Imer

HCLSoftware

HCL BigFix
Cloud Lifecycle Management

Installation Guide

Version 10.9

The data contained in this document shall not be duplicated, used, or disclosed as a whole or in part for any purpose. If a contract is awarded to chosen parties because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Table of Contents

Table of Figures

List of Tables

Document Revision History

This guide is updated with each release of the product or when necessary. This table provides the revision history of this Installation Guide.

Version Date	Description
May, 2020	Dryice MyCloud v9.2 Installation Guide
August, 2020	Dryice MyCloud v10.0 Installation Guide
November, 2020	Dryice MyCloud v10.1 Installation Guide
February, 2021	Dryice MyCloud v10.2 Installation Guide
April, 2021	Dryice MyCloud v10.4 Installation Guide
October, 2021	Dryice MyCloud v10.5 Installation Guide
September, 2022	Dryice MyCloud v10.6 Installation Guide
August, 2023	HCL_DRYiCE_MyCloud_10.7_Installation_Guide
May, 2024	HCL_DRYiCE_MyCloud_10.8_Installation_Guide
September, 2024	HCL_DRYiCE_MyCloud_10.8.1_Installation_Guide
February, 2025	HCL_DRYiCE_MyCloud_10.8.2_Installation_Guide
July, 2025	HCL_BigFix_Cloud_Lifecycle_Managament_10.9_Installation _Guide

1 Preface

This section provides information about the HCL BigFix CLM Installation Guide and includes the following topics.

- Intended Audience
- About This Guide
- Related Documents
- Conventions

1.1 Intended Audience

This information is intended for Business administrators/IT administrators responsible for installing HCL BigFix CLM and infrastructure administrators responsible for provisioning infrastructure required for installation of HCL BigFix CLM.

1.2 About this Guide

This guide has instructions to install HCL BigFix CLM. It includes the software & hardware pre-requisites, HCL BigFix CLM components details and installation procedures for the product. This guide also provides references to other documents for detailed information and consists of the following major sections:

- HCL BigFix CLM Overview
- HCL BigFix CLM Installation
- HCL BigFix CLM Environment Planning
- HCL BigFix CLM Environment Preparation
- HCL BigFix CLM Post Installation Task.

1.3 Related Documents

The following documents can be referenced in addition to this guide for further information on HCL BigFix CLM:

- HCL BigFix CLM Introduction Guide
- HCL BigFix CLM User Guide
- HCL BigFix CLM Configuration Guide – Admin Module
- HCL BigFix CLM Configuration Guide – Provider Module – Part 1
- HCL BigFix CLM Configuration Guide – Provider Module – Part 2
- HCL BigFix CLM Troubleshooting Guide
- HCL BigFix CLM Developer Guide
- HCL BigFix CLM API Guide
- HCL BigFix CLM V3 API Guide

1.4 Conventions

The following typographic conventions are used in this document:

Table 1 – Conventions

Convention	Element
Boldface	Graphical user interface elements associated with an action, or terms defined in text or the glossary
Underlined blue face	Cross-reference and links
`Courier New (Font)`	Commands within a paragraph, URLs, code in examples, and paths including onscreen text and text input from users
Italic	Document titles, occasional emphasis, or glossary terms
Numbered lists	Steps in a procedure to be followed in a sequence
Bulleted lists	List of items that is not necessarily meant to be followed in a sequence

2 HCL BigFix Cloud Lifecycle Management (CLM) Overview

HCL BigFix CLM is a hybrid cloud management product that empowers organizations to optimally govern, provision, monitor, and manage cloud infrastructure.

It combines data exploration and data visualization in an easy-to-use product that enables effective analysis and generates actionable insights for IaaS, PaaS resources and multi-machine blueprints.

HCL BigFix CLM's data-driven recommendations and advisories ensure continuous optimization of enterprise cloud environments across areas, including cost, performance, security, and utilization.

2.1 HCL BigFix CLM Features

- **Self Service Catalog based Provisioning and Auto-decommissioning:**

  Self Service Catalog based Provisioning & Auto-decommissioning– Provisioning of IaaS, PaaS, and multi-machine blueprints in a multi-cloud environment, through an intuitive self-service catalog and auto-decommissioning post a defined interval to avoid cost leakages.

- **Metering & Showback:**

  Track utilization of resources across BUs, enabling transparency and visibility

- **Dynamic User interface:**

  Flexibility to customize the service request form templates to capture configuration parameters while placing provisioning requests.

- **Dynamic Process Workflows:**

  Enables automation of generic & custom tasks like installing agents, machine cloning etc. with support for parallel execution.

- **Script Library**

  Create new or leverage out-of-the-box scripts in process workflows across environments.

- **Role Based Access Control:**

  Manage user privileges based on their roles, eligibility, and policies.

- **Policy driven Orchestration:**

  Be in control of your cloud orchestration ecosystem aligned to your organizational policies.

- **Rich Integration Ecosystem:**

  Enables integration with industry leading third party tools through REST APIs and CLI

- **Enterprise-Grade Security:**

  Ensure security of end-to-end cloud management and orchestration ecosystem through various mechanisms

2.2 HCL BigFix CLM Component Overview

HCL BigFix CLM has various service components, each playing a different role in multi cloud management. Each component has pre-requisites. Below table lists all the components, their roles and responsibilities and pre-requisites required for each component.

Table 2 – HCL BigFix CLM Component with their roles and responsibilities and pre-requisites

Component Name	Description	Pre-Req's
HCL BigFix CLM Portal	It comprises two sub-components: • **WEB UI**: HCL BIGFIX CLM Web Portal • **HCL BIGFIX CLM API**: Rest API to interact HCL BigFix CLM This component requires HCL BigFix CLM database connectivity.	IIS, HCL BigFix CLM Certificate, .Net Framework 4.8
HCL BigFix CLM KRS	**Key Rotation Service**: To rotate encryption key on a periodic basis. This component requires HCL BigFix CLM database connectivity.	IIS, HCL BigFix CLM Certificate, .Net Framework 4.8
Job Listener	It helps in the execution of HCL BigFix CLM jobs and interacting with different components internally. This is a window service. This component requires the HCL BigFix CLM database connectivity.	HCL BigFix CLM Certificate, .Net Framework 4.8
Sync Service	It is responsible for synchronization of the underlying infrastructure cloud resources. It supports vCenter, AWS, Azure RM, SCVMM 2012. This is a self-hosted WCF service.	HCL BigFix CLM Certificate, .Net Framework 4.8
Ad Sync Service	It fetches AD group user data. This is a self-hosted WCF service.	HCL BigFix CLM Certificate, .Net Framework 4.8
Workflow Service	It triggers HCL BigFix CLM process workflow and notification service. This is a self-hosted WCF service. It requires HCL BigFix CLM database connectivity.	HCL BigFix CLM Certificate, .Net Framework 4.8, MSMQ/Rabbit MQ

Orchestrator	It helps in provisioning and automating other Tasks. This is a self-hosted WCF service.	HCL BigFix CLM Certificate, .Net Framework 4.8, PowerShell, Python 3.6
ITSM executor	It helps with interacting with ITSM tools. Currently, it only supports ServiceNow and Remedy. It is a self-hosted WCF service and requires HCL BigFix CLM database connectivity.	HCL BigFix CLM Certificate, .Net Framework 4.8
Generic Task Executor	It helps with Private Cloud Billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service and requires HCL BigFix CLM database connectivity.	HCL BigFix CLM Certificate, .Net Framework 4.8
Billing Service	It enables Public Cloud Billing. This is a self-hosted WCF service and requires HCL BigFix CLM database connectivity.	HCL BigFix CLM Certificate, .Net Framework 4.8
Performance Service	It is responsible for metering and Public Cloud advisory data collection. This is a self-hosted WCF service.	HCL BigFix CLM Certificate, .Net Framework 4.8
Health Monitor Service	It is responsible for monitoring the health of all the HCL BigFix CLM Components. This is a self-hosted WCF Service.	HCL BigFix CLM Certificate, .Net Framework 4.8
Database	HCL BigFix CLM uses DB to store configuration and transactional data of request.	SQL Server 2016/2019/2022 - Standard edition /Enterprise edition
Cisco Intersight Sync Service	It is responsible for syncing Cisco Intersight resources. This is a self-hosted WCF service.	HCL BigFix CLM Certificate, .Net Framework 4.8

2.3 HCL BigFix CLM Benefits

- **Reduce Costs**
  - Higher cost savings through Process standardization & Automation
  - Provide visibility of usage of virtual assets & cost obligations to key custodians
  - Optimize virtual asset utilization to avoid cost leakages.
- **Mitigate Risks**
  - Improve Performance, Fault Tolerance and Compliance of systems and services through proactive advisories.

    - Transform the process from Human driven to Automation driven and eliminate human error from the equation.
    - Mitigate security related risks based on system driven suggestions.

- **Drive Efficiency**
    - Reduce VM provisioning cycle by up to 85%.
    - Achieve up to 50% faster deployment of services through automation.

3 HCL BigFix CLM Installation

The table below describes individual components and steps involved in HCL BigFix CLM installation. Each of those are then detailed in the forthcoming sections.

Table 3 – Components of HCL BigFix CLM Installation

Section Name	Description
HCL BigFix CLM Environment Planning	Help the organization to plan the scale of HCL BigFix CLM deployment for their environment. It creates awareness among the users regarding its environments, architecture, and software and hardware requirements.
HCL BigFix CLM Environment Preparation	It highlights the pre-requisites to run installer & components of HCL BigFix CLM.
Pre-requisites to run the Installer	It highlights the pre-requisites to run the installer.
HCL BigFix CLM Components Pre-requisites Installation	HCL BigFix CLM has multiple components that are designated to perform multiple actions. The section highlights the pre-requisites to install the components.
HCL BigFix CLM Web Layer Installation	The web layer is a part of HCL BigFix CLM architecture that hosts the webserver. Further, the webserver hosts HCL BigFix CLM web UI portal and HCL BigFix CLM APIs.
HCL BigFix CLM App Layer Installation	The app layer is a part of HCL BigFix CLM architecture that hosts the application server. Further, the app server hosts the HCL BigFix CLM components and Job Listener.

A complete installation of HCL BigFix CLM comprises of Databases, Web Interface, and the services i.e., Orchestrator, Workflow, AD Sync etc.

4 HCL BigFix CLM Environment Planning

This section describes how to plan for HCL BigFix CLM deployment. It focusses on architecture, software, and hardware requirements.

4.1 Deployment Environment

The section highlights various HCL BigFix CLM deployment environments to be selected based on the number of managed Virtual Machines (VMs).

Table 4 – Deployment Environment

Environment Type	Small	Medium	Large
No. of VMS managed	<1000	between 1000 and 3000	>3000
Data Retention	6 months	6 months	6 months

4.2 Tiered Architecture of HCL BigFix CLM

HCL BigFix CLM is installed in the following deployment modes:

4.2.1 2- Tier Mode

In this mode, all HCL BigFix CLM components are installed on the following types of servers:

- **Web and App server**- It hosts all HCL BigFix CLM components except the database.
- **Database server**- It hosts all HCL BigFix CLM databases that include the Configuration data, Performance, and Billing.

Table 5 – 2 Tier deployment mode

Layer	HCL BigFix CLM Service Component
Web and App	HCL BigFix CLM Portal
	Job Listener
	Sync Service
	Ad Sync Service
	Workflow Service
	Orchestrator
	ITSM executor
	Generic Task Executor
	Billing Service
	Performance Service

	Health Monitor Service
	Cisco Intersight Sync Service
DB	Database

4.2.2 3-Tier Mode

HCL BigFix CLM 3-Tier mode is different from 2-Tier mode as all the three components are segregated into individual layers, as shown below:

- **Web Server**: It hosts HCL BigFix CLM web UI portal and HCL BigFix CLM APIs. User login to the HCL BigFix CLM portal using LDAP/SAML authentication.
- **App Server**- It hosts HCL BigFix CLM Components & HCL BigFix CLM Job Listener such as Orchestrator and Workflow Service.
- **Database Server**- Database server hosts HCLBigFixCLMDB Configuration DB, Billing DB, and Performance DB.

The installer needs to be run on individual servers, i.e. **Application server**.
Sticky sessions should be configured in the case of load balancer.

Table 6 – 3 Tier Mode

Layer	HCL BigFix CLM Service Component
Web	Portal
	KRS
APP	Job Listener
	Sync Service
	Ad Sync Service
	Workflow Service
	Orchestrator
	ITSM executor
	Generic Task Executor
	Billing Service
	Performance Service
	Health Monitor Service
	Cisco Intersight Sync Service
DB	Database

4.3 Hardware Configuration for HCL BigFix CLM

This section describes the hardware requirements based on the following parameters.

- No. of VMs to be managed.
- High Availability (HA) or Non-HA
- 2- Tier or 3 Tier

4.3.1 Hardware Sizing for Minimal Deployment

Table 7 – Hardware Sizing for Minimal Deployment

Server Name	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Application + Web Server	1	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Database Server	1	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	150 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.2 Hardware Sizing for Small Environment (2 Tier non-HA)

Table 8 – Hardware Sizing for Small Environment (2 Tier non-HA)

Environment Type	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Small	Application + Web Server	Web Tier Application Tier	1	Virtual	4 vCPU, 8 GB RAM	NA	50GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
	Database Server	Data Tier	1	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016/2019/2022 -	150 GB	Operating System - Windows	SQL_Latin1_Genera

						Standard Edition		Server 2016/2019/2022, 64-bit	L_CP1_CI_AS

4.3.3 Hardware Sizing for Small Environment (2 Tier HA)

Table 9 – Hardware Sizing for Small Environment (2 Tier HA)

Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage	Shared Storage	Other Requirements	Remarks
Application + Web Server	Web Tier ----------------- App Tier	2	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	20 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Database Server	Data Tier	2	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	300 GB		SQL Cluster, Always On	

4.3.4 Hardware Sizing for Medium Environment (3 Tier non-HA)

Table 10 – Hardware Sizing for Medium Environment (3 Tier non-HA)

Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Web Tier	1	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Application Tier	1	Virtual	4 vCPU, 8 GB RAM	NA	100 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Data Tier	1	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	300 GB		

4.3.5 Hardware Sizing for Medium Environment (3 Tier HA)

Table 11 – Hardware Sizing for Medium Environment (3 Tier HA)

Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage	Shared Storage	Other Requirements	Remarks
Web Server	Web Tier	2	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	20 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Application Server	Application Tier	2	Virtual	4 vCPU, 8 GB RAM	NA	100 GB	20 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Database Server	Data Tier	2	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	300 GB			SQL Cluster, Always On

4.3.6 Hardware Sizing for Large Environment (3 Tier non-HA)

Table 12 – Hardware Sizing for Large Environment (3 Tier non-HA)

Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Web Server	Web Tier	1	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	Operating System - Windows Server 2016/2019/2022 64-bit	
Application Server	Application Tier	1	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	Operating System - Windows Server 2016/2019/2022 64-bit	
Database Server	Data Tier	1	Virtual	8 vCPU, 32 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	500 GB		

4.3.7 Hardware Sizing for Large Environment (3 Tier HA)

Table 13 – Hardware Sizing for Large Environment (3 Tier HA)

Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage	Shared Storage	Other Requirements	Remarks
Web Server	Web Tier	2	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	50 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Application Server	Application Tier	2	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	50 GB	Operating System - Windows Server 2016/2019/2022, 64-bit	
Database Server	Data Tier	2	Virtual	8 vCPU, 32 GB RAM	Microsoft SQL Server 2016/2019/2022 - Standard Edition	500 GB			SQL Cluster, Always On

5 HCL BigFix CLM Environment Preparation

This section describes how to prepare the environment to perform the physical installation and configuration of HCL BigFix CLM.

Before beginning the installation, identify the installation mode and prepare the environment accordingly.

The following figure gives an overview of HCL BigFix CLM Installation Workflow.

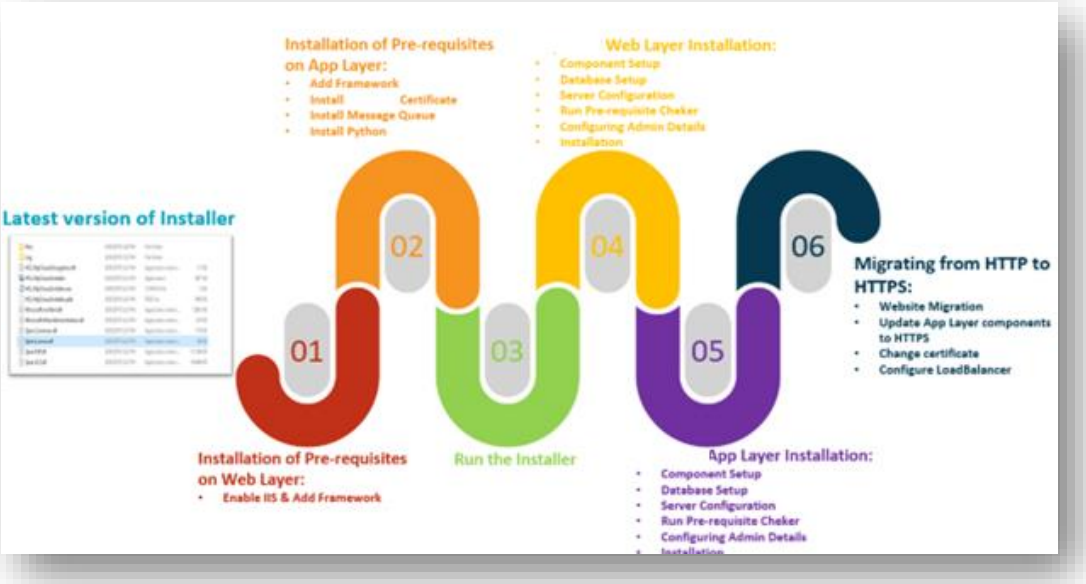


Figure 1 – HCL BigFix CLM Installation Workflow Overview

5.1 Pre-requisites to run the Installer

Once the infrastructure resources are in place, identify the server on which the installer will run. Before executing the installer, the following software pre-requisites need to be in place on the server:

Table 14 – HCL BigFix CLM Server Pre-requisites

Software	Version
Windows Version	Microsoft® Windows® Server 2016 Standard Edition, Windows Server 2019 Enterprise Edition or Microsoft® Windows® Server 2022 Edition,
.Net Framework	.net framework 4.8
Licensed Software	SQL Server 2016/2019/2022 - Standard Edition

Note: Also, we need to install .net Core Hosting Bundle 8.0 and.net Core Runtime 8.0.

5.1.1 Installer

This section describes how to install the HCL BigFix CLM components using installer on any server or standalone machine that can be further used for the deployment of HCL BigFix CLM Web, Application, Database and its underlying components.

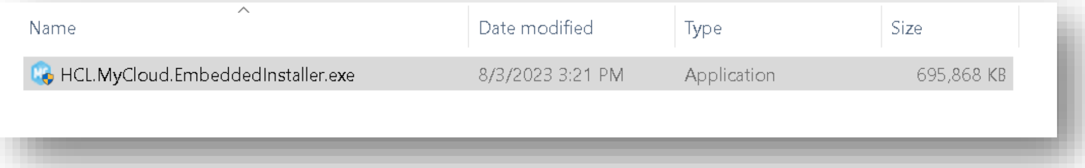
Get the latest version of the installer from the HCL BigFix CLM Product Team or write to bigfixclm-prodsupport-team@hcl-software.com

HCL BigFix CLM installer file includes a **Fully Executable Installer**.

This executable file enables the complete installation of HCL BigFix CLM along with pre-requisite checker for all the servers.

HCL BigFix CLM installation contains the following steps:

- Pre-requisites to run the Installer.
- Run the installer.
- Installation of HCL BigFix CLM using the **Installer**



Name	Date modified	Type	Size
HCL.MyCloud.EmbeddedInstaller.exe	8/3/2023 3:21 PM	Application	695,868 KB

Figure 2 – Installer

Refer to the table below to understand some of the important fields mentioned in the above figure:

Table 15 – Installer Files Description

File Name	Description
Log	This folder contains a log created during the installation process. Initially the folder will not be present, it will be generated once the installation is started.
HCL_BigFix_CLM_Installer	This is the executable file to install HCL BigFix CLM

To Install the prerequisites, download the prerequisites folder from the same place where HCL BigFix CLMInstaller is downloaded.

1. Open the **Prerequisites** folder.

Figure 3 – Install Pre-requisites

2. To install any Prerequisite, Select respective folder (for e.g. Click **Python**).

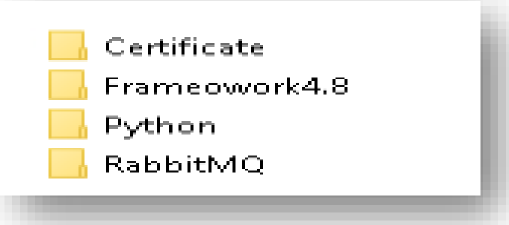

Certificate
Frameowork4.8
Python
RabbitMQ

Figure 4 – Install Python

Refer to the table below to understand the fields mentioned in the above figure:

Table 16 – Description of Certificate

File Name	Description
Certificate	This folder contains a HCL BigFix CLM generated certificate that for inter-component communication
Framework4.8	This folder contains .net 4.8 runtime executable needed to be installed on HCL BigFix CLM App and Web Servers
Python	This folder contains Python executable for windows
RabbitMQ	This folder contains RabbitMQ binaries.

For **Python** installation: Before running the installer, make sure that **Everyone** has the Write Permission on the Python folder.

Installation of Each Prerequisite installation procedure is detailed out in the respective section below.

5.1.2 Enable Log on as Service

The user account/service account by which HCL BigFix CLM services/components are run must have **Log on as Service** rights on both Web and App Servers.

– To check and enable the same (if not already enabled) follow the Microsoft link below:

https://learn.microsoft.com/en-us/system-center/scsm/enable-service-log-on-sm?view=sc-sm-2022#enable-service-log-on-through-a-local-group-policy

5.2 HCL BigFix CLM Components Pre-requisites Installation

The following table lists the component-wise pre-requisites of HCL BigFix CLM. It is important to install all the pre-requisites for the successful installation of HCL BigFix CLM.

Table 17 – HCL BigFix CLM Component Prerequisites Installation

Component Name	Microsoft .NET Framework 4.8	IIS	Certificate	Python/PowerShell	MSMQ/Rabbit MQ	DB
Portal	Y	Y	Y	N	N	N
Job Listener	Y	N	Y	N	N	N
Sync Service	Y	N	Y	Y	N	N

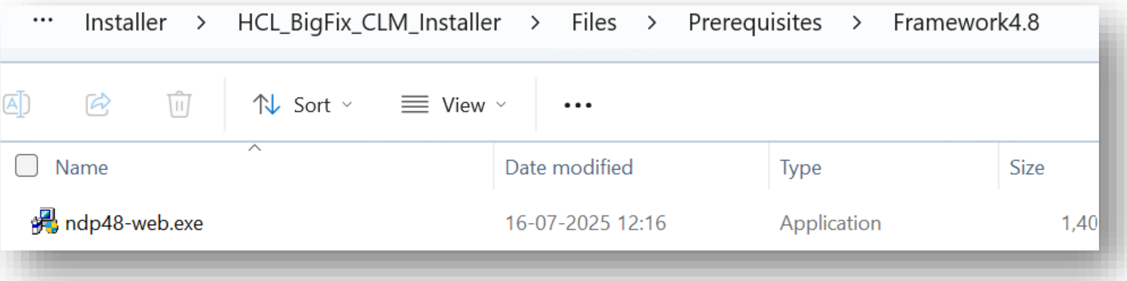
Ad Sync Service	Y	N	Y	N	N	N
Workflow Service	Y	N	Y	N	Y	N
Orchestrator	Y	N	Y	Y	N	N
ITSM executor	Y	N	Y	N	N	N
Generic Task Executor	Y	N	Y	N	N	N
Billing Service	Y	N	Y	N	N	N
Performance Service	Y	N	Y	N	N	N
Health Monitor Service	Y	N	Y	N	N	N
Database	N	N	N	N	N	Y
Cisco Intersight Sync Service	Y	N	Y	N	N	N

5.2.1 Installation of pre-requisites on Web Layer

This section describes how to install the pre-requisites of **HCL BigFix CLM Web Layer**. As stated in Table 17 – HCL BigFix CLM Component Prerequisites Installation, the web layer pre-requisites are **certificate, IIS** and **.Net Framework**.

5.2.1.1 Install .Net Framework 4.8 Runtime

1. Make sure the **HCL_BigFix_CLM_Installerzip (provided by HCL BigFix CLM Support Team)** is present on **Web** server.
2. Unzip the Installer **Zip** file.
3. Go to the .Net 4.8 setup file present in **Prerequisites** folder as shown below.



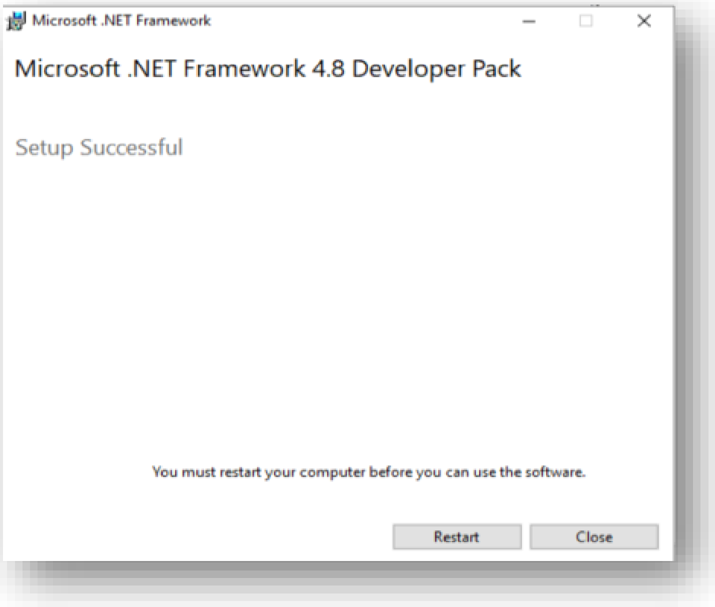
··· Installer > HCL_BigFix_CLM_Installer > Files > Prerequisites > Framework4.8

Name	Date modified	Type	Size
ndp48-web.exe	16-07-2025 12:16	Application	1,40

Figure 5 – Install .Net Framework 4.8

4. Install the .net 4.8 setup on the Web server.

5. On Successful installation, if the below message comes to restart the server, Restart the Web Server. If System doesn't ask for Restart **close** the setup.



Microsoft .NET Framework 4.8 Developer Pack

Setup Successful

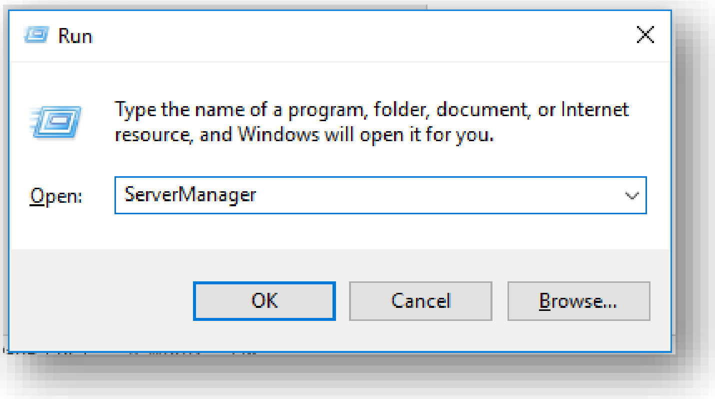
You must restart your computer before you can use the software.

Figure 6 – Install .Net Framework 4.8 (Cont.)

5.2.1.2 Enable IIS and add .Net Framework

To enable IIS on HCL BigFix CLM **Web Server**, login to the server and follow the below steps:

1. Press **Window + R** keys on keyboard to open RUN command window.
2. Type **ServerManager** and click **Ok**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ServerManager

Figure 7 – Enable IIS and add .Net Framework

3. The Server Manager window appears.
4. Click on Add roles and features.

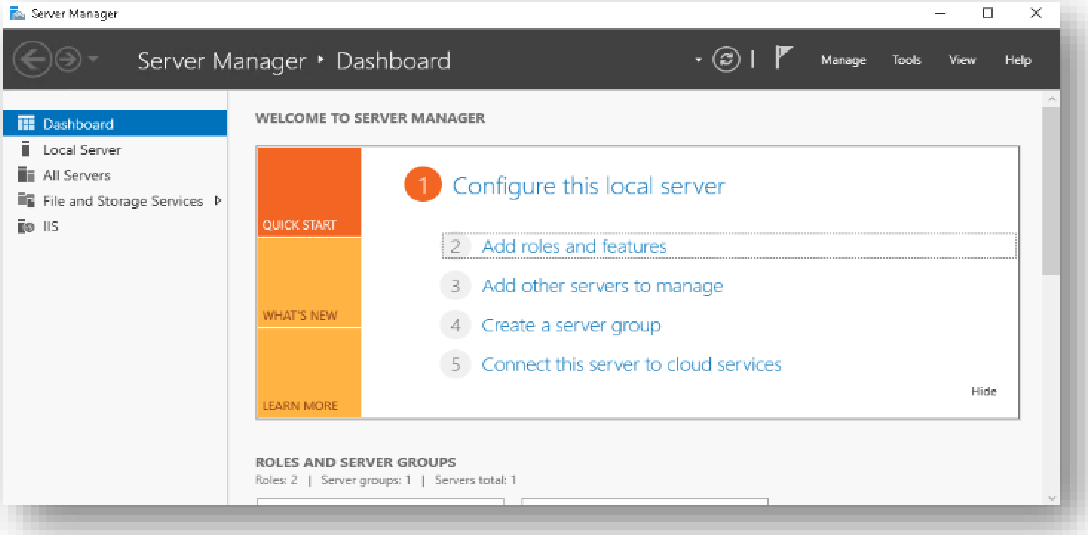
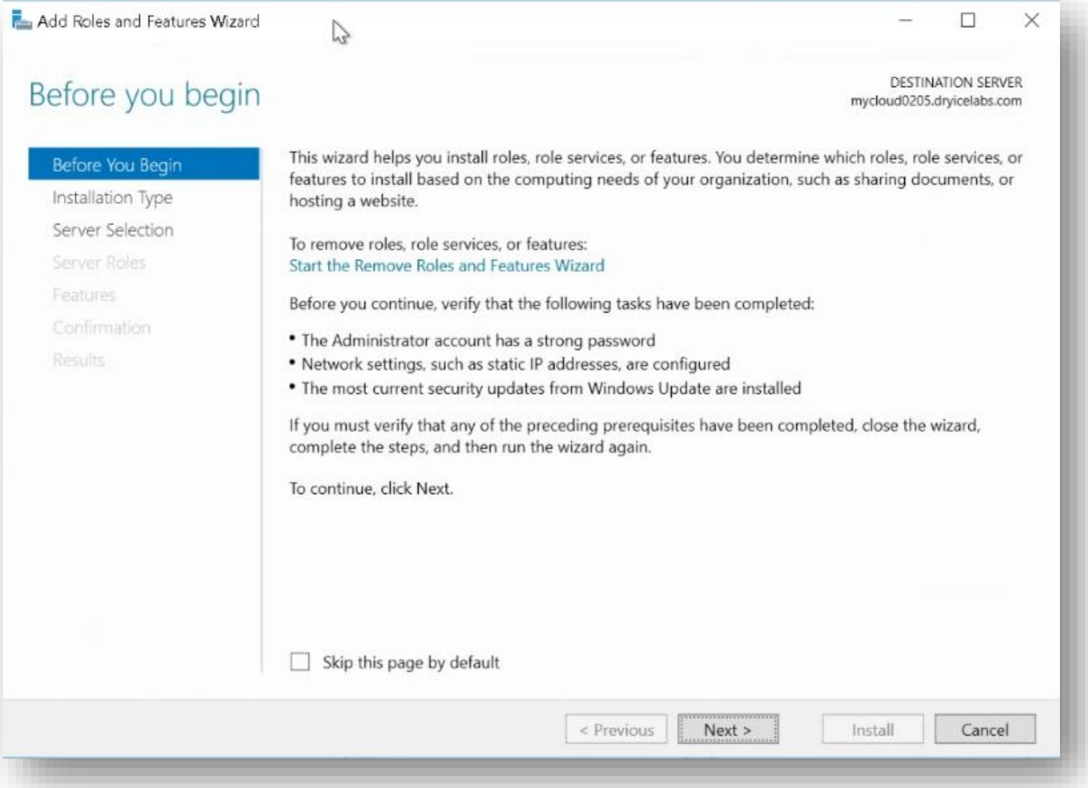

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

Figure 8 – Add Roles and Features

5. The Add roles and features wizard appears. By default, the option Before You Begin is selected in the left panel of the wizard.
6. Click **Next**.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

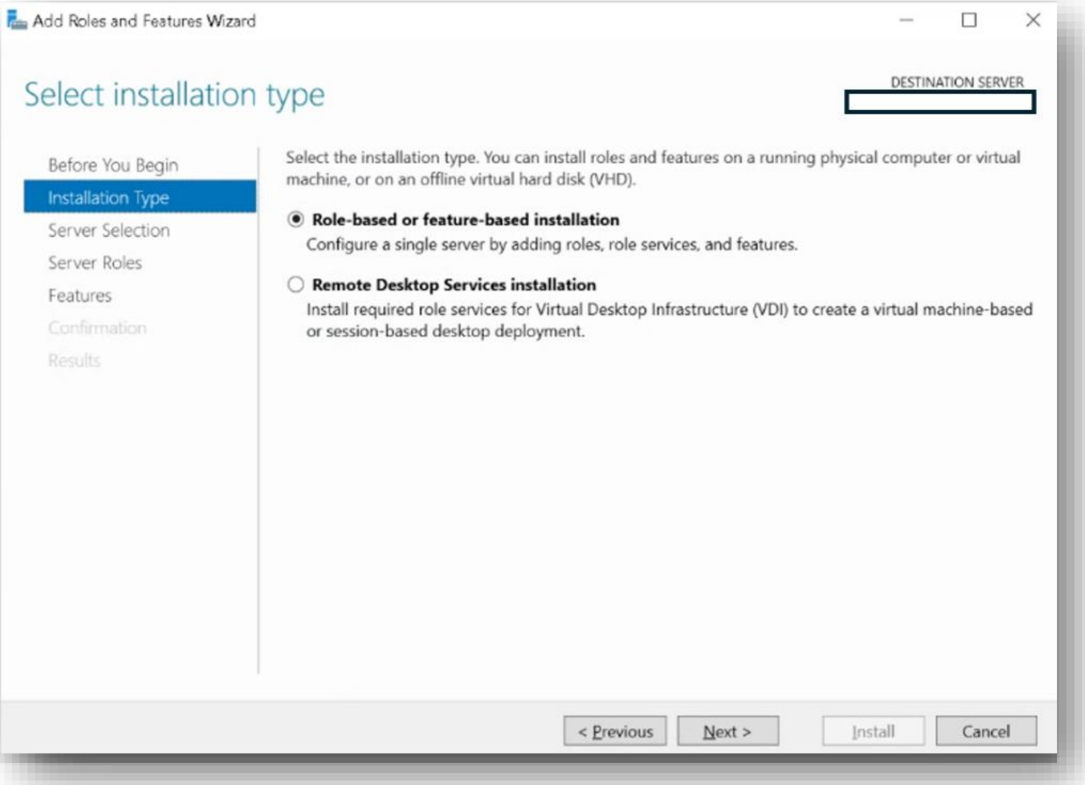
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

Figure 9 – Enable IIS and Add .Net Framework (Cont.)

7. The Installation Type option is auto selected. Enable Role-based or feature-based installation Radio button if not automatically enabled.
8. Click **Next**.



Select installation type

DESTINATION SERVER
[redacted]

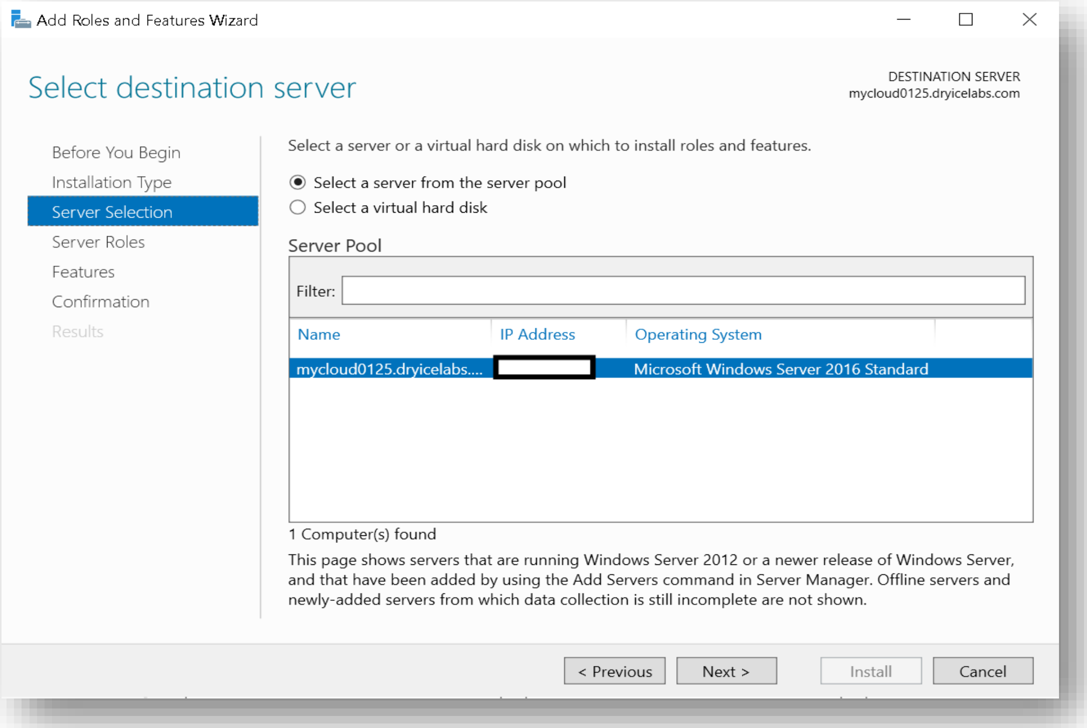
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 10 – Enable IIS and Add .Net Framework (Cont.)

9. The **Server Selection** option is auto selected.



Select destination server

DESTINATION SERVER
mycloud0125.dryicelabs.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
mycloud0125.dryicelabs....	[redacted]	Microsoft Windows Server 2016 Standard

1 Computer(s) found

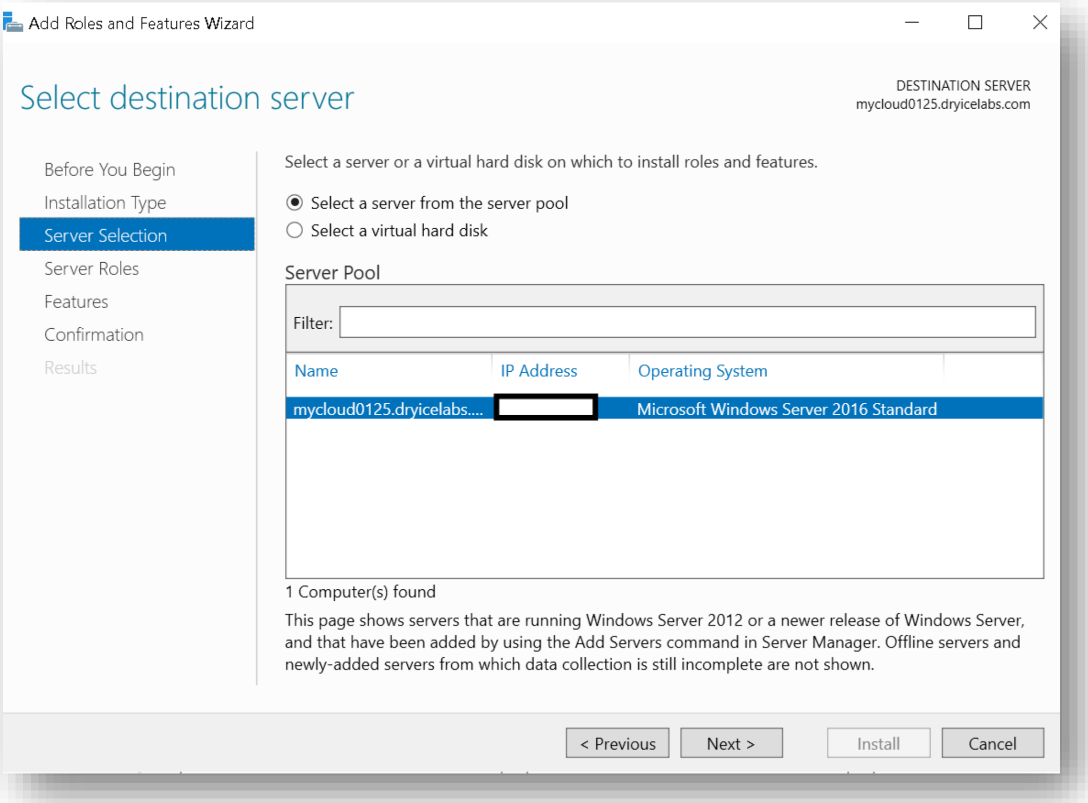
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 11 – Enable IIS and Add .Net Framework (Cont.)

10. Choose Select a server from the Server Pool option.

11. Select the Machine Name in the Server Pool if not automatically selected.

12. Click **Next**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
mycloud0125.dryicelabs.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
mycloud0125.dryicelabs....	[redacted]	Microsoft Windows Server 2016 Standard

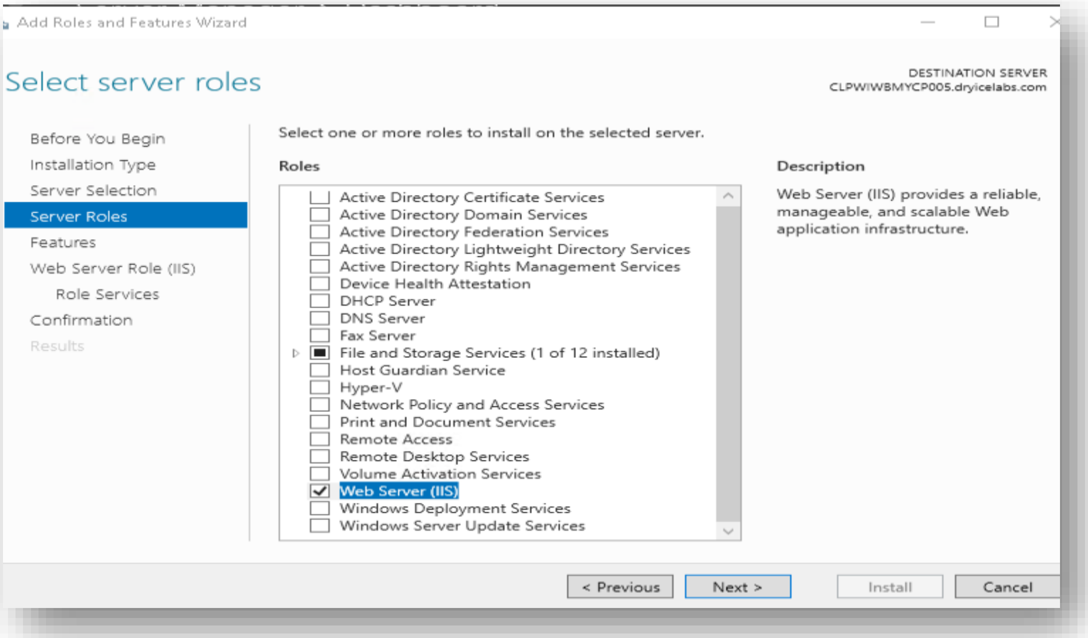
1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 12 – Enable IIS and Add .Net Framework (Cont.)

13. The **Server** Roles Screen appears.

14. Enable IIS by selecting **Web Server (IIS)**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
CLPWIWBMYCP005.dryicelabs.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

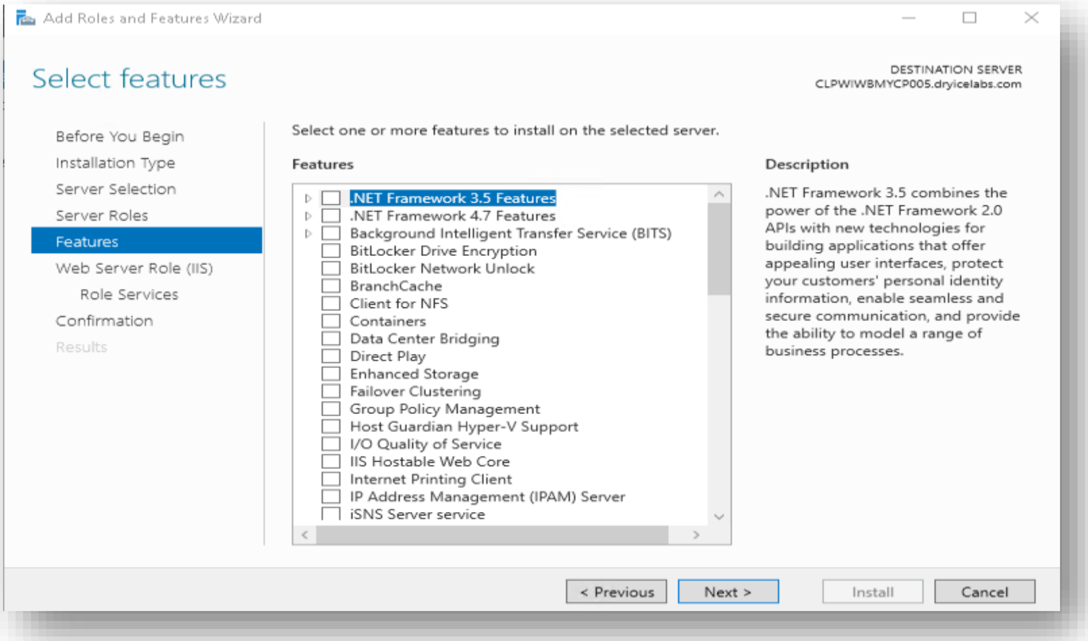
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 13 – Enable IIS and Add .Net Framework (Cont.)

15. Add Roles and Features Wizard appears, Click on Features.

16. Click Next.

17. Features screen gets enabled as below.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
CLPWIWBMYCP005.dryicelabs.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

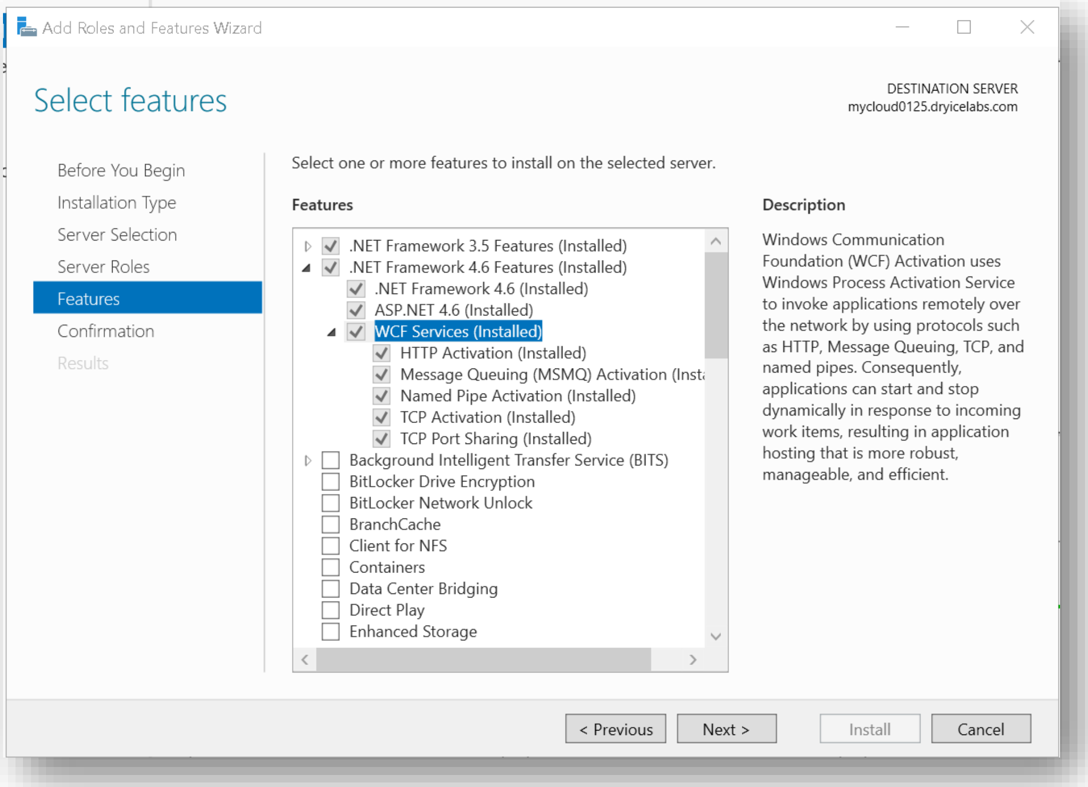
- □ .NET Framework 3.5 Features
- □ .NET Framework 4.7 Features
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 14 – Enable IIS and Add .Net Framework (Cont.)

18. Enable .Net Framework, ASP .Net Framework and WCF Services.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
mycloud0125.dryicelabs.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

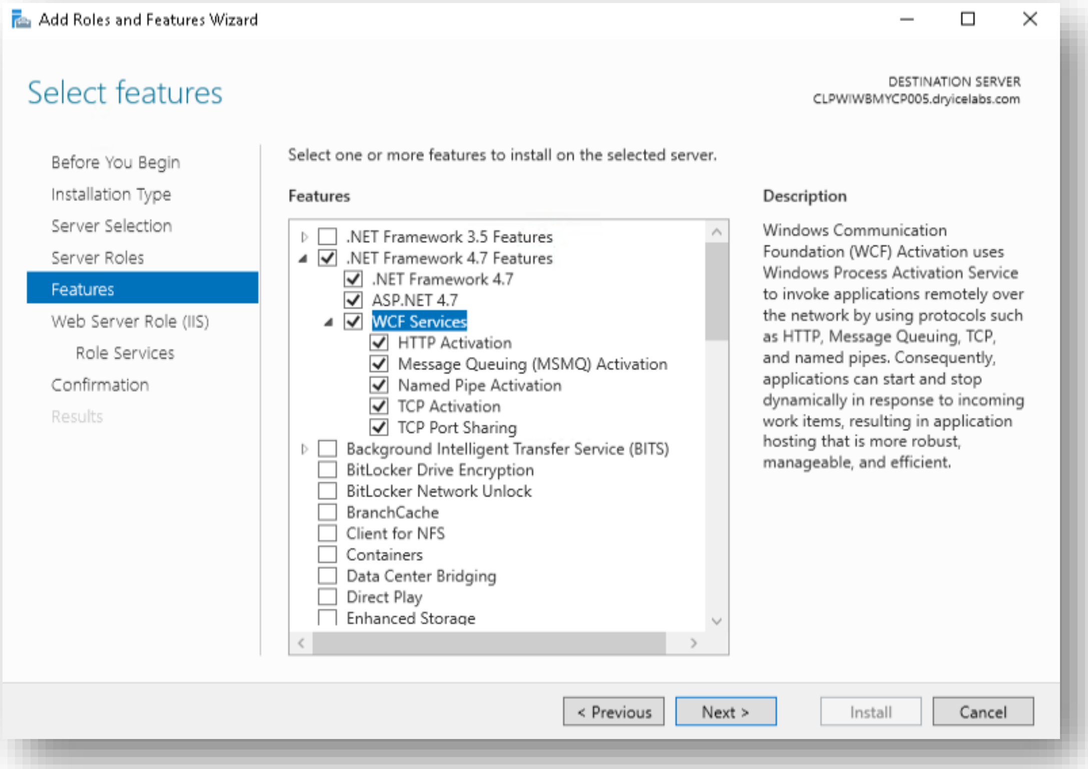
- ☑ .NET Framework 3.5 Features (Installed)
- ☑ .NET Framework 4.6 Features (Installed)
  - ☑ .NET Framework 4.6 (Installed)
  - ☑ ASP.NET 4.6 (Installed)
  - ☑ WCF Services (Installed)
    - ☑ HTTP Activation (Installed)
    - ☑ Message Queuing (MSMQ) Activation (Insta
    - ☑ Named Pipe Activation (Installed)
    - ☑ TCP Activation (Installed)
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage

Description

Windows Communication Foundation (WCF) Activation uses Windows Process Activation Service to invoke applications remotely over the network by using protocols such as HTTP, Message Queuing, TCP, and named pipes. Consequently, applications can start and stop dynamically in response to incoming work items, resulting in application hosting that is more robust, manageable, and efficient.

Figure 15 – Enable IIS and Add .Net Framework (Cont.)

19. Select All WCF Services as shown in below figure:



Add Roles and Features Wizard

Select features

DESTINATION SERVER
CLPWIWBMYCP005.dryicelabs.com

Select one or more features to install on the selected server.

Features

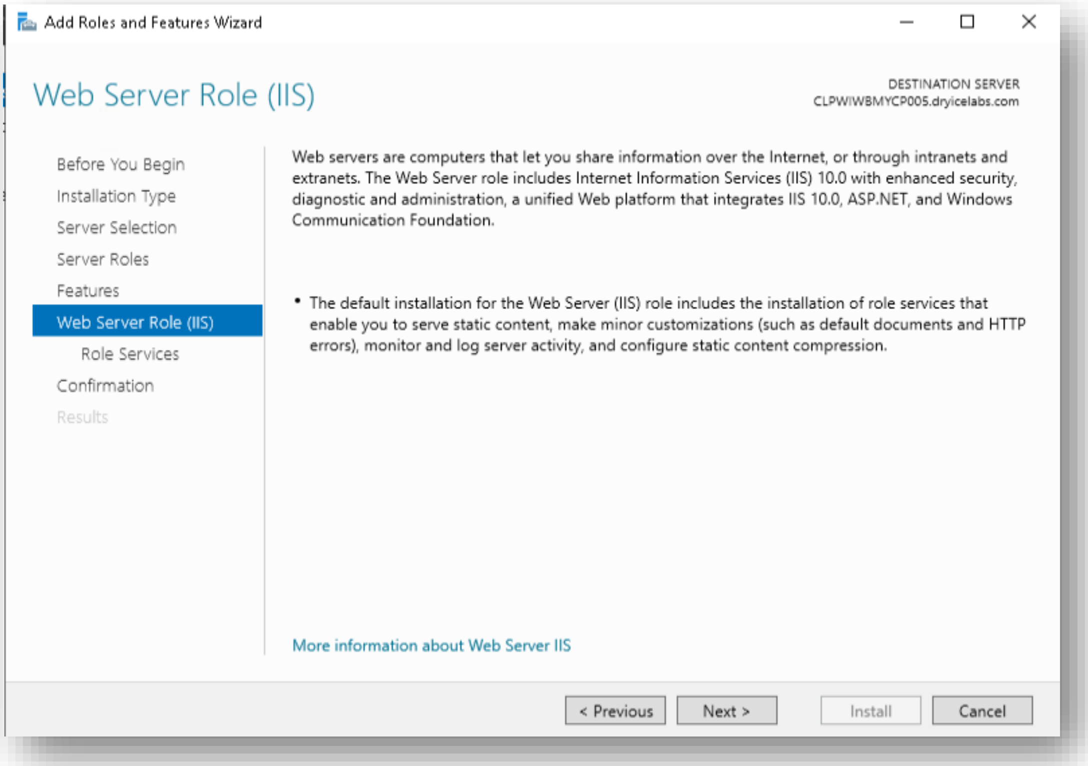
- □ .NET Framework 3.5 Features
- ☑ .NET Framework 4.7 Features
  - ☑ .NET Framework 4.7
  - ☑ ASP.NET 4.7
  - ☑ WCF Services
    - ☑ HTTP Activation
    - ☑ Message Queuing (MSMQ) Activation
    - ☑ Named Pipe Activation
    - ☑ TCP Activation
    - ☑ TCP Port Sharing
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage

Description

Windows Communication Foundation (WCF) Activation uses Windows Process Activation Service to invoke applications remotely over the network by using protocols such as HTTP, Message Queuing, TCP, and named pipes. Consequently, applications can start and stop dynamically in response to incoming work items, resulting in application hosting that is more robust, manageable, and efficient.

Figure 16 – Enable IIS and Add .Net Framework (Cont.)

20. Click **Next**, Web Server Role (IIS) screen appears.



Add Roles and Features Wizard

Web Server Role (IIS)

DESTINATION SERVER
CLPWIWBMYCP005.dryicelabs.com

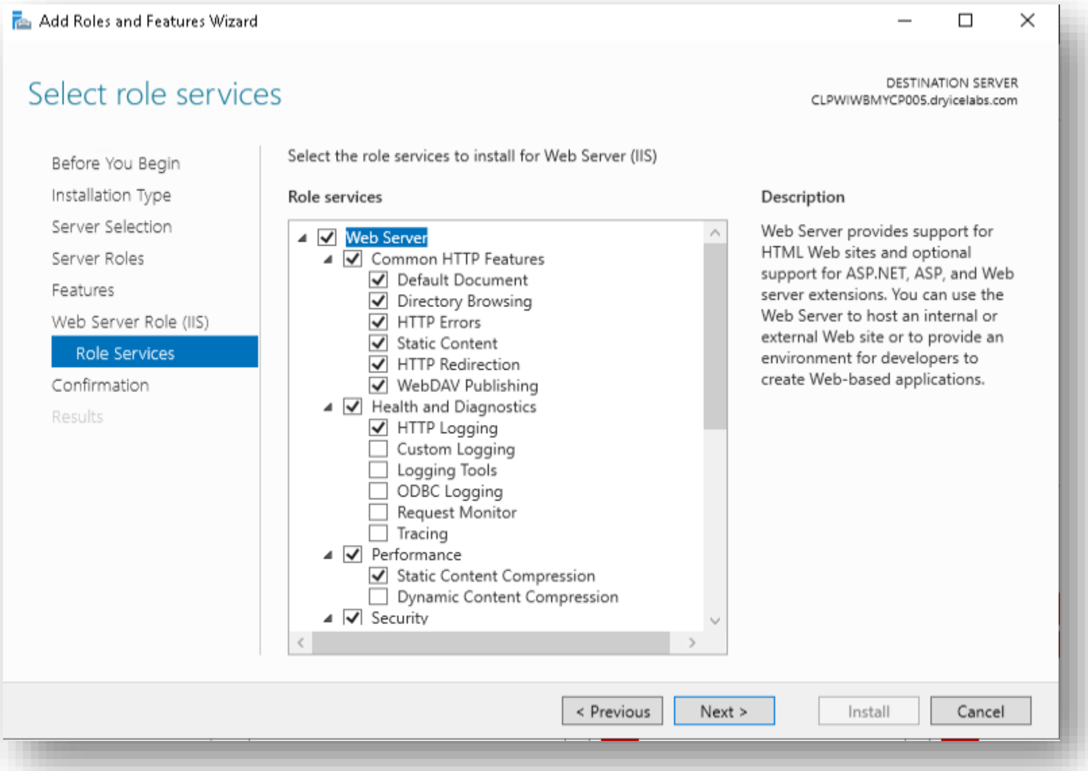
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

Figure 17 – Enable IIS and Add .Net Framework (Cont.)

21. Click Next to go to “**Role Services**”.
22. Under Web Server, Select **Services** as mentioned in below 2 screenshots.



Select role services

DESTINATION SERVER
CLPWIWBMYCP005.dryicelabs.com

Select the role services to install for Web Server (IIS)

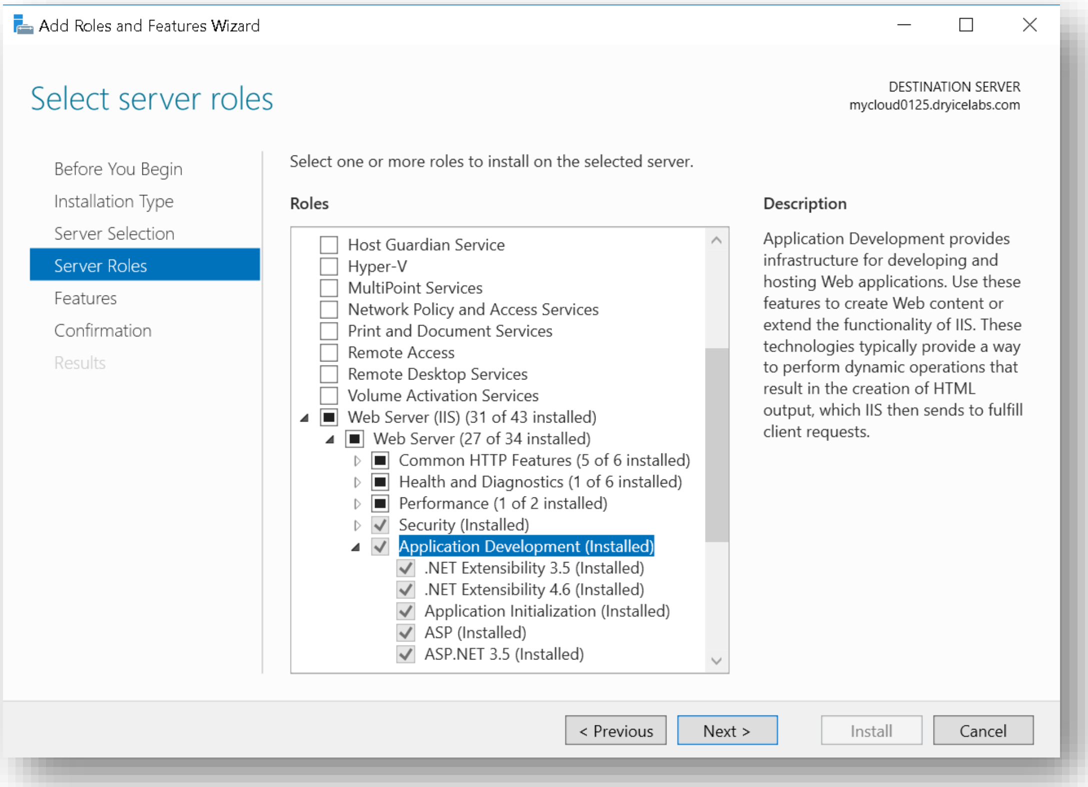
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - ☑ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☐ Custom Logging
    - ☐ Logging Tools
    - ☐ ODBC Logging
    - ☐ Request Monitor
    - ☐ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - ☐ Dynamic Content Compression
  - ☑ Security

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Figure 18 – Enable IIS and Add .Net Framework (Cont.)



Select server roles

DESTINATION SERVER
mycloud0125.dryicelabs.com

Select one or more roles to install on the selected server.

Roles

- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ■ Web Server (IIS) (31 of 43 installed)
  - ■ Web Server (27 of 34 installed)
    - ■ Common HTTP Features (5 of 6 installed)
    - ■ Health and Diagnostics (1 of 6 installed)
    - ■ Performance (1 of 2 installed)
    - ☑ Security (Installed)
    - ☑ Application Development (Installed)
      - ☑ .NET Extensibility 3.5 (Installed)
      - ☑ .NET Extensibility 4.6 (Installed)
      - ☑ Application Initialization (Installed)
      - ☑ ASP (Installed)
      - ☑ ASP.NET 3.5 (Installed)

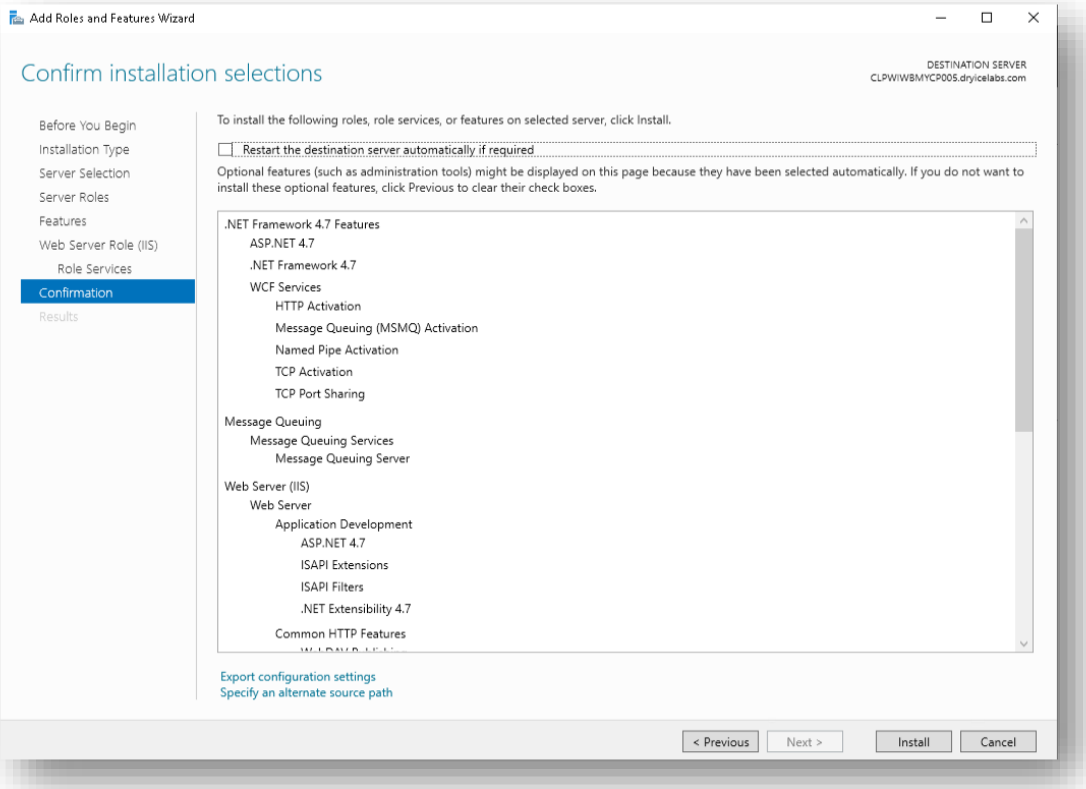
Description

Application Development provides infrastructure for developing and hosting Web applications. Use these features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfill client requests.

Figure 19 – Enable IIS and Add .Net Framework (Cont.)

23. Click **Next**

24. On Confirmation Screen, Click **Install**



To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

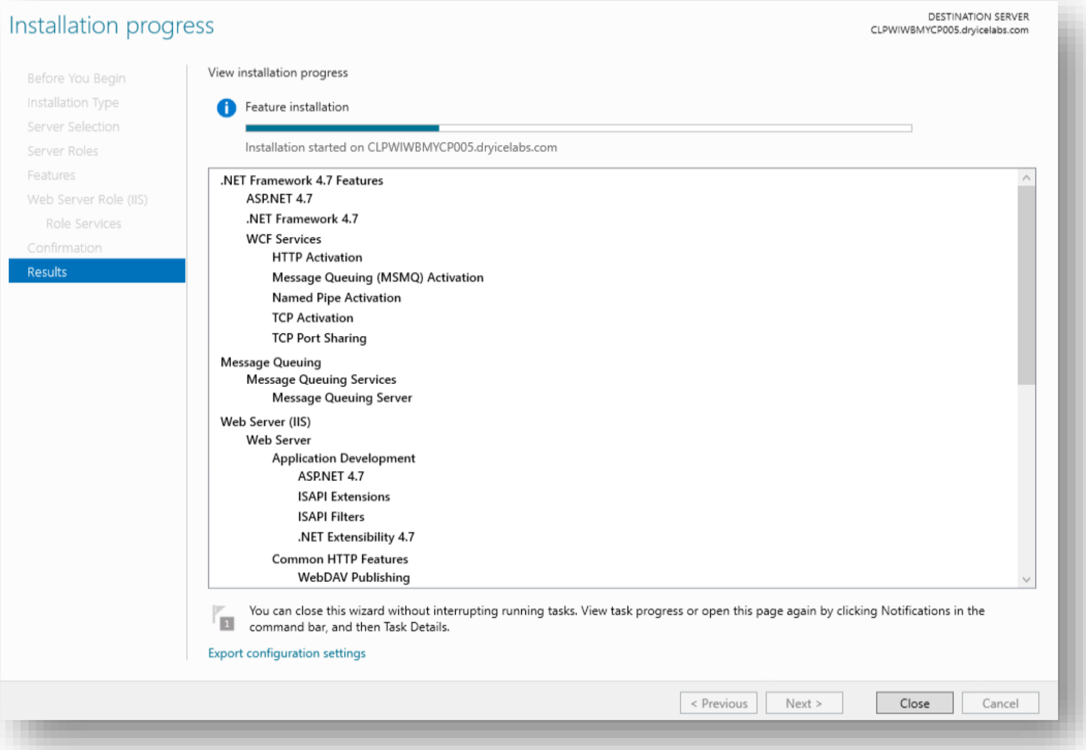
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
.NET Framework 4.7 Features
    ASP.NET 4.7
    .NET Framework 4.7
    WCF Services
        HTTP Activation
        Message Queuing (MSMQ) Activation
        Named Pipe Activation
        TCP Activation
        TCP Port Sharing
Message Queuing
    Message Queuing Services
        Message Queuing Server
Web Server (IIS)
    Web Server
        Application Development
            ASP.NET 4.7
            ISAPI Extensions
            ISAPI Filters
            .NET Extensibility 4.7
        Common HTTP Features
```

Figure 20 - Enable IIS and Add .Net Framework (Cont.)

Do not select the check box to **Restart Destination Server.**

The Installation progress screen shows the current installation status.



View installation progress

Feature installation

Installation started on CLPWIWBMYCP005.dryicelabs.com

```
.NET Framework 4.7 Features
    ASP.NET 4.7
    .NET Framework 4.7
    WCF Services
        HTTP Activation
        Message Queuing (MSMQ) Activation
        Named Pipe Activation
        TCP Activation
        TCP Port Sharing
Message Queuing
    Message Queuing Services
        Message Queuing Server
Web Server (IIS)
    Web Server
        Application Development
            ASP.NET 4.7
            ISAPI Extensions
            ISAPI Filters
            .NET Extensibility 4.7
        Common HTTP Features
            WebDAV Publishing
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

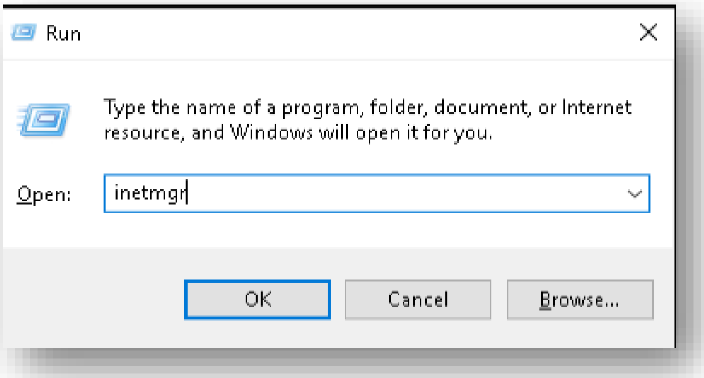
Figure 21 – Installation Status

25. Once the **IIS & .Net framework** are installed successfully, click on the **Close** button to exit the wizard.

A default website is configured on port ‘80’ after the installation of IIS.
Please delete the website.

5.2.1.3 Delete Default Website on Port

1. Press **Window + R** keys on keyboard to open RUN command window.
2. Type **inetmgr** and click **Ok**.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: inetmgr

Figure 22 – Open IIS Manager

3. From **Connections** Menu on left panel, Click on **Web Server name.**
   a. Expand and go to **Sites**, Expand **Sites** and delete Default Web Site (if exists) by clicking on **Remove** as shown in following figure:

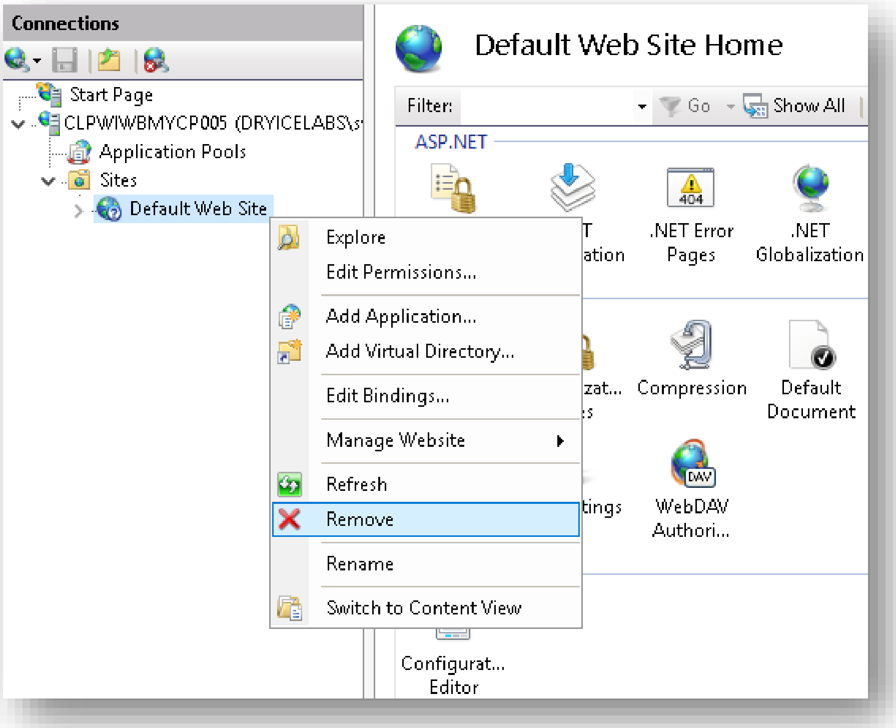


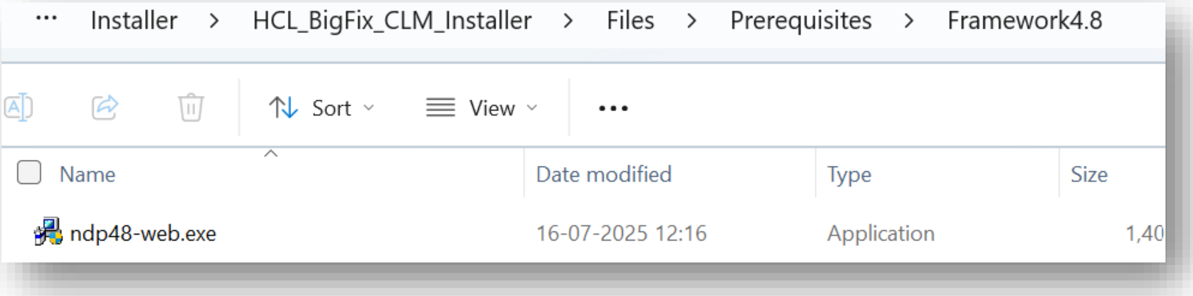
Figure 23 – Delete Default Website

5.2.2 Installation of Pre-requisites on App Layer

This section describes how to install the pre-requisites of **HCL BigFix CLM App Layer**. As stated in Table 17 – HCL BigFix CLM Component Prerequisites Installation, the App layer pre-requisites are **Certificate**, **Messaging Queue**, **.Net Framework,** and **Python**.

5.2.2.1 Install .Net Framework 4.8 Runtime

1. Make sure the HCL BigFix CLM Installer zip (provided by HCL BigFix CLM Support Team) is present on App server.
2. Unzip the Installer Zip file.
3. Go to the .Net 4.8 setup file present in **Prerequisites** folder as shown below.

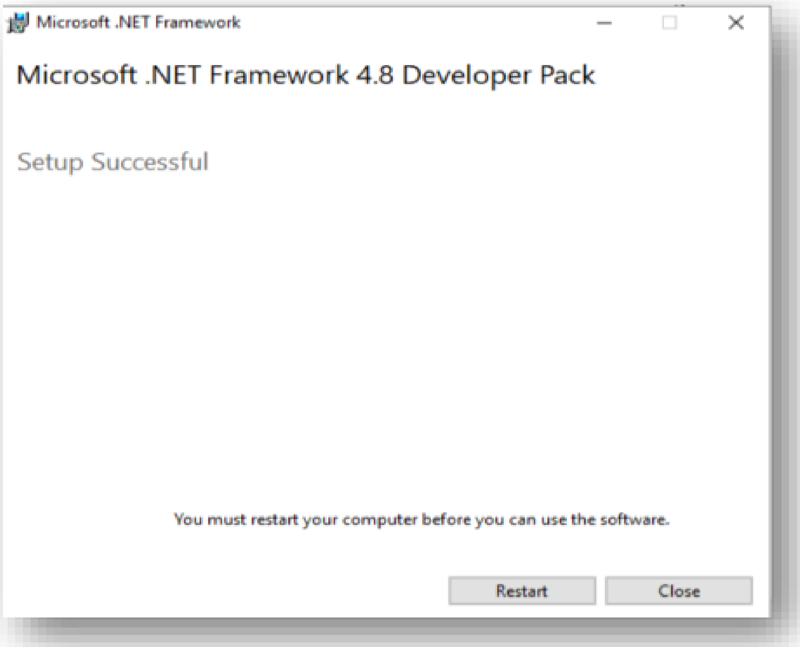


··· Installer > HCL_BigFix_CLM_Installer > Files > Prerequisites > Framework4.8

Name	Date modified	Type	Size
ndp48-web.exe	16-07-2025 12:16	Application	1,40

Figure 24 - Install .Net Framework 4.8 Runtime

4. Install the .net 4.8 setup on the App server.
5. On Successful installation if below message comes to restart the server, Restart the **App** Server. If System doesn't ask for Restart **close** the setup



Microsoft .NET Framework

Microsoft .NET Framework 4.8 Developer Pack

Setup Successful

You must restart your computer before you can use the software.

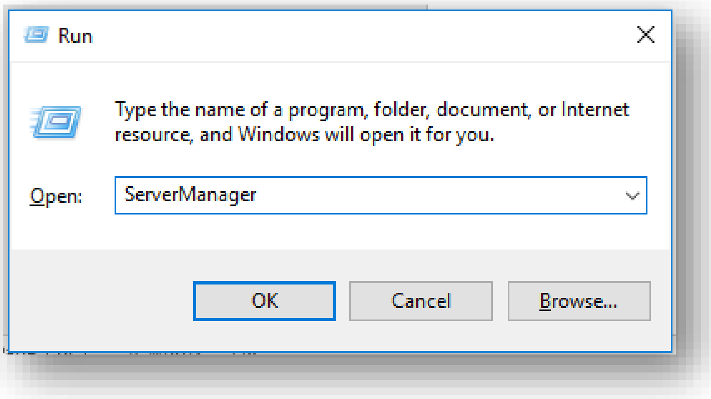
Figure 25 - Install .Net Framework 4.8 Runtime (Cont.)

5.2.2.2 Add .Net Framework

To add .Net framework, refer to Enable IIS and Add .Net Framework section.

5.2.2.3 Installing Messaging Queue

1. Press **Window + R** keys on the keyboard to open the **RUN** command window.
2. Type ServerManager and click **OK**.

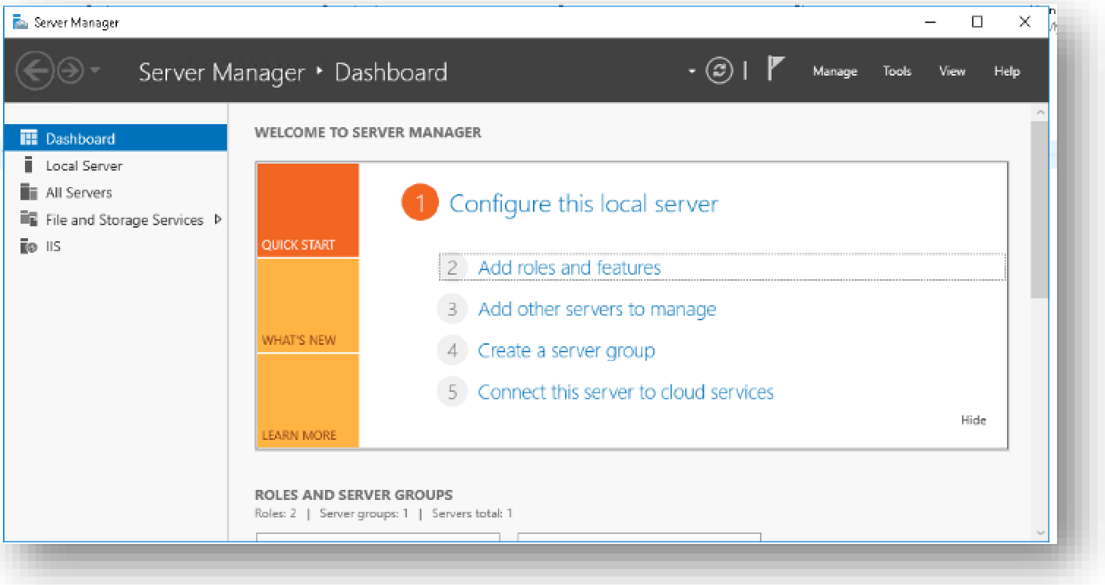


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ServerManager

Figure 26 – Installing Messaging Queue

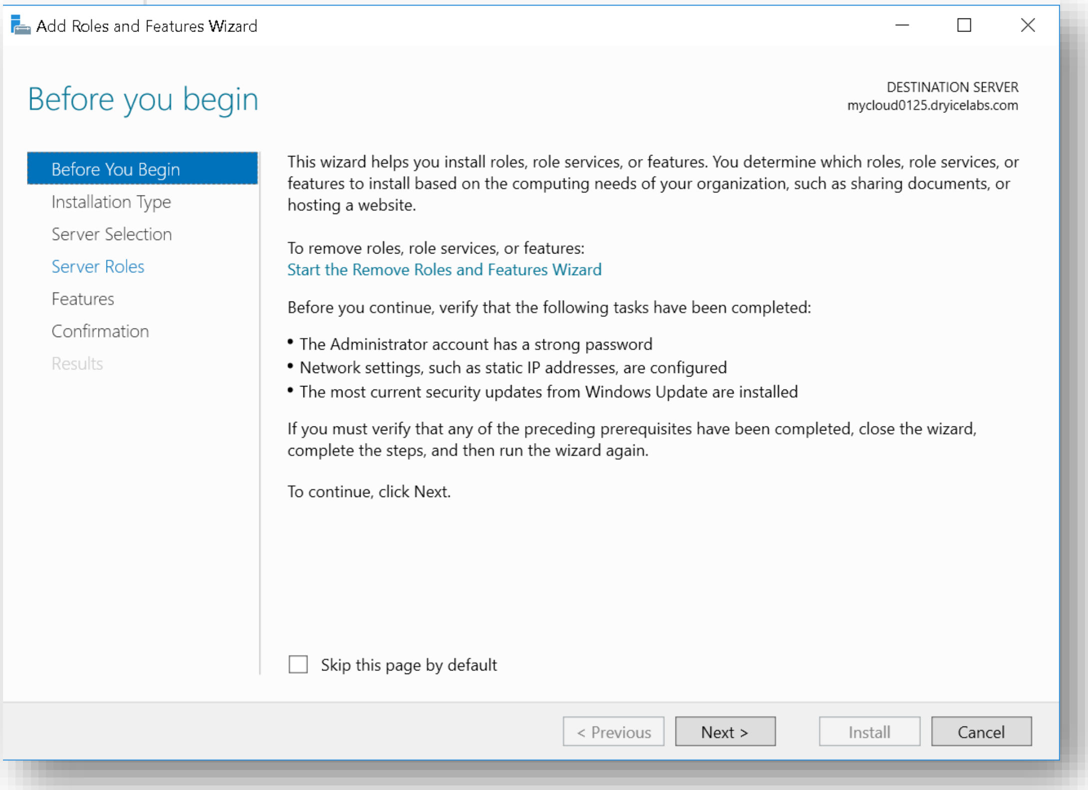
3. The Server Manager window appears.
4. Click on Add roles and features.



Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

Figure 27 - Installing Messaging Queue (Cont.)

5. The Add roles and features wizard appears. By default, the Before you begin option is selected.
6. Click **Next**.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

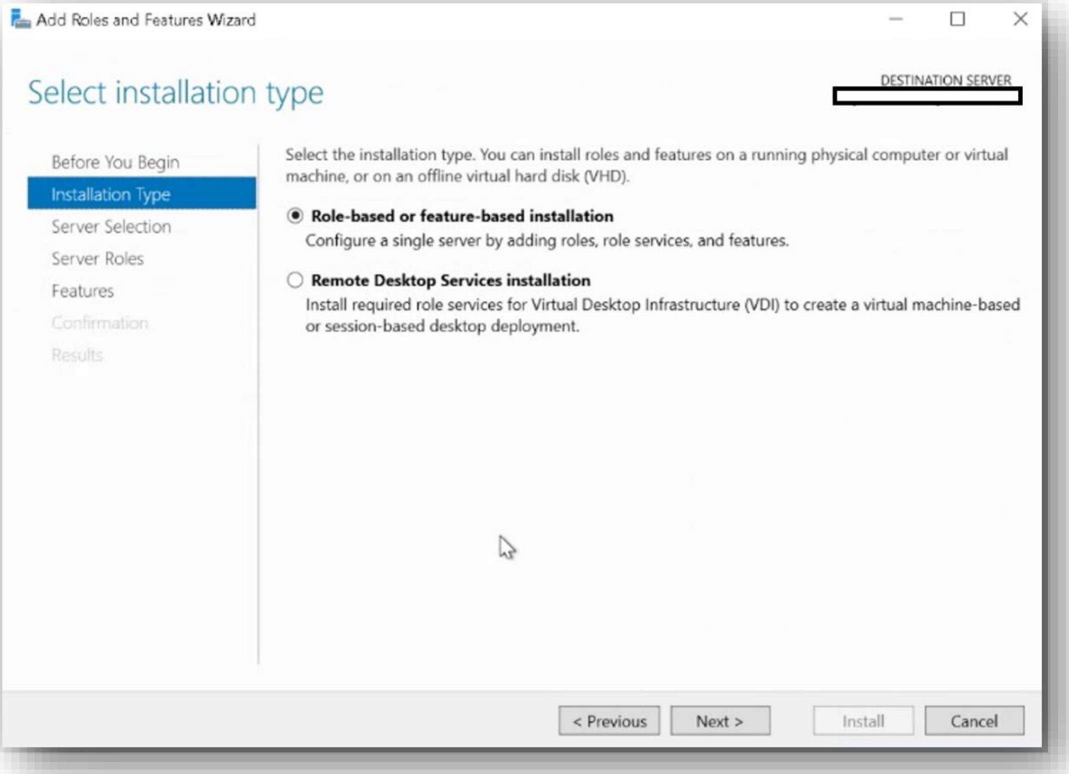
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Figure 28 – Installing Messaging Queue (Cont.)

7. The Select installation Type page appears.
8. Select Role-based or feature-based installation and then click **Next**.



[redacted]

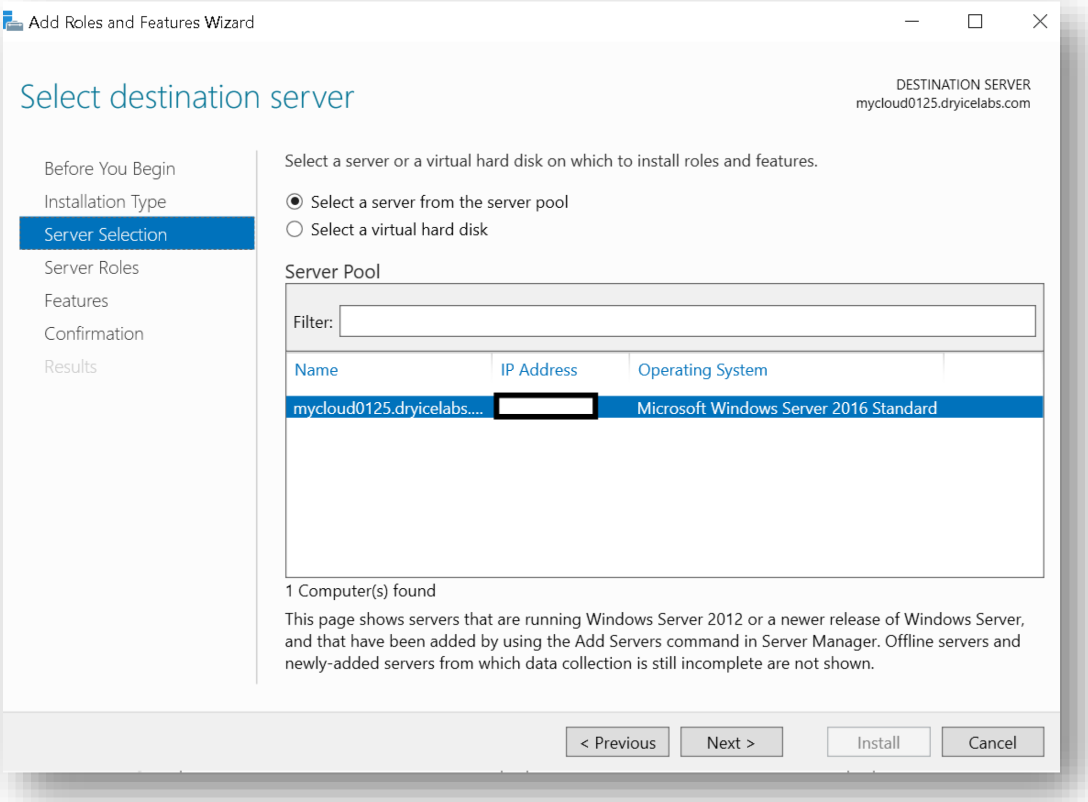
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 29 – Installing Messaging Queue (Cont.)

9. The Server Selection page appears.
10. Select the option Select a server from the server pool.
11. Select the **Machine Name** in the **Server Pool** field and then click **Next**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
mycloud0125.dryicelabs.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

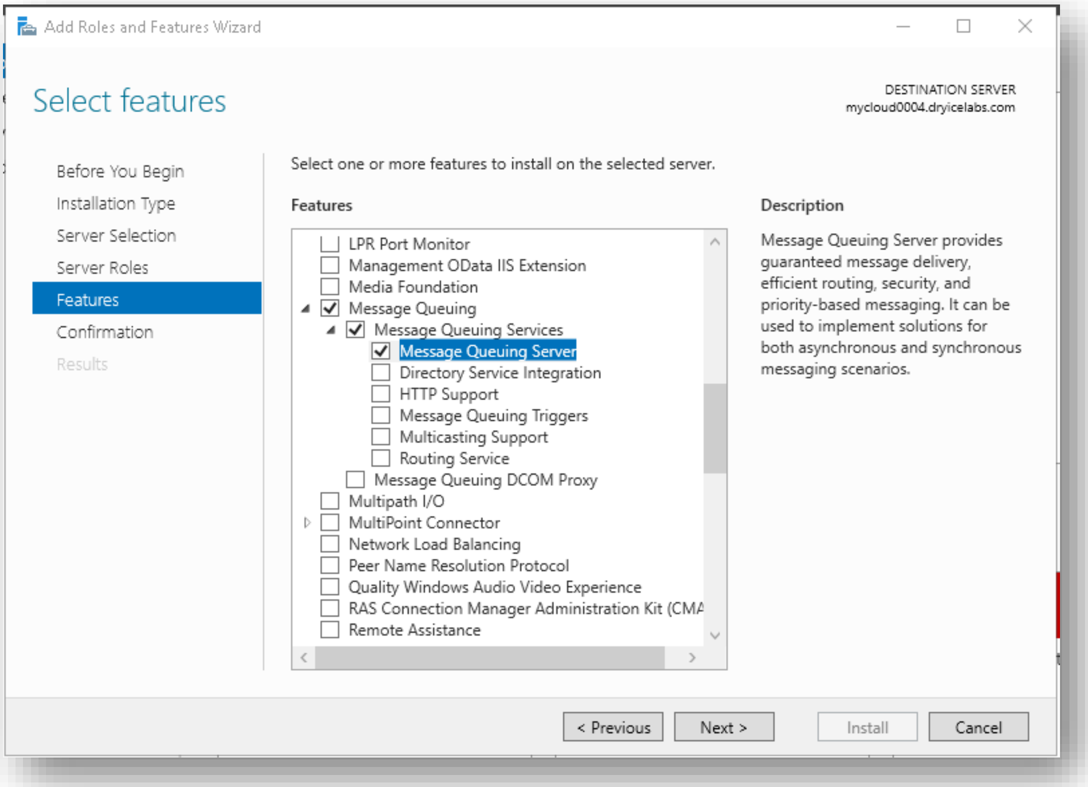
Name	IP Address	Operating System
mycloud0125.dryicelabs....	[redacted]	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 30 - Installing Messaging Queue (Cont.)

12. On **Features,** select **Message Queuing Server** (if not already selected) as shown in the following figure:



Add Roles and Features Wizard

Select features

DESTINATION SERVER
mycloud0004.dryicelabs.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- □ LPR Port Monitor
- □ Management OData IIS Extension
- □ Media Foundation
- ☑ Message Queuing
  - ☑ Message Queuing Services
    - ☑ Message Queuing Server
    - □ Directory Service Integration
    - □ HTTP Support
    - □ Message Queuing Triggers
    - □ Multicasting Support
    - □ Routing Service
  - □ Message Queuing DCOM Proxy
- □ Multipath I/O
- □ MultiPoint Connector
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ RAS Connection Manager Administration Kit (CMA
- □ Remote Assistance

Description

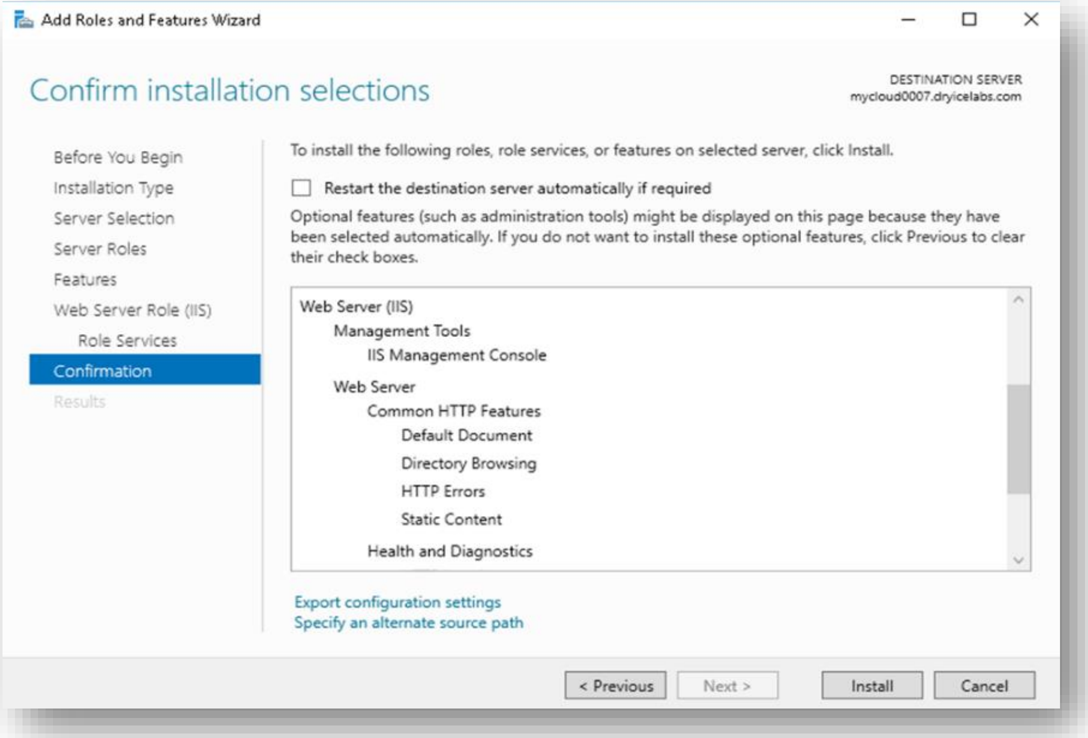
Message Queuing Server provides guaranteed message delivery, efficient routing, security, and priority-based messaging. It can be used to implement solutions for both asynchronous and synchronous messaging scenarios.

Figure 31 – Installing Messaging Queue (Cont.)

If Messaging Queue Server already showing as Installed, click on Cancel and close the wizard and skip below steps for Installing the same.

13. Click **Next**.

14. The Confirmation page appears.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
mycloud0007.dryicelabs.com

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Figure 32 – Installing Messaging Queue (Cont.)

15. Click **Install**.

HCL BigFix CLM supports **Microsoft Messaging Queue** and **RabbitMQ**. In this guide, we have considered **MSMQ** for installation. If the user wishes to use Rabbit MQ, the user needs to do configuration changes against **Workflow Service** in **Manage Component Keys Section** using Admin login credentials. The user also needs to install RabbitMQ and configure stand-alone or in HA according to their architectural requirement.

16. Installation progress screen shows the installation status.
17. Once the Messaging Queue is installed, **Close** the Installation wizard and **Exit**.

5.2.2.4 Installing Python

Follow the steps below to install Python.

1. Go to the following location where Python setup file is available:
2. {drive where HCL_BigFix_CLM_Installer exists}

   \HCL_BigFix_CLM_Installer\Files\Prerequisites\Python\python-3.6.8-amd64.exe}.
3. Right-click on the setup file and click on **Run as administrator**.

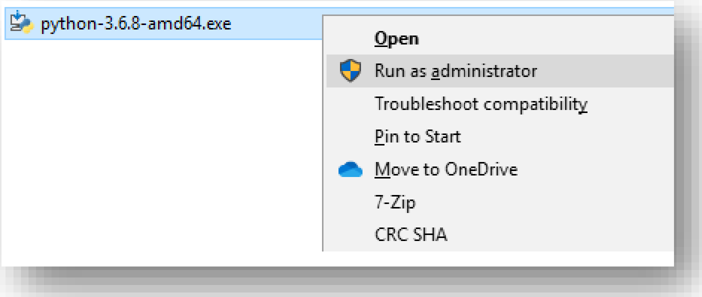
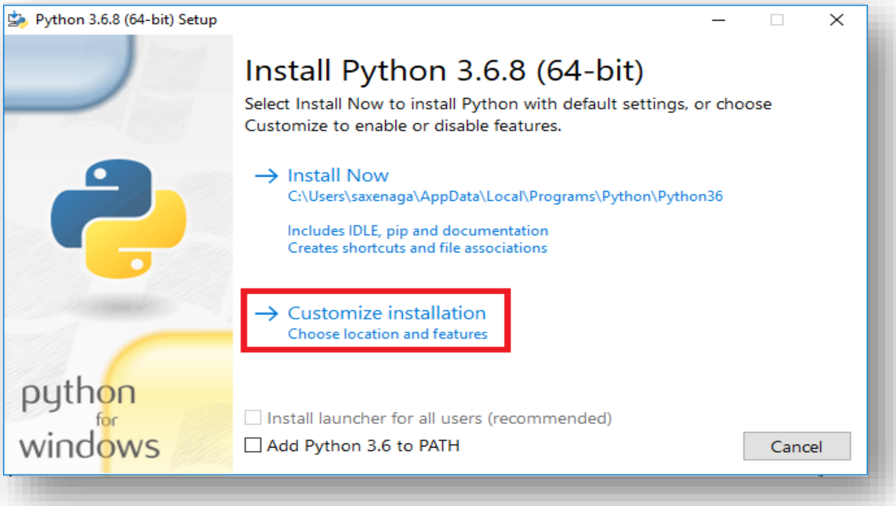


Figure 33 – Installing Python

4. The Python Setup wizard appears.
5. Click on Customize Installation.


Python 3.6.8 (64-bit) Setup

Install Python 3.6.8 (64-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

→ Install Now
C:\Users\saxenaga\AppData\Local\Programs\Python\Python36

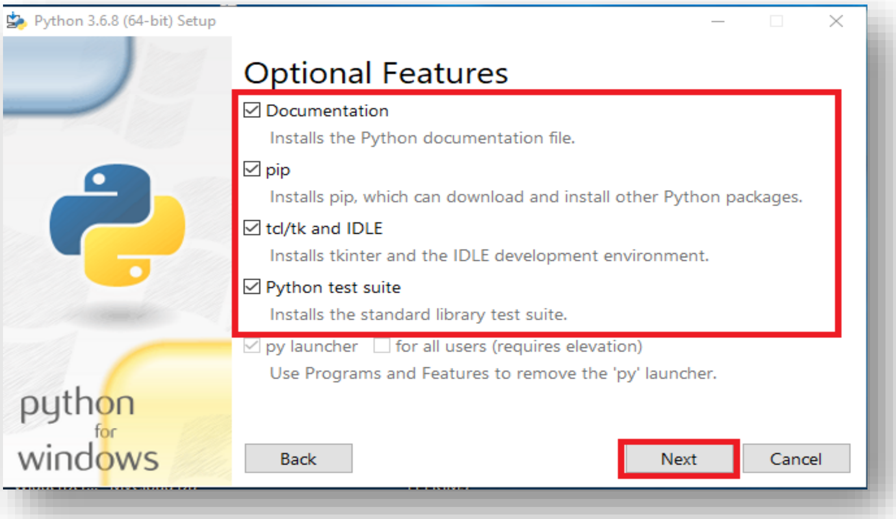
Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ Customize installation
Choose location and features

□ Install launcher for all users (recommended)
□ Add Python 3.6 to PATH

Figure 34 – Installing Python (Cont.)

6. The Optional Features screen appears.
7. Select options highlighted in red box below and Click **Next**.


Python 3.6.8 (64-bit) Setup

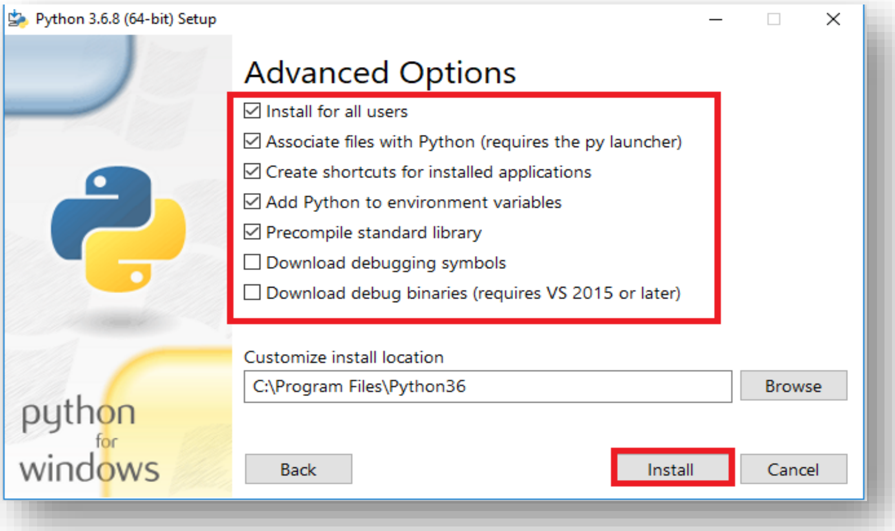
Optional Features

☑ Documentation
Installs the Python documentation file.
☑ pip
Installs pip, which can download and install other Python packages.
☑ tcl/tk and IDLE
Installs tkinter and the IDLE development environment.
☑ Python test suite
Installs the standard library test suite.
☑ py launcher □ for all users (requires elevation)
Use Programs and Features to remove the 'py' launcher.

Figure 35 – Installing Python (Cont.)

8. The Advanced Options screen appears.

9. Select the check boxes as shown in the following figure and click Install.



Python 3.6.8 (64-bit) Setup

Advanced Options

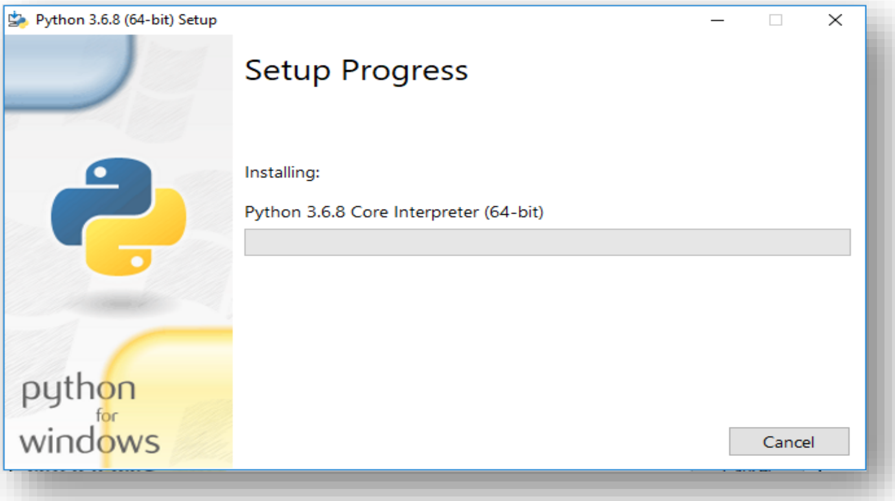
☑ Install for all users
☑ Associate files with Python (requires the py launcher)
☑ Create shortcuts for installed applications
☑ Add Python to environment variables
☑ Precompile standard library
☐ Download debugging symbols
☐ Download debug binaries (requires VS 2015 or later)

Customize install location
C:\Program Files\Python36

Figure 36 – Installing Python (Cont.)

Ensure Install for all users is checked.

10. Setup progress screen shows the current setup status.



Python 3.6.8 (64-bit) Setup

Setup Progress

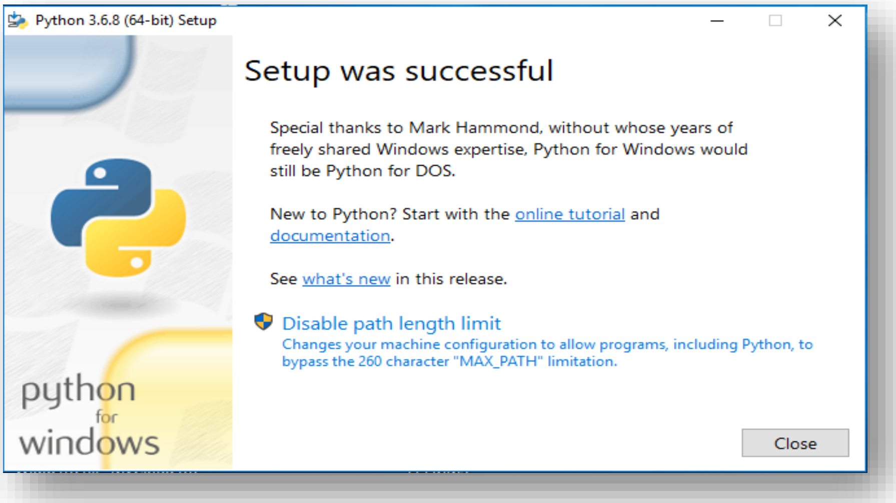
Installing:

Python 3.6.8 Core Interpreter (64-bit)

Figure 37 – Installing Python (Cont.)

11. After the completion of the setup process, the Setup was Successful message is displayed,

12. Click **Close** to close the installation wizard.


Python 3.6.8 (64-bit) Setup

Setup was successful

Special thanks to Mark Hammond, without whose years of freely shared Windows expertise, Python for Windows would still be Python for DOS.

New to Python? Start with the online tutorial and documentation.

See what's new in this release.

Disable path length limit

Changes your machine configuration to allow programs, including Python, to bypass the 260 character "MAX_PATH" limitation.

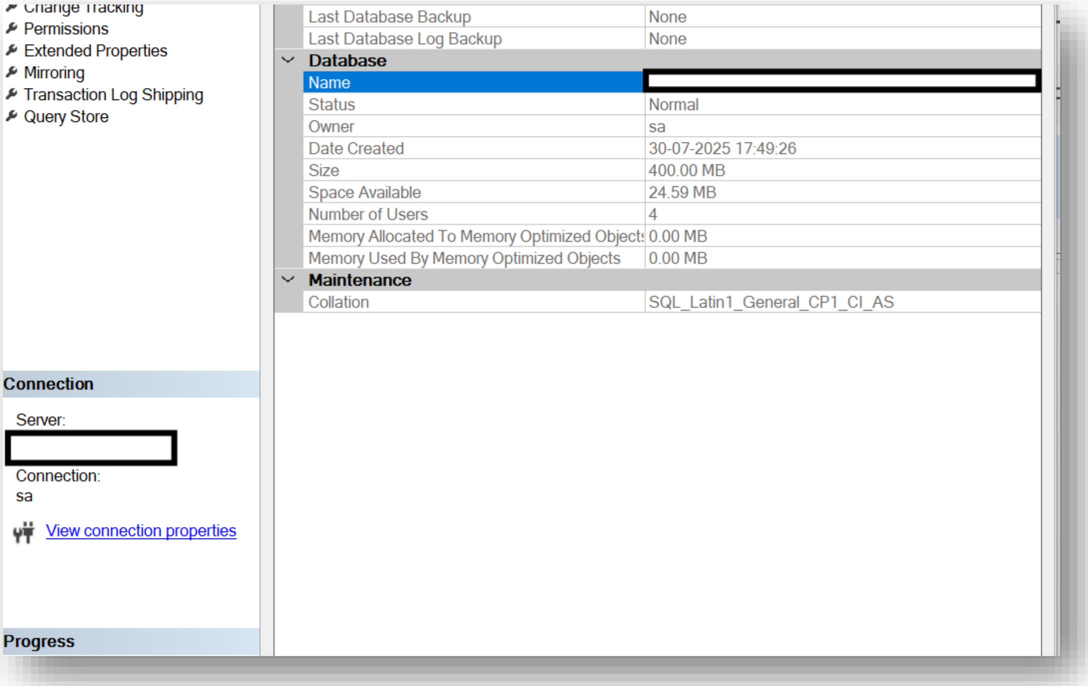
Figure 38 – Installing Python (Cont.)

Python version 3.6.8 and above is supported.

5.2.3 Installation of Pre-requisites on Database Layer

This section describes the pre-requisites of database.

1. SQL server version should be SQL Server 2016/2019/2022 - Standard Edition (sp2),2017 and 2019 edition.
2. Default SQL server and database collation is SQL_Latin1_General_CP1_CI_AS as shown in below.



- Change Tracking
- Permissions
- Extended Properties
- Mirroring
- Transaction Log Shipping
- Query Store

Last Database Backup	None
Last Database Log Backup	None
Database	
Name	[redacted]
Status	Normal
Owner	sa
Date Created	30-07-2025 17:49:26
Size	400.00 MB
Space Available	24.59 MB
Number of Users	4
Memory Allocated To Memory Optimized Object:	0.00 MB
Memory Used By Memory Optimized Objects	0.00 MB
Maintenance	
Collation	SQL_Latin1_General_CP1_CI_AS

Connection

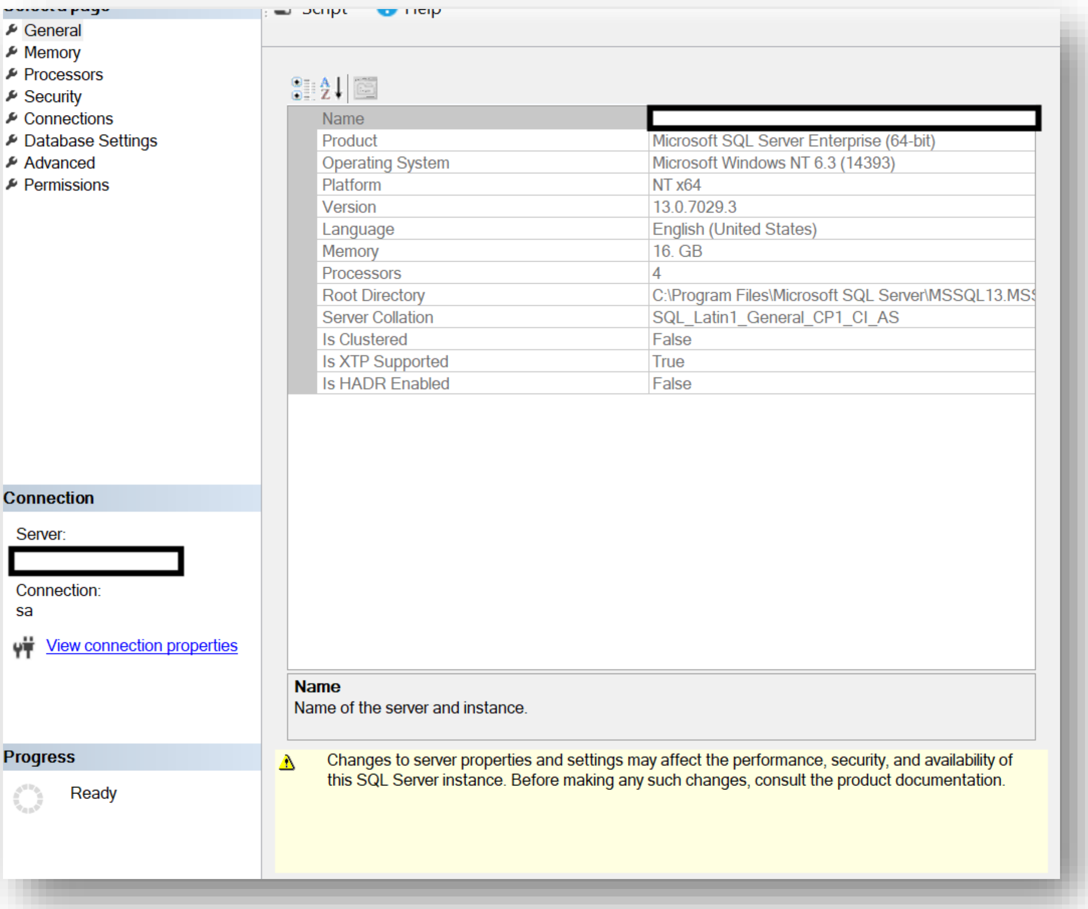
Server:
[redacted]

Connection:
sa

View connection properties

Progress

Figure 39 – Database Properties



Select a page

- General
- Memory
- Processors
- Security
- Connections
- Database Settings
- Advanced
- Permissions

Name	[redacted]
Product	Microsoft SQL Server Enterprise (64-bit)
Operating System	Microsoft Windows NT 6.3 (14393)
Platform	NT x64
Version	13.0.7029.3
Language	English (United States)
Memory	16. GB
Processors	4
Root Directory	C:\Program Files\Microsoft SQL Server\MSSQL13.MSS
Server Collation	SQL_Latin1_General_CP1_CI_AS
Is Clustered	False
Is XTP Supported	True
Is HADR Enabled	False

Name
Name of the server and instance.

⚠ Changes to server properties and settings may affect the performance, security, and availability of this SQL Server instance. Before making any such changes, consult the product documentation.

Connection

Server:
[redacted]

Connection:
sa

View connection properties

Progress

Ready

Figure 40 – Server Properties

5.3 Deployment

This section describes how to deploy HCL BigFix CLM on required infrastructure. It includes the following steps:

- HCL BigFix CLM Web Layer Installation using the HCL BigFix CLM installer
- HCL BigFix CLM App Layer Installation using the HCL BigFix CLM Installer

5.3.1 HCL BigFix CLM Web Layer Installation

Run the installer with Administrator permission.

This section describes how to configure HCL BigFix CLM Web Layer server.

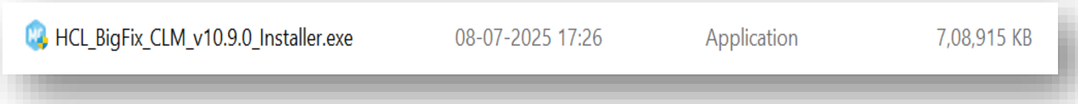
HCL BigFix CLM web layer has two components.

- UI Portal
- Key Rotation Service (KRS)

5.3.1.1 Components Setup

To set up the Web components, follow the following steps:

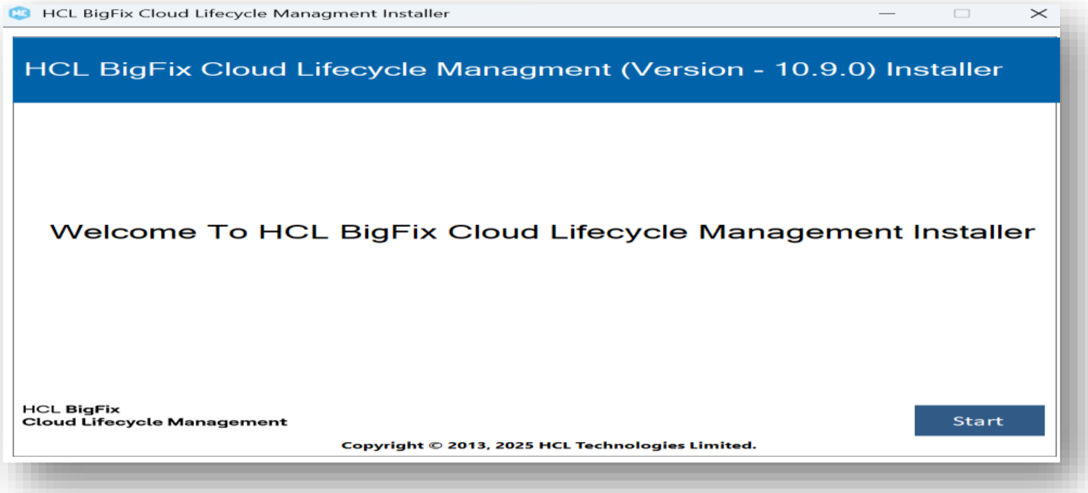
1. Make sure the HCL_BigFix_CLM_Installerzip (provided by HCL BigFix CLM Support Team) is present on Web server.
2. Unzip the Installer **Zip** file.
3. Go to the unzipped HCL_BigFix_CLM_Installer→ HCL_BigFix_CLM_Installerfolder
4. Right-click on HCL_BigFix_CLM_Installer Application file and Run as Administrator



HCL_BigFix_CLM_v10.9.0_Installer.exe 08-07-2025 17:26 Application 7,08,915 KB

Figure 41 – HCL BigFix CLM Installer

5. Click on the start button to start the installation.



HCL BigFix Cloud Lifecycle Managment Installer

HCL BigFix Cloud Lifecycle Managment (Version - 10.9.0) Installer

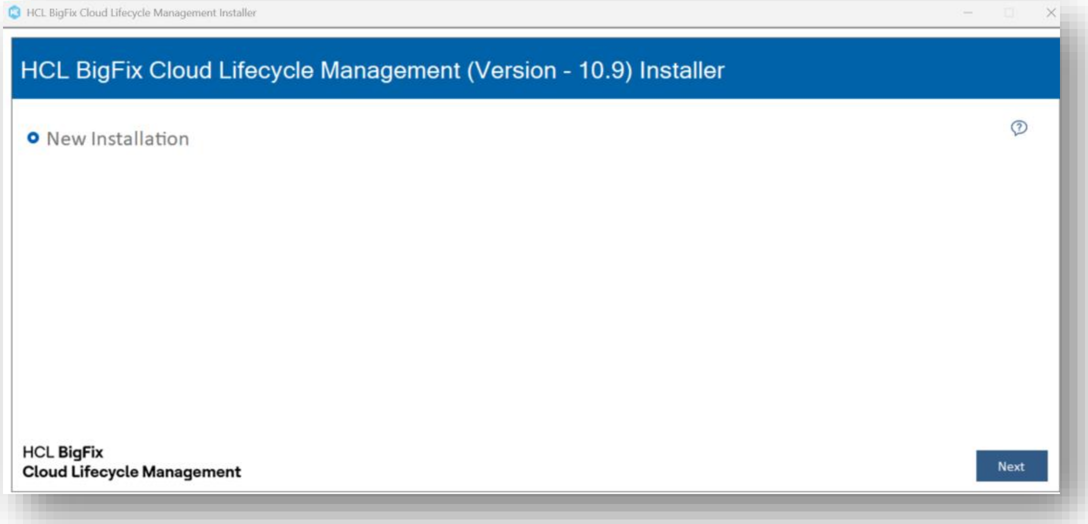
Welcome To HCL BigFix Cloud Lifecycle Management Installer

HCL BigFix
Cloud Lifecycle Management

Copyright © 2013, 2025 HCL Technologies Limited.

Figure 42 – HCL BigFix CLM - New Installation

6. In case of fresh/new installation below screen will appear with the "**New installation**" radio checked.

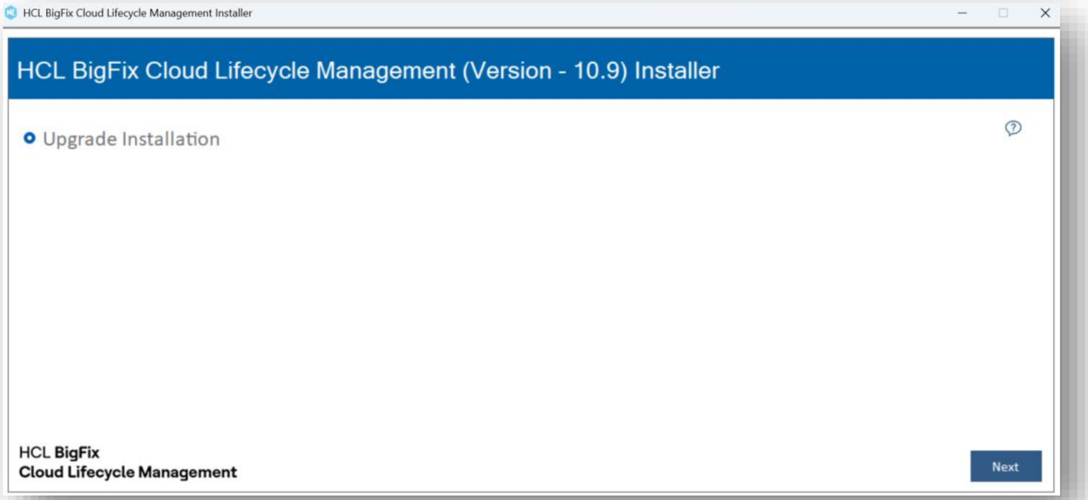

HCL BigFix Cloud Lifecycle Management Installer

HCL BigFix Cloud Lifecycle Management (Version - 10.9) Installer

● New Installation

Figure 43 – HCL BigFix CLM - New Installation

In case of Upgrade, below screen will appear for upgrade Installation

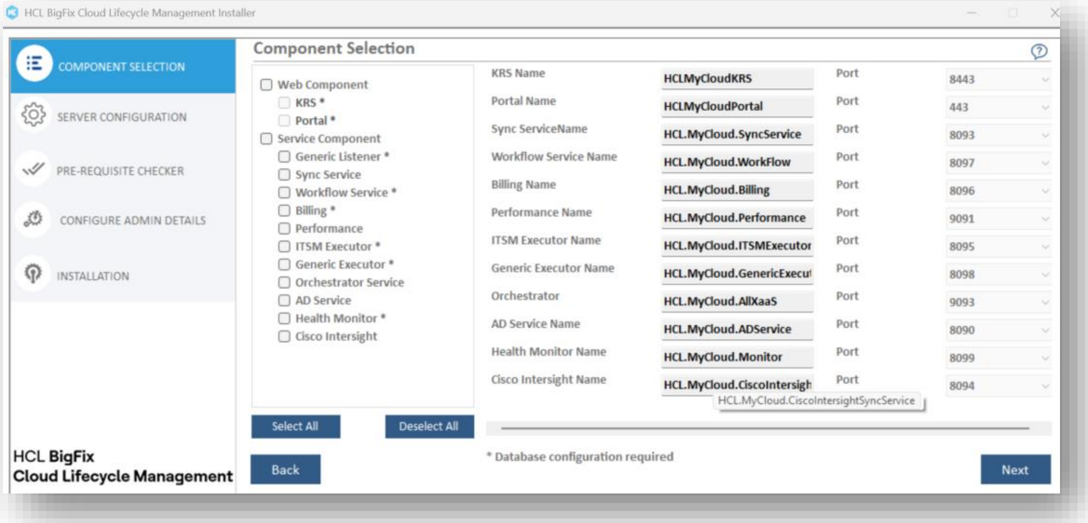

HCL BigFix Cloud Lifecycle Management Installer

HCL BigFix Cloud Lifecycle Management (Version - 10.9) Installer

● Upgrade Installation

Figure 44 – HCL BigFix CLM - Upgrade Installation

7. Click **Next.**
8. On the left navigation bar, Component Selection is auto selected.
9. As HCL BigFix CLM **Web layer** is being configured, select the **Web Component**.



Component Selection

- ☐ Web Component
  - ☐ KRS *
  - ☐ Portal *
- ☐ Service Component
  - ☐ Generic Listener *
  - ☐ Sync Service
  - ☐ Workflow Service *
  - ☐ Billing *
  - ☐ Performance
  - ☐ ITSM Executor *
  - ☐ Generic Executor *
  - ☐ Orchestrator Service
  - ☐ AD Service
  - ☐ Health Monitor *
  - ☐ Cisco Intersight

KRS Name	HCLMyCloudKRS	Port	8443
Portal Name	HCLMyCloudPortal	Port	443
Sync ServiceName	HCL.MyCloud.SyncService	Port	8093
Workflow Service Name	HCL.MyCloud.WorkFlow	Port	8097
Billing Name	HCL.MyCloud.Billing	Port	8096
Performance Name	HCL.MyCloud.Performance	Port	9091
ITSM Executor Name	HCL.MyCloud.ITSMExecutor	Port	8095
Generic Executor Name	HCL.MyCloud.GenericExecut	Port	8098
Orchestrator	HCL.MyCloud.AllXaaS	Port	9093
AD Service Name	HCL.MyCloud.ADService	Port	8090
Health Monitor Name	HCL.MyCloud.Monitor	Port	8099
Cisco Intersight Name	HCL.MyCloud.CiscoIntersigh	Port	8094

HCL.MyCloud.CiscoIntersightSyncService

* Database configuration required

Figure 45 - Web Component Selection

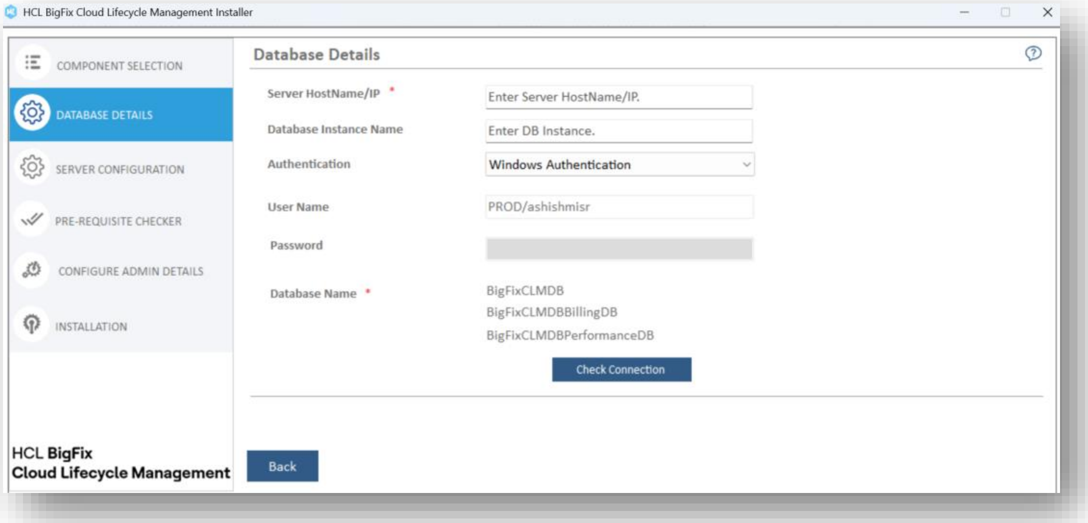
In case of UPGRADE, Web Components which are already installed are auto selected

10. Select the **Port** against both selected web component and leave them as it for default.
    - HCL BigFix CLM KRS – port 8080 (default)
    - HCL BigFix CLM Portal – port 80 (default)
11. Click **Next** to go to Database **Setup**.

5.3.1.2 Database Setup

HCL BigFix CLM Installer uses database screens to capture details which are required to connect to the **Database Server** and create the required databases. The following are the steps:

1. After **Web Components** are selected, On clicking **Next**, User is redirected to **Database Details** screen. The **Database Details** pane appears as below:



Database Details

Server HostName/IP *	Enter Server HostName/IP.
Database Instance Name	Enter DB Instance.
Authentication	Windows Authentication
User Name	PROD/ashishmisr
Password	
Database Name *	BigFixCLMDB BigFixCLMDBBillingDB BigFixCLMDBPerformanceDB

Figure 46 - Database Details

Refer to the table below to understand the fields mentioned in the above figure:

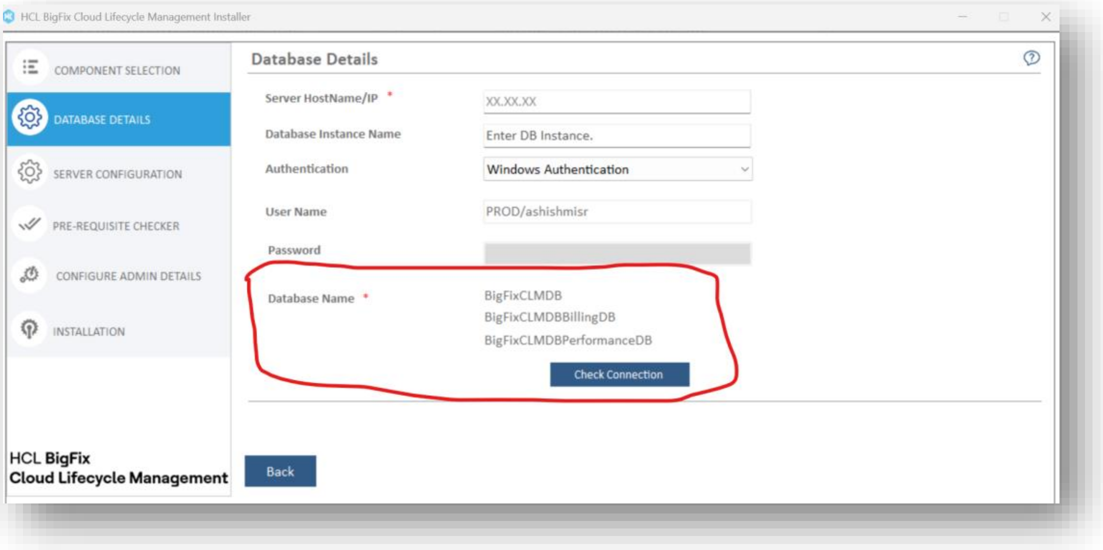
Table 18 – Database Setup

Field Name	Description
Database Details	This pane captures details of the database like server name, authentication type, username, password, that are being used for database creation.
Server HostName/IP	Field to input database server hostname or IP address.
Database Instance Name	Field to input database server instance. This is **Optional** field.
Authentication	Authentication type to be used to connect to the database server/instance. options are **windows authentication** or **SQL Server authentication**.
UserName and Password	These credentials are used to login to the database server to authenticate & establish the connection. These fields cannot be overridden if authentication type is **windows authentication.** If authentication type is **SQL Server Authentication**, then username and password are mandatory and need to be provided.
Check Connection	Upon clicking the option, it validates whether connection (between Web layer and Database) has been established successfully or not.

2. Enter the Database Server **Hostname** or **IP Address**.
3. Enter Database Instance Name. (**Optional**)
4. Select **Authentication**. Database configuration is done with the following authentication:
   - Windows Authentication
   - SQL Server Authentication

If Authentication is "**SQL Server Authentication** ", Enter the login credentials i.e., the **Username and Password** for getting access to the database server.

By default, HCL BigFix CLM installer will create the databases with the **default database names** as shown in figure below:



Database Details

Server HostName/IP * XX.XX.XX

Database Instance Name Enter DB Instance.

Authentication Windows Authentication

User Name PROD/ashishmisr

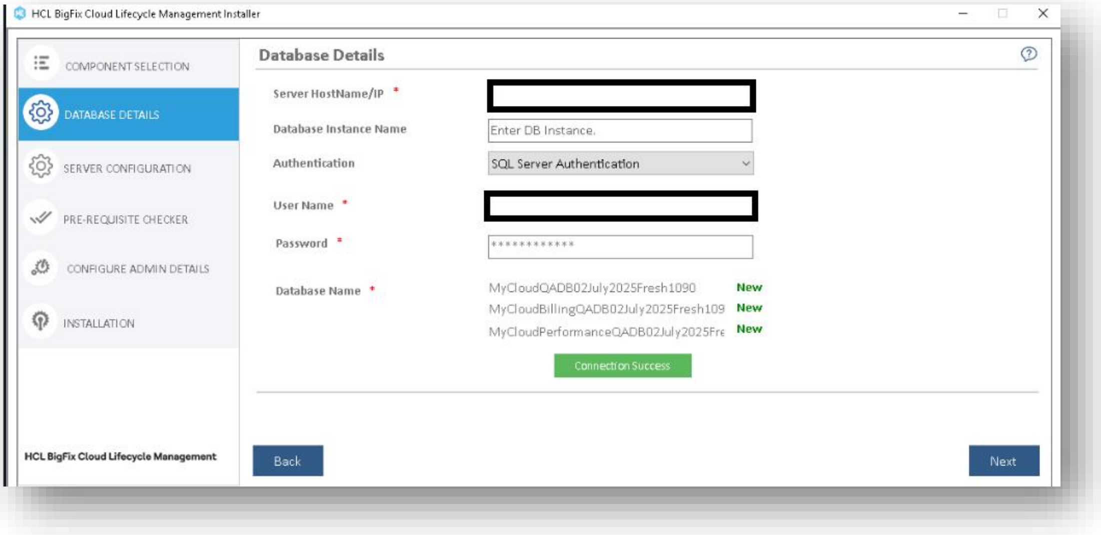
Password

Database Name * BigFixCLMDB
BigFixCLMDBBillingDB
BigFixCLMDBPerformanceDB

Figure 47 – Default Database Names

While doing HCL BigFix CLM UPGRADE make sure the database name is the same as it was provided during installation.

5. Click **Check** Connection to check the connection to the respective server.



Database Details

Server HostName/IP * [redacted]

Database Instance Name Enter DB Instance.

Authentication SQL Server Authentication

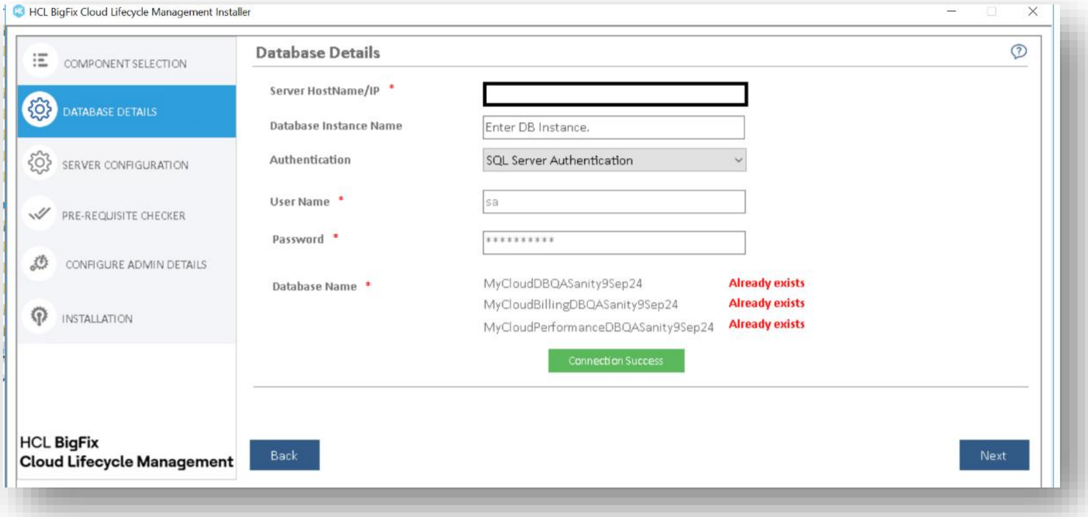
User Name * [redacted]

Password * ************

Database Name * MyCloudQADB02July2025Fresh1090 New
MyCloudBillingQADB02July2025Fresh109 New
MyCloudPerformanceQADB02July2025Fre New

Figure 48 - Database Check Connection

Above Screenshot shows that Database Names has been Changed from Config file as per step 6 above.
During Installation If database names already exist on the database server as shown in below figure, change the database name as mentioned in step 7 above.



Database Details

Server HostName/IP *

Database Instance Name: Enter DB Instance.

Authentication: SQL Server Authentication

User Name *: sa

Password *: **********

Database Name *:
MyCloudDBQASanity9Sep24 Already exists
MyCloudBillingDBQASanity9Sep24 Already exists
MyCloudPerformanceDBQASanity9Sep24 Already exists

Connection Success

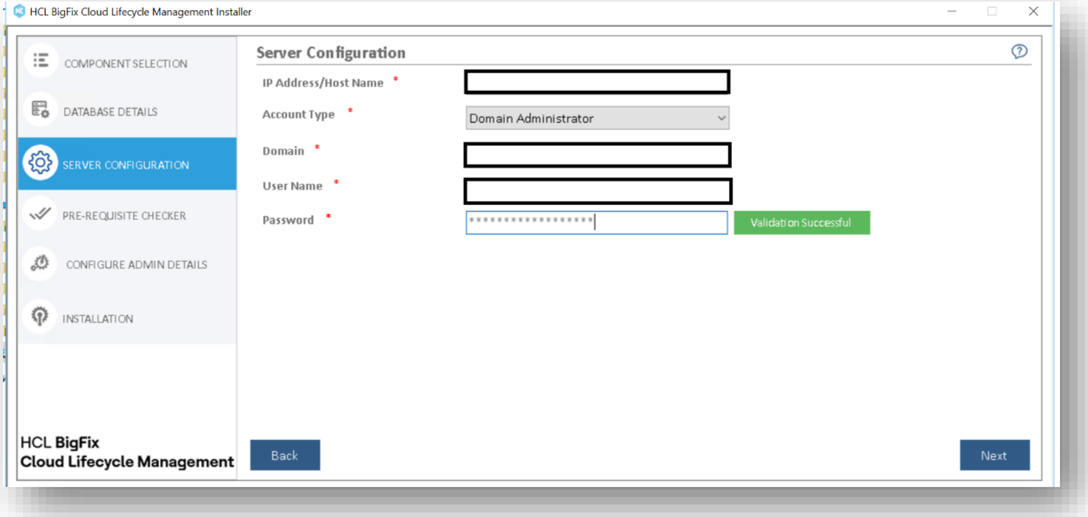
Figure 49 – HCL BigFix CLM Installer – Database Already Exist

6. Click Next to go to Server Configuration page.

5.3.1.3 Server Configuration

In this section, details of HCL BigFix CLM Web Server using the installer is being captured.

1. IP Address/Host Name is auto populated.
2. Enter the Account Type (Domain Administrator or Local Administrator).
3. Provide the Domain
4. Enter the UserName to access the Web server.
5. Enter the Password for the web server.
6. Click on **Check User Validity** button.



Server Configuration

IP Address/Host Name *

Account Type *: Domain Administrator

Domain *

User Name *

Password *: *****************

Validation Successful

Figure 50 - Server Configuration

7. If Validation Success message appears, Click Next.
8. The Prerequisite Checker screen appears.

All the fields marked with asterisk (*) are mandatory.

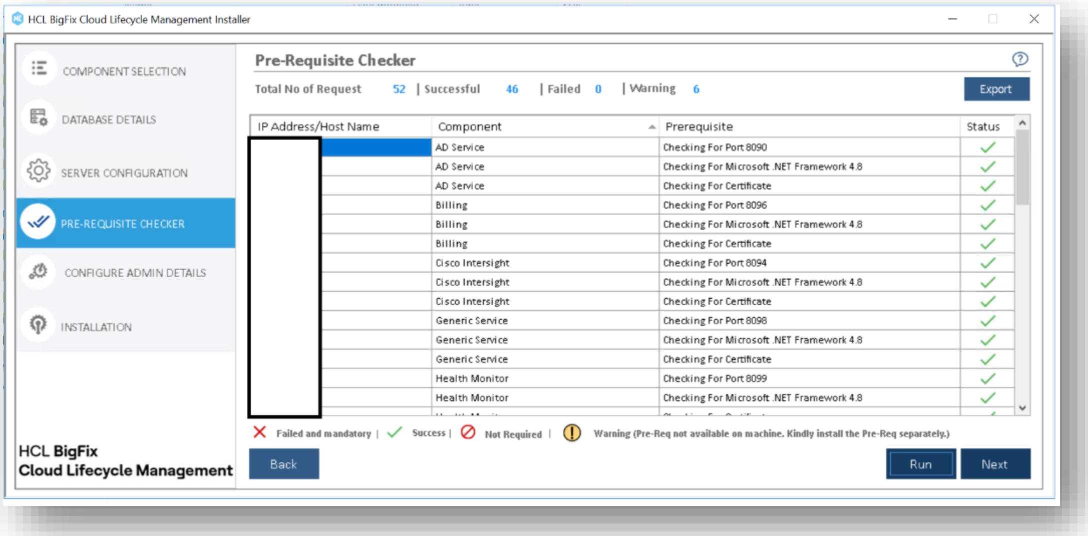
5.3.1.4 Run Prerequisite Checker

This section describes how to run the prerequisite checker to verify that the installation pre-requisites have been installed.

The **Prerequisite Checker** screen lists the configurations that are mandatory for the components selected on previous screen.

Prerequisite Checker always runs as part of Setup.

1. Click **Run** to start the pre-requisite checker against components selected for installation on the web server.



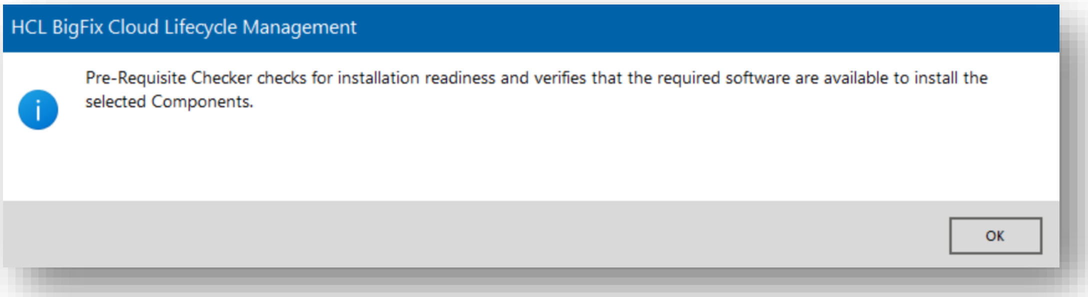
Pre-Requisite Checker

Total No of Request 52 | Successful 46 | Failed 0 | Warning 6

IP Address/Host Name	Component	Prerequisite	Status
[redacted]	AD Service	Checking For Port 8090	✓
[redacted]	AD Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	AD Service	Checking For Certificate	✓
[redacted]	Billing	Checking For Port 8096	✓
[redacted]	Billing	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Billing	Checking For Certificate	✓
[redacted]	Cisco Intersight	Checking For Port 8094	✓
[redacted]	Cisco Intersight	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Cisco Intersight	Checking For Certificate	✓
[redacted]	Generic Service	Checking For Port 8098	✓
[redacted]	Generic Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Generic Service	Checking For Certificate	✓
[redacted]	Health Monitor	Checking For Port 8099	✓
[redacted]	Health Monitor	Checking For Microsoft .NET Framework 4.8	✓

✕ Failed and mandatory | ✓ Success | ⊘ Not Required | ⓘ Warning (Pre-Req not available on machine. Kindly install the Pre-Req separately.)

Figure 51 - Prerequisite Checker

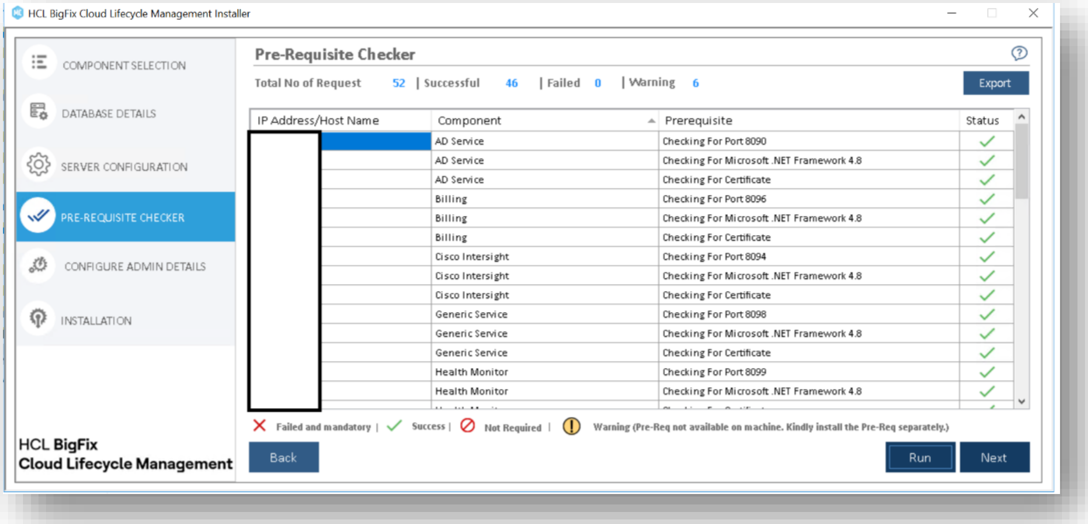


HCL BigFix Cloud Lifecycle Management

Pre-Requisite Checker checks for installation readiness and verifies that the required software are available to install the selected Components.

Figure 52 - Prerequisite Checker Information Assistance

The **Prerequisite Checker** identifies the existing host, component, list of relevant pre-requisites and performs the check for installation readiness. If any pre-requisite is missing, it gets listed under the **Status** field as (X). If any pre-requisite is not required, it gets listed under the **Status** field as (⊘) means **Not Required**. Pre-requisites which show as **Warning** can be ignored.



Pre-Requisite Checker

Total No of Request 52 | Successful 46 | Failed 0 | Warning 6

IP Address/Host Name	Component	Prerequisite	Status
[redacted]	AD Service	Checking For Port 8090	✓
[redacted]	AD Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	AD Service	Checking For Certificate	✓
[redacted]	Billing	Checking For Port 8096	✓
[redacted]	Billing	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Billing	Checking For Certificate	✓
[redacted]	Cisco Intersight	Checking For Port 8094	✓
[redacted]	Cisco Intersight	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Cisco Intersight	Checking For Certificate	✓
[redacted]	Generic Service	Checking For Port 8098	✓
[redacted]	Generic Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Generic Service	Checking For Certificate	✓
[redacted]	Health Monitor	Checking For Port 8099	✓
[redacted]	Health Monitor	Checking For Microsoft .NET Framework 4.8	✓

✕ Failed and mandatory | ✓ Success | ⊘ Not Required | ⓘ Warning (Pre-Req not available on machine. Kindly install the Pre-Req separately.)

Figure 53 – Prerequisite Checker (Cont.)

2. If all the checks succeed, the **Next** button is enabled, click **Next** to proceed.

If any of the mandatory checks fails, the **Next** button is disabled.

3. On completion of these steps, click **Next** and configure the **admin Details**.

All fields marked with asterisk (*) are mandatory.

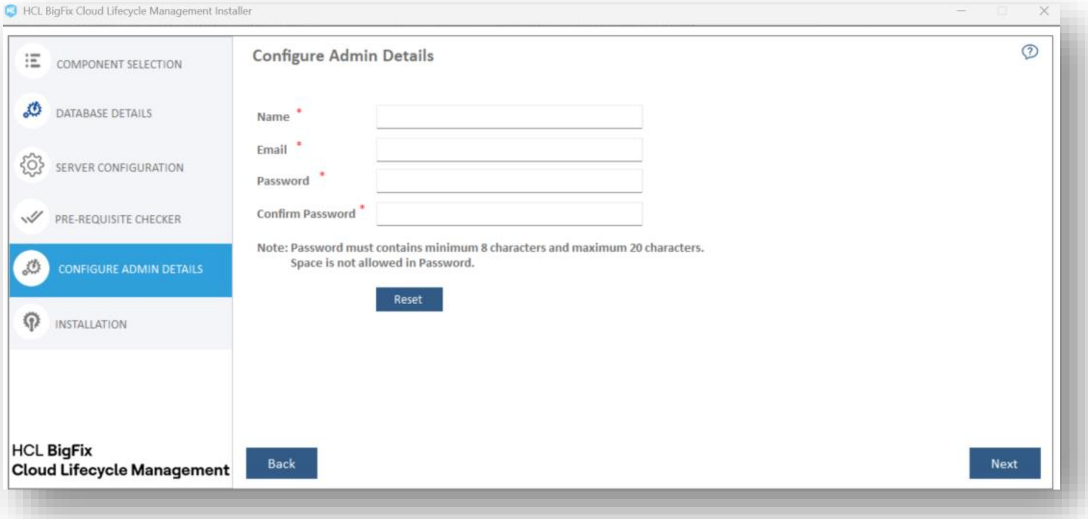
5.3.1.5 Configuring Admin Details

Configure Admin Details Section comes only during the New Installation, and this does not appear during HCL BigFix CLM UPGRADE.

This section will capture details of an admin user with full access to HCL BigFix CLM to add admins, manage settings and perform governance actions.

To add the admin details, follow the following steps:

1. On the Configure **Admin Details** screen, enter the **Administrator Name, Administrator Email**, **Password,** and **Confirm Password**. These credentials are used to access HCL BigFix CLM Web portal for configuration.



Configure Admin Details

Name *

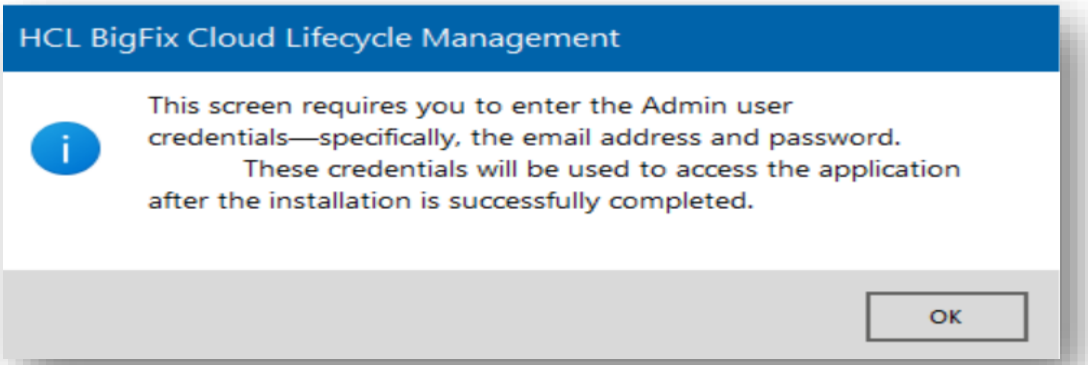
Email *

Password *

Confirm Password *

Note: Password must contains minimum 8 characters and maximum 20 characters.
Space is not allowed in Password.

Figure 54 – Configure Admin Details



HCL BigFix Cloud Lifecycle Management

This screen requires you to enter the Admin user credentials—specifically, the email address and password. These credentials will be used to access the application after the installation is successfully completed.

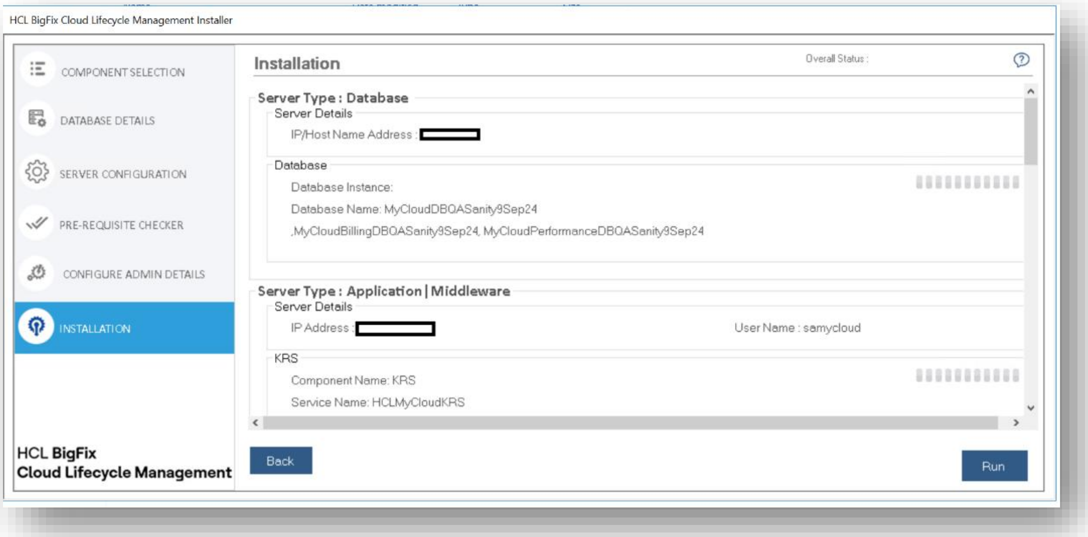
Figure 55- Admin Details Information Assistance

2. Click **Next**.

5.3.1.6 Installation

This section lists all the configurations as entered (server and component wise). Review the details and verify that the responses provided are correct.

1. Verify the Details which were provided and click on **Run** to start the Web Components installation.



HCL BigFix Cloud Lifecycle Management Installer

Installation

Overall Status :

Server Type : Database

Server Details

IP/Host Name Address : [redacted]

Database

Database Instance:

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address : [redacted] User Name : samycloud

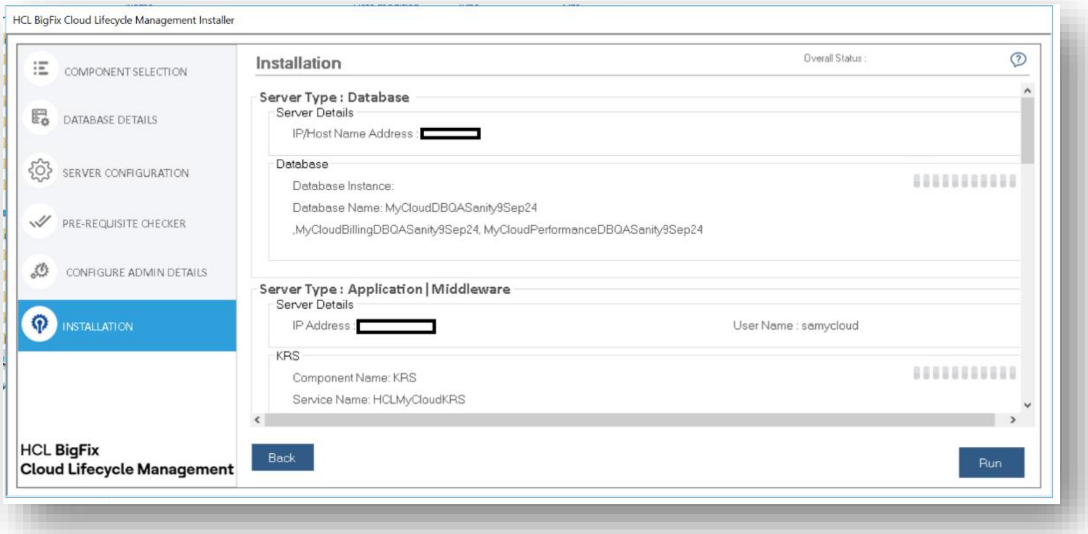
KRS

Component Name: KRS

Service Name: HCLMyCloudKRS

Figure 56 - HCL BigFix CLM Installation

2. Installation progress can be seen as shown below.



HCL BigFix Cloud Lifecycle Management Installer

Installation

Overall Status :

Server Type : Database

Server Details

IP/Host Name Address : [redacted]

Database

Database Instance:

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address : [redacted] User Name : samycloud

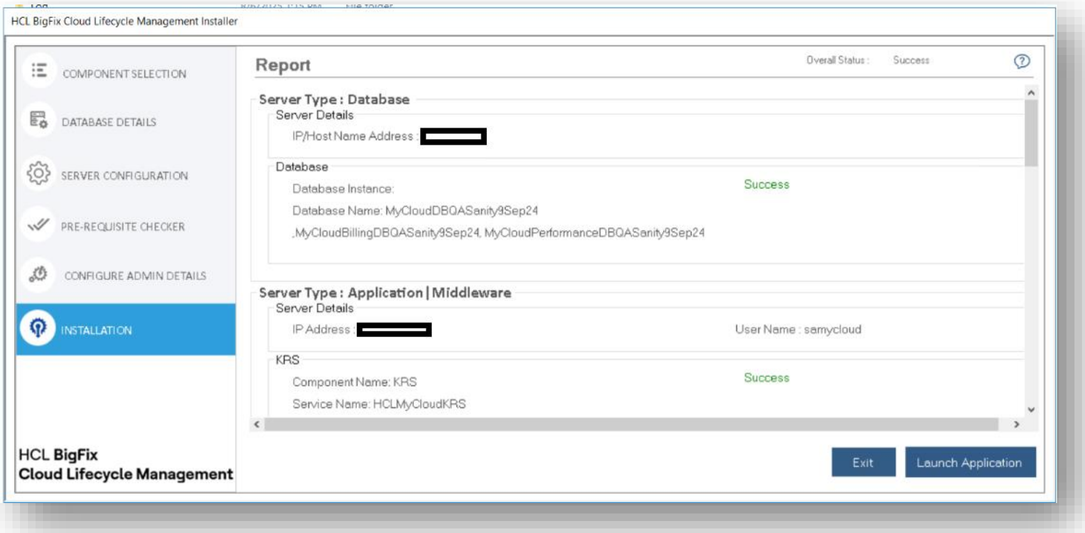
KRS

Component Name: KRS

Service Name: HCLMyCloudKRS

Figure 57 – HCL BigFix CLM Installation Progress

3. On successful installation of web components, below screen will appear with **Launch Application** Button.



HCL BigFix Cloud Lifecycle Management Installer

Report

Overall Status : Success

Server Type : Database

Server Details

IP/Host Name Address [redacted]

Database

Database Instance: Success

Database Name: MyCloudDBQASanity9Sep24

,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address [redacted] User Name : samycloud

KRS

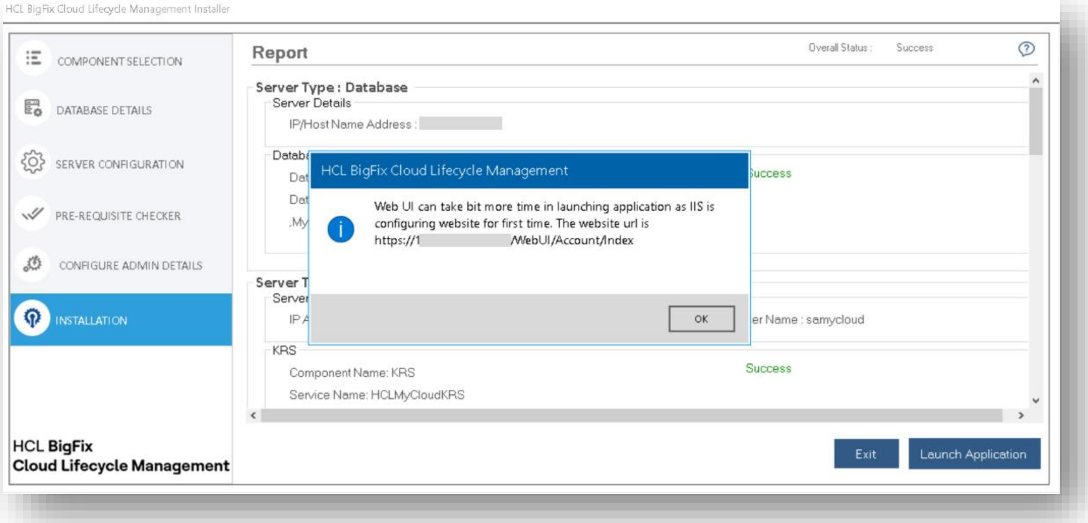
Component Name: KRS Success

Service Name: HCLMyCloudKRS

Figure 58 – HCL BigFix CLM Installer – Success

4. Click on Launch **Application** to launch the HCL BigFix Cloud Life Cycle Management Web portal.

HCL BigFix CLM takes some time to configure the website, below the screen will appear, click on OK.



HCL BigFix Cloud Lifecycle Management Installer

Report

Overall Status : Success

Server Type : Database

Server Details

IP/Host Name Address : [redacted]

HCL BigFix Cloud Lifecycle Management

Web UI can take bit more time in launching application as IIS is configuring website for first time. The website url is https://1[redacted]/WebUI/Account/Index

er Name : samycloud

KRS

Component Name: KRS Success

Service Name: HCLMyCloudKRS

Figure 59 – HCL BigFix CLM Installer - Launch

5. Click **OK.**

6. Copy the URL in your notepad for future reference and open the portal in browser.

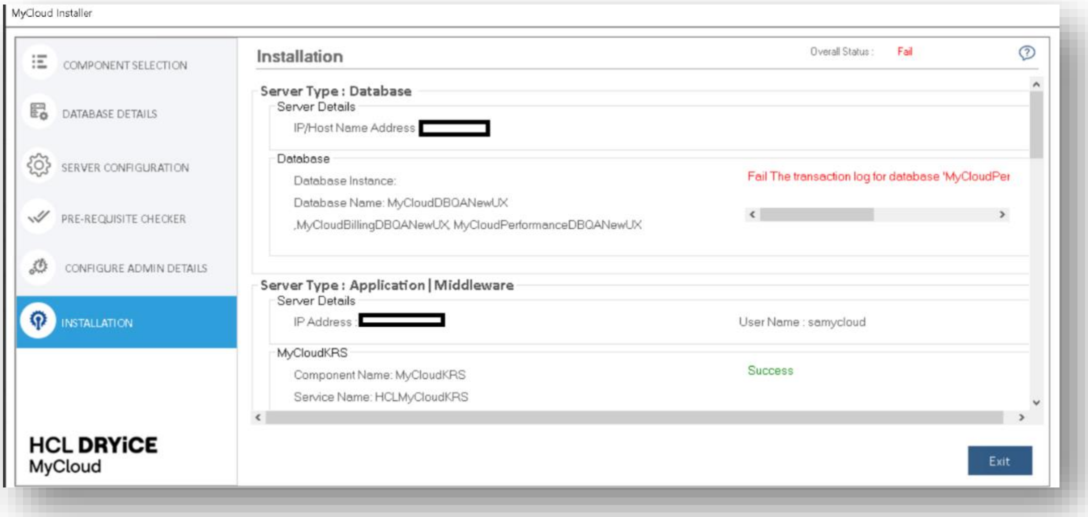
In case of any failure the error is displayed in Red on the screen and it's advisable to reach out to bigfixclm-prodsupport-team@hcl-software.com for further help.

5.3.1.7 Rollback

This section describes the rollback functionality. Rollback is only applicable to installed components in the case of a new installation. Rollback does not delete or remove the database as it is only applicable to installed components.

For a New Installation, if installation fails for any reason, then the Rollback option gets enabled and clicking it removes the installed component.

During the installation of components and DB for the first time, if the DB is created successfully and if any component installation fails, the Rollback button gets enabled.



Installation

Overall Status : Fail

Server Type : Database

Server Details

IP/Host Name Address [redacted]

Database

Database Instance:

Database Name: MyCloudDBQANewUX ,MyCloudBillingDBQANewUX, MyCloudPerformanceDBQANewUX

Fail The transaction log for database 'MyCloudPer

Server Type : Application | Middleware

Server Details

IP Address : [redacted]

User Name : samycloud

MyCloudKRS

Component Name: MyCloudKRS

Service Name: HCLMyCloudKRS

Success

Figure 60 – Rollback

When Rollback action is performed, all selected components get rolled back except DB. So, there is no impact on DB while performing Rollback.

5.3.2 HCL BigFix CLM App Layer Installation

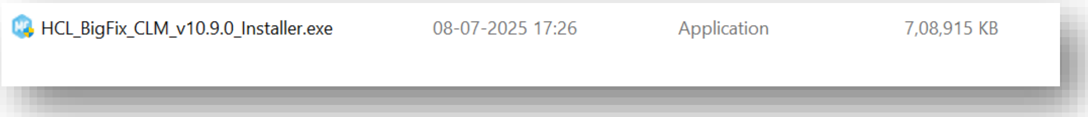
Run the installer with Administrator permission.

This section describes how to configure **HCL BigFix CLM App Layer server**.

5.3.2.1 Components Setup

To set up the App Layer components, follow the following steps:

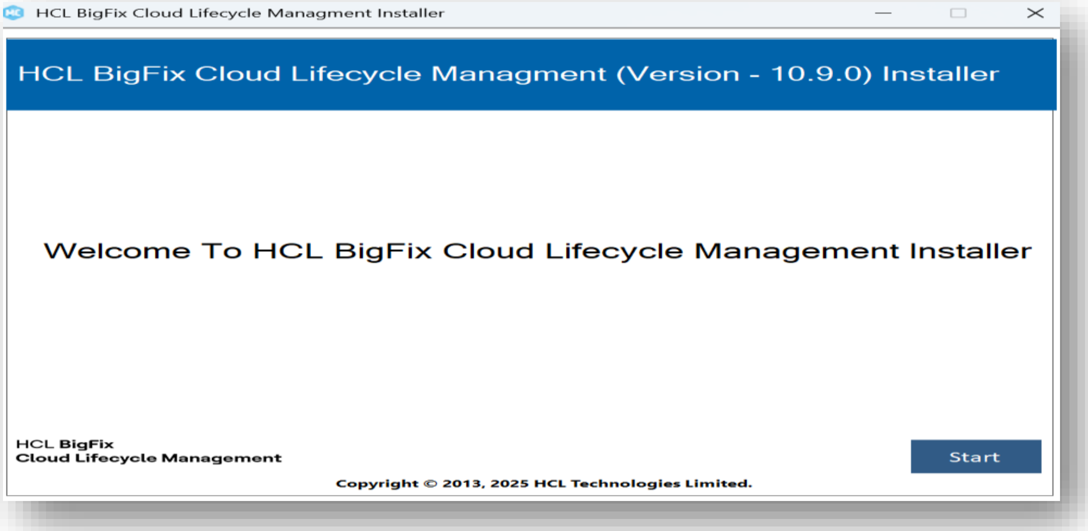
1. Copy the **HCL_BigFix_CLM_Installer zip (provided by HCL BigFix CLM Support Team)** to **App** server.
2. Unzip the Installer **Zip** file.
3. Go to the unzipped HCL_BigFix_CLM_Installer → HCL_BigFix_CLM_Installer folder.
4. Right-click on **HCL_BigFix_CLM_Installer** Application file and Run as **Administrator**



HCL_BigFix_CLM_v10.9.0_Installer.exe 08-07-2025 17:26 Application 7,08,915 KB

Figure 61 – HCL BigFix CLM Installer

5. Click on **Start** button to start the installation.



HCL BigFix Cloud Lifecycle Managment Installer

HCL BigFix Cloud Lifecycle Managment (Version - 10.9.0) Installer

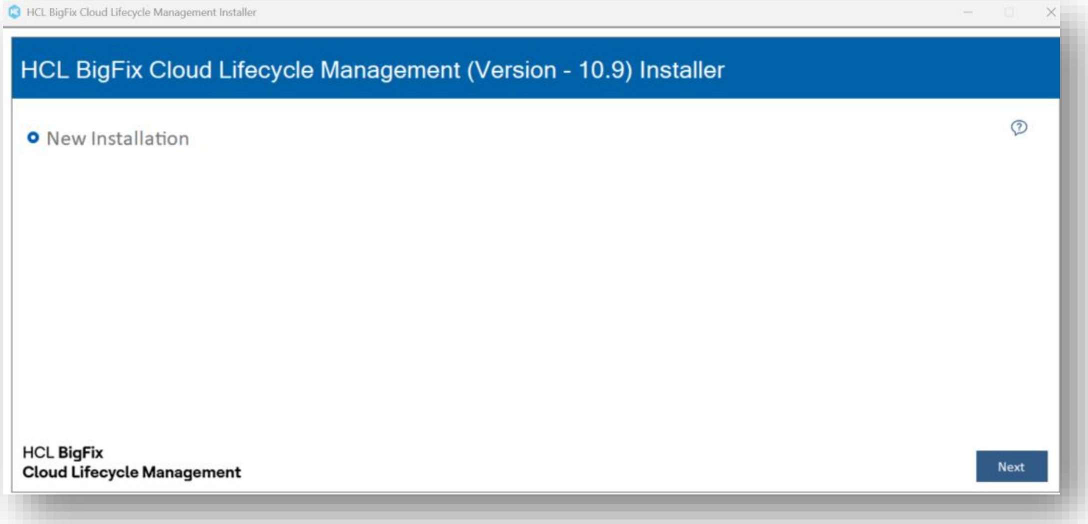
Welcome To HCL BigFix Cloud Lifecycle Management Installer

HCL BigFix
Cloud Lifecycle Management

Copyright © 2013, 2025 HCL Technologies Limited.

Figure 62 – HCL BigFix CLM Installer – New Installation

6. In case of fresh/new installation below screen will appear with the “**New installation**” radio checked.



HCL BigFix Cloud Lifecycle Management Installer

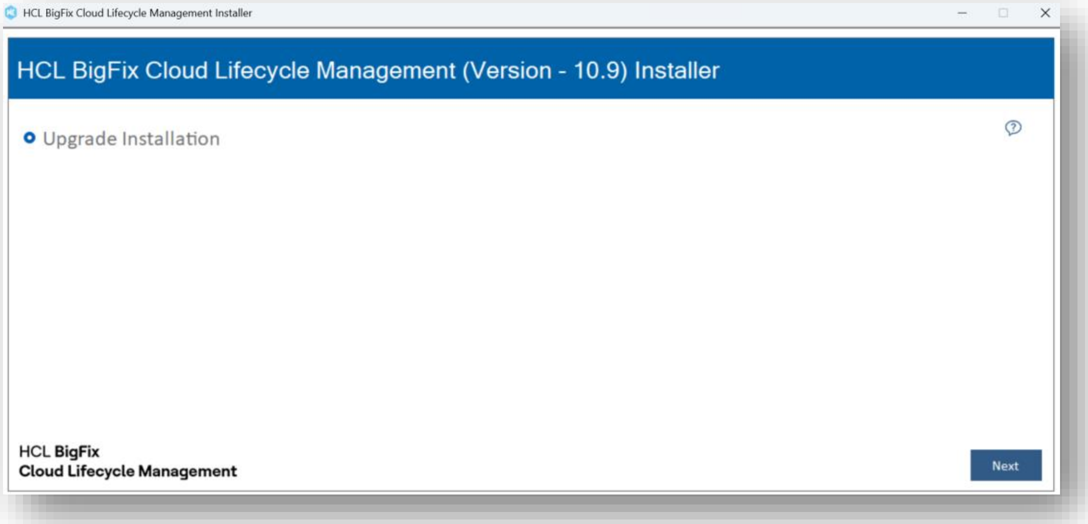
HCL BigFix Cloud Lifecycle Management (Version - 10.9) Installer

● New Installation

HCL BigFix
Cloud Lifecycle Management

Figure 63 – HCL BigFix CLM Installer – New Installation

In case of Upgrade, the screen below will appear for upgrade Installation.

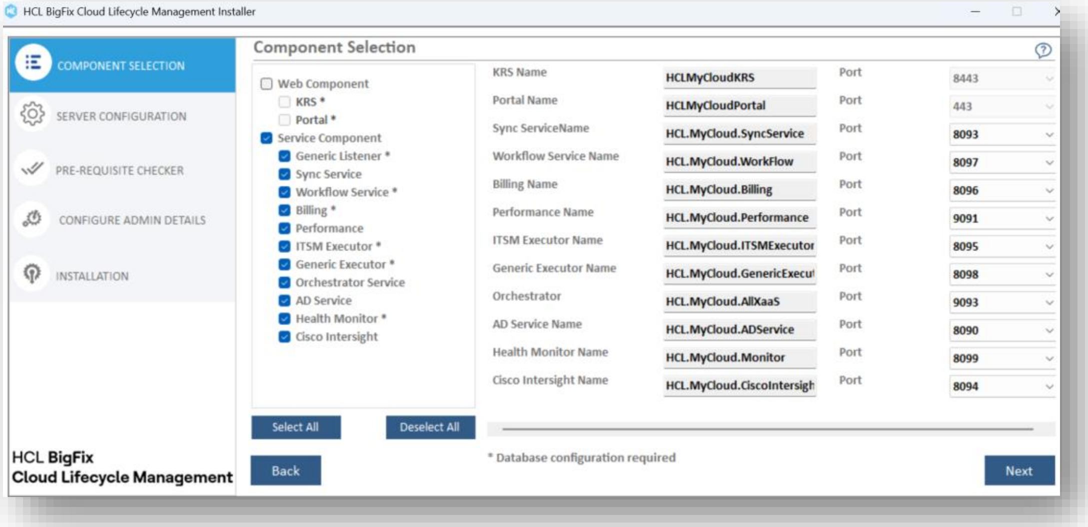


HCL BigFix Cloud Lifecycle Management Installer
HCL BigFix Cloud Lifecycle Management (Version - 10.9) Installer
HCL BigFix
Cloud Lifecycle Management
Next

● Upgrade Installation

Figure 64 – HCL BigFix CLM Installer – Upgrade Installation

7. Click **Next**
8. On the left navigation bar, click Component **Selection**.
9. The **Component Selection** pane comes prepopulated with the components.
10. As **HCL BigFix CLM App layer** is being configured, select the **Service Component**.



Component Selection

- □ Web Component
  - □ KRS *
  - □ Portal *
- ☑ Service Component
  - ☑ Generic Listener *
  - ☑ Sync Service
  - ☑ Workflow Service *
  - ☑ Billing *
  - ☑ Performance
  - ☑ ITSM Executor *
  - ☑ Generic Executor *
  - ☑ Orchestrator Service
  - ☑ AD Service
  - ☑ Health Monitor *
  - ☑ Cisco Intersight

KRS Name	HCLMyCloudKRS	Port	8443
Portal Name	HCLMyCloudPortal	Port	443
Sync ServiceName	HCL.MyCloud.SyncService	Port	8093
Workflow Service Name	HCL.MyCloud.WorkFlow	Port	8097
Billing Name	HCL.MyCloud.Billing	Port	8096
Performance Name	HCL.MyCloud.Performance	Port	9091
ITSM Executor Name	HCL.MyCloud.ITSMExecutor	Port	8095
Generic Executor Name	HCL.MyCloud.GenericExecut	Port	8098
Orchestrator	HCL.MyCloud.AllXaaS	Port	9093
AD Service Name	HCL.MyCloud.ADService	Port	8090
Health Monitor Name	HCL.MyCloud.Monitor	Port	8099
Cisco Intersight Name	HCL.MyCloud.CiscoIntersigh	Port	8094

* Database configuration required

Figure 65 – App Layer - Service Component Setup

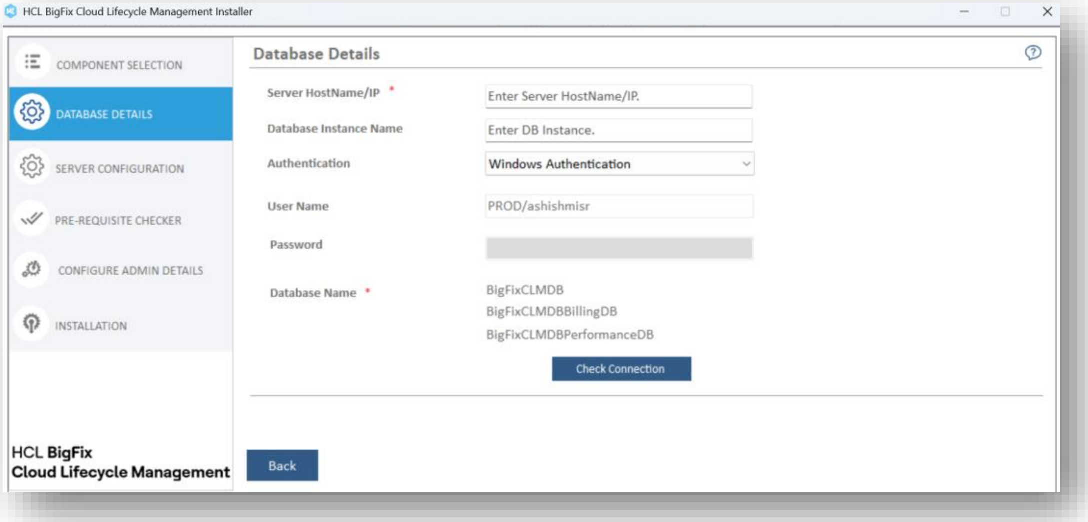
In case of **UPGRADE, Service Components** are auto selected.

11. Select the **Port** against both selected **Service Component** and leave them as it with default.
12. Click **Next** to go to **Database Setup**.

5.3.2.2 Database Setup

HCL BigFix CLM Installer uses database screens to capture details which are required to connect to the **Database Server** and create the required databases. The following are the steps:

1. After **Service Components** are selected, On clicking **Next**, User is redirected to **Database Details** screen.
2. The **Database Details** pane appears as below:



Database Details

Server HostName/IP * Enter Server HostName/IP.

Database Instance Name Enter DB Instance.

Authentication Windows Authentication

User Name PROD/ashishmisr

Password

Database Name * BigFixCLMDB
BigFixCLMDBBillingDB
BigFixCLMDBPerformanceDB

Figure 66 - Database Details

Refer to the table below to understand the fields mentioned in the above figure:

Table 19 – Database Setup (Cont.)

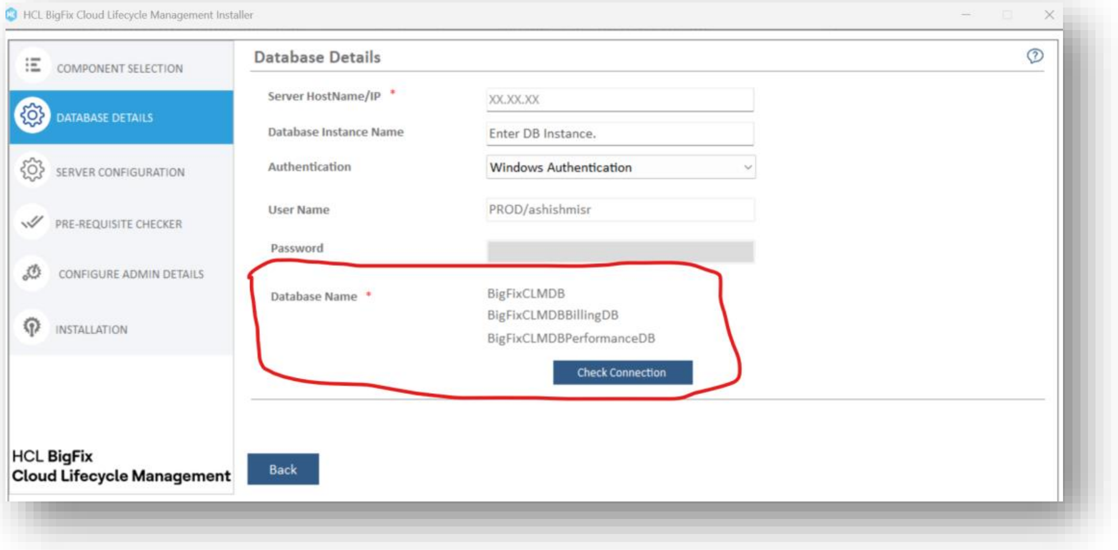
Field Name	Description
Database Details	This panel captures details of the database like server name, authentication type, username, password, that are being used for database creation.
Server HostName/IP	Field to input database server hostname or IP address.
Database Instance Name	Field to input database server instance. This is **Optional** field.
Authentication	Authentication type to be used to connect to the database server/instance. options are **windows authentication** or **SQL Server authentication**.
UserName and Password	These credentials are used to login to the database server to authenticate & establish the connection. These fields cannot be overridden if authentication type is **windows authentication.** If authentication type is **SQL Server Authentication**, then username and password are mandatory and need to be provided.
Check Connection	Upon clicking the option, it validates whether connection (between Web layer and Database) has been established successfully or not.

3. Enter the Database Server **Hostname** or **IP Address**.

4. Enter Database Instance Name. (**Optional**)
5. Select **Authentication**. Database configuration is done with the following authentication:
   - Windows Authentication
   - SQL Server Authentication

If Authentication is "**SQL Server Authentication** ", Enter the login credentials i.e., the **Username and Password** for getting access to the database server.

6. By default, HCL BigFix CLM installer will populate the database with the default database names as shown in figure below:



Database Details

Server HostName/IP * XX.XX.XX

Database Instance Name Enter DB Instance.

Authentication Windows Authentication

User Name PROD/ashishmisr

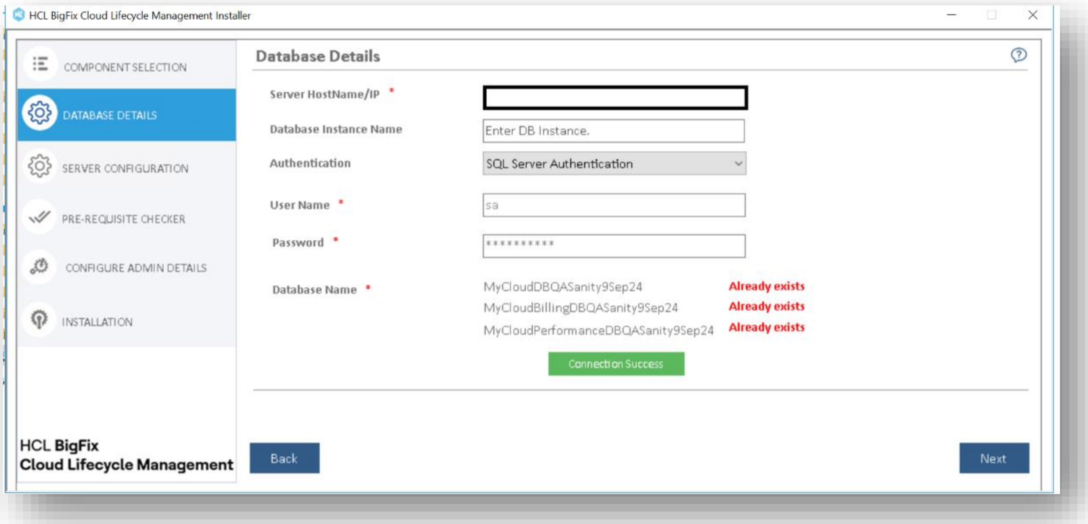
Password

Database Name * BigFixCLMDB
BigFixCLMDBBillingDB
BigFixCLMDBPerformanceDB

Figure 67 – HCL BigFix CLM Default Database Names

While doing HCL BigFix CLM UPGRADE make sure the database name is same as it was provided during installation.
Make sure the database names provided during App layer database setup are same as provided during installation for Web Components (Section 5.3.1.2)

7. Click **Check Connection** to check the connection to the respective server.



Database Details

Server HostName/IP *

Database Instance Name: Enter DB Instance.

Authentication: SQL Server Authentication

User Name *: sa

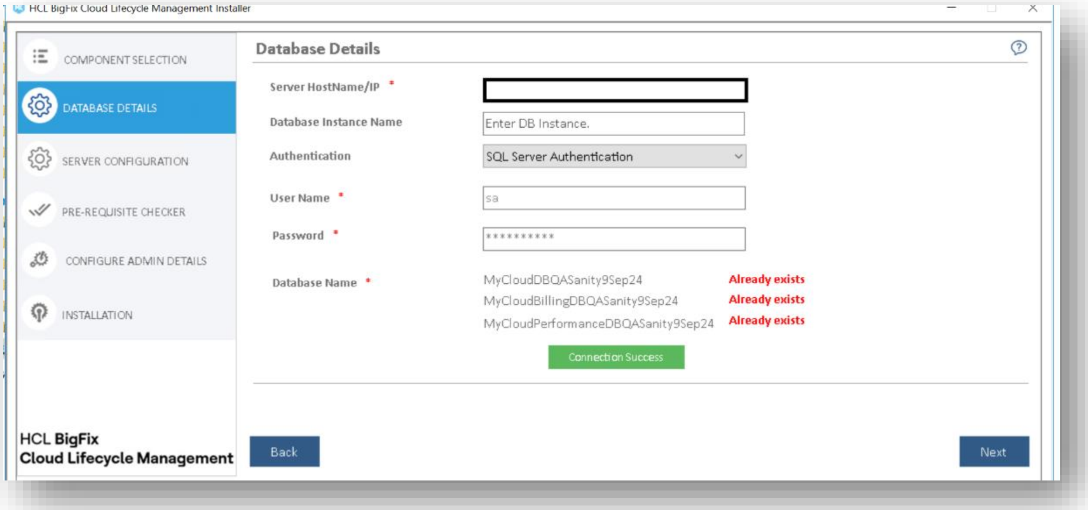
Password *: **********

Database Name *: MyCloudDBQASanity9Sep24 Already exists
MyCloudBillingDBQASanity9Sep24 Already exists
MyCloudPerformanceDBQASanity9Sep24 Already exists

Connection Success

Figure 68 - Database Details

All fields marked with asterisk (*) are mandatory.
During Installation of App Layer on App Server, Since Web layer is already installed on Web Server with the same database names below highlighted in red will appear.



Database Details

Server HostName/IP *

Database Instance Name: Enter DB Instance.

Authentication: SQL Server Authentication

User Name *: sa

Password *: **********

Database Name *: MyCloudDBQASanity9Sep24 Already exists
MyCloudBillingDBQASanity9Sep24 Already exists
MyCloudPerformanceDBQASanity9Sep24 Already exists

Connection Success

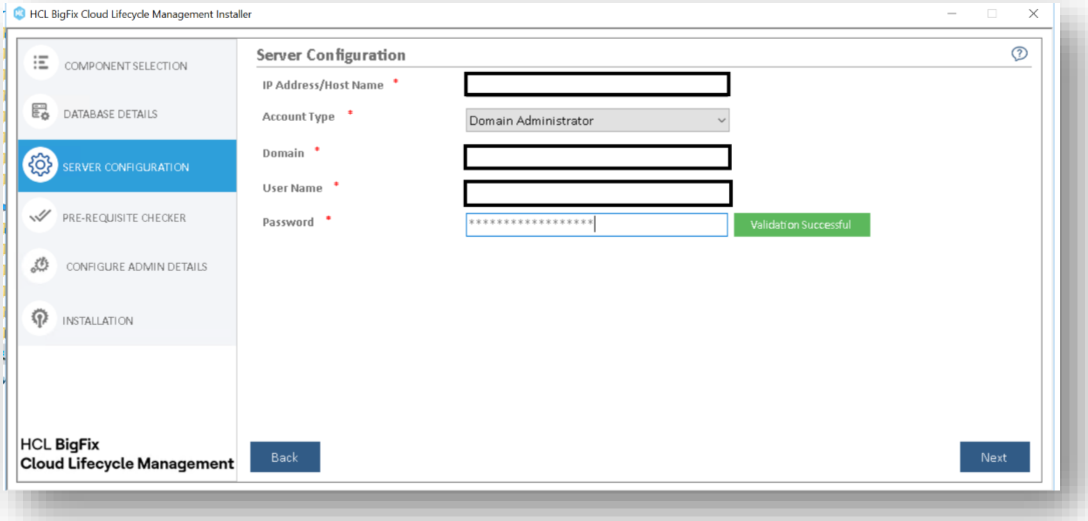
Figure 69 – HCL BigFix CLM Installer- Database Names

8. Click **Next** to go to Server Configuration page.

5.3.2.3 Server Configuration

In this section, details of HCL BigFix CLM App Server using the installer is being captured.

1. IP Address/Host Name is auto populated.
2. Enter the Account Type (Domain Administrator or Local Administrator).
3. Provide the Domain
4. Enter the UserName to access the Web server.
5. Enter the Password for the web server.
6. Click on Check User Validity button.



Server Configuration

IP Address/Host Name *

Account Type * Domain Administrator

Domain *

User Name *

Password * ****************** Validation Successful

Figure 70 - Server Configuration

7. Select Messaging Queue as MSMQ (if not already selected)
8. Click **Next**.
9. The Prerequisite Checker screen appears.

All the fields marked with asterisk (*) are mandatory.

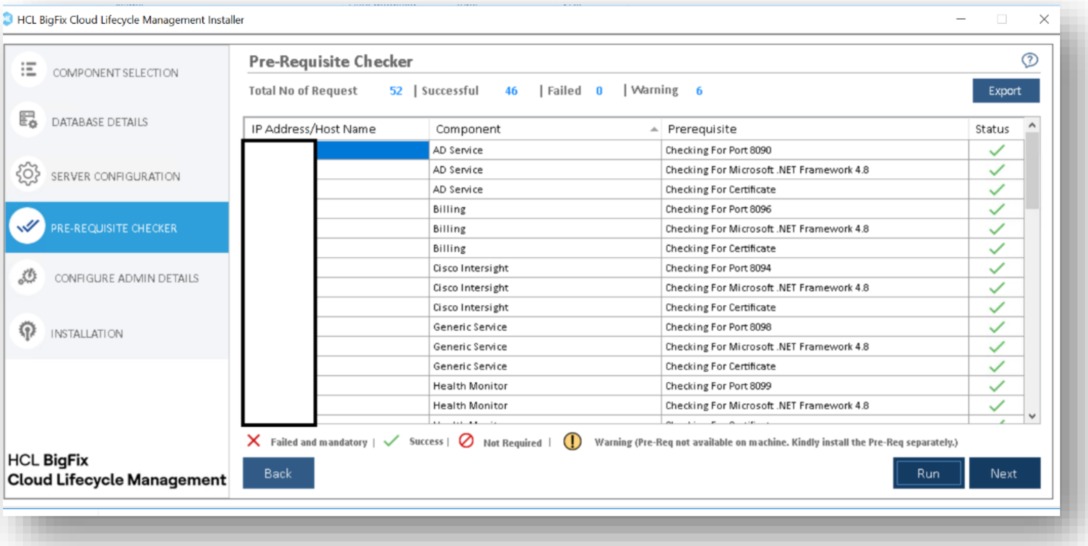
5.3.2.4 Run Prerequisite Checker

This section describes how to run the prerequisite checker to verify that the installation pre-requisites have been installed.

The **Prerequisite Checker** screen lists the configurations that are mandatory for the components selected on previous screen.

Prerequisite Checker always runs as part of Setup.

1. Click **Run** to start the pre-requisite checker.



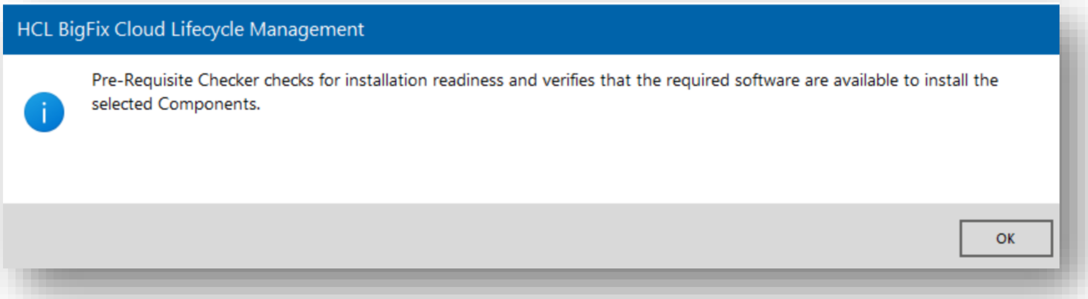
Pre-Requisite Checker

Total No of Request 52 | Successful 46 | Failed 0 | Warning 6

IP Address/Host Name	Component	Prerequisite	Status
	AD Service	Checking For Port 8090	✓
	AD Service	Checking For Microsoft .NET Framework 4.8	✓
	AD Service	Checking For Certificate	✓
	Billing	Checking For Port 8096	✓
	Billing	Checking For Microsoft .NET Framework 4.8	✓
	Billing	Checking For Certificate	✓
	Cisco Intersight	Checking For Port 8094	✓
	Cisco Intersight	Checking For Microsoft .NET Framework 4.8	✓
	Cisco Intersight	Checking For Certificate	✓
	Generic Service	Checking For Port 8098	✓
	Generic Service	Checking For Microsoft .NET Framework 4.8	✓
	Generic Service	Checking For Certificate	✓
	Health Monitor	Checking For Port 8099	✓
	Health Monitor	Checking For Microsoft .NET Framework 4.8	✓

✕ Failed and mandatory | ✓ Success | ⊘ Not Required | ⓘ Warning (Pre-Req not available on machine. Kindly install the Pre-Req separately.)

Figure 71 - Prerequisite Checker

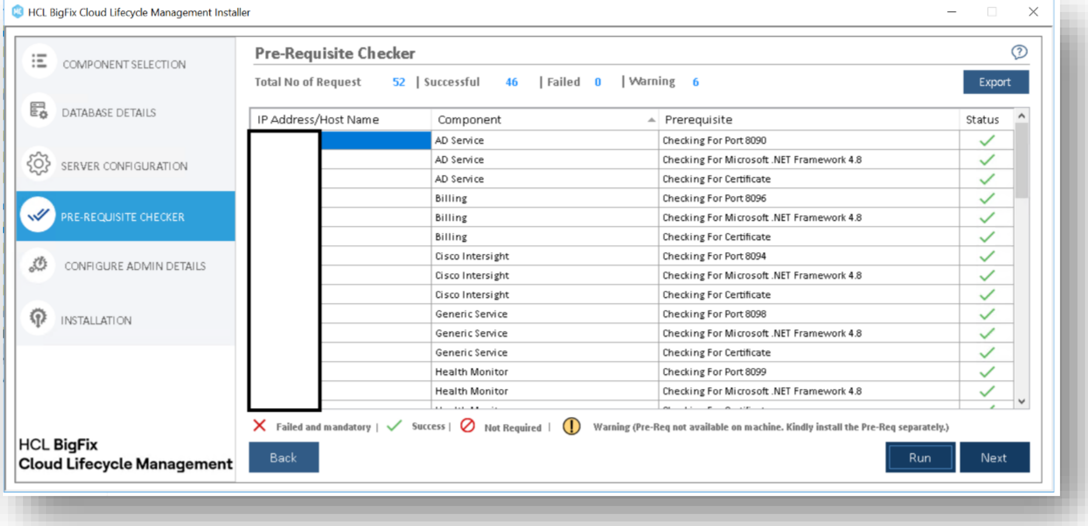


HCL BigFix Cloud Lifecycle Management

Pre-Requisite Checker checks for installation readiness and verifies that the required software are available to install the selected Components.

Figure 72 - Prerequisite Checker Information Assistance

The **Prerequisite Checker** identifies the existing host, component, list of relevant pre-requisites and performs the check for installation readiness. If any pre-requisite is missing, it gets listed under the **Status** field as (X). If any pre-requisite is not required, it gets listed under the **Status** field as (⊘) means **Not Required**. Pre-requisites which show as **Warning** can be ignored.



HCL BigFix Cloud Lifecycle Management Installer

Pre-Requisite Checker

Total No of Request 52 | Successful 46 | Failed 0 | Warning 6

IP Address/Host Name	Component	Prerequisite	Status
[redacted]	AD Service	Checking For Port 8090	✓
[redacted]	AD Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	AD Service	Checking For Certificate	✓
[redacted]	Billing	Checking For Port 8096	✓
[redacted]	Billing	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Billing	Checking For Certificate	✓
[redacted]	Cisco Intersight	Checking For Port 8094	✓
[redacted]	Cisco Intersight	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Cisco Intersight	Checking For Certificate	✓
[redacted]	Generic Service	Checking For Port 8098	✓
[redacted]	Generic Service	Checking For Microsoft .NET Framework 4.8	✓
[redacted]	Generic Service	Checking For Certificate	✓
[redacted]	Health Monitor	Checking For Port 8099	✓
[redacted]	Health Monitor	Checking For Microsoft .NET Framework 4.8	✓

✕ Failed and mandatory | ✓ Success | ⊘ Not Required | ⓘ Warning (Pre-Req not available on machine. Kindly install the Pre-Req separately.)

Figure 73 – Prerequisite Checker (Cont.)

2. If all the checks succeed, the **Next** button is enabled, click **Next** to proceed.

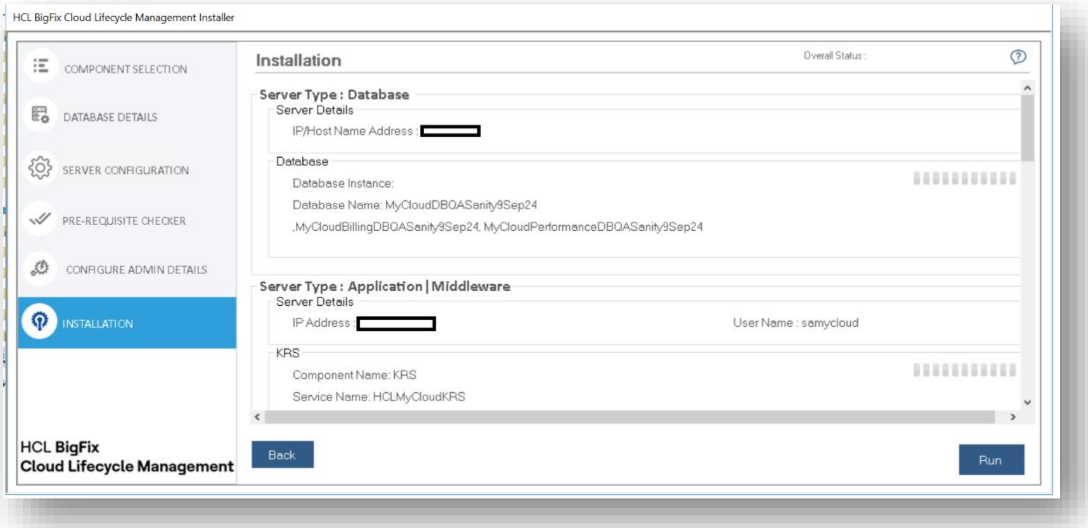
If any of the mandatory checks fails, the **Next** button is disabled.

3. On completion of these steps, click **Next**.

5.3.2.5 Installation

This section lists all the configurations as entered (server and component wise). Review the details and verify that the responses provided are correct.

1. Verify the Details which were provided and click on **Run** to start the App Layer Service Components installation.



Server Type : Database

Server Details

IP/Host Name Address : [redacted]

Database

Database Instance:

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address : [redacted] User Name : samycloud

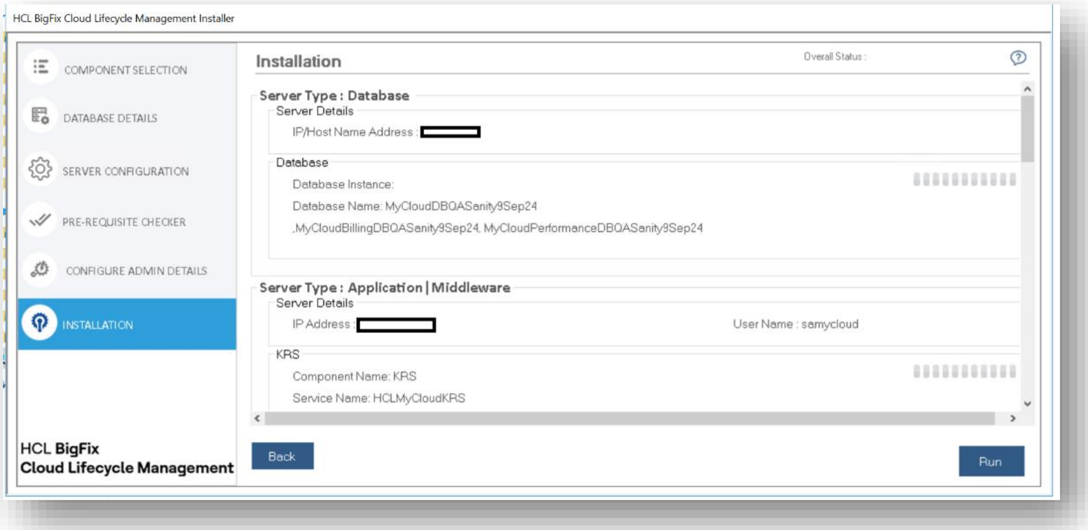
KRS

Component Name: KRS

Service Name: HCLMyCloudKRS

Figure 74 – HCL BigFix CLM Installation Details

2. Installation progress can be seen as shown below.



Server Type : Database

Server Details

IP/Host Name Address : [redacted]

Database

Database Instance:

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address : [redacted] User Name : samycloud

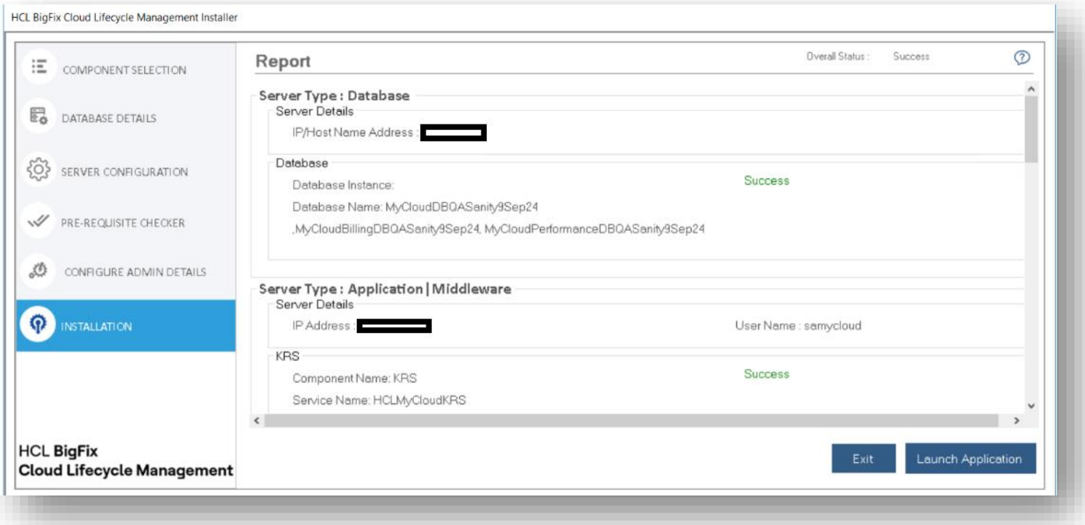
KRS

Component Name: KRS

Service Name: HCLMyCloudKRS

Figure 75 – HCL BigFix CLM Installer- Progress

3. On successful installation of web components, below screen will appear.



Report

Overall Status : Success

Server Type : Database

Server Details

IP/Host Name Address [redacted]

Database

Database Instance: Success

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address [redacted] User Name : samycloud

KRS

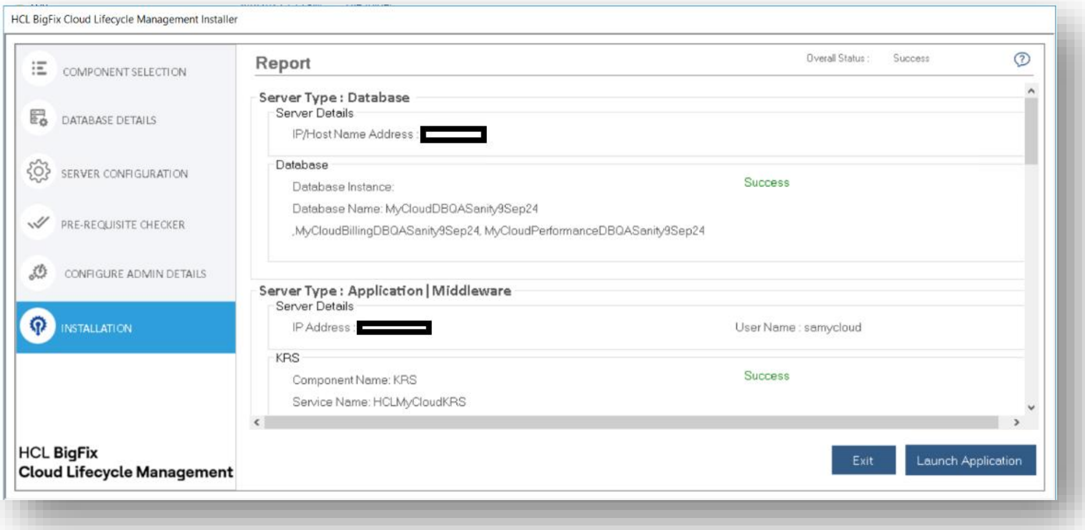
Component Name: KRS Success

Service Name: HCLMyCloudKRS

Figure 76 – HCL BigFix CLM Installer – Success

4. Click **Finish** and below popup message will display with" **Setup Completed**". Click **OK**

Also, in case of Upgrade/Fresh Installation, KMS URL will be updated in config file. First this URL will be fetched from DB and will be updated. If does not exist, the default URL will be updated.



Report

Overall Status : Success

Server Type : Database

Server Details

IP/Host Name Address [redacted]

Database

Database Instance: Success

Database Name: MyCloudDBQASanity9Sep24 ,MyCloudBillingDBQASanity9Sep24, MyCloudPerformanceDBQASanity9Sep24

Server Type : Application | Middleware

Server Details

IP Address [redacted] User Name : samycloud

KRS

Component Name: KRS Success

Service Name: HCLMyCloudKRS

Figure 77 – HCL BigFix CLM Installer – Setup Complete

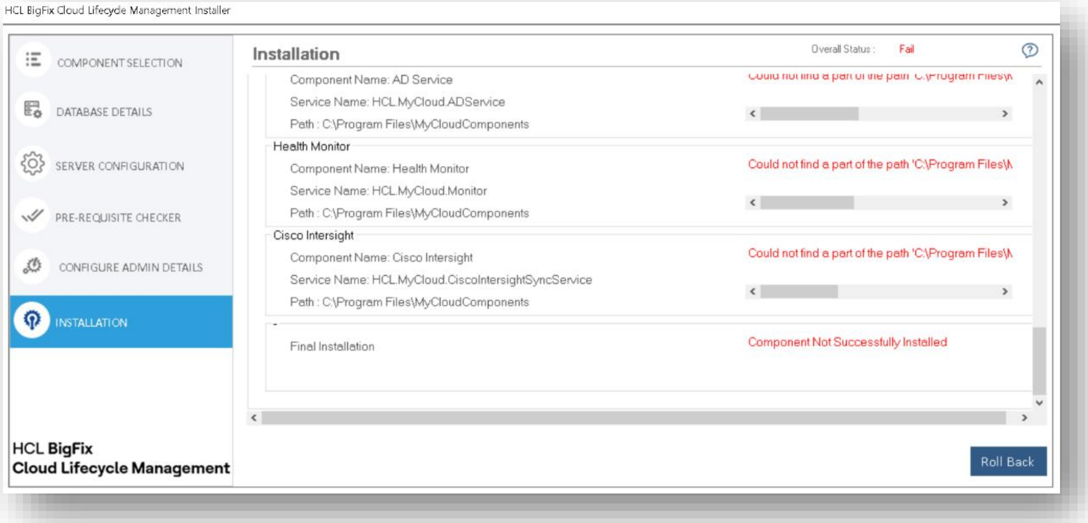
If the Installation fails, go to Rollback.

5.3.2.6 Rollback

This section describes the rollback functionality. Rollback is only applicable to installed components in the case of a new installation. Rollback does not delete or remove the database as it is only applicable to installed components.

For a New Installation, if installation fails for any reason, then the Rollback option gets enabled and clicking it removes the installed component.

During the installation of components and DB for the first time, if the DB is created successfully and if any component installation fails, the Rollback button gets enabled.



Installation

Overall Status : Fail

Component Name: AD Service
Service Name: HCL.MyCloud.ADService
Path : C:\Program Files\MyCloudComponents
Could not find a part of the path 'C:\Program Files\

Health Monitor
Component Name: Health Monitor
Service Name: HCL.MyCloud.Monitor
Path : C:\Program Files\MyCloudComponents
Could not find a part of the path 'C:\Program Files\

Cisco Intersight
Component Name: Cisco Intersight
Service Name: HCL.MyCloud.CiscoIntersightSyncService
Path : C:\Program Files\MyCloudComponents
Could not find a part of the path 'C:\Program Files\

Final Installation
Component Not Successfully Installed

Figure 78 - Rollback

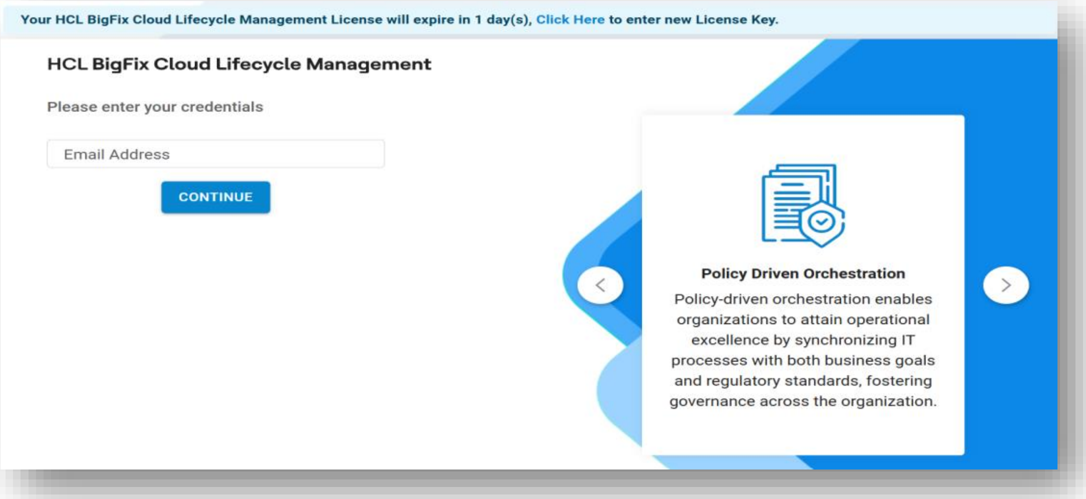
When Rollback action is performed, all selected components get rolled back except DB. So, there is no impact on DB while performing Rollback.

6 HCL BigFix CLM Post Installation Task

Once HCL BigFix CLM is installed and configured as per default settings, the admin user can change the product configurations to add another layer of security. It can be done by making the following configuration changes:

6.1 Provide HCL BigFix CLM License

1. Launch HCL BigFix CLM Web by providing HCL BigFix CLM Web URL in supported browser.
2. Enter Admin email id.



Your HCL BigFix Cloud Lifecycle Management License will expire in 1 day(s), Click Here to enter new License Key.

HCL BigFix Cloud Lifecycle Management

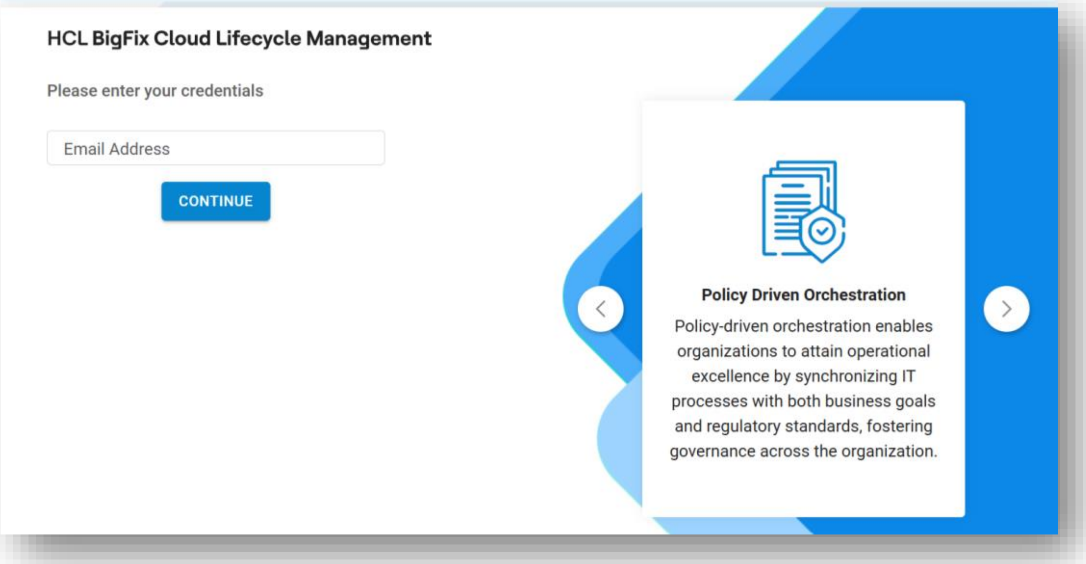
Please enter your credentials

Policy Driven Orchestration

Policy-driven orchestration enables organizations to attain operational excellence by synchronizing IT processes with both business goals and regulatory standards, fostering governance across the organization.

Figure 79 – HCL BigFix CLM Login

3. Click **Next**
4. Message will appear mentioning license key is expired or not available.



HCL BigFix Cloud Lifecycle Management

Please enter your credentials

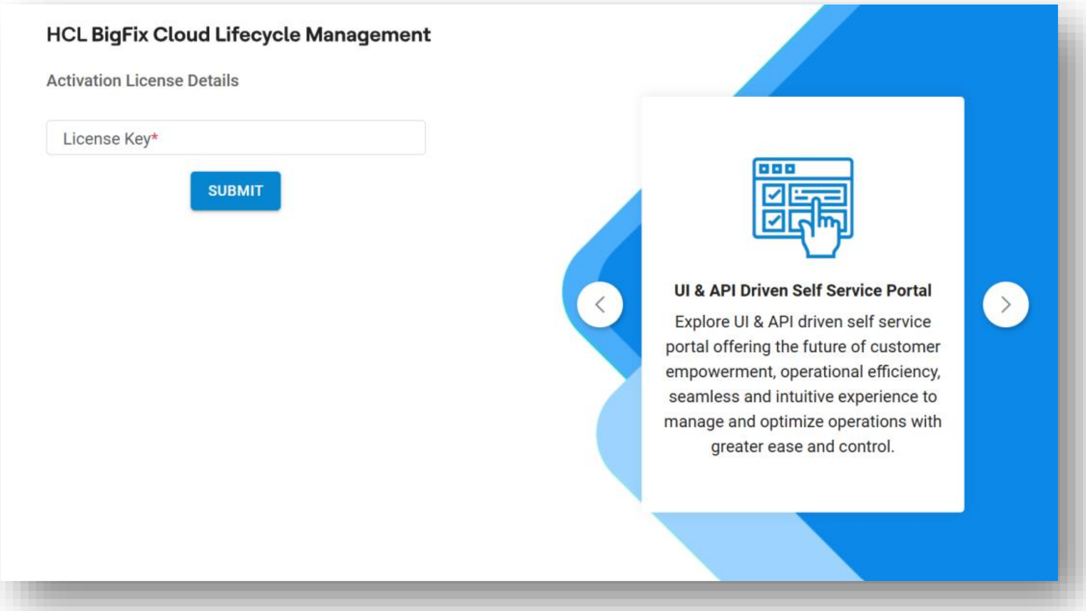
Policy Driven Orchestration

Policy-driven orchestration enables organizations to attain operational excellence by synchronizing IT processes with both business goals and regulatory standards, fostering governance across the organization.

Figure 80 – HCL BigFix CLM -Enter License Key

5. Click on **Click Here** to enter the license Key.

6. Enter the License Key and click **Submit** button.



HCL BigFix Cloud Lifecycle Management

Activation License Details

License Key*

UI & API Driven Self Service Portal

Explore UI & API driven self service portal offering the future of customer empowerment, operational efficiency, seamless and intuitive experience to manage and optimize operations with greater ease and control.

Figure 81 – HCL BigFix CLM -Enter License Key

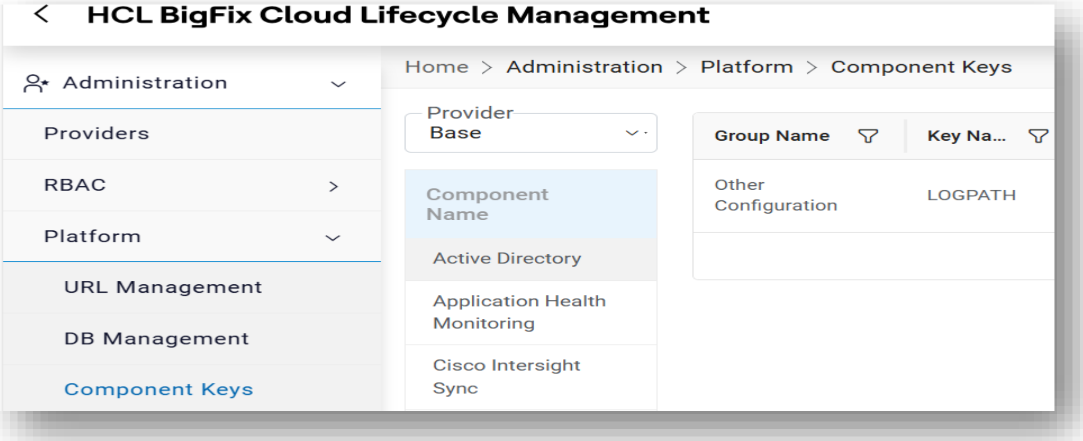
Contact to administrator to get the license key.

7. Click on "**Click Here**" to login again.
8. Provide the HCL BigFix CLM Admin email id and Password and check if login is successful.

6.1.1 Master Data changes

1. Login into HCL BigFix CLM Portal with http protocol URL.

   protocol URL.: **<http://{webserverhostname}/WebUI/Account/Index>**.
2. Change webserver hostname in the URL with actual webserver hostname.
3. After the login, user is redirected to the landing page. Navigate to **Administration > Platform > Component Keys** as shown in Figure 82 - Admin Home Page.



HCL BigFix Cloud Lifecycle Management

Home > Administration > Platform > Component Keys

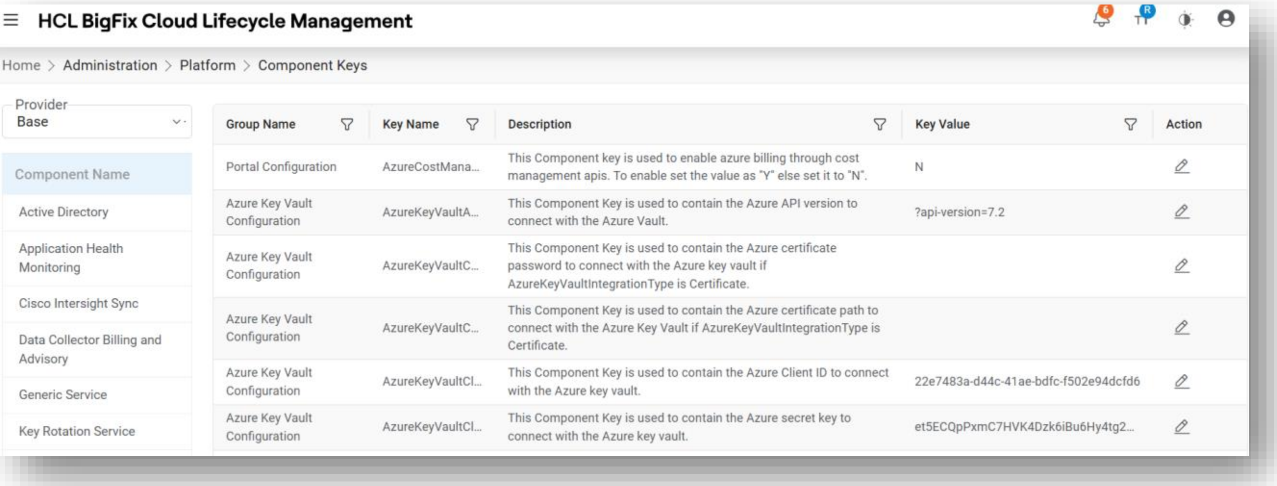
Provider: Base

Group Name	Key Na...
Other Configuration	LOGPATH

Figure 82 – Admin Home Page

4. User will be redirected to the **Component Keys** page, as shown in Figure 83 – Manage Components.

5. Select **Website Service (WEBSITE)** in the Component Name dropdown and click on **Go** button.
6. Change the Key value for the following Key Name(s):
   - *JsURL* from http://XX.X.XXX.XX:443/WebUI/JS to https://XX.X.XXX.XX/WebUI/JS
   - *SiteURL* from http://XX.X.XXX.XX:443/WebUI to https://XX.X.XXX.XX/WebUI



HCL BigFix Cloud Lifecycle Management

Home > Administration > Platform > Component Keys

Provider: Base

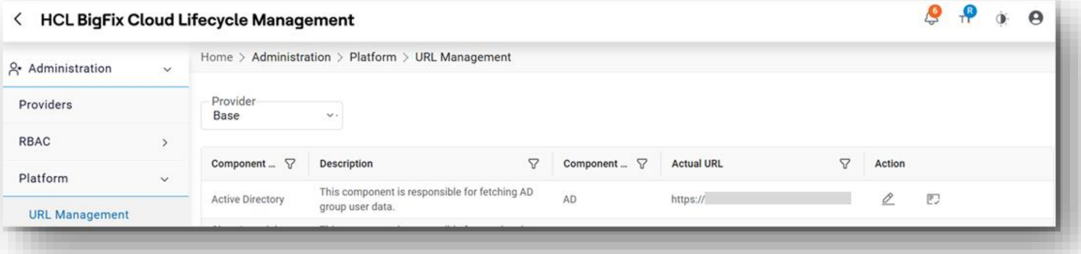
Component Name

- Active Directory
- Application Health Monitoring
- Cisco Intersight Sync
- Data Collector Billing and Advisory
- Generic Service
- Key Rotation Service

Group Name	Key Name	Description	Key Value	Action
Portal Configuration	AzureCostMana...	This Component key is used to enable azure billing through cost management apis. To enable set the value as "Y" else set it to "N".	N	
Azure Key Vault Configuration	AzureKeyVaultA...	This Component Key is used to contain the Azure API version to connect with the Azure Vault.	?api-version=7.2	
Azure Key Vault Configuration	AzureKeyVaultC...	This Component Key is used to contain the Azure certificate password to connect with the Azure key vault if AzureKeyVaultIntegrationType is Certificate.		
Azure Key Vault Configuration	AzureKeyVaultC...	This Component Key is used to contain the Azure certificate path to connect with the Azure Key Vault if AzureKeyVaultIntegrationType is Certificate.		
Azure Key Vault Configuration	AzureKeyVaultCl...	This Component Key is used to contain the Azure Client ID to connect with the Azure key vault.	22e7483a-d44c-41ae-bdfc-f502e94dcfd6	
Azure Key Vault Configuration	AzureKeyVaultCl...	This Component Key is used to contain the Azure secret key to connect with the Azure key vault.	et5ECQpPxmC7HVK4Dzk6iBu6Hy4tg2...	

Figure 83 – Manage Components Keys

7. Navigate to **Administration > Platform > URL Management**.



HCL BigFix Cloud Lifecycle Management

Administration

- Providers
- RBAC
- Platform
  - URL Management

Home > Administration > Platform > URL Management

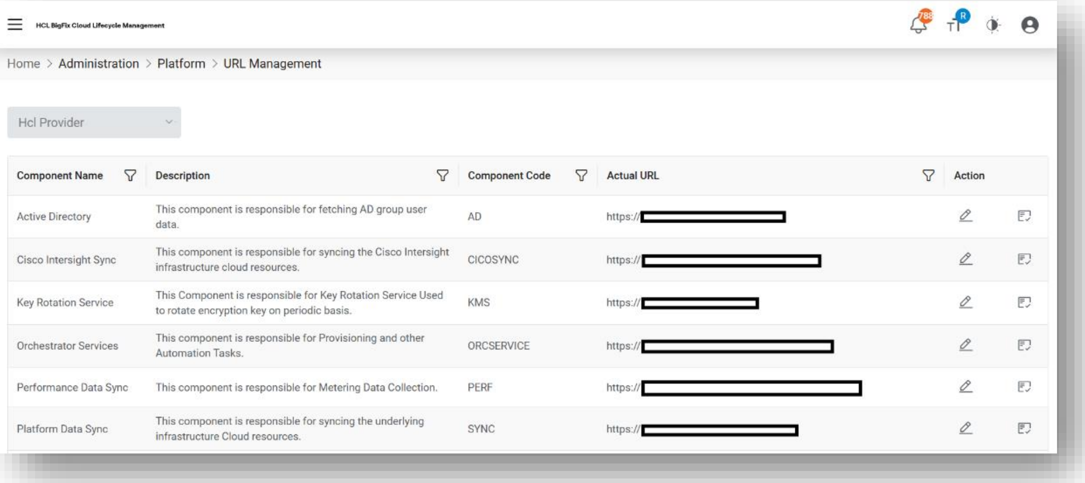
Provider: Base

Component ...	Description	Component ...	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	

Figure 84 - Landing Page with selected URL Management

8. Select **Base** in the **Provider** dropdown and click on **Go** button.
9. Change the URL for the following Component Name(s):
   - Web API from http://XX.X.XXX.XX:443/WebAPI to https://XX.X.XXX.XX/WebAPI
   - Key Management Services (Rotation Key) from http://XX.X.XXX.XX:80/KMS to https://XX.X.XXX.XX:8443/KMS.
10. To test Middleware Components, click **Test URL**.

If Test URL for Web API gets failed, Copy the WebAPI URL and open in browser and click Advanced and proceed. After this test the WebAPI URL again for success.



Home > Administration > Platform > URL Management

Hcl Provider

Component Name	Description	Component Code	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	
Cisco Intersight Sync	This component is responsible for syncing the Cisco Intersight infrastructure cloud resources.	CICOSYNC	https://[redacted]	
Key Rotation Service	This Component is responsible for Key Rotation Service Used to rotate encryption key on periodic basis.	KMS	https://[redacted]	
Orchestrator Services	This component is responsible for Provisioning and other Automation Tasks.	ORCSERVICE	https://[redacted]	
Performance Data Sync	This component is responsible for Metering Data Collection.	PERF	https://[redacted]	
Platform Data Sync	This component is responsible for syncing the underlying infrastructure Cloud resources.	SYNC	https://[redacted]	

Figure 85 – URL Management

11. Restart the IIS. Steps are as follows:
12. Open Command Prompt by clicking on Start on windows task bar → Type cmd → right-click on the Command Prompt → select **Run as administrator**.

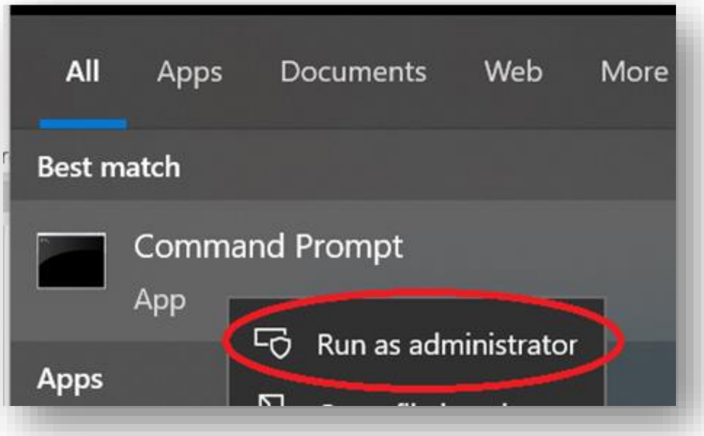
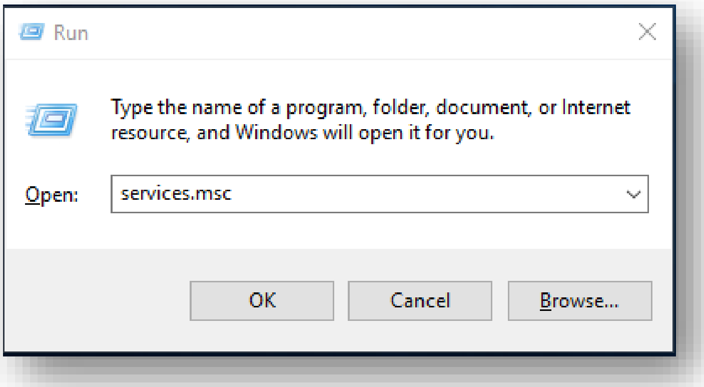


Figure 86 – Command Prompt as Administrator

13. Run Command: "**IISRESET**"
14. Now Close the browser and open the webapplication with HTTPS URL.

6.1.1.1 Stop All Services

1. Stop all the Services and find services file location. This step must be performed on the server where the middleware components/App Layer are installed.
2. Press **Window + R** keys to open run window, then type **services.msc** and click **OK**.



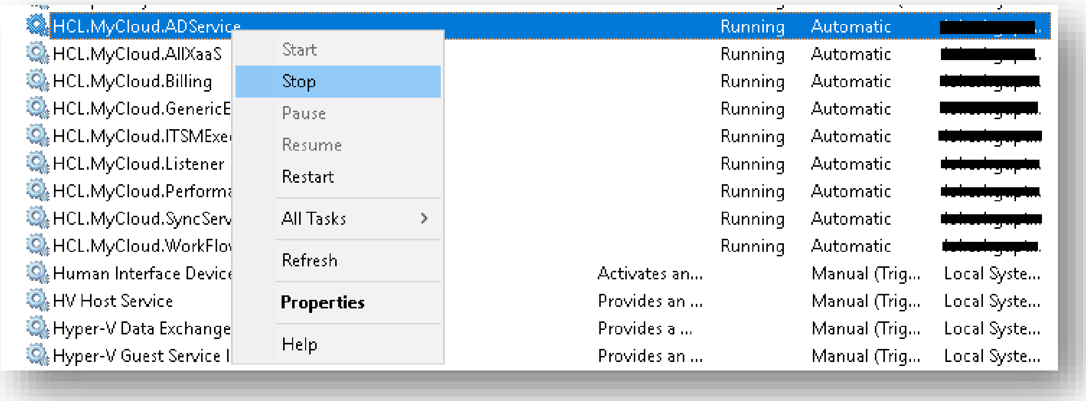
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Figure 87 – Run Command Window

3. User will be redirected to the **Windows Service Manager**.

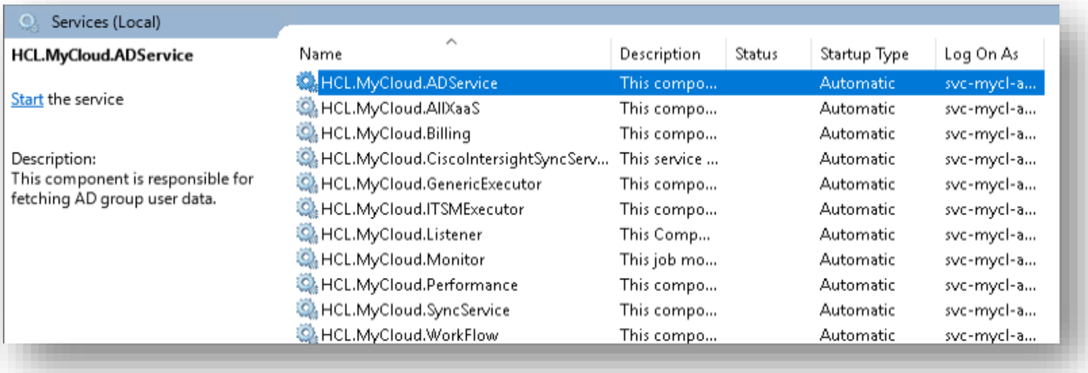


HCL.MyCloud.ADService		Running	Automatic	[redacted]
HCL.MyCloud.AllXaaS		Running	Automatic	[redacted]
HCL.MyCloud.Billing		Running	Automatic	[redacted]
HCL.MyCloud.GenericE		Running	Automatic	[redacted]
HCL.MyCloud.ITSMExe		Running	Automatic	[redacted]
HCL.MyCloud.Listener		Running	Automatic	[redacted]
HCL.MyCloud.Performa		Running	Automatic	[redacted]
HCL.MyCloud.SyncServ		Running	Automatic	[redacted]
HCL.MyCloud.WorkFlo		Running	Automatic	[redacted]
Human Interface Device	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service I	Provides an ...		Manual (Trig...	Local Syste...

Figure 88 – Windows Services Manager

4. Stop the below mentioned services. Each of these services is responsible for a component in HCL BigFix CLM. Select the service, then right-click and select **Stop**.

   - HCL.MyCloud.ADService
   - HCL.MyCloud.AllXaaS
   - HCL.MyCloud.Billing
   - HCL.MyCloud.GenericExecutor
   - HCL.MyCloud.ITSMExecutor
   - HCL.MyCloud.Listener
   - HCL.MyCloud.Performance
   - HCL.MyCloud.SyncService
   - HCL.MyCloud.WorkFlow
   - HCL.MyCloud.Monitor
   - HCL.MyCloud.CiscoIntersightSyncService



Services (Local)

HCL.MyCloud.ADService

Start the service

Description:
This component is responsible for fetching AD group user data.

Name	Description	Status	Startup Type	Log On As
HCL.MyCloud.ADService	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.AllXaaS	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.Billing	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.CiscoIntersightSyncServ...	This service ...		Automatic	svc-mycl-a...
HCL.MyCloud.GenericExecutor	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.ITSMExecutor	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.Listener	This Comp...		Automatic	svc-mycl-a...
HCL.MyCloud.Monitor	This job mo...		Automatic	svc-mycl-a...
HCL.MyCloud.Performance	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.SyncService	This compo...		Automatic	svc-mycl-a...
HCL.MyCloud.WorkFlow	This compo...		Automatic	svc-mycl-a...

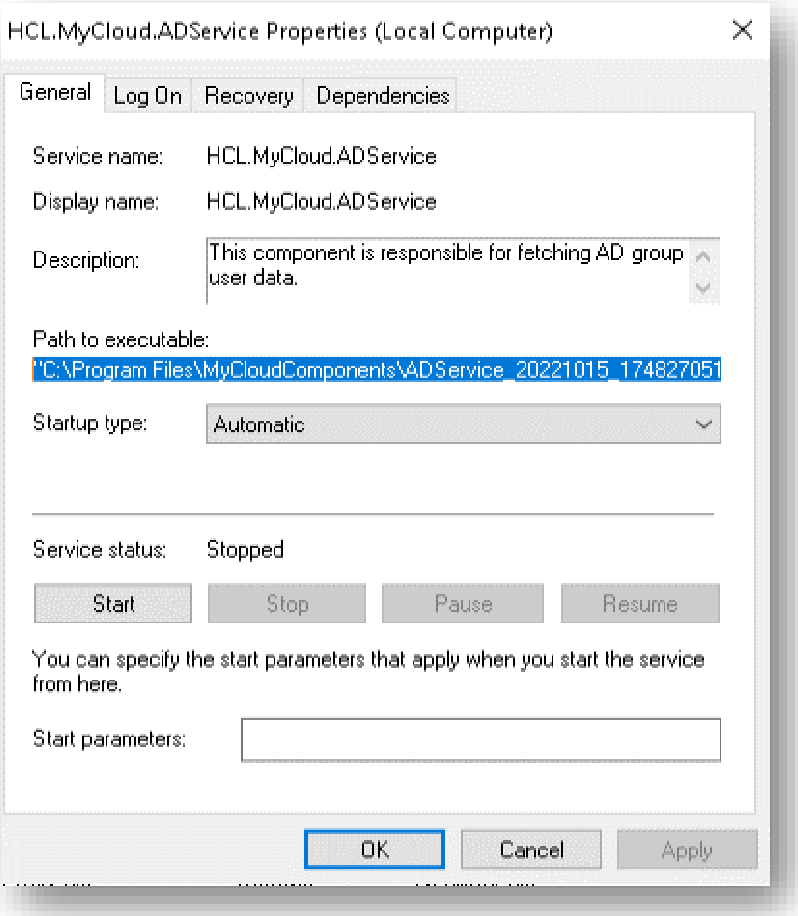
Figure 89 – Windows Services Manager

5. After stopping all the services, the next step is to find out the Middleware Components file location.

6.1.1.2 Path To Executable Services

Once the user has stopped all the services mentioned above, the next step is to find the **PathToExecutable** of the deployed service(s).

1. Open Services.msc from run.
2. Select the service (HCL.MyCloud.ADService), right-click and select Properties.
3. This will open the properties window for that service as shown in Figure 90.
4. Locate the "**Path to Executable**" section in this window.
5. Copy the path and save it in a notepad or a document for future reference.
6. Similarly, copy and save the path to executable for all the services mentioned above in section 6.2.2.1.



HCL.MyCloud.ADService Properties (Local Computer)

Service name: HCL.MyCloud.ADService

Display name: HCL.MyCloud.ADService

Description: This component is responsible for fetching AD group user data.

Path to executable:
"C:\Program Files\MyCloudComponents\ADService_20221015_174827051

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 90 – Windows Services Manager

6.1.1.3 Find Port Number

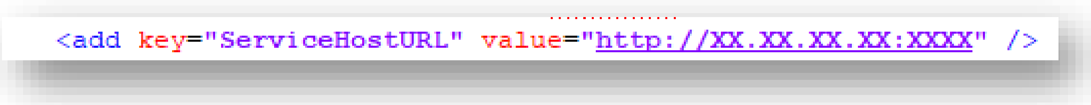
1. Find the Port Number on which services are running.
2. Go to PathToExecutable.
3. For example:

   “C:\ProgramFiles\MyCloudComponents\ADService_XXXXXXXX_XXXXXXXXX“
4. Open the respective service config file (exe.config):

Files names for reference is given below:

- HCL.MyCloud.Service.AD.exe.config
- HCL.CloudBilling.DataCollector.Service.Host.exe.config
- HCL.MyCloud.CiscoIntersightSyncService.Host.exe.config
- HCL.MyCloud.Generic.Host.exe.config
- HCL.MyCloud.Monitor.Host.exe
- HCL.MyCloud.Snow.Host.exe
- HCL.MyCloud.AllXaaS.Host.exe
- HCL.CloudPerformance.DataCollector.Service.Host.exe
- HCL.MyCloud.SyncJobService.Host.exe
- HCL.MyCloud.WorkflowEngine.exe

5. Now find the ***ServiceHostURL*** key



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 91 – Service Host URL in Configuration File

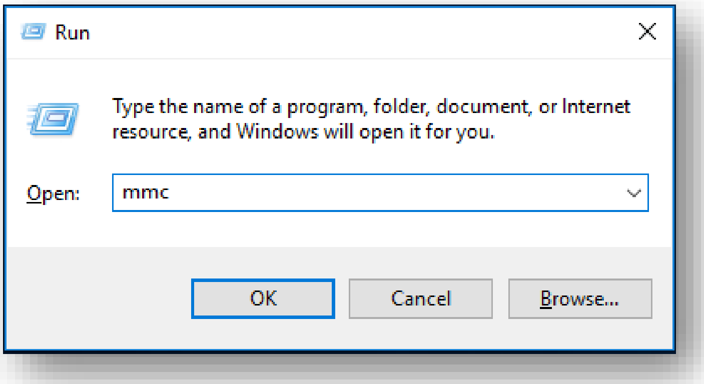
6. Copy the **Port** as shown in the above figure and save it in a notepad or a document for future reference.
7. In a similar way, copy and save the ports for all the services.

6.1.1.4 Certificate changes

During installation (New/Upgrde), all certificates will be installed automatically.

Make sure HCL BigFix CLM Certificate is present in the **personal** folder of **Window Certificate** console and if not present then copy the certificate.

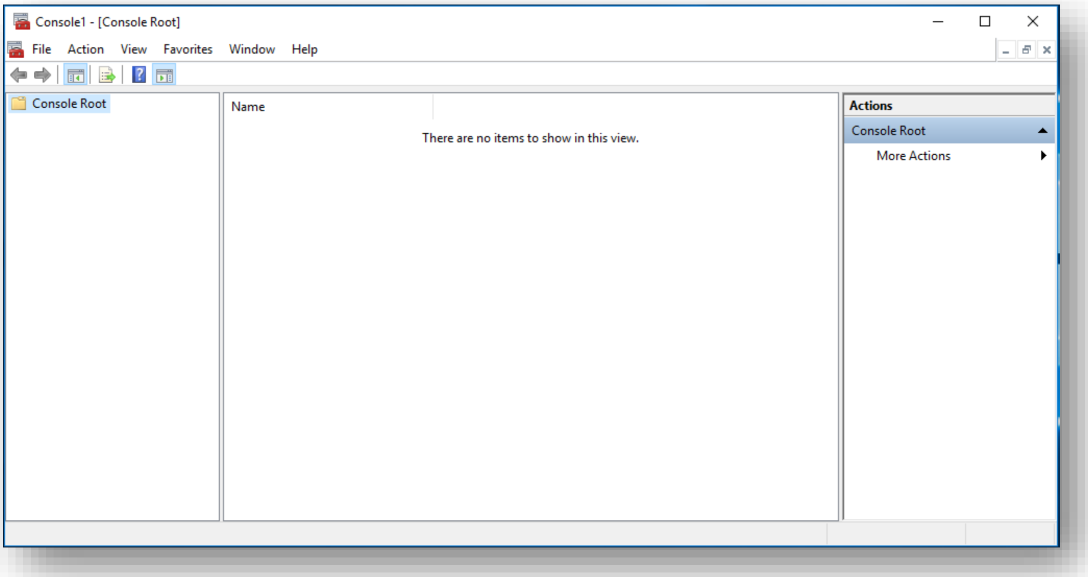
1. Press **Window + R** keys to open the run command window.
2. Now type "**mmc**" and click **OK**.
3. The Certificate Console will open.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

Figure 92 – Run Command Windows



There are no items to show in this view.

Figure 93 – Windows Certificate Console

4. On the console window, in the top menu, click **File → Add/Remove Snap-in**

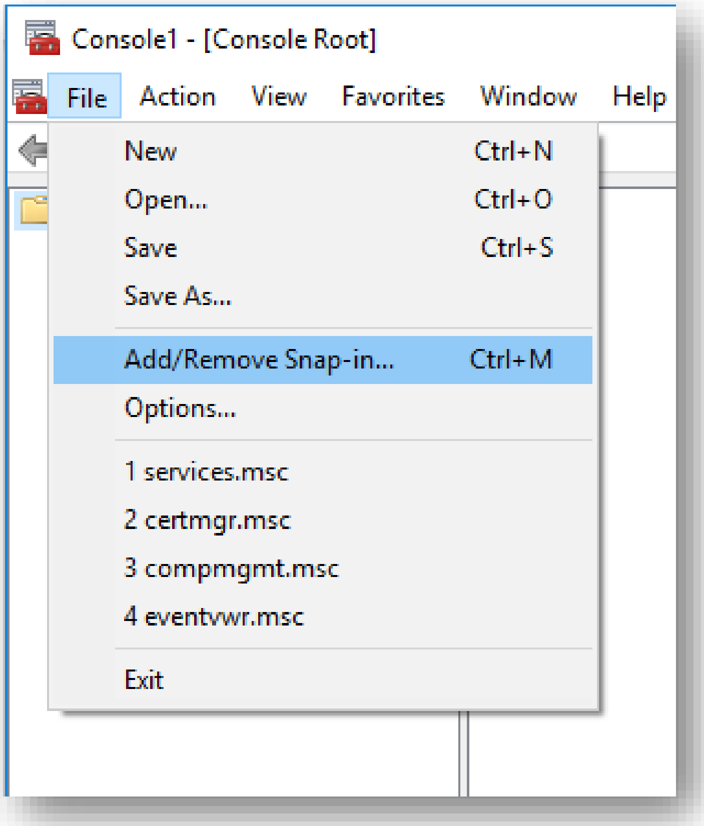
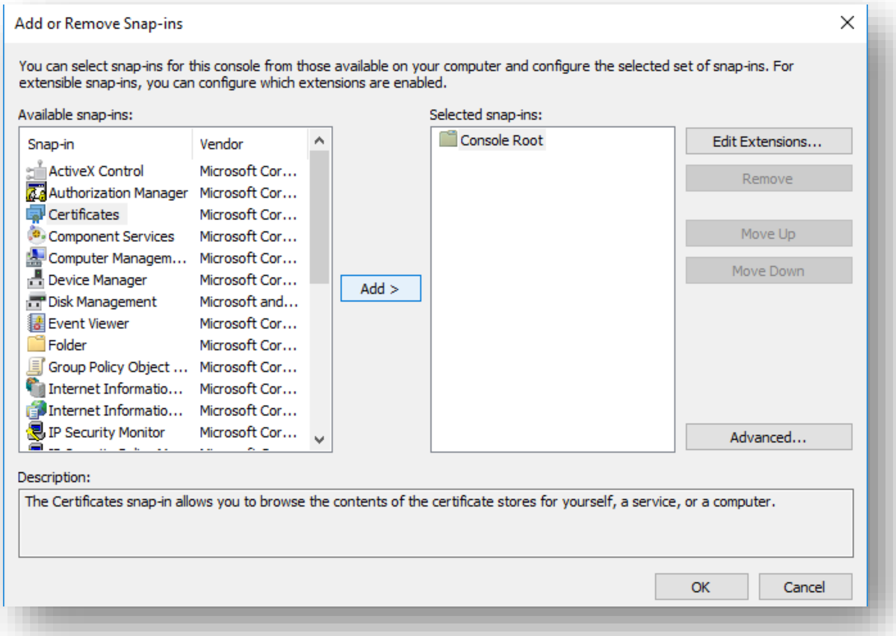


Figure 94 – Windows Certificate Console with File Menu

5. In the **Add or Remove Snap-ins** window, in the **Available snap-ins** pane (left side), select **Certificates**, then click on **Add** button.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...

Selected snap-ins:

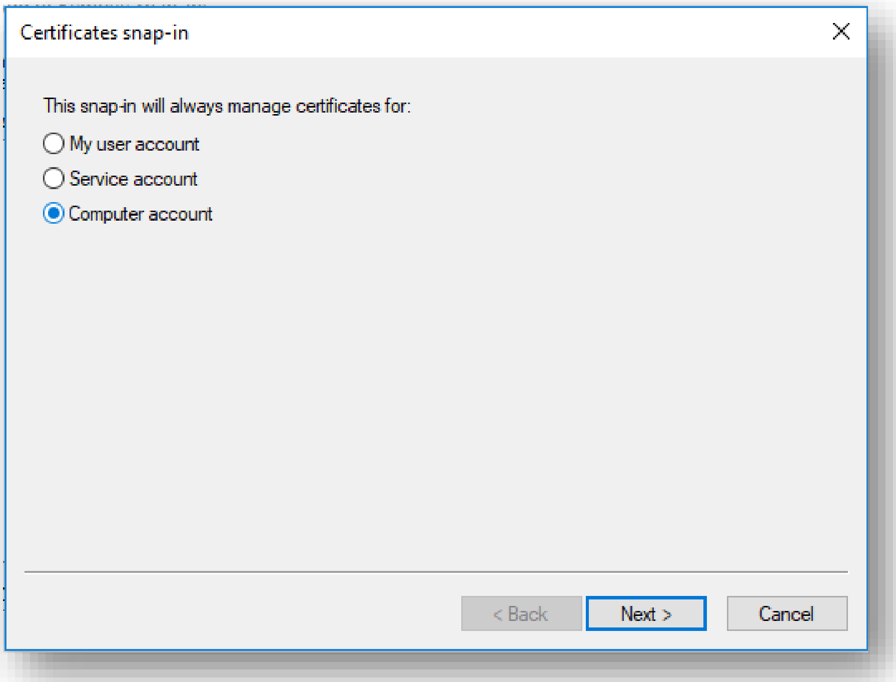
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 95 – Add or Remove screen in Certificate Console

6. In the Certificate snap-in window, select Computer account and then click Next.



Certificates snap-in

This snap-in will always manage certificates for:

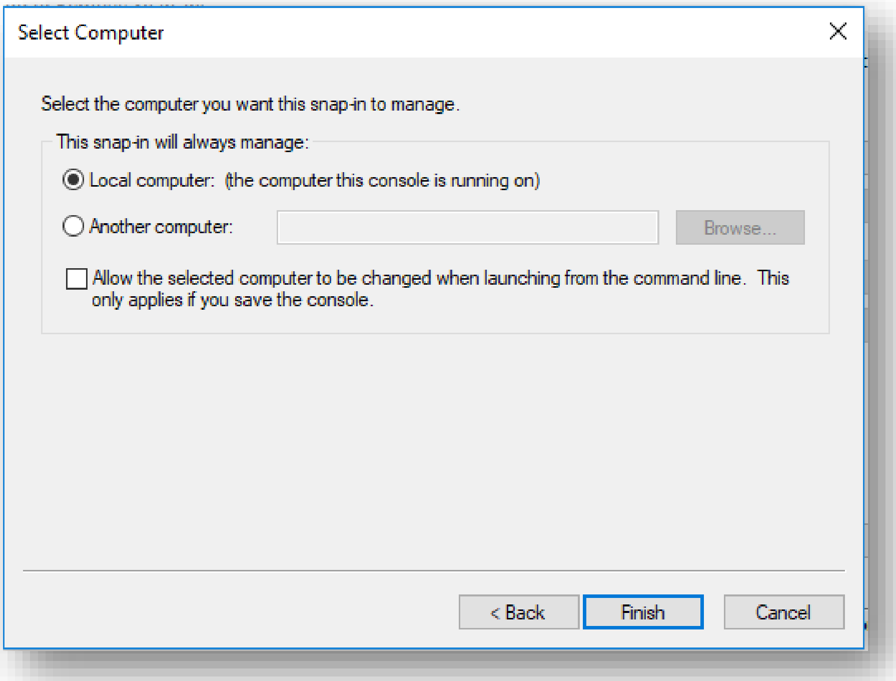
○ My user account

○ Service account

● Computer account

Figure 96 – Certificate snap-in Window

7. In the **Select Computer** window, select **Local computer** and then click **Finish**.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

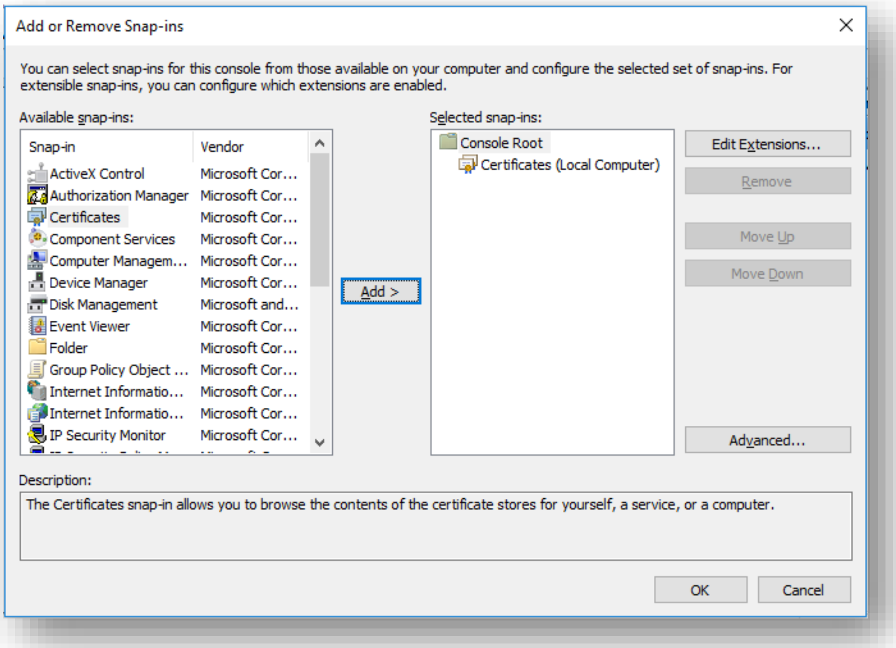
● Local computer: (the computer this console is running on)

○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Figure 97 – Select Computer

8. In the **Add or Remove Snap-ins** window, click **OK** as shown in below figure.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...

Selected snap-ins:

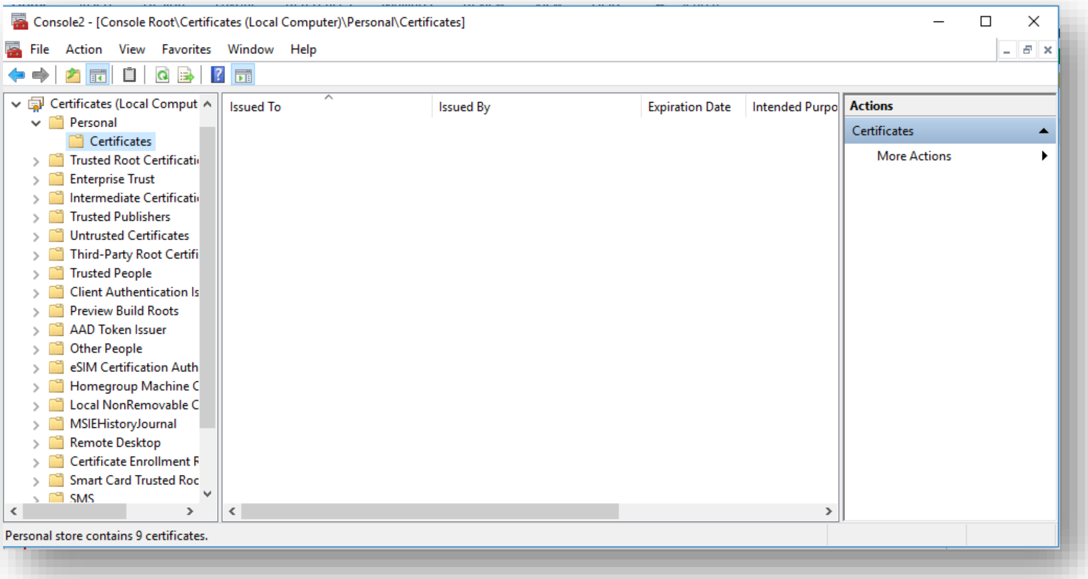
Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 98 – Add or Remove Snap-ins Window

9. Navigate to the certificate console window, as mentioned in step 3. In the **Console Root** pane expand **Certificates (Local Computer), Personal** folder and then select the **Certificate** folder. Check if it contains "**HclTech.MyCloud.App**" certificate as shown below:

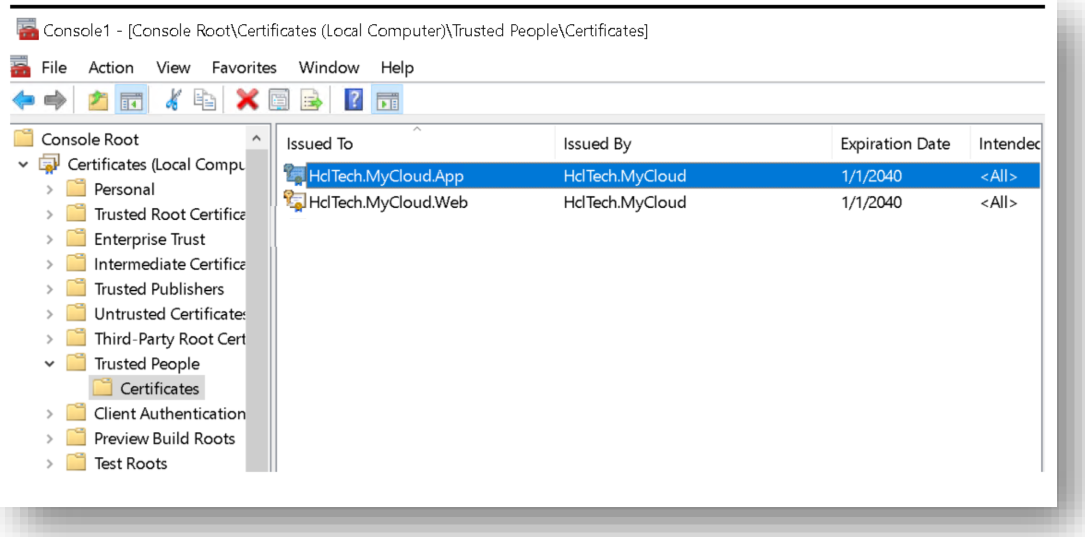


Personal store contains 9 certificates.

Figure 99 - Personal Certificate Console

10. If the Certificate is not present, follow the below steps.

    a. In the Console window, under the Console Root pane (left side), expand Certificates (Local Computer), expand the Trusted People folder, click **Certificates** and then right-click "**HclTech.MyCloud.App**" certificate and select Copy as shown in below figure.



Issued To	Issued By	Expiration Date	Intendec
HclTech.MyCloud.App	HclTech.MyCloud	1/1/2040	<All>
HclTech.MyCloud.Web	HclTech.MyCloud	1/1/2040	<All>

Figure 100 – Certificate Console with selected Certificate

    b. Now right-click on **Personal folder** in the left Console Root window, then click on **Paste** as shown below.

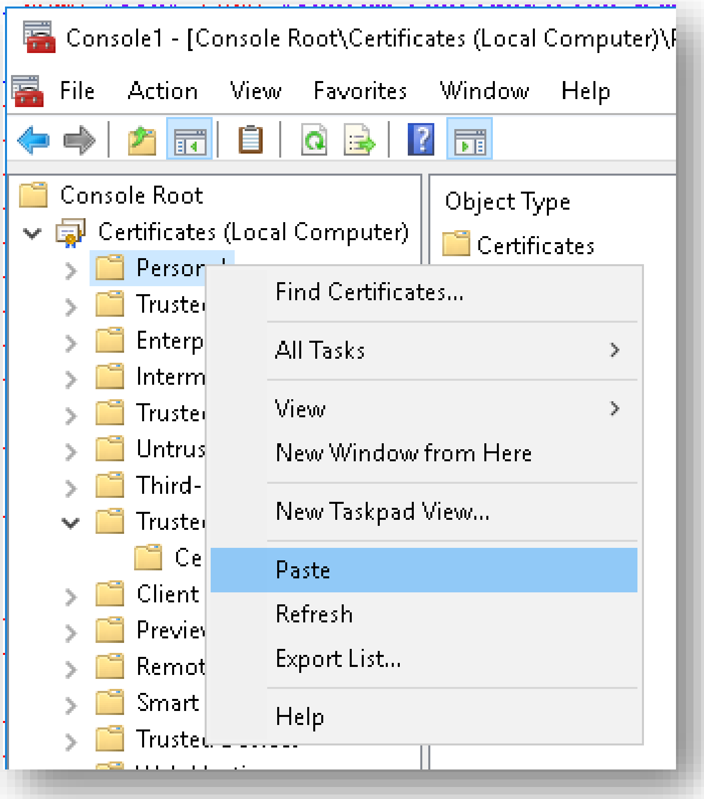
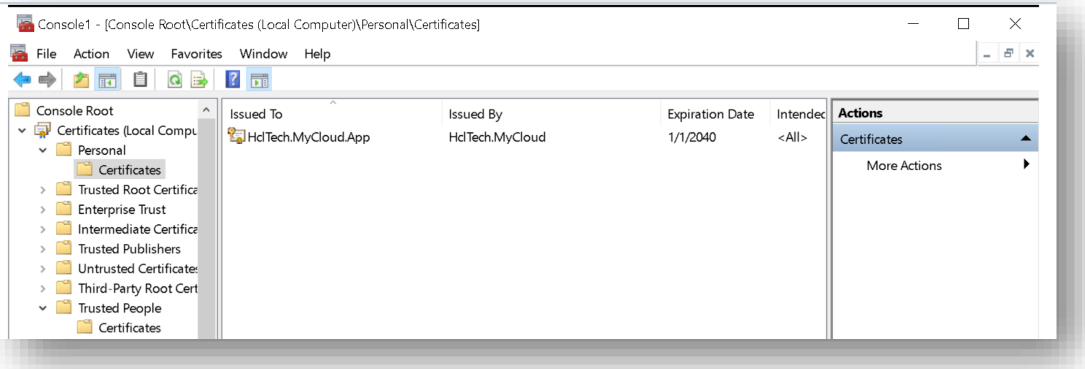


Figure 101 – Copy Certificate

c. Now expand Personal folder and click on **Certificate** folder, now it will show the recently pasted certificate in the main window.



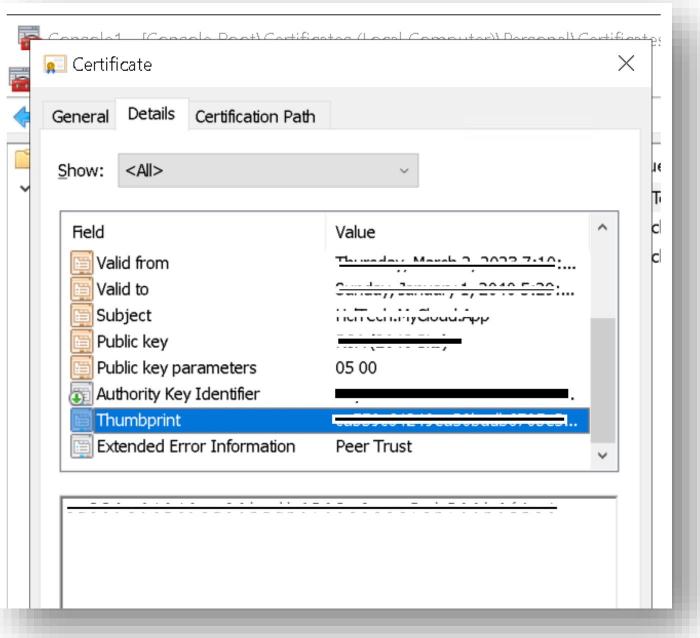
Issued To	Issued By	Expiration Date	Intended
HclTech.MyCloud.App	HclTech.MyCloud	1/1/2040	<All>

Figure 102 – Showing recently added Certificate

d. Double click on the recently pasted certificate. Certificate Properties window will open.

e. Click on the **Details** tab and scroll down to field **Thumbprint**.

f. Copy the thumbprint value. The value is used as "certhash" in below commands.



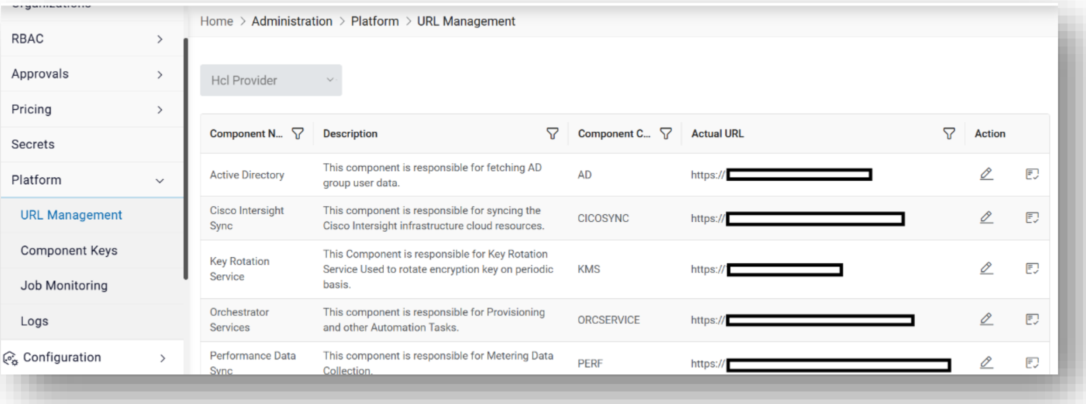
Field	Value
Valid from	[redacted]
Valid to	[redacted]
Subject	[redacted]
Public key	[redacted]
Public key parameters	05 00
Authority Key Identifier	[redacted]
Thumbprint	[redacted]
Extended Error Information	Peer Trust

[redacted]

Figure 103 – Showing Recently Added Certificate

6.1.1.4.1 Master Data changes

1. Login the website with **HCL BigFix CLM Admin account**.
2. Go to **Administration → Platform** and then click **URL Configuration**.



Component N...	Description	Component C...	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	
Cisco Intersight Sync	This component is responsible for syncing the Cisco Intersight infrastructure cloud resources.	CICOSYNC	https://[redacted]	
Key Rotation Service	This Component is responsible for Key Rotation Service Used to rotate encryption key on periodic basis.	KMS	https://[redacted]	
Orchestrator Services	This component is responsible for Provisioning and other Automation Tasks.	ORCSERVICE	https://[redacted]	
Performance Data Sync	This component is responsible for Metering Data Collection.	PERF	https://[redacted]	

Figure 104 – Admin Landing Page

3. Select **Base** in the **Provider** drop down and click on **Go** button.
4. Change the URL for the following Component Name(s) as shown in Figure 105 – Component URL Configuration.
   - Workflow Service
   - from http://<ip>:<port>/WorkflowService to https://<ip>:<port>/WorkflowService
   - Data Collector Billing and Advisory
   - from http://<ip>:<port>/DataCollector to https://<ip>:<port>/DataCollector
   - ServiceNow Executer
   - from http://<ip>:<port>/SnowService to https://<ip>:<port>/SnowService

- Generic Service
- from http://<ip>:<port>/GenericService xxxxxxx
- Application Health Monitoring
- from http://<ip>:<port>/ MonitorService to https://<ip>:<port>/ MonitorService

5. Click on **Test URL** against each service and check for success.
6. Click **Update**.

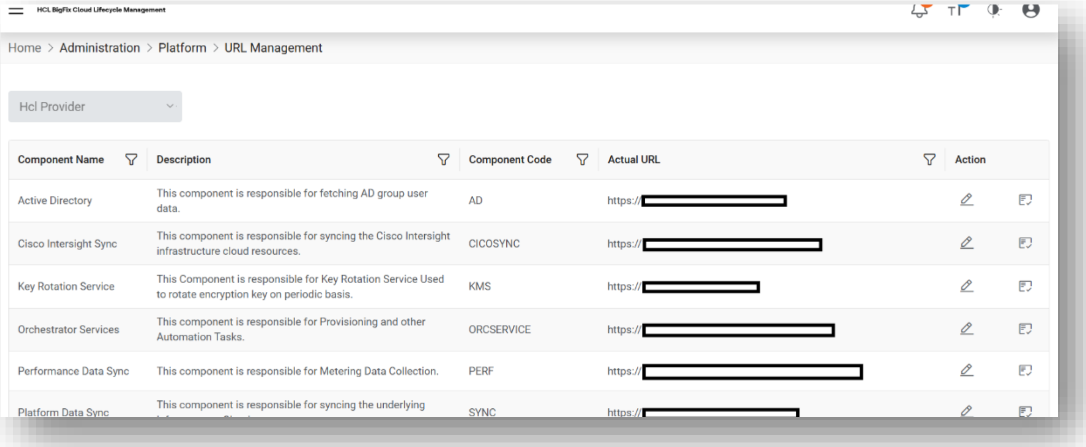
Kindly update the Provider level Components URLs after creating new Provider(s).

Follow Below steps only if you have created provider, if not created, ignore the below steps as of now. However. After creating the Provider, HCL BigFix CLM admin must configure the below configuration.

1. Select **Provider** in the Provider drop down and click on **Go** button.
2. Change the **URL** for the following Component Name(s):

- Platform Data Sync
- from http://<ip>:<port>/SyncService to https://<ip>:<port>/SyncService
- Performance Data Sync
- from http://<ip>:<port>/PerformanceDataCollector to https://<ip>:<port>/PerformanceDataCollector
- Orchestrator Services
- from http://<ip>:<port>/OrchestratorService to https://<ip>:<port>/OrchestratorService
- Active Directory
- from http://<ip>:<port>/ADService to https://<ip>:<port>/ADService.
- Cisco Intersight Sync
- From http://<ip>:<port>/CiscoSyncService to https://<Hostname/IP>:<port>/CiscoSyncService.

Kindly update the Provider level Components URLs after creating new Provider(s).



Home > Administration > Platform > URL Management

Hcl Provider

Component Name	Description	Component Code	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	✎
Cisco Intersight Sync	This component is responsible for syncing the Cisco Intersight infrastructure cloud resources.	CICOSYNC	https://[redacted]	✎
Key Rotation Service	This Component is responsible for Key Rotation Service Used to rotate encryption key on periodic basis.	KMS	https://[redacted]	✎
Orchestrator Services	This component is responsible for Provisioning and other Automation Tasks.	ORCSERVICE	https://[redacted]	✎
Performance Data Sync	This component is responsible for Metering Data Collection.	PERF	https://[redacted]	✎
Platform Data Sync	This component is responsible for syncing the underlying	SYNC	https://[redacted]	✎

Figure 105 – Component URL Configuration

6.2 Change Certificate to CA Signed (Optional)

This section describes the steps to use Certificate provided by the customer instead of HCL BigFix CLM Default certificate. The same certificate can be used for HTTP(S) communication between components.

1. HCL BigFix CLM application has server wise certificates. Below are the details of default certificates installed by HCL BigFix CLM Installer:

– **Web Server Certificates**

- HclTech.Mycloud.Web – Private (.pfx)
- HclTech.MyCloud.App - Public (.cer)

– **App Server Certificates**

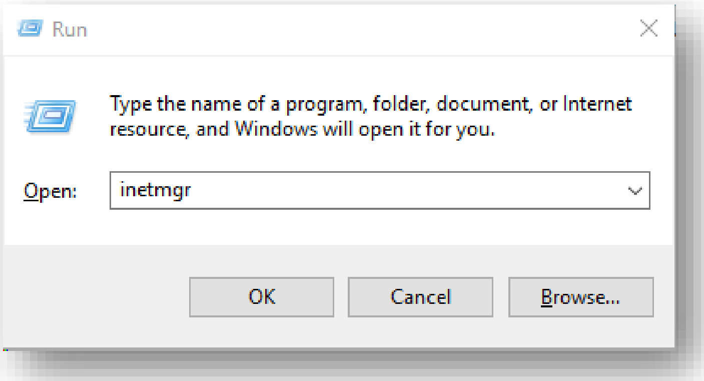
- HclTech.Mycloud.Web – Public (.cer)
- HclTech.MyCloud.App – Private (.pfx)

2. Next step is to find Website, Web API and Key Rotation Service, ApplicationBasePath.
3. Follow the steps mentioned below to do that:

a. Press **Window + R** keys to open run command window.

b. Now type "inetmgr" and click OK.

c. The IIS Console will open.



Run

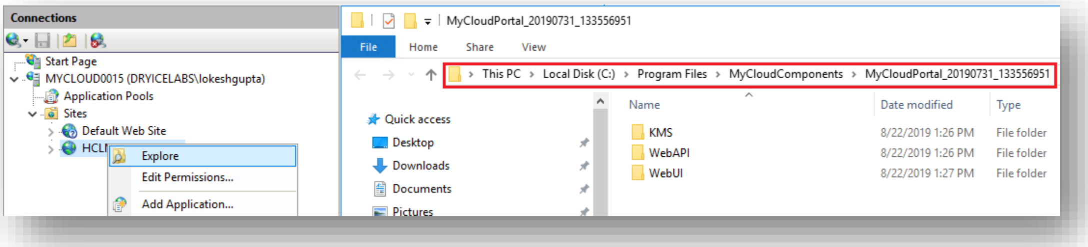
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: inetmgr

Figure 106 – Run window command

d. Now expand the Server Name node → Sites node using the connections section and right-click on the HCLMyCloudPortal node and click on Explore.

e. This will locate the ApplicationBasePath for Website, WebAPI and Key Rotation Service as highlighted in Figure 107 – Application Base Path Locator.



This PC › Local Disk (C:) › Program Files › MyCloudComponents › MyCloudPortal_20190731_133556951

Name	Date modified	Type
KMS	8/22/2019 1:26 PM	File folder
WebAPI	8/22/2019 1:26 PM	File folder
WebUI	8/22/2019 1:27 PM	File folder

Figure 107 – Application Base Path Locator

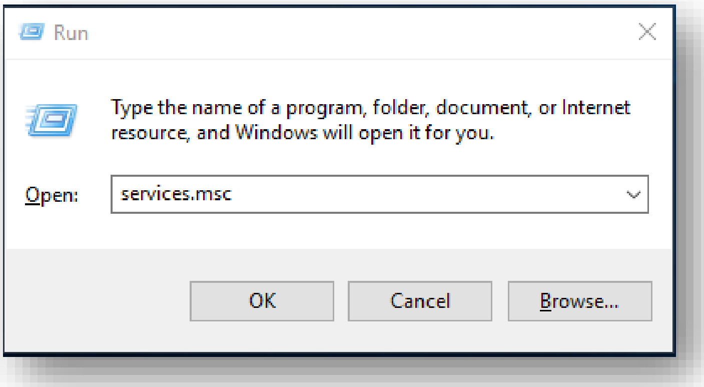
4. Copy the base path and save for future reference.

5. The next step is to find the path of the Middleware component configuration files. The steps are mentioned below:

    a. Find the PathToExecutable of the service(s).

    b. Press **Window + R** keys to open **RUN** window.

    c. Type services.msc and click **Ok**.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

services.msc

Figure 108 – Run Command Window

    d. For the below mentioned services: (Select the service, then right-click, then select Properties and save the highlighted Path to Executable as shown in Figure 107 – Application Base Path Locator for future steps).

    ○ HCL.MyCloud.ADService

    ○ HCL.MyCloud.AllXaaS

    ○ HCL.MyCloud.Billing

    ○ HCL.MyCloud.GenericExecutor

    ○ HCL.MyCloud.ITSMExecutor

    ○ HCL.MyCloud.Listener

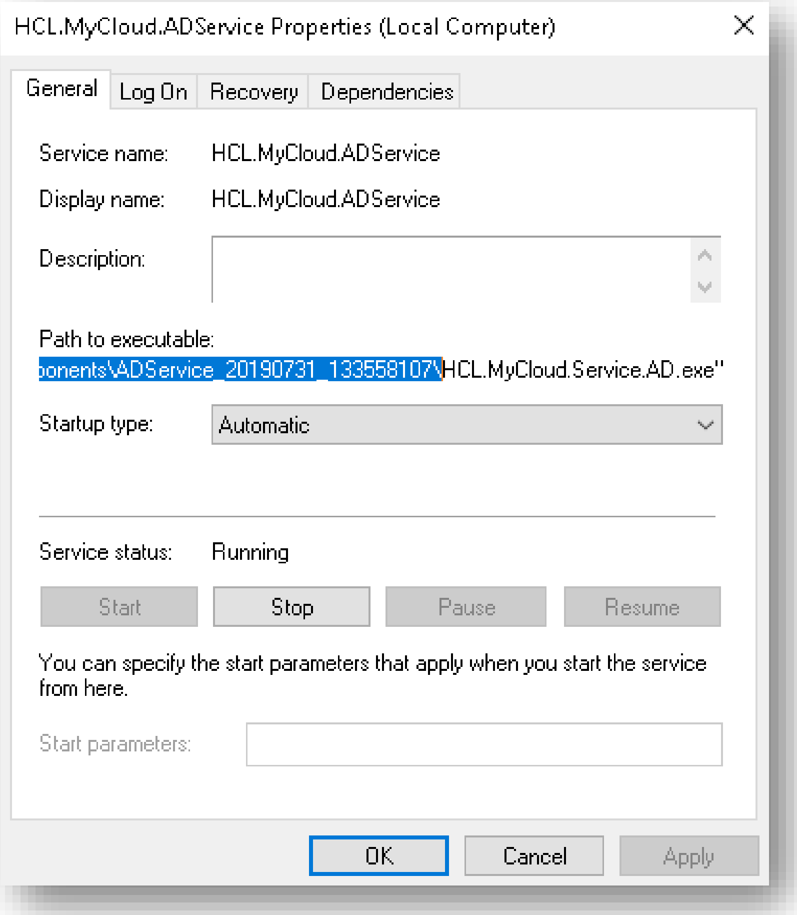
    ○ HCL.MyCloud.Performance

    ○ HCL.MyCloud.SyncService

    ○ HCL.MyCloud.WorkFlow

    ○ HCL.MyCloud.Monitor

    ○ HCL.MyCloud.CiscoIntersightSyncService



Service name: HCL.MyCloud.ADService

Display name: HCL.MyCloud.ADService

Description:

Path to executable:
ponents\ADService_20190731_133558107\HCL.MyCloud.Service.AD.exe"

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 109 – Service Properties Window

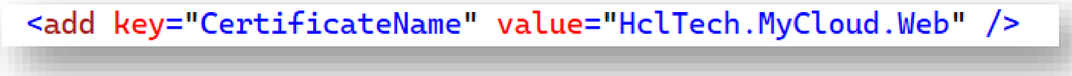
6. Copy the string as highlighted in Figure 109 – Service Properties Window and save it in a notepad or a document for future reference.
7. In a similar way, copy and save the path to executable for all the services mentioned above.
8. Once the configuration path is saved then the next step is to make the website, Web API, and middleware component changes.
9. Let us begin with website, Web API and key rotation changes. These steps must be performed on the server where the website is installed. This information can be obtained from the administrator or by dropping an email to bigfixclm-prodsupport-team@hcl-software.com

6.2.1 WebAPI changes

6.2.1.1 Web. Config changes

1. Go to ApplicationBasePath of WebAPI.
2. **For example**:

   "C:\ProgramFiles\MyCloudComponents\MyCloudPortal_XXXXXXXX_XXXXXXXXX\ WebAPI"
3. Update the following keys in the web.config files:
   - **CertificateName** key value from HCl.MyCloud.Web to Web Server Private Certificate name XXXX.



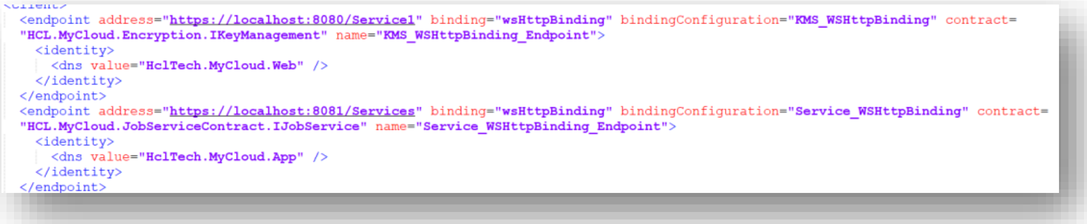
```
<add key="CertificateName" value="HclTech.MyCloud.Web" />
```

Figure 110 – Certificate Web.Config Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below

  For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Private Certificate Name of Web Server.

  For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Public Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 111 – Certificate Web.Config Certificate Name

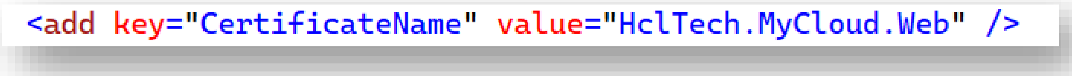
6.2.2 Key Rotation changes

6.2.2.1 Web.config changes

1. Go to ApplicationBasePath as of WebAPI.
2. For example:

   "C:\ProgramFiles\MyCloudComponents\MyCloudPortal_XXXXXXXX_XXXXXXXXX\KMS"
3. Update the following keys in the web.config files:

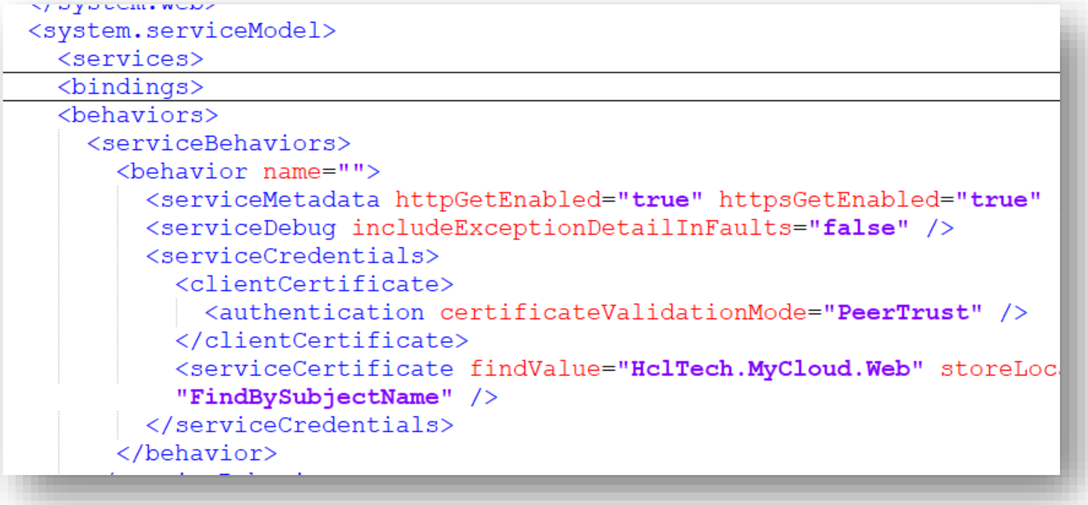
   - **CertificateName key** value from HCl.MyCloud.Web to Web Server Private Certificate name XXXX.



```
<add key="CertificateName" value="HclTech.MyCloud.Web" />
```

Figure 112 – Certificate Web.Config Certificate name (Cont.)

- Certificate Name in Behaviour of system.serviceModel, Change the HclTech.Mycloud.Web to Private Certificate Name of the App Server.



```
  </system.web>
  <system.serviceModel>
    <services>
    <bindings>
    <behaviors>
      <serviceBehaviors>
        <behavior name="">
          <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true"
          <serviceDebug includeExceptionDetailInFaults="false" />
          <serviceCredentials>
            <clientCertificate>
              <authentication certificateValidationMode="PeerTrust" />
            </clientCertificate>
            <serviceCertificate findValue="HclTech.MyCloud.Web" storeLoc
            "FindBySubjectName" />
          </serviceCredentials>
        </behavior>
```

Figure 113 – Web Config Certificate Name (Cont.)

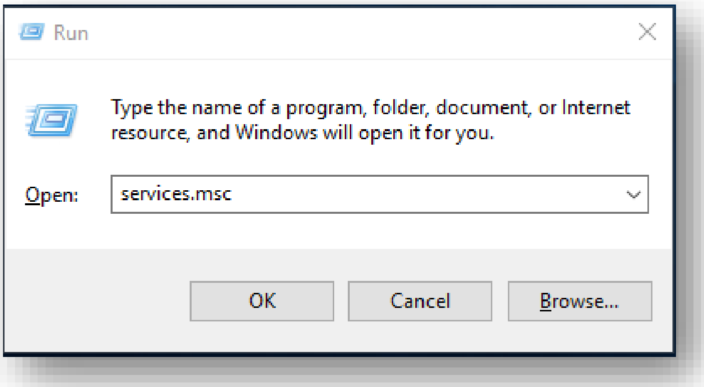
6.2.3 Middleware Component changes

Middleware components are part of App Server. Thus, we need to Update the following certificate:

- **Public Web Certificate** (.cer)
- **Private App Certificate** (.pfx)

Stop all the Services and find out the services file location. The step must be performed on the server where the middleware components have been installed. This information can be obtained from the administrator or by dropping an email to HCL BigFix CLM-Product-Supp@hcl.com.

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.

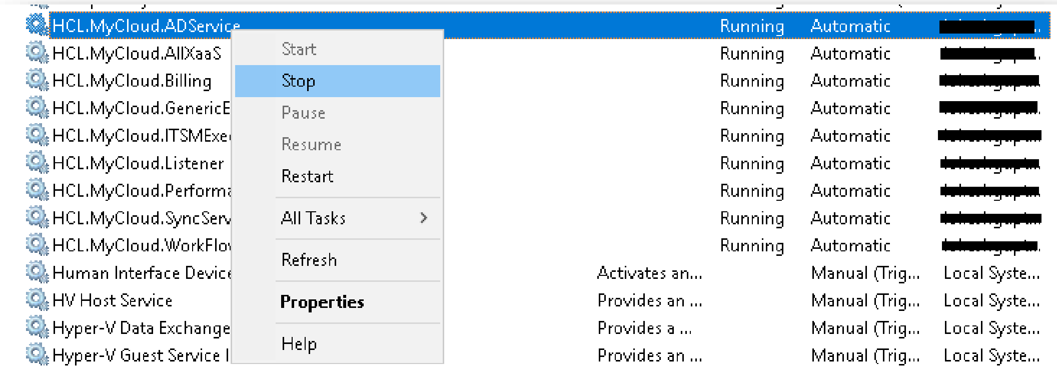


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Figure 114 – Run Command Windows

3. User will be redirected to the **Windows Service Manager**.

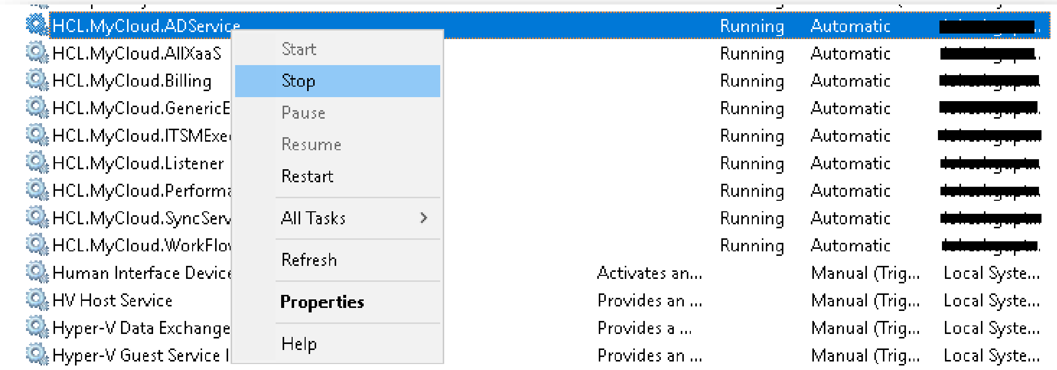


HCL.MyCloud.ADService		Running	Automatic	[redacted]
HCL.MyCloud.AllXaaS		Running	Automatic	[redacted]
HCL.MyCloud.Billing		Running	Automatic	[redacted]
HCL.MyCloud.GenericE		Running	Automatic	[redacted]
HCL.MyCloud.ITSMExe		Running	Automatic	[redacted]
HCL.MyCloud.Listener		Running	Automatic	[redacted]
HCL.MyCloud.Performa		Running	Automatic	[redacted]
HCL.MyCloud.SyncServ		Running	Automatic	[redacted]
HCL.MyCloud.WorkFlo		Running	Automatic	[redacted]
Human Interface Device	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service I	Provides an ...		Manual (Trig...	Local Syste...

Figure 115 – Windows Services Manager

4. Stop the below mentioned services. Each of these services is responsible for a component in HCL BigFix CLM. Select the service, right click on it and select Stop.

   - HCL.MyCloud.ADService
   - HCL.MyCloud.AllXaaS
   - HCL.MyCloud.Billing
   - HCL.MyCloud.GenericExecutor
   - HCL.MyCloud.ITSMExecutor
   - HCL.MyCloud.Listener
   - HCL.MyCloud.Performance
   - HCL.MyCloud.SyncService
   - HCL.MyCloud.WorkFlow
   - HCL.MyCloud.Monitor
   - HCL.MyCloud.CiscoIntersightSyncService



HCL.MyCloud.ADService		Running	Automatic	[redacted]
HCL.MyCloud.AllXaaS		Running	Automatic	[redacted]
HCL.MyCloud.Billing		Running	Automatic	[redacted]
HCL.MyCloud.GenericE		Running	Automatic	[redacted]
HCL.MyCloud.ITSMExe		Running	Automatic	[redacted]
HCL.MyCloud.Listener		Running	Automatic	[redacted]
HCL.MyCloud.Performa		Running	Automatic	[redacted]
HCL.MyCloud.SyncServ		Running	Automatic	[redacted]
HCL.MyCloud.WorkFlo		Running	Automatic	[redacted]
Human Interface Device	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service I	Provides an ...		Manual (Trig...	Local Syste...

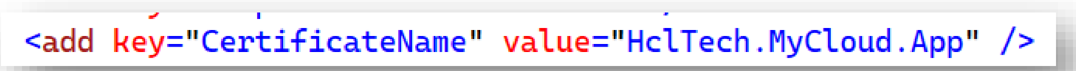
Figure 116 – Stop Services

5. After stopping all the services, perform the configuration changes in the Middleware components.

6.2.3.1 Listener Component Changes

This component is responsible for execution of HCL BigFix CLM Jobs and Interacting with different components internally and is a self-hosted WCF service that requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Listener.
2. **For example:**
   "C:\ProgramFiles\MyCloudComponents\MyCloudListener_XXXXXXXX_XXXXXXXXX\"
3. Open HCL.MyCloud.Listner.Service.Host.exe.config and change the following keys:
   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



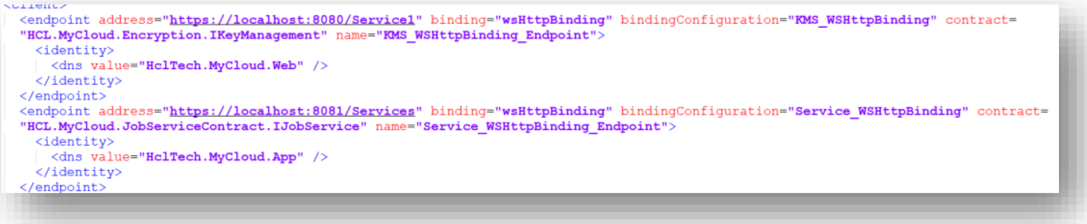
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 117 – Certificate Web.Config Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 118 – Certificate Web.Config Certificate Name

4. In Listener, we also need to add some configuration mentioned below:
   - <add key="KRSRetryCount" value="1"/>
   - <! --KRS Retry | Default Values KRSRetryCount=1 and KRSRetrySleepTime (MS) = 2000 -->
     When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

- <add key="MaxDBConnectionRetryCount" value="100"/>

  This Key defines the Max number of tries to be made to successfully establish a connection between the Listener component and database. Once the Maximum retry has been achieved and successful database connection has not been established then Listener Service will be marked as Stop. Default value of **MaxDBConnectionRetryCount** is 100 and user can change its value from the application config file of the component.

In case of an upgrade or fresh installation, the KMS URL will also be updated in the config file of the listener on the app server. The installer will first check the database to retrieve the URL and in case of no value in DB, system will set it to the default value.

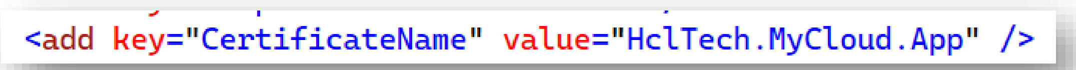
6.2.3.2 AD Changes

This component is responsible for fetching AD group user data. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.ADService.
2. **For example**:

   "C:\ProgramFiles\MyCloudComponents\ADService_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Service.AD.exe.config** and change the following keys:

   - Update *CertificateName* key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



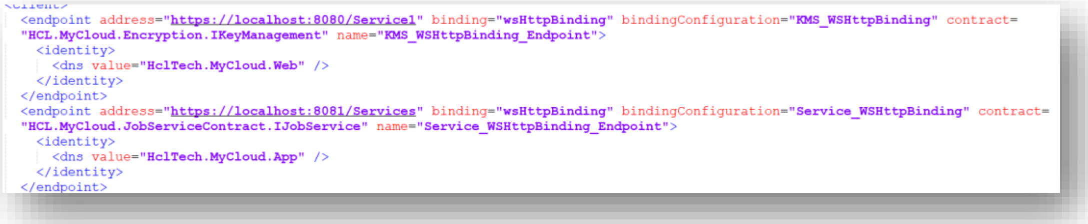
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 119 – Middleware AD Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 120 – Middleware AD Certificate Name

4. In AD Service component, we also need to add some configuration key which are mentioned below:

   - <add key="KRSRetryCount" value="1"/>

     When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

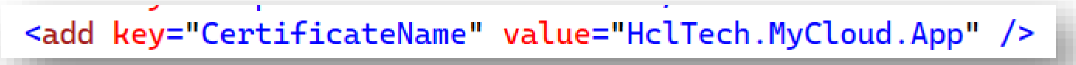
- <add key="KRSRetrySleepTime" value="2000"/>

  When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.3 Orchestrator Changes

This component is responsible for Provisioning and other Automation Tasks. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.AllXaaS.
2. **For example:**
   "C:\ProgramFiles\MyCloudComponents\Orchestrator_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.AllXaaS.Host.exe.config** and change the following keys:
   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



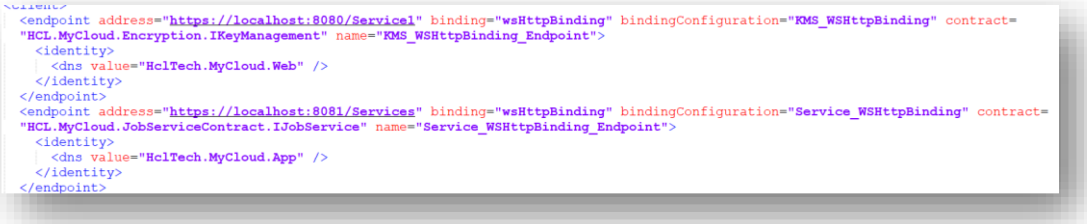
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 121 – Middleware Orchestrator Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 122 – Middleware Orchestrator Certificate Name

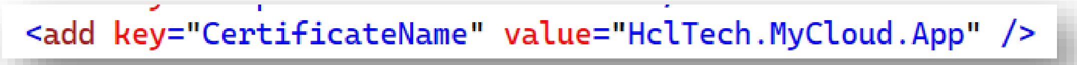
4. In Orchestrator component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
   - When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

- When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.4 WorkFlow Changes

This component is responsible for triggering HCL BigFix CLM Process workflow and notification service. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.HCL BigFix CLM.WorkFlow.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\WorkFlow_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.WorkflowEngine.exe.config** and change the following keys:
   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



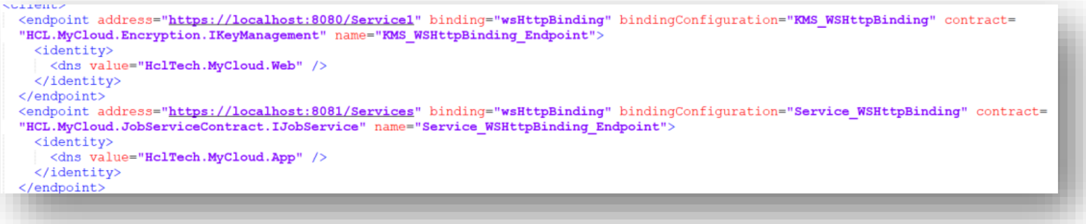
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 123 – Middleware Workflow Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "**HclTech.MyCloud.Web**" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 124 – Middleware WorkFlow Certificate Name

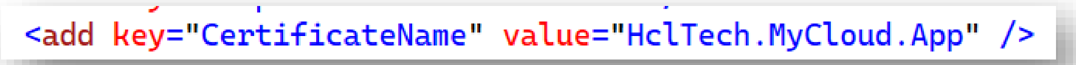
4. In Worflow component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
   - When Worflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

- When Worflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.5 SyncService Changes

This component is responsible for syncing the underlying infrastructure Cloud resources. It supports vCenter, AWS, AzureRM, SCVMM 2012. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.SyncService.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\SyncService_XXXXXXXX_XXXXXXXXX\")
3. Open **HCL.MyCloud.SyncJobService.Host.exe.config** and change the following keys:
   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



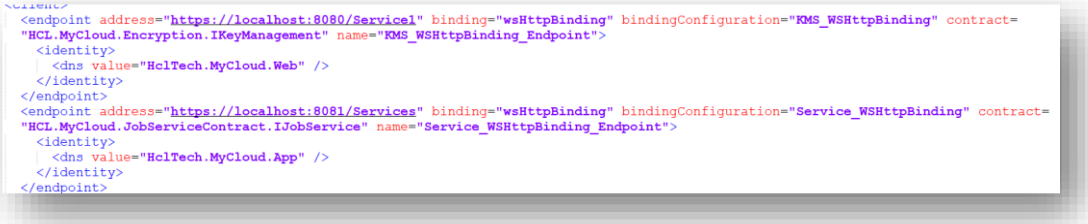
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 125 – Middleware SyncService Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 126 – Middleware SyncService Certificate Name

4. In Sync Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
   - When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

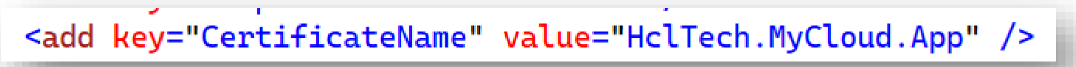
- When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.6 ITSM Executor Changes

This component is responsible for ITSM Tools Interaction. Currently this supports ServiceNow and Remedy. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.ITSMExecutor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\ITSMExecutor_XXXXXXXX_XXXXXXXXX\")
4. Open **HCL.MyCloud.Snow.Host.exe.config** and change the following keys:

   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



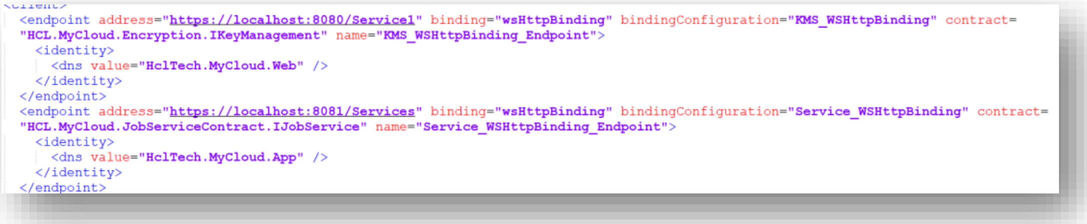
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 127 – Middleware ITSM Executor Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 128 – Middleware ITSM Executor Certificate Name

5. In ITSM Executer component, we also need to add some configuration key which are mentioned below:

   - <add key="KRSRetryCount" value="1"/>
   - When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

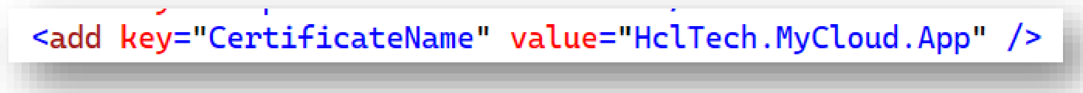
- When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.7 Billing Changes

This component is responsible for Public Cloud billing. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Billing.
2. **For example,** "C:\ProgramFiles\MyCloudComponents\Billing_XXXXXXXX_XXXXXXXXX\")
3. Open HCL.CloudBilling.DataCollector.Service.Host.exe.config and change the following keys:

- Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



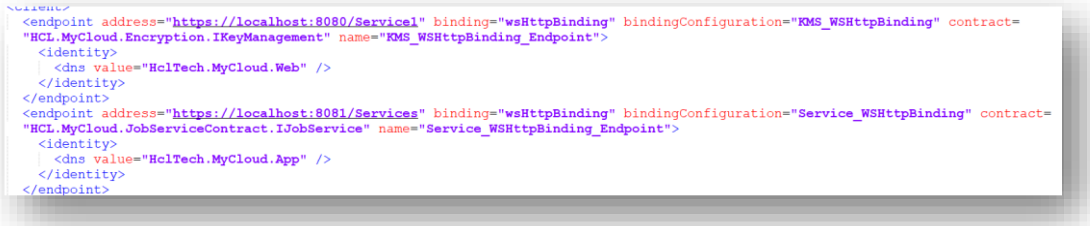
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 129 – Middleware Billing Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below

  For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

  For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 130 – Middleware Billing Certificate Name

4. In Billing component, we also need to add some configuration key which are mentioned below:

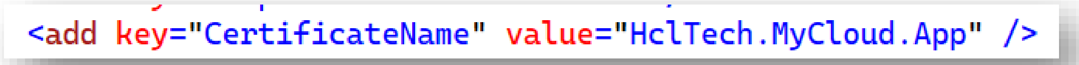
- <add key="KRSRetryCount" value="1"/>
- When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
- <add key="KRSRetrySleepTime" value="2000"/>

- When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.8 Generic Service Changes

This component is responsible for Private Cloud billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.GenericExecutor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\GenericService_XXXXXXXX_XXXXXXXXX\")
4. Open **HCL.MyCloud.Generic.Host.exe.config** and change the following keys:
    - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



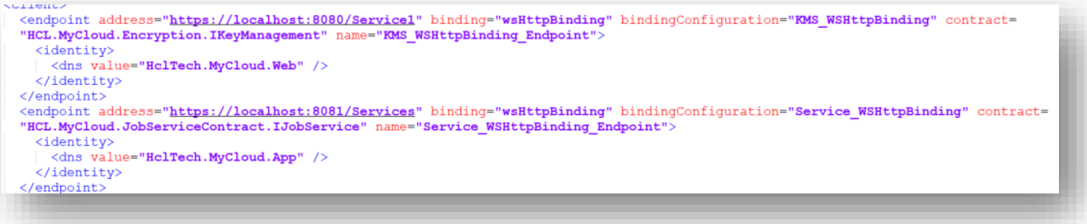
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 131 – Middleware Generic Service Certificate Name

    - Update DNS Certificate name in System.serviceModel.clients as mentioned below

      For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

      For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 132 – Middleware Generic service Certificate Name

5. In Generic Service component, we also need to add some configuration key which are mentioned below:
    - <add key="KRSRetryCount" value="1"/>
      When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
    - <add key="KRSRetrySleepTime" value="2000"/>

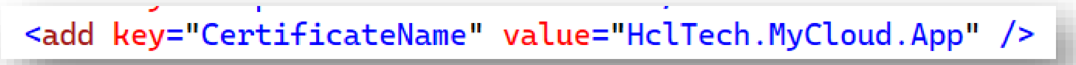
When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.9 Health Monitor Changes

This component is responsible for monitoring the health of HCL BigFix CLM Components. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.HCL BigFix CLM.Monitor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\HealthMonitor_XXXXXXXX_XXXXXXXXX\"
4. Open **HCL.MyCloud.Monitor.Host.exe.config** and change the following keys:

- Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



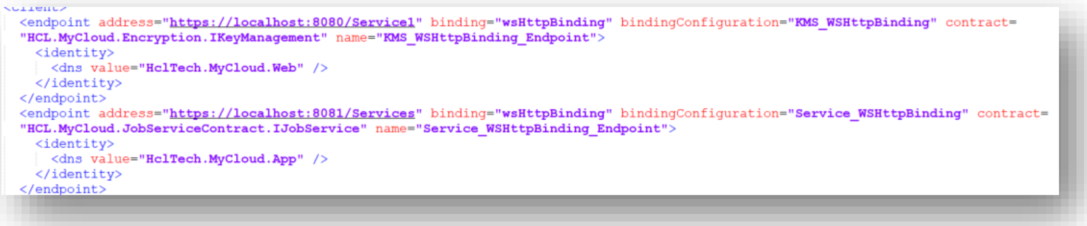
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 133 – Middleware Monitor Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below

  For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

  For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 134 – Middleware Monitor Certificate Name

5. In Health Monitor component, we also need to add some configuration key which are mentioned below:

- <add key="KRSRetryCount" value="1"/>

  When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

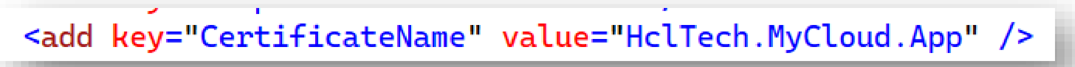
- <add key="KRSRetrySleepTime" value="2000"/>

When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.10 Performance Changes

This component is responsible for Metering and Public Cloud Advisory Data Collection. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.Performance.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\Performance_XXXXXXXX_XXXXXXXXX\"
3. Open HCL.CloudPerformance.DataCollector.Service.Host.exe.config and change the following keys:
   - Update ***CertificateName*** key value from HclTech.MyCloud.Web to **Private Certificate of APP Server**XXXX.



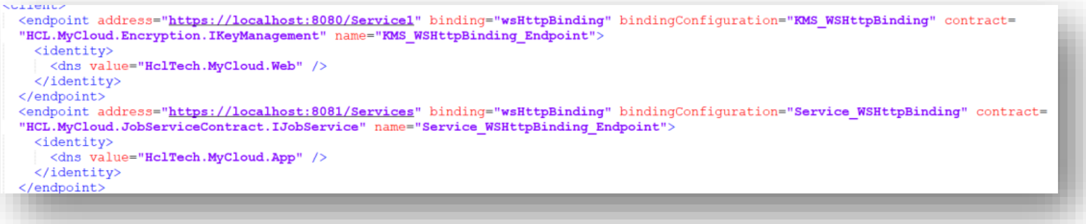
```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 135 – Middleware Performance Certificate Name

   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 136 – Middleware Performance Certificate Name

4. In Performance component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>

     When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

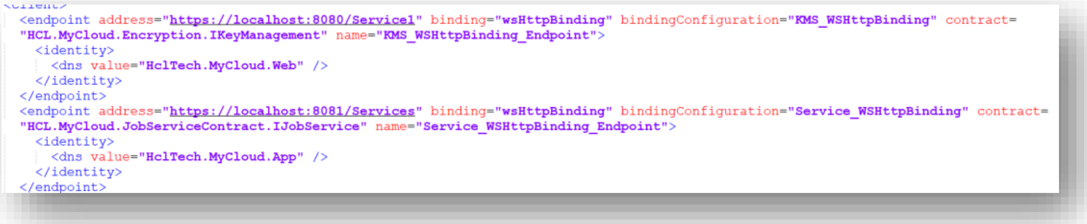
6.2.3.11 Cisco Intersight Sync Service Changes

This component is responsible to sync organizations, Operating System Files, Physical Summary, Profile Templates, SCUtility Distributable, Server Profile, Device Registration, Organization, Array, Host, Host Group, Host Lun, Volume, Targets, Virtualization (Cluster, Cluster Storage, Data Store, Data Center, Distributed Network, Distributed Switch, Folder, Host, Instance, Resource Group, Template, VCenter), Workflow. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.HCL BigFix CLM.
2. For example:
   - Update DNS Certificate name in System.serviceModel.clients as mentioned below

     For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

     For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Private Certificate Name of App Server.



```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
  "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
  "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
```

Figure 137 – Middleware Cisco Intersight Certificate Name

3. In Cisco Intersight Sync Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>

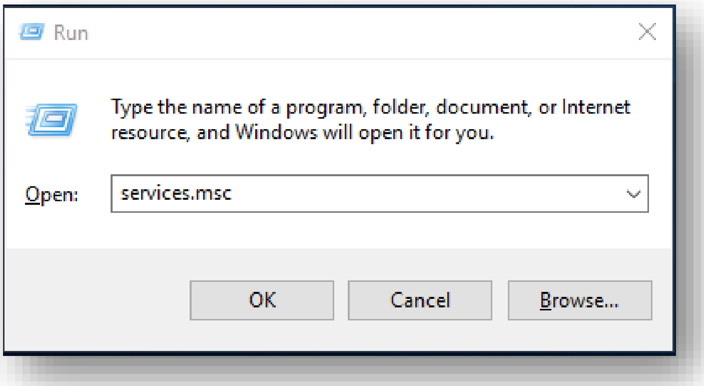
     When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of KRSRetryCount is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

     When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of KRSRetrySleepTime is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.3.12 Start all the Services

Once the changes are made, each of these services must be started again. Follow the steps mentioned below to do that:

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
services.msc
OK
Cancel
Browse...

Figure 138 – Run Command Windows

3. Start the below mentioned services: (Select the service, right-click on it, and select **Start**.)
   - HCL.MyCloud.ADService
   - HCL.MyCloud.AllXaaS
   - HCL.MyCloud.Billing
   - HCL.MyCloud.GenericExecutor
   - HCL.MyCloud.ITSMExecutor
   - HCL.MyCloud.Performance
   - HCL.MyCloud.SyncService
   - HCL.MyCloud.Listener
   - HCL.MyCloud.Monitor
   - HCL.MyCloud.CiscoIntersightSyncService

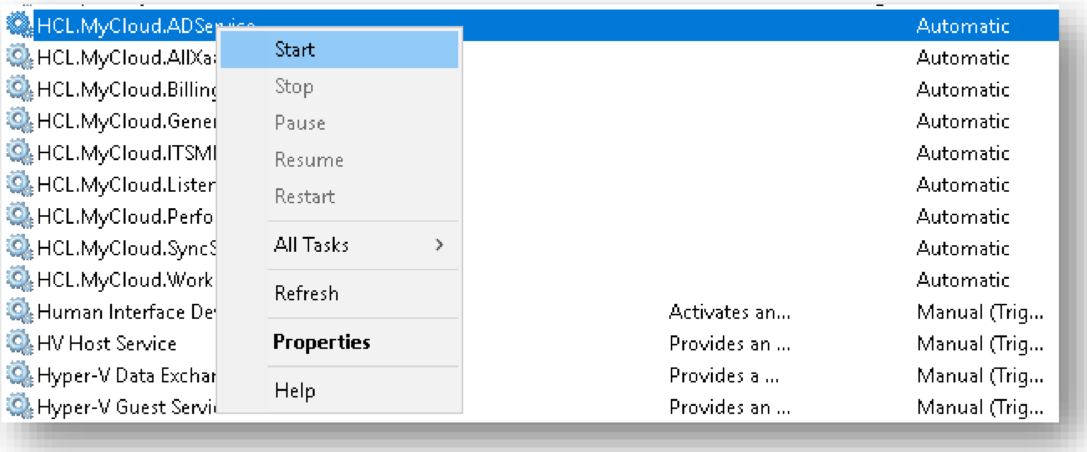
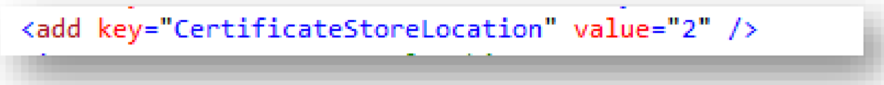


Figure 139 – Start Services

If the certificate location is changed, then repeat all the steps, and change the below-mentioned properties accordingly:

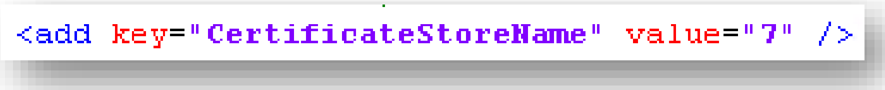
- ***CertificateStoreLocation*** key value from "2" to one of the following options:
  - 1 for CurrentUser
  - 2 for LocalMachine



```
<add key="CertificateStoreLocation" value="2" />
```

Figure 140 – Middleware Certificate Store Location

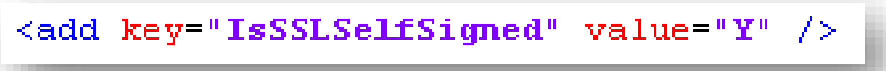
- ***CertificateStoreName*** key value from "7" to one of the following options:
  - 1 for AddressBook
  - 2 for AuthRoot
  - 3 for CertificateAuthority
  - 4 for Disallowed
  - 5 for My
  - 6 for Root
  - 7 for TrustedPeople
  - 8 for TrustedPublisher



```
<add key="CertificateStoreName" value="7" />
```

Figure 141 – Middleware Certificate Store Location (Cont.)

- ***IsSSLSelfSigned*** key value from "N" to "Y"



```
<add key="IsSSLSelfSigned" value="Y" />
```

Figure 142 – Middleware Start Service IsSSLSelfSigned

Once all the configuration is done in all the components, HCL BigFix CLM components will start using the custom Certificate configuration.

6.3 Load Balancer Configuration (Optional)

If High Availability is required for HCL BigFix CLM, then the website must be configured with the Load Balancer.

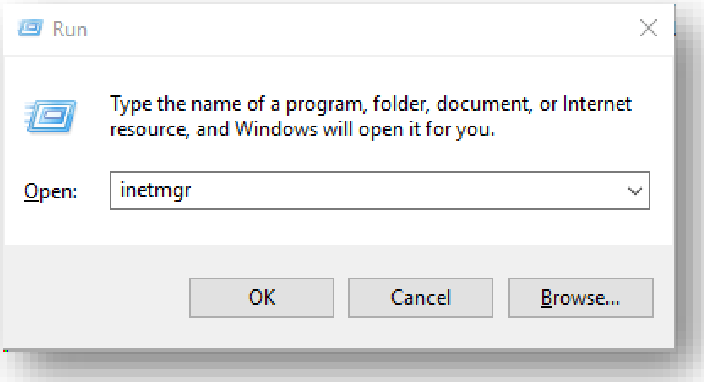
Sticky session must be enabled in the case of Load Balancer.

Follow the steps mentioned below to do that.

1. Find Website, WebAPI and Key Rotation Service ApplicationBasePath.
2. Press **Window + R** keys to open RUN command window.

a. Now type inetmgr and click OK.

b. The IIS Console will open.



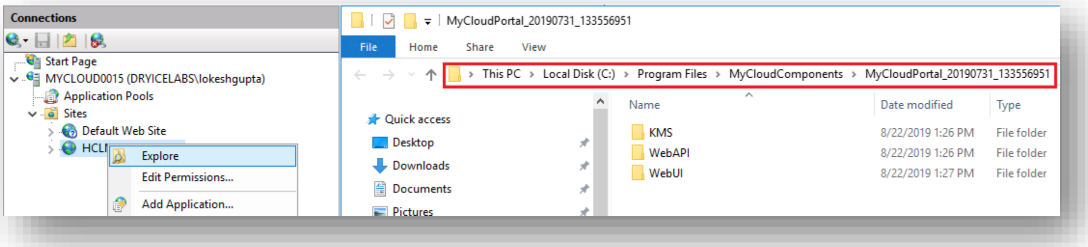
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: inetmgr

Figure 143 – Run Command Window

c. Now expand the Server Name node → Sites node using the Connections section. Right-click on the HCL BigFix CLMPortal Node and click on Explore.

d. This will locate the ApplicationBasePath for Website and Web API as highlighted in below Figure 144 - ApplicationBasePath Locator.



This PC › Local Disk (C:) › Program Files › MyCloudComponents › MyCloudPortal_20190731_133556951

Name	Date modified	Type
KMS	8/22/2019 1:26 PM	File folder
WebAPI	8/22/2019 1:26 PM	File folder
WebUI	8/22/2019 1:27 PM	File folder

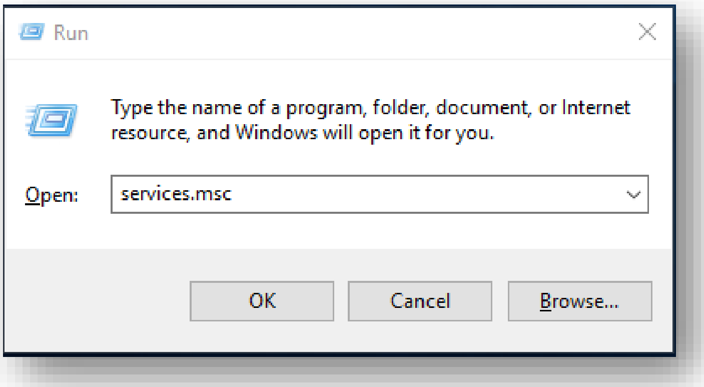
Figure 144 – ApplicationBasePath Locator

3. Copy the base path and save for future reference.

4. The next step is to find the path of the Middleware component configuration files. The steps are mentioned below:

5. Find the PathToExecutable of HCL.MyCloud.Listener service.

    a. Press **Window + R** keys to open RUN window, then type services.msc and click OK.



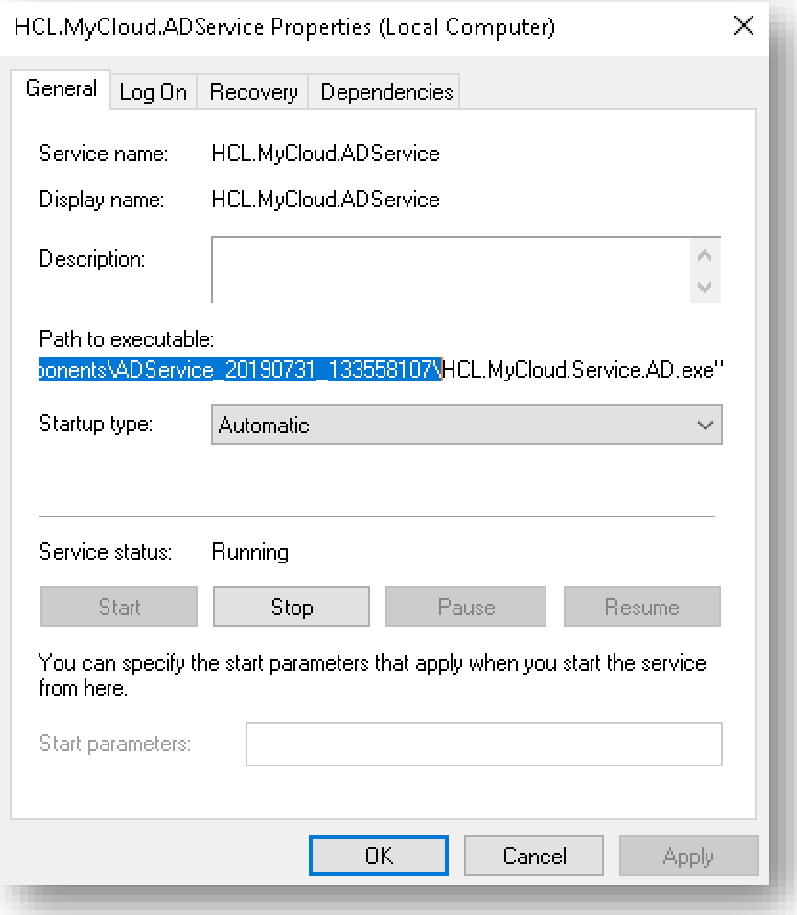
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

services.msc

Figure 145 – Run Command Window

b. For the below mentioned services: (Select the service, right-click to select Properties and save the highlighted Path to executable as shown in the following screenshot).

- HCL.MyCloud.ADService
- HCL.MyCloud.AllXaaS
- HCL.MyCloud.Billing
- HCL.MyCloud.GenericExecutor
- HCL.MyCloud.ITSMExecutor
- HCL.MyCloud.Listener
- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.WorkFlow
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService



HCL.MyCloud.ADService Properties (Local Computer)

Service name: HCL.MyCloud.ADService

Display name: HCL.MyCloud.ADService

Description:

Path to executable:
ponents\ADService_20190731_133558107\HCL.MyCloud.Service.AD.exe"

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 146 – AD Service Properties

c. Copy the string as highlighted in Figure 109 – Service Properties Window and save it in a notepad or a document for future reference.

d. Also, copy and save the path to executable for all the services mentioned above.

6. Once the configuration path is saved then the next step is to make the website, Web API and middleware component changes.

7. Let us begin with website and Web API. These steps must be performed on the server where the website has been installed. This information can be obtained from the administrator who has run the installer or by dropping an email to bigfixclm-prodsupport-team@hcl-software.com

6.3.1 Web API changes

6.3.1.1 Web. Config changes

1. Go to the ApplicationBase Path of WebUI.

2. For example:

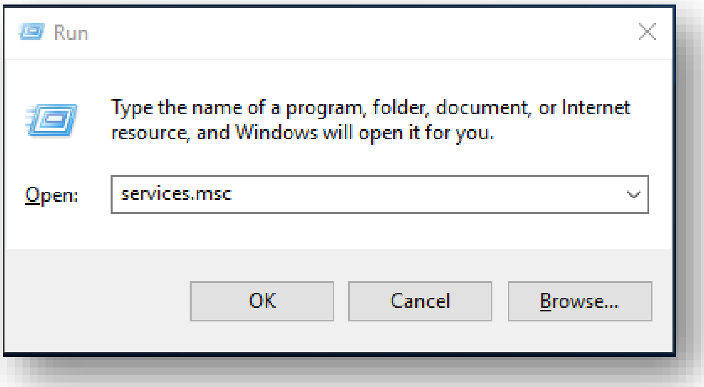
C:\Program Files\MyCloudComponents\MyCloudPortal_XXXXXXX_XXXXXXXX\WebUI

Update LB URL in appsetting.json as mentioned below

For WebapiConnectivity - Change the "SelfSignedCertificate " value under WebApi> SelfSignedCertificate > to "Y"
And BaseUrl will be WebApi> BaseUrl> https://XX.X.XXX.XXX/webapi/

6.3.2 Middleware Component changes

1. Stop all the Services and find the services file location where they have been installed by default. This step must be performed on the server where the middleware components have been installed. This information can be obtained from the administrator or by dropping an email to bigfixclm-prodsupport-team@hcl-software.com
2. Press **Window + R** keys to open the **RUN** window.
3. Type **services.msc** and click **OK**.

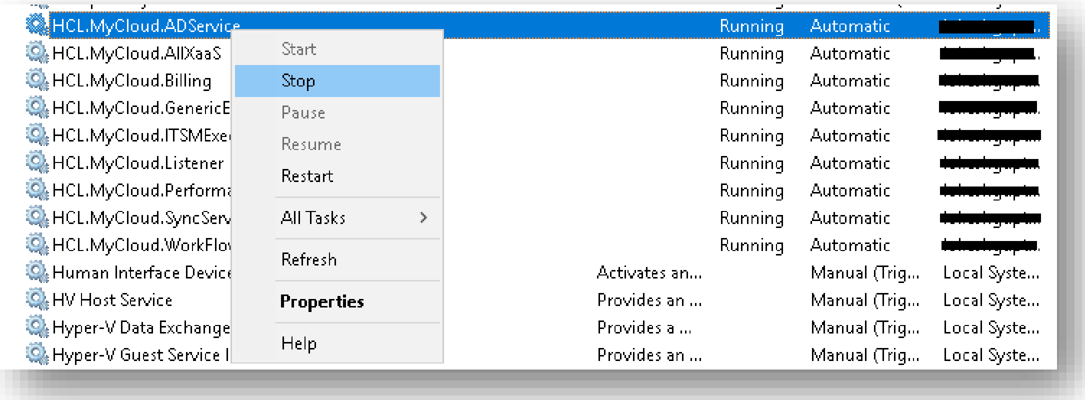


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Figure 147 – Run Command Window

4. User will be redirected to the **Windows Service Manager.**

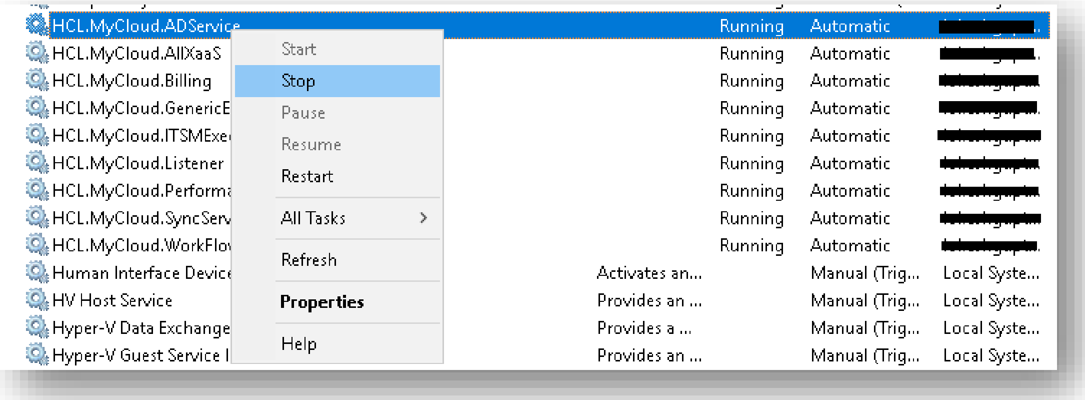


HCL.MyCloud.ADService		Running	Automatic	[redacted]
HCL.MyCloud.AllXaaS		Running	Automatic	[redacted]
HCL.MyCloud.Billing		Running	Automatic	[redacted]
HCL.MyCloud.GenericE		Running	Automatic	[redacted]
HCL.MyCloud.ITSMExe		Running	Automatic	[redacted]
HCL.MyCloud.Listener		Running	Automatic	[redacted]
HCL.MyCloud.Performa		Running	Automatic	[redacted]
HCL.MyCloud.SyncServ		Running	Automatic	[redacted]
HCL.MyCloud.WorkFlov		Running	Automatic	[redacted]
Human Interface Device	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service I	Provides an ...		Manual (Trig...	Local Syste...

Figure 148 – Windows Service Manager

5. Stop the below mentioned services: (Select the service, **right click** on it, and select **Stop**)
   - HCL.MyCloud.ADService
   - HCL.MyCloud.AllXaaS
   - HCL.MyCloud.Billing
   - HCL.MyCloud.GenericExecutor
   - HCL.MyCloud.ITSMExecutor
   - HCL.MyCloud.Listener

- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.WorkFlow
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService



HCL.MyCloud.ADService		Running	Automatic	[redacted]
HCL.MyCloud.AllXaaS		Running	Automatic	[redacted]
HCL.MyCloud.Billing		Running	Automatic	[redacted]
HCL.MyCloud.GenericE		Running	Automatic	[redacted]
HCL.MyCloud.ITSMExe		Running	Automatic	[redacted]
HCL.MyCloud.Listener		Running	Automatic	[redacted]
HCL.MyCloud.Performa		Running	Automatic	[redacted]
HCL.MyCloud.SyncServ		Running	Automatic	[redacted]
HCL.MyCloud.WorkFlo		Running	Automatic	[redacted]
Human Interface Device	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service I	Provides an ...		Manual (Trig...	Local Syste...

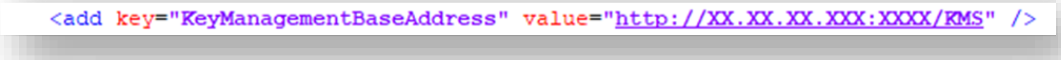
Figure 149 – Stop Below Service

6. Once a user has stopped all the services, perform the configuration changes in the Middleware components.

6.3.2.1 Listener Component Changes

This Component is responsible for execution of HCL BigFix CLM Jobs and Interacting with different components internally. This is a window service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Listener.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\MyCloudListener_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Listner.Service.Host.exe.config** and change the following keys:
   - Update *KeyManagementBaseAddress* key value from http://<ip>:<port>/KMS or https://<ip>:<port>/KMS to http://<LBIP>:<port>/KMS or https://<LBIP>:<port>/KMS



```
<add key="KeyManagementBaseAddress" value="http://XX.XX.XX.XXX:XXXX/KMS" />
```

Figure 150 – Load Balancer Listener Key Management Base Address

4. In Listener, we also need to add some configuration key which are mentioned below:
   - <! --KRS Retry | Default Values KRSRetryCount=1 and KRSRetrySleepTime (MS) = 2000 -->
   - <add key="KRSRetryCount" value="1"/>
   - When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string

from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- <add key="KRSRetrySleepTime" value="2000"/>

  When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.
- <add key="MaxDBConnectionRetryCount" value="100"/>

  This Key defines the Max number of tries to be made to successfully establish a connection between the Listener component and database. Once the Maximum retry has been achieved and successful database connection has not been established then Listener Service will be marked as Stop. Default value of **MaxDBConnectionRetryCount** is 100 and user can change its value from the application config file of the component.

In case of an upgrade or fresh installation, the KMS URL will also be updated in the config file of the listener on the app server. The installer will first check the database to retrieve the URL and in case of no value in DB, the system will set it to the default value.

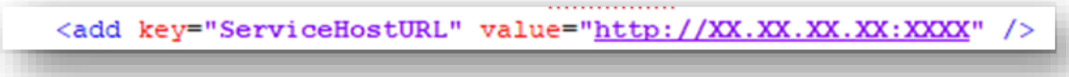
6.3.2.2 AD Changes

This component is responsible for fetching AD group user data. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.ADService.
2. **For example,**

   "C:\Program Files\MyCloudComponents\ADService_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Service.AD.exe.config** and change the following keys:

   - **ServiceHostURL** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 151 – Load Balancer AD Service Host

4. In AD Service component, we also need to add some configuration key which are mentioned below:

   - <add key="KRSRetryCount" value="1"/>

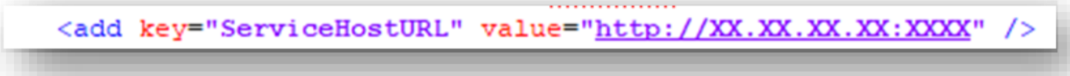
     When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

     When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.3 Orchestrator Changes

This component is responsible for Provisioning and other Automation Tasks. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.AllXaaS.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\Orchestrator_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.AllXaaS.Host.exe.config** and change the following keys:
   - ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

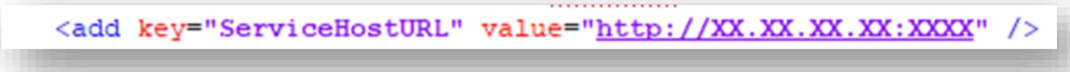
Figure 152 – Load Balancer Orchestrator Service Host URL

4. In Orchestrator Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
     When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.4 WorkFlow Changes

This component is responsible for triggering HCL BigFix CLM Process workflow and notification service. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.WorkFlow.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\WorkFlow_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud**.**WorkflowEngine.exe.config** and change the following keys:
   - Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

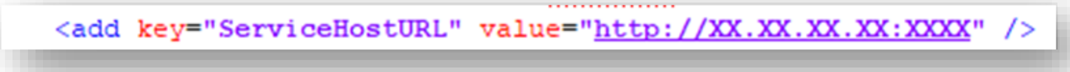
Figure 153 – Load Balancer Workflow Service Host URL

4. In Workflow Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
     When Workflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When Workflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.5 SyncService Changes

This component is responsible for syncing the underlying infrastructure Cloud resources. It supports vCenter, AWS, AzureRM, SCVMM 2012. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.SyncService.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\SyncService_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.SyncJobService.Host.exe.config** and change the following keys:
   - Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 154 – Load Balancer SyncService Service Host URL

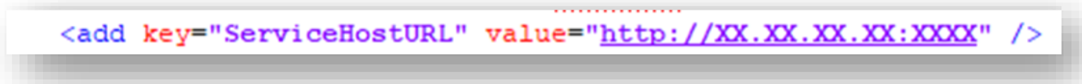
4. In Sync Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
     When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.6 ITSM Executor Changes

This component is responsible for ITSM Tools Interaction. Currently this supports ServiceNow and Remedy. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.ITSMExecutor.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\ITSMExecutor_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Snow.Host.exe.config** and change the following keys:
   - Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 155 – Load Balancer ITSM Executor Service Host URL

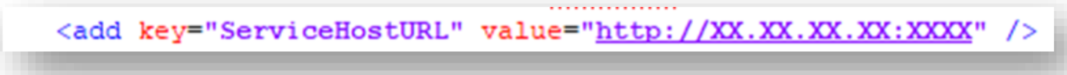
4. In ITSM Executer component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
     When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.7 Billing Changes

This component is responsible for Public Cloud billing. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Billing.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\Billing_XXXXXXXX_XXXXXXXXX\"
3. Open HCL.CloudBilling.DataCollector.Service.Host.exe.config and change the following keys:

- Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 156 – Load Balancer Billing Service Host URL

4. In Billing component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>

     When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>

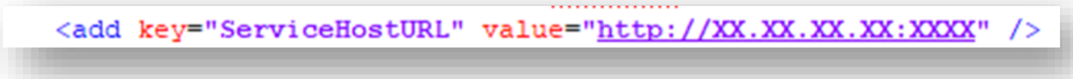
     When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.8 GenericService Changes

This component is responsible for Private Cloud billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service. This component requires HCL BigFix CLM database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.GenericExecutor.
2. **For example**:

   "C:\ProgramFiles\MyCloudComponents\GenericService_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Generic.Host.exe.config** and change the following keys:
   - Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 157 – Load Balancer GenericService Service Host URL

4. In Generic Service component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>

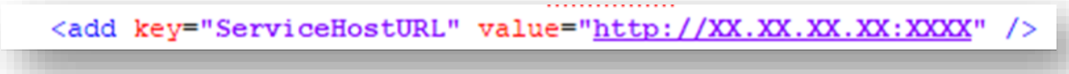
     When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- <add key="KRSRetrySleepTime" value="2000"/>
  When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.9 HealthMonitor Changes

This component is responsible for Monitoring the health of HCL BigFix CLM Components. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.Monitor.
2. **For example**:
   "C:\ProgramFiles\MyCloudComponents\HealthMonitor_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.Monitor.Host.exe.config** and change the following keys:
   - Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 158 – Load Balancer Performance Service Host URL

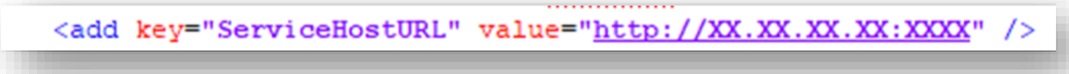
4. In Health Monitor component, we also need to add some configuration key which are mentioned below:
   - <add key="KRSRetryCount" value="1"/>
     When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.10 Performance Changes

This component is responsible for Metering and Public Cloud Advisory Data Collection. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.Performance.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\Performance_XXXXXXXX_XXXXXXXXX\"
3. Open HCL.CloudPerformance.DataCollector.Service.Host.exe.config and change the following keys:

- Update ***ServiceHostURL*** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 159 – Load Balancer Performance Service Host URL

4. In Performance component, we also need to add some configuration key which are mentioned below:

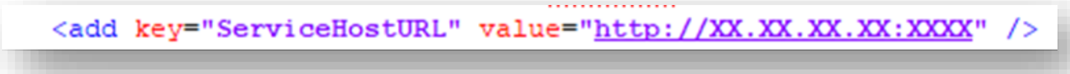
   - <add key="KRSRetryCount" value="1"/>
     When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
   - <add key="KRSRetrySleepTime" value="2000"/>
     When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.11 Cisco Intersight Sync Service Changes

This component is responsible to sync organizations, Operating System Files, Physical Summary, Profile Templates, SCUtility Distributable, Server Profile, Device Registration, Organization, Array, Host, Host Group, Host Lun, Volume, Targets, Virtualization (Cluster, Cluster Storage, Data Store, Data Center, Distributed Network, Distributed Switch, Folder, Host, Instance, Resource Group, Template, VCenter), Workflow. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.CiscoIntersightSyncService.
2. **For example,**
   "C:\ProgramFiles\MyCloudComponents\CiscoIntersightSyncService _XXXXXXXX_XXXXXXXXX\"
3. Open HCL.MyCloud.CiscoIntersightSyncService.Host.exe.config and change the following keys:

   - Update ServiceHostURL key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<portxxxxxxxxx>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 160 – Load Balancer Cisco Intersight Sync Service Host URL

4. In Cisco Intersight Sync Service component, we also need to add some configuration key which are mentioned below:

   - <add key="KRSRetryCount" value="1"/>

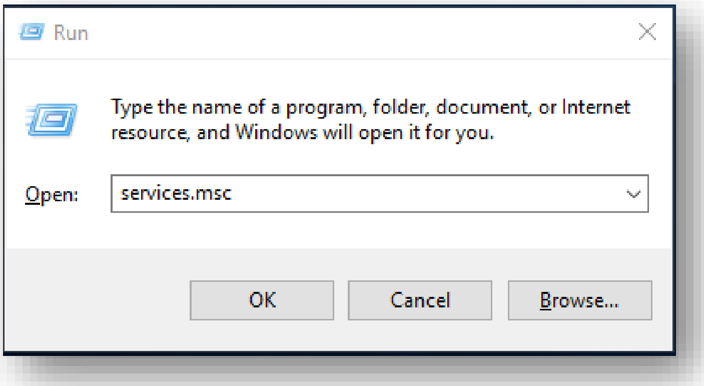
When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of KRSRetryCount is 1 and user can change its value from the application config file of the component.

- <add key="KRSRetrySleepTime" value="2000"/>
  When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of KRSRetrySleepTime is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.2.12 Start All the Services

Once the changes are made, each of these services needs to be restarted. Follow the steps mentioned below to do that:

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.

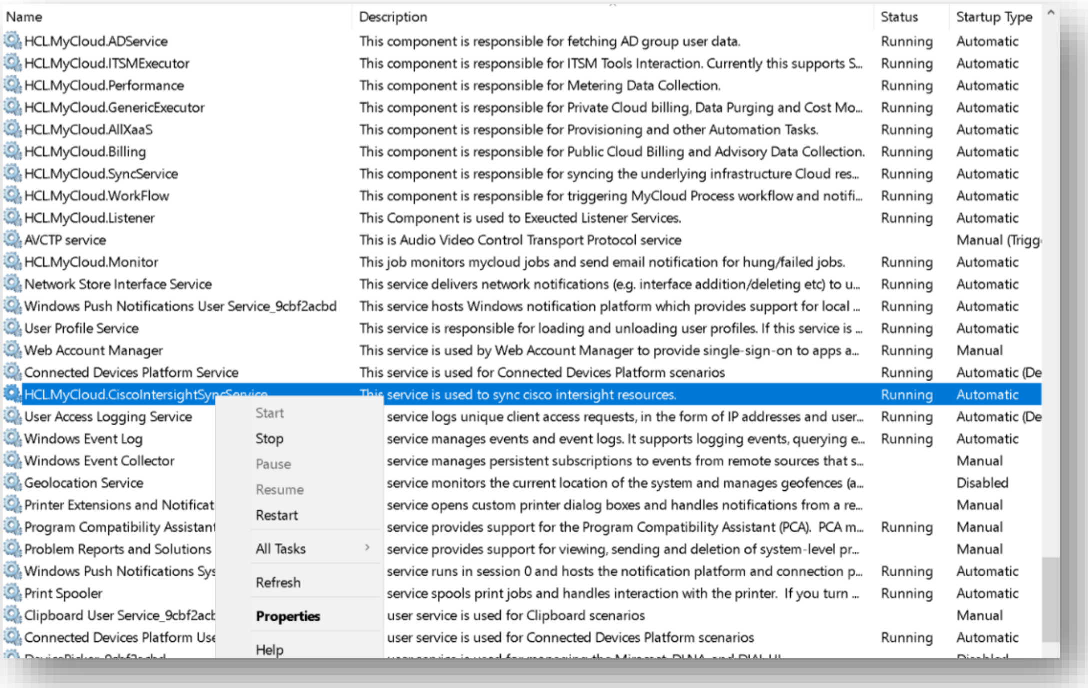


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Figure 161 – Run Command Window

3. Start the below mentioned services: (Select the service, right-click on it, and select Start)
   - HCL.MyCloud.ADService
   - HCL.MyCloud.AllXaaS
   - HCL.MyCloud.Billing
   - HCL.MyCloud.GenericExecutor
   - HCL.MyCloud.ITSMExecutor
   - HCL.MyCloud.Performance
   - HCL.MyCloud.SyncService
   - HCL.MyCloud.Listener
   - HCL.MyCloud.Monitor
   - HCL.MyCloud.CiscoIntersightSyncService



Name	Description	Status	Startup Type
HCLMyCloud.ADService	This component is responsible for fetching AD group user data.	Running	Automatic
HCLMyCloud.ITSMExecutor	This component is responsible for ITSM Tools Interaction. Currently this supports S...	Running	Automatic
HCLMyCloud.Performance	This component is responsible for Metering Data Collection.	Running	Automatic
HCLMyCloud.GenericExecutor	This component is responsible for Private Cloud billing, Data Purging and Cost Mo...	Running	Automatic
HCLMyCloud.AllXaaS	This component is responsible for Provisioning and other Automation Tasks.	Running	Automatic
HCLMyCloud.Billing	This component is responsible for Public Cloud Billing and Advisory Data Collection.	Running	Automatic
HCLMyCloud.SyncService	This component is responsible for syncing the underlying infrastructure Cloud res...	Running	Automatic
HCLMyCloud.WorkFlow	This component is responsible for triggering MyCloud Process workflow and notifi...	Running	Automatic
HCLMyCloud.Listener	This Component is used to Exeucted Listener Services.	Running	Automatic
AVCTP service	This is Audio Video Control Transport Protocol service		Manual (Trigg
HCLMyCloud.Monitor	This job monitors mycloud jobs and send email notification for hung/failed jobs.	Running	Automatic
Network Store Interface Service	This service delivers network notifications (e.g. interface addition/deleting etc) to u...	Running	Automatic
Windows Push Notifications User Service_9cbf2acbd	This service hosts Windows notification platform which provides support for local ...	Running	Automatic
User Profile Service	This service is responsible for loading and unloading user profiles. If this service is ...	Running	Automatic
Web Account Manager	This service is used by Web Account Manager to provide single-sign-on to apps a...	Running	Manual
Connected Devices Platform Service	This service is used for Connected Devices Platform scenarios	Running	Automatic (De
HCLMyCloud.CiscoIntersightSyncService	This service is used to sync cisco intersight resources.	Running	Automatic
User Access Logging Service	service logs unique client access requests, in the form of IP addresses and user...	Running	Automatic (De
Windows Event Log	service manages events and event logs. It supports logging events, querying e...	Running	Automatic
Windows Event Collector	service manages persistent subscriptions to events from remote sources that s...		Manual
Geolocation Service	service monitors the current location of the system and manages geofences (a...		Disabled
Printer Extensions and Notificat	service opens custom printer dialog boxes and handles notifications from a re...		Manual
Program Compatibility Assistant	service provides support for the Program Compatibility Assistant (PCA). PCA m...	Running	Manual
Problem Reports and Solutions	service provides support for viewing, sending and deletion of system-level pr...		Manual
Windows Push Notifications Sys	service runs in session 0 and hosts the notification platform and connection p...	Running	Automatic
Print Spooler	service spools print jobs and handles interaction with the printer. If you turn ...	Running	Automatic
Clipboard User Service_9cbf2acb	user service is used for Clipboard scenarios		Manual
Connected Devices Platform Use	user service is used for Connected Devices Platform scenarios	Running	Automatic

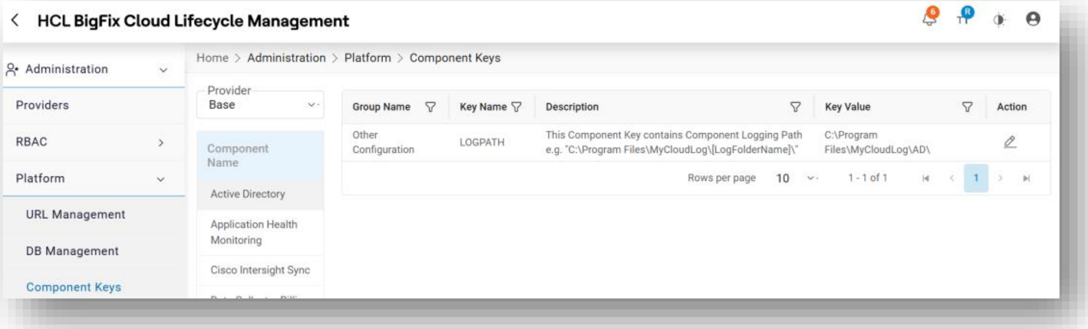
Figure 162 – Start Services

6.3.3 Master Data changes

These changes can be made after the user logs into HCL BigFix CLM portal. In order to do that, the user must have the admin credentials. If user doesn't have the credentials, please contact HCL BigFix CLM Admin or drop an email to bigfixclm-prodsupport-team@hcl-software.com.

After login, the user will be redirected to the landing page as shown in Figure 163 – Landing Page. To make the changes, the user needs to follow the following steps:

1. **Go to Administration -> Platform →** Components Keys.



HCL BigFix Cloud Lifecycle Management
Administration
Providers
RBAC
Platform
URL Management
DB Management
Component Keys
Home > Administration > Platform > Component Keys
Active Directory
Application Health Monitoring
Cisco Intersight Sync

Provider: Base

Component Name

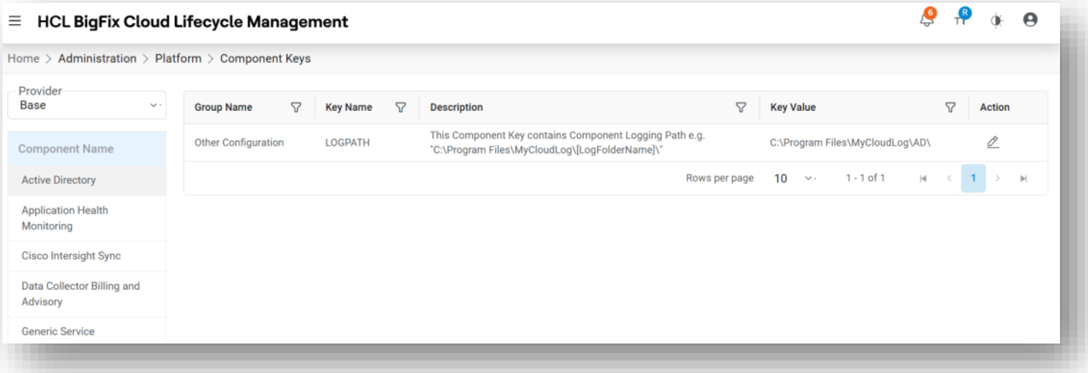
Group Name	Key Name	Description	Key Value	Action
Other Configuration	LOGPATH	This Component Key contains Component Logging Path e.g. "C:\Program Files\MyCloudLog\[LogFolderName]\"	C:\Program Files\MyCloudLog\AD\	

Rows per page 10 1 - 1 of 1

Figure 163 – Landing Page

2. User will be redirected to the **Component Keys** page.
3. Select **Website Service** (WEBSITE) in the **Component Name** dropdown and click on **Go** button.
4. Change the Key value for the following Key Name(s):

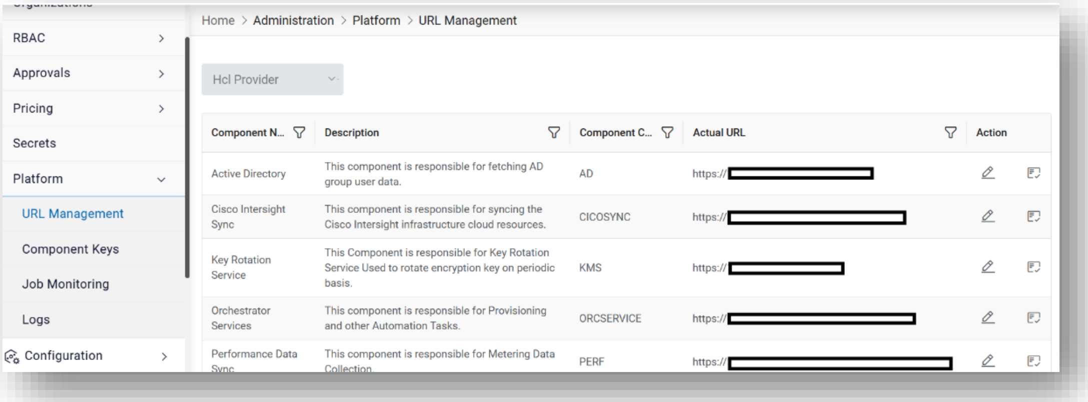
- **JsURL** from http://<ip>:<port>/WebUI/JS to https://<LBIP>:<port>/WebUI/JS
- **SiteURL** from http://<ip>:<port>/WebUI to https://<LBIP>:<port>/WebUI


HCL BigFix Cloud Lifecycle Management
6
R
Home > Administration > Platform > Component Keys
Provider
Base
Component Name
Active Directory
Application Health Monitoring
Cisco Intersight Sync
Data Collector Billing and Advisory
Generic Service
Rows per page
10
1 - 1 of 1
1

Group Name	Key Name	Description	Key Value	Action
Other Configuration	LOGPATH	This Component Key contains Component Logging Path e.g. "C:\Program Files\MyCloudLog\[LogFolderName]\"	C:\Program Files\MyCloudLog\AD\	

Figure 164 – Manage base Components

5. Go to **Administration > Platform** and then click **Component Keys**.

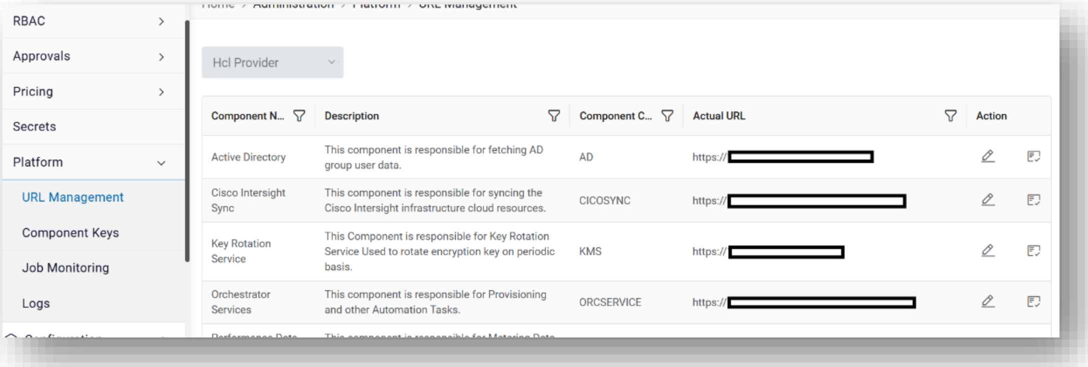


Component N...	Description	Component C...	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	
Cisco Intersight Sync	This component is responsible for syncing the Cisco Intersight infrastructure cloud resources.	CICOSYNC	https://[redacted]	
Key Rotation Service	This Component is responsible for Key Rotation Service Used to rotate encryption key on periodic basis.	KMS	https://[redacted]	
Orchestrator Services	This component is responsible for Provisioning and other Automation Tasks.	ORCSERVICE	https://[redacted]	
Performance Data Sync	This component is responsible for Metering Data Collection.	PERF	https://[redacted]	

Figure 165 – Landing Page with selected URL Configuration

6. Select **Base** in the **Provider** dropdown and click on **Go** button.
7. Change the **URL** for the following Component Name(s):
   - **Workflow Service** from http://<ip>:<port>/WorkflowService to https://<LBIP>:<port>/WorkflowService
   - **Data Collector Billing and Advisory** from http://<ip>:<port>/DataCollector to https://<LBIP>:<port>/DataCollector
   - **ServiceNow Executer** from http://<ip>:<port>/SnowService to https://<LBIP>:<port>/SnowService
   - **Generic Service** from http://<ip>:<port>/GenericService to https://<LBIP>:<port>/GenericService
8. Select {**Provider**} in the **Provider** dropdown and click on **Go** button.
9. Change the URL for the following Component Name(s):
   - **Platform Data Sync** from http://<ip>:<port>/SyncService to https://<LBIP>:<port>/SyncService
   - **Performance Data Sync** from http://<ip>:<port>/PerformanceDataCollector to https://<LBIP>:<port>/PerformanceDataCollector

- **Orchestrator Services** from http://<ip>:<port>/OrchestratorService to https://<LBIP>:<port>/OrchestratorService
- **Active Directory** from http://<ip>:<port>/ADService xxxxxx
- **Cisco Intersight Sync** from http://<ip>:<port>/CiscoSyncService xxxxxxx https://<LBIP>:<port>/CiscoSyncService



Component N...	Description	Component C...	Actual URL	Action
Active Directory	This component is responsible for fetching AD group user data.	AD	https://[redacted]	
Cisco Intersight Sync	This component is responsible for syncing the Cisco Intersight infrastructure cloud resources.	CICOSYNC	https://[redacted]	
Key Rotation Service	This Component is responsible for Key Rotation Service Used to rotate encryption key on periodic basis.	KMS	https://[redacted]	
Orchestrator Services	This component is responsible for Provisioning and other Automation Tasks.	ORCSERVICE	https://[redacted]	

Figure 166 – URL Configuration

6.3.4 KRS Database String Encryption

1. Open Internet Manager.
2. Select **HCL.MyCloudKRS**.
3. Right click and Explore to the web.config under **KMS** folder.

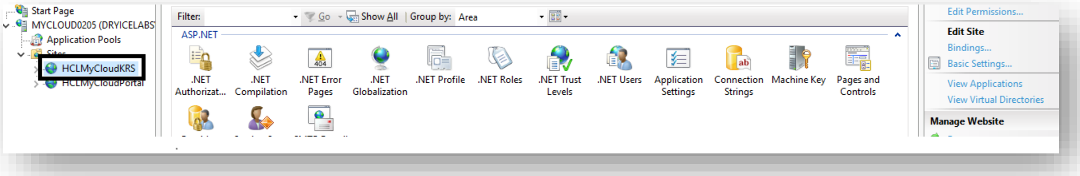
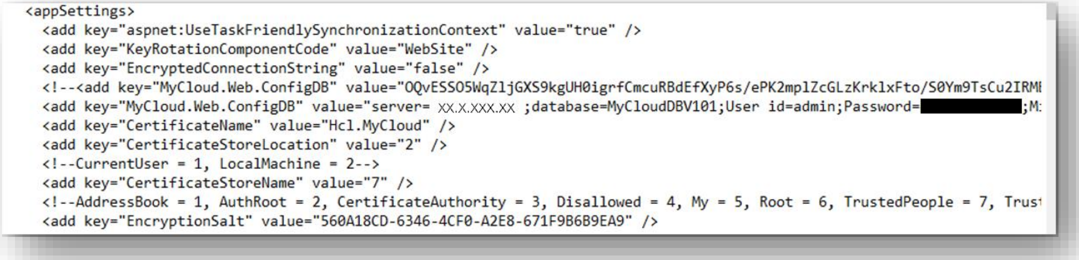


Figure 167 – Component URL Configuration

4. Open Web.Config.
5. By default, "EncryptedConnectionString" key is set to false. In case to use encrypted DB string, update key to True.



```
<appSettings>
  <add key="aspnet:UseTaskFriendlySynchronizationContext" value="true" />
  <add key="KeyRotationComponentCode" value="WebSite" />
  <add key="EncryptedConnectionString" value="false" />
  <!--<add key="MyCloud.Web.ConfigDB" value="OQvESSO5WqZ1jGXS9kgUH0igrfCmcuRBdEfXyP6s/ePK2mplZcGLzKrklxFto/S0Ym9TsCu2IRMI
  <add key="MyCloud.Web.ConfigDB" value="server= XX.X.XXX.XX ;database=MyCloudDBV101;User id=admin;Password=[redacted];M:
  <add key="CertificateName" value="Hcl.MyCloud" />
  <add key="CertificateStoreLocation" value="2" />
  <!--CurrentUser = 1, LocalMachine = 2-->
  <add key="CertificateStoreName" value="7" />
  <!--AddressBook = 1, AuthRoot = 2, CertificateAuthority = 3, Disallowed = 4, My = 5, Root = 6, TrustedPeople = 7, Trus
  <add key="EncryptionSalt" value="560A18CD-6346-4CF0-A2E8-671F9B6B9EA9" />
```

Figure 168 – Component URL Configuration

This marks the completion of HCL BigFix CLM Installation.

7 Support

To get support for this product, please drop an email to bigfixclm-prodsupport-team@hcl-software.com.

HCLSoftware

hcltechsw.com