbu:category = WebAppStats, component0 = AggregateWebappStats	4000
processCPULoad	The CPU load in this process.	java.lang:type = OperatingSystem	0.6
NumOfActiveAgentsLoggedIn	The number of agents logged in with XMPP Presence as available in the current side.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	1500
NumOfAgentsLoggedIn	The number of agents and supervisors logged in currently.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	2010

Table 2: JMX Counters on Tomcat Processes (Port 12399) - Steady Phase Thresholds

JMX Counter	Description	JMX Object Name	Threshold at Steady Phase
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	400
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	500
TotalCallsInSystem	The total number of active calls in the system.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	1400
AverageProcessingTime	The average time taken for processing CTI messages, in milliseconds.	com.cisco.ccbu:category = AWSSubsystem, component0 = CTIMesssage Statistics Counter	20 ms
currentThreadCount	The number of threads the thread pool currently has (both busy and free).	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	120
currentThreadsBusy	The number of threads currently processing requests.	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	20
RunnablesQueued	Runnables (CTI Messages) still queued.	com.cisco.ccbu:category = AWSSubsystem, component0 = CommandDispatcher	20

JMX Counter	Description	JMX Object Name	Threshold at Steady Phase
TasksQueued	The tasks (such as client requests and CTI messages) queued.	com.cisco.ccbu:category = AWSSubsystem, component0 = CommandDispatcher	20
RequestLongestTime	The maximum amount of time taken to complete an API request, in milliseconds.	com.cisco.ccbu:category = WebAppStats, component0 = AggregateWebappStats	4000
processCPULoad	The CPU load in this process.	java.lang:type = OperatingSystem	0.5
NumOfAgentsLoggedIn	The number of agents and supervisors logged in currently.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	2010

The following table lists the thresholds for counters related to Openfire processes.

Table 3: Counters Related to Openfire (JMX Port 12348)

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
ExecutingTaskCount	The number of tasks (messages published to node) that are running currently.	com.cisco.ccbu.finesse.openfire: type = PubSubOrderedExecutorStatistics	60
QueuedTaskCount	The number of tasks in the queue. Messages that are getting published to a node are placed in the queue.	com.cisco.ccbu.finesse.openfire: type = PubSubOrderedExecutorStatistics	10
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	300
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	300
processCPULoad	The recent CPU usage for the Java Virtual Machine process.	java.lang:type = OperatingSystem	0.6

Check Logs

AppDynamics-related logs are used by the administrators for troubleshooting the failures that are encountered while enabling or disabling or testing the connectivity for performance monitoring from the Cloud Connect server.

AppDynamics related logs are used while debugging failures such as performance metrics not appearing in the AppDynamics controller. All AppDynamics-related logs are stored in their respective target nodes.

Audit Logs

The Audit trail for AppDynamics administrative operation that is initiated from the AppDynamics CLI on Cloud Connect server captures the user, action, and date/time details of the CLI operation.

command: file get activelog orchestration-audit/audit.log*

CLI Logs

Run the following command on the Cloud Connect node to retrieve AppDynamics CLI logs:

command: file get activelog platform/log/cli*.log

Ansible Logs

Run the following commands on the Cloud Connect node to retrieve AppDynamics related Ansible logs:

- Current transaction logs:**file get activelog ansible/ansible.log**
- Historical logs:**file get activelog ansible/ansible_history.log**

AppDynamics Logs (on the target host)

Refer to the following table for information on retrieving the AppDynamics-related Logs on target host:

Node	Performance Configuration	AppD Configuration
VOS	NA	file get activelog appdynamics/appdynamics.log file get activelog appdynamics/machineagent/logs file get activelog appdynamics/appserveragent/logs
ICM	<Install Directory> :\Cisco\AppDynamics \log\AppDynamics_ Perf_Configuration.log	<Install Directory> :\Cisco\AppDynamics \log\AppDynamics_ _Configuration.log
CVP	NA	<Install Directory> :\Cisco\CVP\ AppDynamics\log AppDynamics_ Configuration.log

Note For ICM and CVP, the install directory location changes based on your system configuration.

You can also view the below-mentioned logs using the Real-Time Monitoring Tool (RTMT):

- Ansible logs by selecting 'Ansible Controller' as the Cloud Connect service
- Audit logs by selecting 'Orchestration Audit' as the Cloud Connect service

- AppDynamics related logs by selecting 'Cisco APM Service' as the service on the target nodes

To download RTMT from Cloud Connect or target VOS nodes, use https://FQDN:8443/plugins/CcmServRtmtPlugin.exe.

For more information, refer to the Cisco Unified Real-Time Monitoring Tool Administration Guide at:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Things to Know

- AppDynamics cannot be enabled on FIPS-enabled deployment. Disable the FIPS mode before enabling AppDynamics.
- You can disable or enable AppDynamics through AppDynamics CLI on Cloud Connect. If AppDynamics is disabled and re-enabled with a different application name (taken from the inventory), a new instance is created in the AppDynamics controller with the new application name. However, the instance with the old application name exists and should be manually deleted by logging into the AppDynamics controller. The new application name will be updated in the configuration on the target node once AppDynamics is re-enabled successfully with the new application name.
- Performance monitoring for ECE, CCP and Cloud Connect is currently not supported.