

Contents

Introduction.....	7
Lab Systems Architecture.....	7
IDs and Passwords for Use in the Lab Exercises	8
Connecting to the Lab Environment: Instructor Led Training (ILT).....	8
Connecting to the Lab Environment: Assisted Self-Paced Training (ASP)	11
Connecting to Systems.....	15
Connecting to the Linux hosts: emserver and linserver.....	15
Connecting to the winserver Windows host	16
Sign in to the Control-M Configuration Manager (CCM) and Verify Agent Status	17
Module 1: Control-M Migration	19
Lab 1.1: Ordering Jobs to Validate Migration.....	19
Task 1: Order Jobs for the CTM-A and CTM-B Control-M/Servers.....	19
Lab 1.2: Migrating the Control-M/Enterprise Manager	21
Task 1: Install the Target Control-M/EM on linserver.....	21
Task 2: Verify the Availability of the New Control-M/EM Components	26
Task 3: Export the Control-M/EM Data from emserver.....	28
Task 4: Import the Control-M/EM Data from the Source (emserver) to the Target (linserver).....	31
Task 5: Verify the Status of the Control-M/EM Components and the Migrated Job Data	34
Lab 1.3: Migrating the CTM-B Control-M/Server Automatically	37
Task 1: Install the Target Control-M/Server onto winserver	37
Task 2: Migrate the CTM-B Control-M/Server Automatically	43
Task 3: Connect the Gateway to the New Control-M/Server	46
Task 4: Verify the Control-M/Server Jobs on CTM-B Run.....	48
Task 5: Uninstall the Control-M/Enterprise Manager on emserver.....	51
Module 2: Installing an Additional Distributed Control-M/Enterprise Manager.....	53
Lab 2.1: Installing a Distributed Control-M/EM on emserver.....	53
Task 1: Install a Distributed Control-M/Enterprise Manager on emserver.....	53
Task 2: Verify the Distributed Control-M/Enterprise Manager Installation	58
Module 3: Workload Archiving Installation	59
Lab 3.1: Installing Control-M Workload Archiving on emserver	59
Task 1: Install the Control-M Workload Archiving Add-On.....	59
Task 2: Verify the Workload Archiving Installation.....	63
Task 3: Update the Automatic Startup and Shutdown Procedure for the Workload Archiving Server Host	63
Lab 3.2: Defining Workload Archiving Policies.....	67
Task 1: Define an Archiving Policy	67
Task 2: Order Inventory Jobs for the CTM-B Control-M/Server	69
Task 3: Search the History Domain for Archive Data	70
Task 4: Perform an Archive Search from the Monitoring Domain	71
Module 4: Role-Based Administration	72

Lab 4.1: Assigning Role-Based Administration Privileges	72
Task 1: Create a Role for Control-M Schedulers	72
Task 2: Create a User and Assign Them to the Schedulers Role	78
Task 3: Verify the ssched User's Access With No Role-Based Administration Privileges Defined.....	80
Task 4: Add a Host Tag and Define Host Groups	83
Task 5: Update the Schedulers Role to Include Role-Based Administration Authorization	87
Task 6: Verify the ssched User's Access With Role-Based Administration Privileges Defined.....	89
Module 5: Administering Control-M Using Automation API	93
Lab 5.1: Installing the Automation API on the Control-M/Enterprise Manager Server	93
Task 1: Download the Latest Automation API.....	93
Task 2: Transfer and Install Automation API on the Control-M/Enterprise Manager	94
Lab 5.2: Configuring an Automation API Environment.....	98
Task 1: Create an API Token.....	98
Task 2: Configure the Control-M Production Environment as an Automation API Command Line Interface Environment.....	101
Lab 5.3: Using the Authentication Service.....	102
Task 1: Listing Defined API Tokens Through the Control-M Automation API Command Line Interface	102
Task 2: Create a JSON Configuration File That Will Update the Expiration Date for the emuser API Token	103
Task 3: Update the Expiration Date for the emuser API Token.....	106
Module 6: Using the Automation API Config Service	107
Lab 6.1: Configuring an Agentless Host Using the API.....	107
Task 1: Create an Agentless Host Configuration File.....	107
Task 2: Add linagent as an Agentless Host.....	108
Lab 6.2: Generating an SSH Key Using the API.....	109
Task 1: Add an SSH Key to the CTM-A Control-M/Server	109
Task 2: Get the Public SSH Key for linagent.....	109
Task 3: Add the Public SSH Key to the linagent Host.....	110
Lab 6.3: Analyzing, Enabling and Disabling Control-M/Agents Using the API	112
Task 1: Analyze the Status of a Host.....	112
Task 2: Disable a Control-M/Agent	112
Task 3: Enable a Control-M/Agent	113
Lab 6.4: Adding a Host Restriction Using the API.....	114
Task 1: Add a Host Restriction for winapp	114
Task 2: Add a Second Host Restriction for ctmserver.....	114
Task 3: List the Defined Host Restrictions	115
Task 4: Update the winapp Host Restriction.....	115
Task 5: List the Defined Host Restrictions	116
Lab 6.5: Adding and Testing a Run As User Using the API.....	116
Task 1: Add a Run As User's SSH Key Passphrase to the Secrets Vault.....	116
Task 2: Create a Run As User Configuration File.....	117
Task 3: Test the Run As User	117
Task 4: Add the Run As User.....	118
Task 5: Add a Second Run As User.....	118

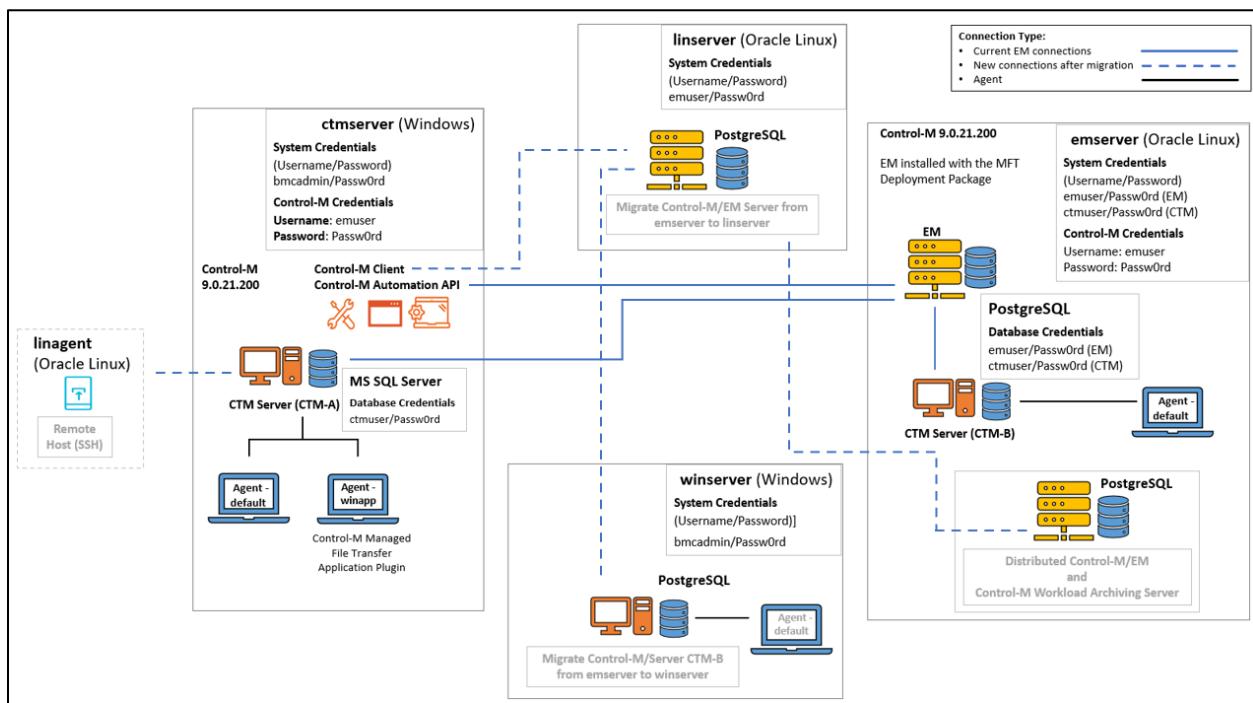
Task 6: List the Defined Run As Users.....	119
Lab 6.6: Setting System Parameters Using the API	120
Task 1: List Control-M/Enterprise Manager System Parameters.....	120
Task 2: Update the CmsCommMode Control-M/Enterprise Manager System Parameter	121
Task 3: List Control-M/Server System Parameters.....	122
Task 4: Update the IOALOGLM, OS_DIAG_LIMIT_LOG_FILE_SIZE and OS_DIAG_LIMIT_LOG_VERSIONS Control-M/Server System Parameters.....	124
Task 5: List Control-M/Agent System Parameters	125
Task 6: Update the LOGKEEPDAYS and MEASURE_USAGE_DAYS Control-M/Agent System Parameters on the WinApp Control-M/Agent	126
Lab 6.7: Listing and Defining a Role Using the API.....	126
Task 1: List All Roles and Export the Settings for the TeamLeader Role.....	127
Task 2: Use the TeamLeader JSON Template to Create a SAP Developers Role.....	127
Task 3: Add the SAP_Developers Role to the Control-M Environment.....	134
Task 4: Review the Defined Permissions in Control-M Web.....	134
(Optional) Task 5: Export the Viewer Role	140
(Optional) Task 6: Modify the Viewer Role and Import it via Control-M Web	140
Lab 6.8: Defining a Control-M User Using the API.....	141
Task 1: Create a User Definitions File.....	141
Task 2: Add the sdev User to the Control-M Environment	143
Task 3: Simulate sdev's Authorizations.....	144
Task 4: Assign the SAP_Developers Role to the sdev User.....	145
Task 5: Simulate sdev's Modified Authorizations	145
Task 6: Get a List of All Defined Users and Assign the SAP_Developers Role to the s01 User	146
Module 7: Using Automation API Provision and Usage Services	149
Lab 7.1: Provision a Control-M/Agent Using the API.....	149
Task 1: Place the Control-M/Agent Installation Package on the Control-M/Enterprise Manager Server	149
Task 2: Install the Automation API for All Users on linserver and Create an Automation API Environment	152
Task 3: Verify the Control-M Images That Are Available to Install.....	155
Task 4: Download and Prepare the Linux Agent Image	155
Task 5: Register the New Control-M/Agent With the Control-M/Server.....	156
Task 6: Upgrade the linserver Control-M/Agent.....	158
Task 7: Install the Application Pack on the linserver Control-M/Agent	160
Lab 7.2: Generate a Usage Report Using the API.....	162
Task 1: Generate a Usage Report Using the Automation API CLI.....	162
Task 2: Create an API Token Using the Authentication Service	163
Task 3: Generate a Usage Report using Curl.....	164
Module 8: SSL Configuration.....	165
Lab 8.1: Generating Self-Signed Certificates	165
Task 1: Create a Certificate Authority and Generate Self-Signed Certificates for All Control-M Components	165
Lab 8.2: Configuring SSL in Zone 1	168

Task 1: Copy the Control-M/Enterprise Manager Server Certificate to the Control-M/Enterprise Manager Server	168
Task 2: Deploy the Certificate to the Control-M/Enterprise Manager Web Server.....	170
Task 3: Extract and Install the Root CA Certificate Onto ctmserver.....	173
Lab 8.3: Configuring SSL in Zones 2 and 3	179
Task 1: Deploy the SSL Certificate to the Control-M/Enterprise Manager Server (to enable Control-M/EM to Control-M/Server communication).....	179
Task 2: Deploy the SSL Certificate to the CTM-B Control-M/Server	179
Task 3: Deploy the SSL Certificate to the winserver Control-M/Agent.....	183
Task 4: Deploy the SSL Certificate to the emserver Control-M/Agent	185
Task 5: Set the linserver Control-M/Agent SSL Mode to Disabled	188
Task 6: Enable SSL on the Control-M/Server and Control-M/Agents.....	190
Task 7: Verify the SSL configuration on different components	191
Module 9: Control-M Health Checking.....	195
Lab 9.1: Implementing Control-M/Enterprise Manager Process Monitoring.....	195
Task 1: Implement a Cyclic Control-M Job to Verify Configuration Agent Availability	195
Task 2: Implement a Cyclic Control-M Job to Verify the CTM-B Gateway Availability	199
Lab 9.2: Inspect the Control-M/Agent Daily Log.....	202
Task 1: Count the Jobs Submitted to a Control-M/Agent Today	202
Task 2: Search for Starvation or DEBUG DUMP Messages.....	204
Lab 9.3: Optimizing the New Day Procedure	205
Task 1: Stop the Statistics Clean Up During the New Day Procedure	205
Task 2: Change the Statistics Retention Period and Number of Retained Statistics Records in the Control-M/Server CTM-A.....	208
Lab 9.4: Defining a Job to Run the ctmjsa Utility	209
Task 1: Modify the Statistics Mode Parameter.....	209
Task 2: Define a Job to Test Statistics Gathering	210
Task 3: Define a Job to Run the ctmjsa Utility.....	211
Lab 9.5: Deleting Old Events (Conditions) and Global Variables	212
Task 1: Delete Old Events (Conditions).....	212
Task 2: Delete Global Variables.....	213
Lab 9.6: Configuring File System Clean Up Parameters	216
Task 1: Setup the Log Retention Parameters for the Control-M/Enterprise Manager	216
Task 2: Setup the Log Retention Parameters for the Control-M/Server	216
Task 3: Setup the Log Retention Parameters for a Control-M/Agent	218
Lab 9.7: Using the Control-M/Agent Toolbox.....	220
Task 1: Test the CPU Performance for the winapp Control-M/Agent.....	220
Task 2: Test the Disk Performance for the winapp Control-M/Agent.....	222

Introduction

Lab Systems Architecture

The lab environment consists of a set of Microsoft Windows and Oracle Linux servers running as virtual machines. The systems are configured on a private network, which allows them to communicate only with each other.



Host Details

The following are details for each of the individual servers contained in the environment:

- **ctmserver (192.168.1.5)** – A Microsoft Windows Server 2022 host that serves as the landing server desktop, with the Control-M Client locally installed. Also installed is a Control-M Server (CTM-A) running on an MSSQL database with two local Control-M/Agents (ctmserver and WinApp).
 - **emserver (IP address 192.168.1.6)** – An Oracle Linux 8 server with the Control-M/Enterprise Manager, Control-M/Server (CTM-B) and Control-M/Agent installed. The Enterprise Manager installation also contains Control-M Automation API, Workload Change Manager, and the Managed File Transfer deployment package.
- Once the Control-M/EM has been migrated, this will serve as a Distributed Control-M/Enterprise Manager and Workload Archiving Server.

- **winserver (192.168.1.7)** – A Microsoft Windows Server 2022 host that will be the migration target Control-M/Server (CTM-B).
- **linserver (IP address 192.168.1.8)** – An Oracle Linux 8 CentOS 7 Linux server that will be the migration target Control-M/Enterprise Manager.
- **linagent (192.168.1.8)** – DNS alias for the linserver host, used as a Remote Host with SSH.

IDs and Passwords for Use in the Lab Exercises

System Credentials:

System	User	Password	Notes
Windows	BMCEDUCATION\\bmcadmin	Passw0rd	Active Directory administrator account used to access the ctmserver host
Linux	emuser	Passw0rd	Operating system user account where the Control-M/Enterprise Manager is installed on the emserver host
	ctmuser	Passw0rd	Operating system user account where the CTM-B Control-M/Server and its associated Agent is installed on the emserver host
	root	password	Operating system super user on the emserver host
Database (PostgreSQL and MSSQL)	emuser	Passw0rd	Control-M/Enterprise Manager database owner account
	ctmuser	Passw0rd	Control-M/Server database owner (CTM-A and CTM-B) account
	sa	Passw0rd	Database administrator account on the MSSQL (CTM-A) database
	postgres	Passw0rd	Database administrator account on the PostgreSQL databases (EM and CTM-B)

Control-M Credentials:

Role	User	Password
Control-M super user	emuser	Passw0rd
Control-M scheduler	s01	Passw0rd

Connecting to the Lab Environment: Instructor Led Training (ILT)

Steps:

1. In a web browser, open the URL: <https://bmc.instructorled.training>.

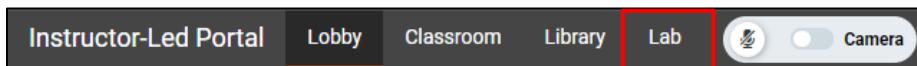
2. On the **Welcome to the Instructor-Led Training portal** page, set the interface language (default is English) and enter the **Access Code** sent by the instructor or received in the session assignment email.

The screenshot shows the login page for the Instructor-Led Training portal. At the top, it says "Welcome to the Instructor-Led Training portal." Below that, a message reads "For information about Certifications and other Learning, please check our [website](#)." There are two input fields: one for "English" (selected) and another for "32DA5372D001". A large blue "Log in" button is centered below the fields. A note at the bottom states: "In many cases the access code is provided by the instructor at the start of class."

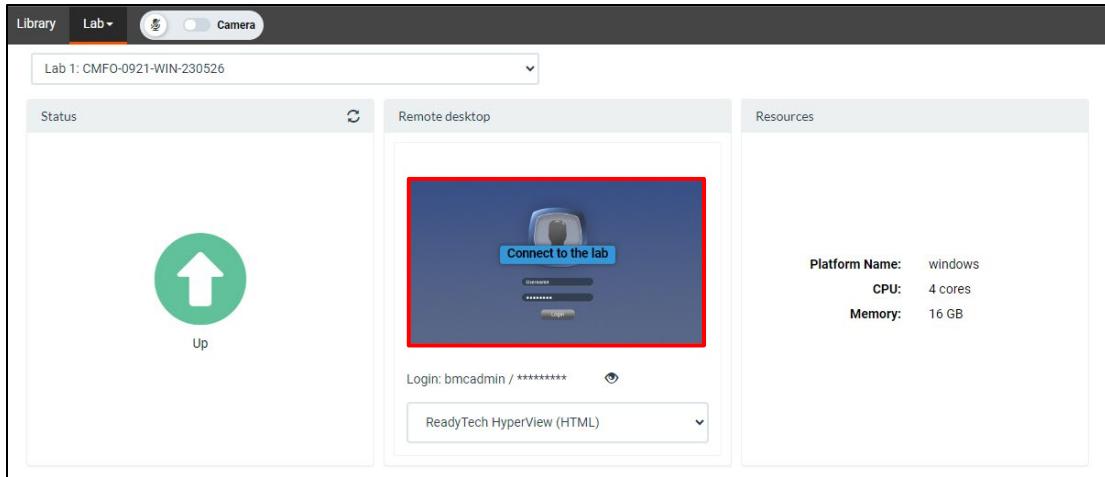
3. Click **Log in**.
4. If it is not already populated, enter your first and last name.
5. Leave the **Enable password protection (optional)** check box unchecked.
6. Select the **Click to consent to our TOS, Privacy Policy, and Cookie Policy** check box.
7. Click **OK**.

The screenshot shows a modal dialog titled "Access code activation". It contains fields for "First name" (filled with "Ben") and "Last name" (filled with "Tovey"). There is an unchecked checkbox for "Enable password protection (optional)". At the bottom, there is a checked checkbox for "Click to consent to our [TOS, Privacy Policy, and Cookie Policy](#)". The "OK" button is highlighted in blue.

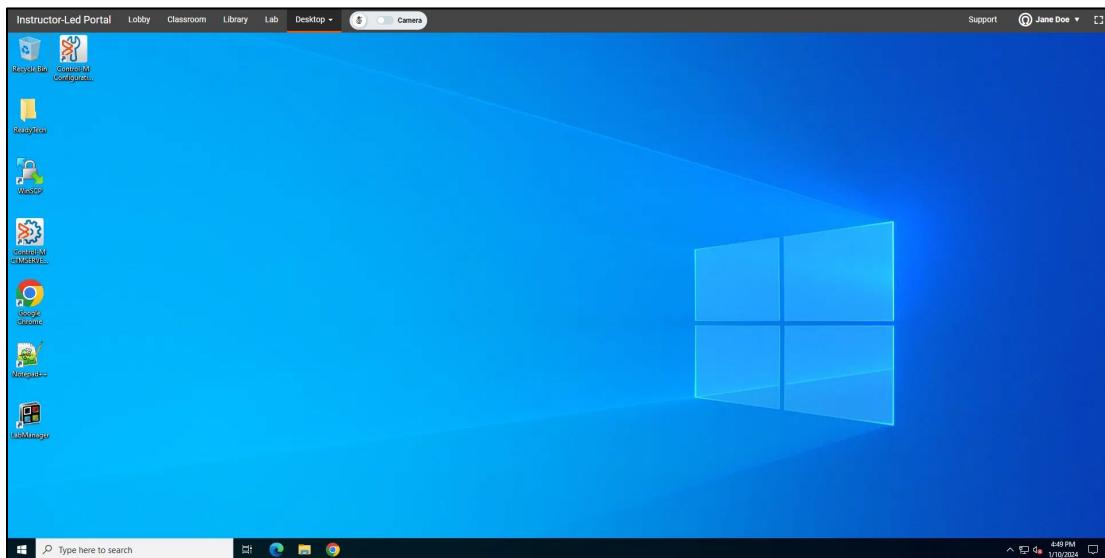
8. You will now be in the **Lobby**. To access the lab, click the **Lab** tab.



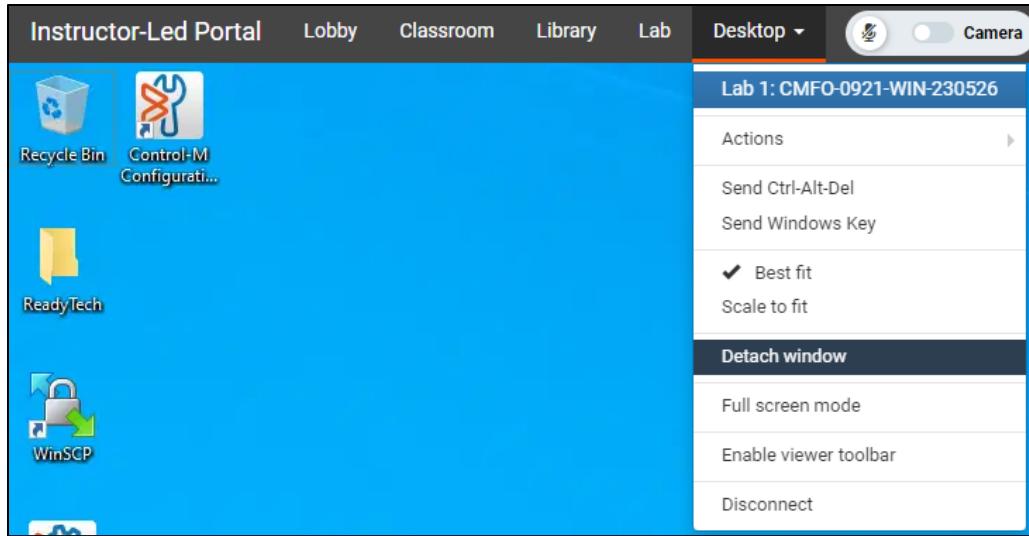
9. To access the landing server desktop, click **Connect to lab** from the **Remote desktop** section in the middle of the screen.



10. A new tab (**Desktop**) opens along the access panel and the lab opens to the landing server's desktop.



11. When the class starts, open the **Classroom** tab.
12. (Optional) to save having to switch between the **Classroom** and **Desktop** (lab) tabs, the **Desktop** tab can be detached to a separate window. To do this, from the **Desktop** tab, select the **Desktop** drop-down and then **Detach window**.



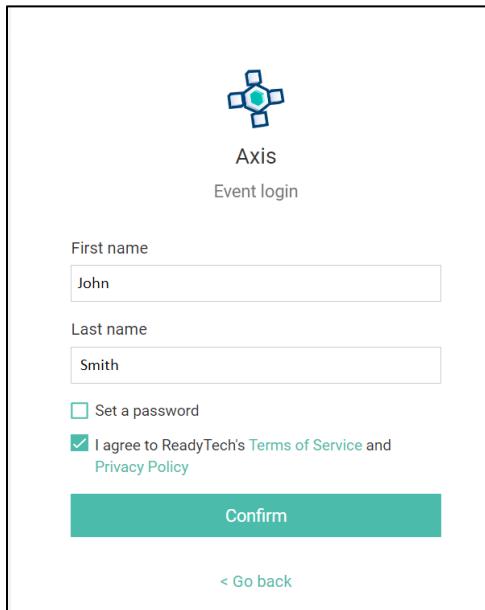
Connecting to the Lab Environment: Assisted Self-Paced Training (ASP)

Assisted Self-Paced (ASP) courses are On-Demand lab sessions. Hence, you can control the start and end time of the sessions as per your requirements.

Steps:

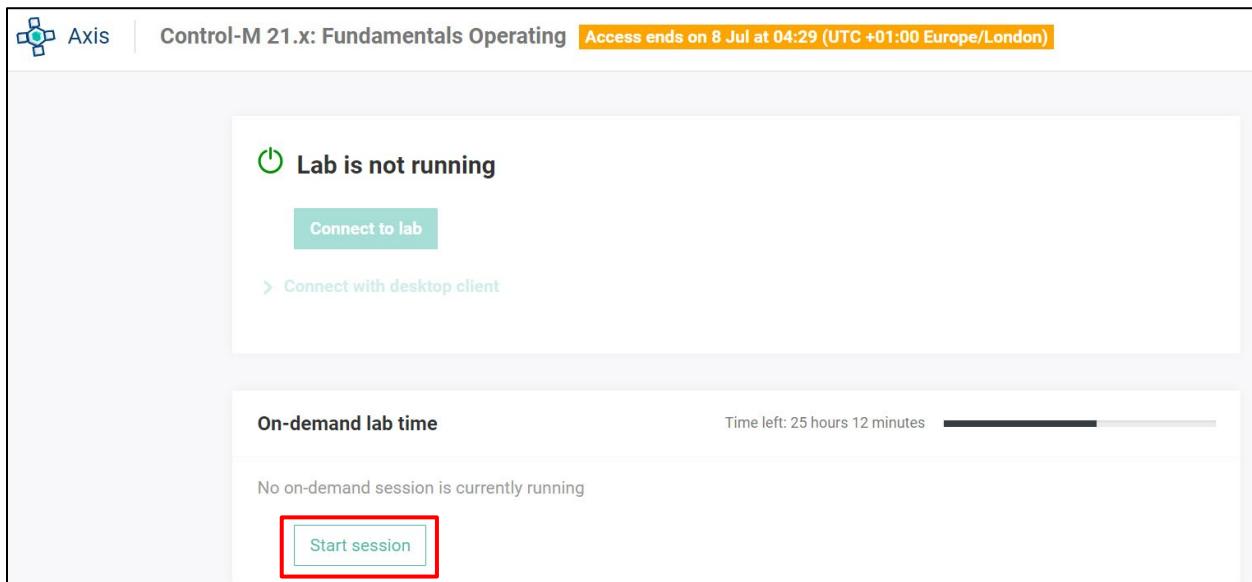
1. In a web browser, open the URL: <http://axis.readytech.com/#/seat-login>.
2. On the **ReadyTech Axis Event** login page, enter the **Access Code** received in the session assignment email.
3. Click **Log In**.
4. Leave the **Set a password** field unchecked.
5. Select the check box to accept the **Terms of Services** and **Privacy Policy**.
6. Click **Confirm**.

The User Portal opens.



The image shows a web-based event login form. At the top is a logo consisting of four blue squares forming a cross-like shape with a central green circle. Below it is the word "Axis". Underneath the logo is the text "Event login". The form contains fields for "First name" (with "John" typed in) and "Last name" (with "Smith" typed in). There are also two checkboxes: one for "Set a password" which is unchecked, and another for "I agree to ReadyTech's Terms of Service and Privacy Policy" which is checked. A large teal "Confirm" button is at the bottom, and a link "[Go back](#)" is located just below it.

- After you log in with the provided access code, the session screen will open. Click the **Start session** button.



The image shows a session management interface. At the top left is the Axis logo. To its right is the text "Control-M 21.x: Fundamentals Operating" and a yellow status bar that says "Access ends on 8 Jul at 04:29 (UTC +01:00 Europe/London)". The main area has a heading "Lab is not running" with a green circular icon containing a white power symbol. Below it is a teal "Connect to lab" button and a link "[Connect with desktop client](#)". Further down is a section titled "On-demand lab time" with a progress bar indicating "Time left: 25 hours 12 minutes". Below this is a message "No on-demand session is currently running" and a red-bordered "Start session" button.

- State the amount of time (HH:MM) required for the current session. Sessions can later be extended by clicking **Extend Session**, or the time banked by clicking **Stop Session**. Please be aware that there is no warning inside of the labs stating the session will expire. To review the remaining time, return to the session screen (the page where you clicked **Start session**).

Start on-demand session

Specify how much time you want to allocate for this on-demand session.

Duration	Time remaining
Hours 2	Minutes 12
Hours 25	Minutes 12

Start **Cancel**

- The session initially takes about 7-8 minutes to start. Resuming a session takes approximately 3-4 minutes.

You will see that the **Connect to lab** button is enabled once the lab session is started. The session timer is indicated next to the **On-demand lab time** section on the screen. In this example, there are 25 hours and 41 minutes left in total, with 4 hours and 57 minutes remaining in the current session.

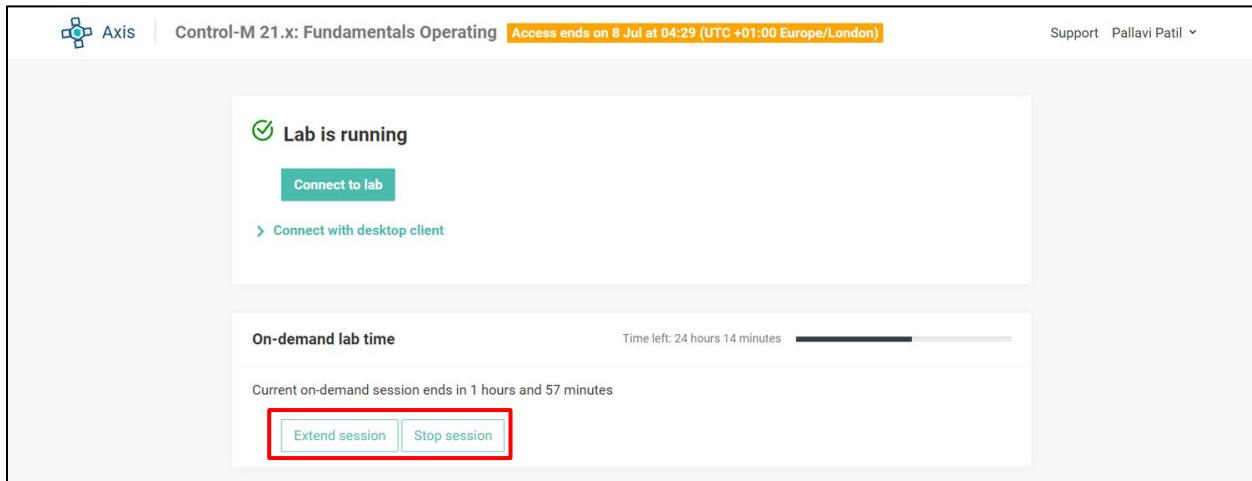
The screenshot shows the Control-M interface for a scheduled session. At the top, it says "ReadyTech Axis" and "Test- Control-M 20.x: Fundamentals Scheduling-210302 | Access ends on 12 Mar at 23:59 (UTC +05:30 Asia/Calcutta)".

Lab is running: A green checkmark icon is followed by the text "Lab is running". Below it is a red box around the "Connect to lab" button. A callout bubble points to this button with the text "Remaining duration for which the Lab session is available for your entire class.".

On-demand lab time: This section shows "25 hours 41 minutes left" with a progress bar. Below it, it says "Current on-demand session ends in 4 hours and 57 minutes" and has "Extend session" and "Stop session" buttons.

Annotations: Two orange callout bubbles highlight information: one on the left pointing to the "On-demand lab time" section with the text "Remaining duration for the end of the current connected session.", and another pointing to the "Connect to lab" button with the same text as the callout above it.

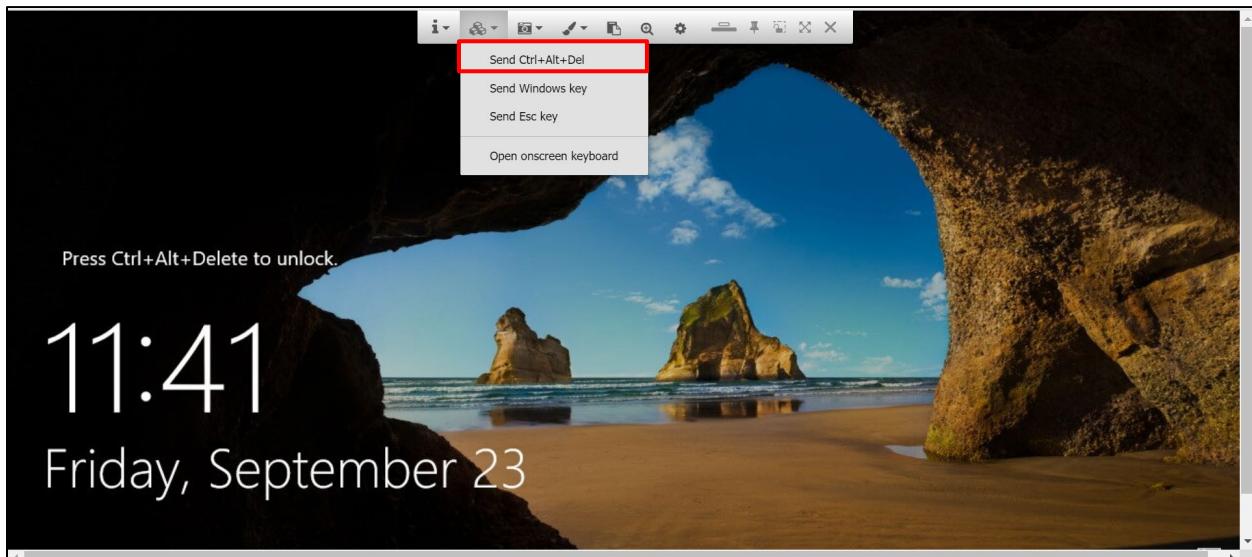
- If you want to extend the session, click the **Extend Session** button.
- If you want to stop the session, click the **Stop Session** button. Your remaining session minutes/hours will be added back to the **On-demand lab time**.



12. After you click the **Connect to lab** button, the ReadyTech MatchMaker session will open in a new web browser tab with the Windows login screen as shown below. The credentials for the Windows system are as follows:

- User name = **bmcadmin**
- Password = **Passw0rd**

Note: If you do not see the Login screen, move your mouse to the upper side of the screen to pull down the **Access** toolbar. Click the **Keys** drop-down arrow and click **Send Ctrl+Alt+Del**.



Note: The lab session will end without any notification as soon as the connected session time is over. Hence, it is important to monitor the session time and if required, extend it before the connected session ends.

You will be redirected back to the ReadyTech MatchMaker window when the On-Demand Class session has expired.

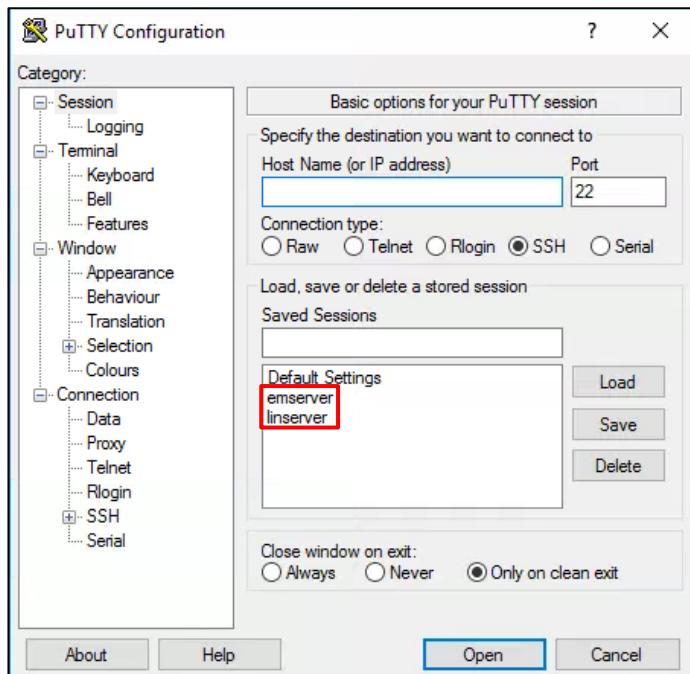
Important Note: For Assisted Self-paced sessions (ASP), the lab demonstration can be accessed using the video marker available in the module video.

Connecting to Systems

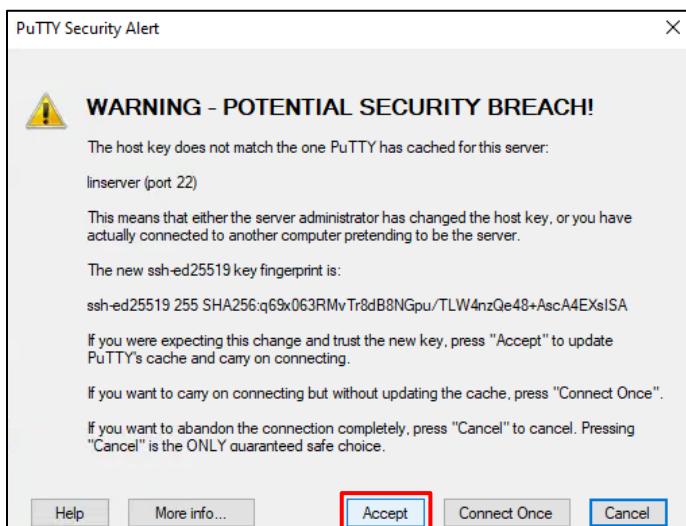
Connecting to the Linux hosts: emserver and linserver

Steps:

1. From the landing server (**ctmserver**) desktop, double-click the **PuTTY** icon. The **PuTTY Configuration** window opens.
2. Double-click **emserver** or **linserver** from the **Saved Sessions** section.



3. A **PuTTY Security Alert** window will open, click **Accept**:

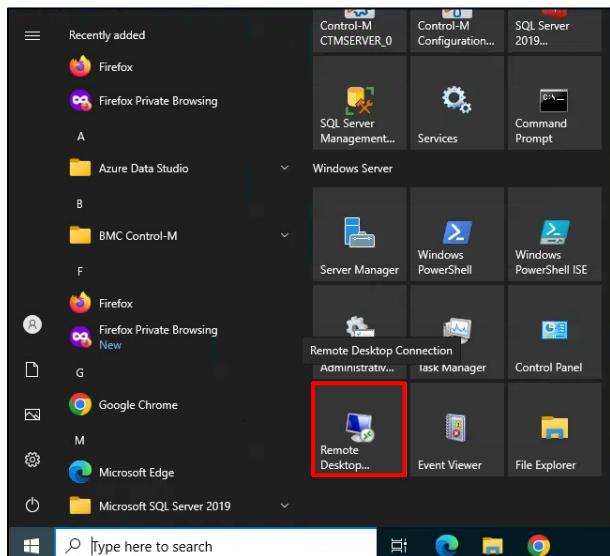


4. Enter the username and password when prompted.

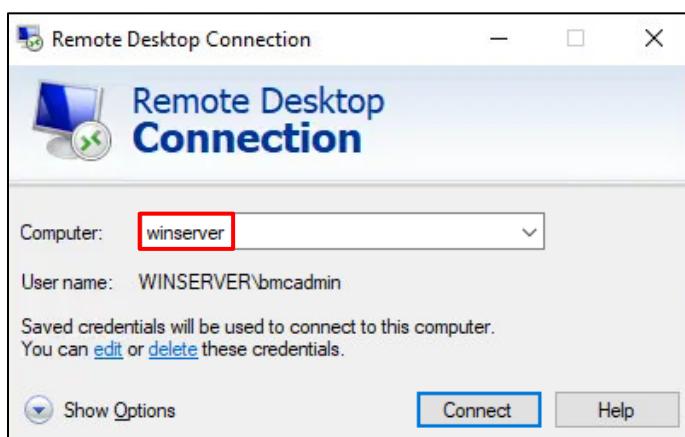
Connecting to the winserver Windows host

Steps:

1. From the landing server (**ctmserver**) desktop, click **Start**.
2. Scroll down on the application tiles section to find **Remote Desktop**. Click the **Remote Desktop Connection** icon.



3. From the **Remote Desktop Connection** window that opens, enter **winserver** into the **Computer** field.



4. Click **Connect**.
5. Enter the password: **Passw0rd**.

- From the popup that appears, check the **Don't ask me again for connections to this computer** box and click **Yes**.



- To return to the **ctmserver** landing server, minimise or close the **Remote Desktop** window from the blue **Remote Desktop Connection** bar at the top of the screen.

Note, this may be partially or totally obstructed by the gray **ReadyTech Access** bar. Click and drag either bar (**ReadyTech Access** or the **Remote Desktop Connection**) to display both side-by-side:



Sign in to the Control-M Configuration Manager (CCM) and Verify Agent Status

Steps:

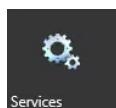
- To launch the CCM interface, from the landing server (**ctmserver**) desktop, double-click **Control-M Configuration Manager CTMSERVER_0**.



- In the log in window, you should see the **Server** listed as **emserver**. Select **Show advanced setting** to open the communication settings details section.
- Verify the **Host Name** is **emserver** and the **Port Number** is **18080**.

Note: After completing **Lab 1.2** the **Host Name** thereafter will be **linserver**.

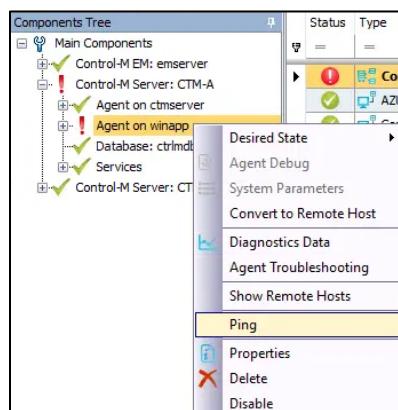
4. Click **Apply** to hide the parameters.
5. Sign in as **emuser**, with the password: **Passw0rd**.
6. In the **Components Tree**, click to expand **Main Components** and the component **Control-M Server: CTM-A**. Verify both **ctmserver** and **winapp** Control-M/Agents are running. If either are stopped:
 - Press **Start** and open **Services**.



- Identify the **Control-M Agent** service that isn't running, denoted by the **Status** column.
- Right-click it and select **Start**.

Name	Description	Status	Startup Type	Log On As
Control-M Agent ctmserver	BMC Softw...	Running	Automatic	Local Syste...
Control-M Agent FileWatch...	BMC Softw...		Manual	Local Syste...
Control-M Agent FileWatch...	BMC Softw...		Manual	Local Syste...
Control-M Agent winapp	BMC Softw...	Auto	Start	
Control-M/Server	BMC Softw...	Running	Auto	Stop
Control-M/Server Configur...	BMC Softw...	Running	Auto	Pause
CoreMessaging	Manages co...	Running	Auto	Resume
Credential Manager	Provides se...		Mar	Restart
CredentialEnrollmentMana...	Credential E...		Mar	
Cryptographic Services	Provides thr...	Running	Auto	All Tasks >
Data Sharing Service	Provides da...		Mar	Refresh
DCOM Server Process Laun...	The DCOML...	Running	Auto	
dcsvc	Declared Co...		Mar	
Delivery Optimization	Performs co...		Mar	
Device Association Service	Enables pair...	Mar	Help	

- Return to the CCM. Right-click the unavailable Control-M/Agent and select **Ping**. In a few seconds, the Agent should show as **Available**.



Module 1: Control-M Migration

Objectives:

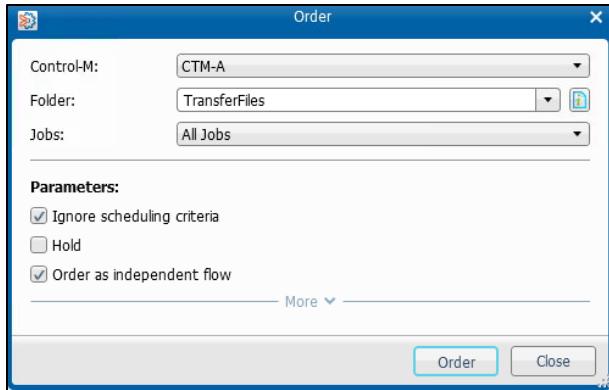
- Order jobs to validate the Control-M migration
- Migrate the Control-M/Enterprise Manager
- Migrate the CTM-B Control-M/Server automatically

Lab 1.1: Ordering Jobs to Validate Migration

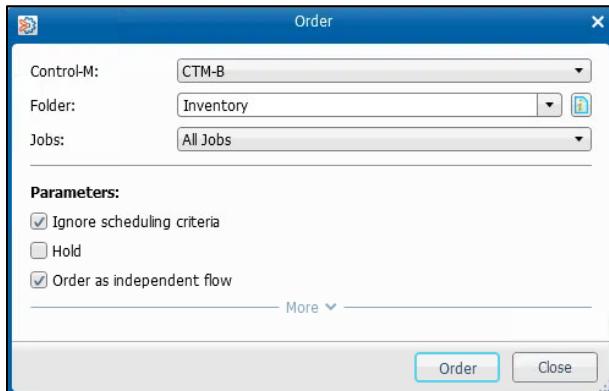
Task 1: Order Jobs for the CTM-A and CTM-B Control-M/Servers

Steps:

1. To launch the Control-M interface, from the landing server (**ctmserver**) desktop, double-click  **Control-M CTMSERVER_0**.
2. Log in as **emuser** with the password: **Passw0rd**.
3. Click **Monitoring** to display the **Monitoring** domain.
4. Open the **All Active Jobs** viewpoint from the **All ViewPoints** tab.
5. From the ribbon, click **Order** (from the **Viewpoint** tab).
6. In the **Order** dialog box, specify the following:
 - **Control-M:** CTM-A
 - **Folder:** TransferFiles
 - **Jobs:** All Jobs
7. Ensure that the **Ignore scheduling criteria** and **Order as independent flow** options are selected.

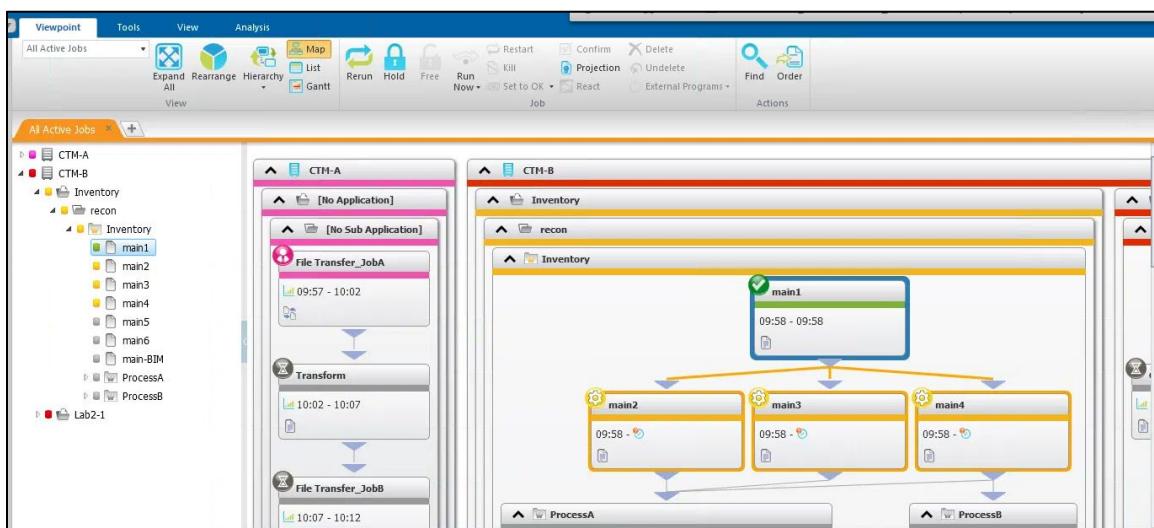


8. Click **Order** and confirm it.
9. Repeat steps 5 to 8 to order the **Inventory** folder from the **CTM-B** Control-M/Server.



10. From the ribbon, click **Expand All** (from the **Viewpoint** tab).

11. Verify that the ordered jobs appear in the interface:



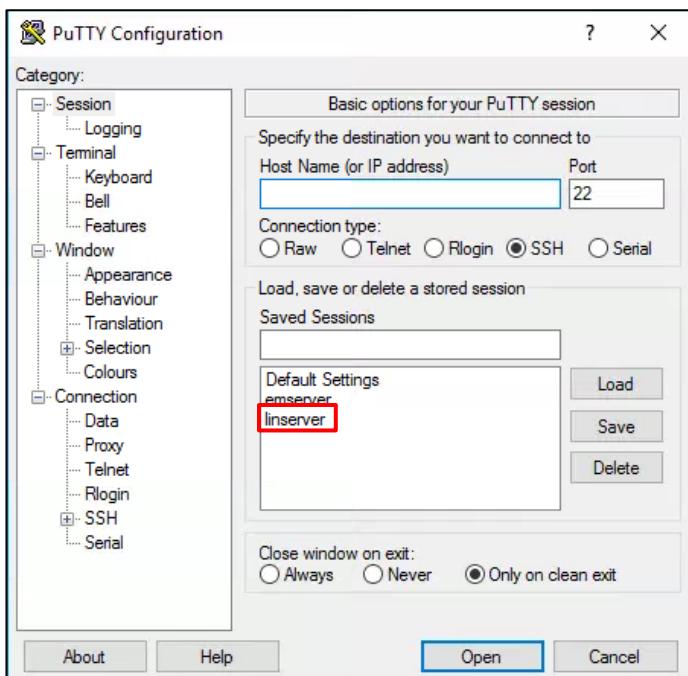
12. Logout of the **Control-M GUI** (**File > Logout**).

Lab 1.2: Migrating the Control-M/Enterprise Manager

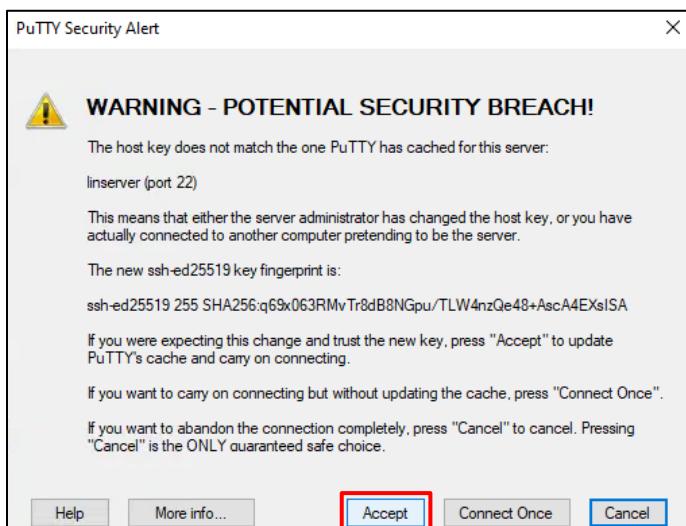
Task 1: Install the Target Control-M/EM on linserver

Steps:

1. From the landing server (**ctmserver**) desktop, double-click the **PuTTY** icon. The **PuTTY Configuration** window opens.
2. Double-click **linserver** from the **Saved Sessions** section.



3. A **PuTTY Security Alert** window will open, click **Accept**:



4. Sign in as **emuser** with the password: **Passw0rd**.
5. The installation requires **Java**, which has been installed into the directory **/home/emuser/OpenJDK/**. To direct the installer to use this directory, the **BMC_INST_JAVA_HOME** environment variable must be defined. To do so, run the command:
setenv BMC_INST_JAVA_HOME /home/emuser/OpenJDK/
6. Verify the variable is correctly defined by running:
echo \$BMC_INST_JAVA_HOME

```
linserver% setenv BMC_INST_JAVA_HOME /home/emuser/OpenJDK/
linserver% echo $BMC_INST_JAVA_HOME
/home/emuser/OpenJDK/
linserver%
```

7. Type **/home/emuser/InstallationFiles/DROST.9.0.21.200_Linux/setup.sh** to run the installer.
8. When the setup starts, type **Y** to continue in non-graphical mode.

```
linserver% /home/emuser/InstallationFiles/DROST.9.0.21.200_Linux/setup.sh
Starting graphical user interface...

The $DISPLAY environment variable is not defined.

Install will continue in non graphical mode.
Are you sure you want to continue?
== <N> No  <Y> Yes ==

Enter command:
Y
```

9. Type **S** to skip the **License Agreement** section.
10. Type **Y** to agree to the **License Agreement**.

```
"Territory" means the country(ies) where Customer is licensed to install the Product as specified in the Order.
2. SCOPE. Licenses are granted, and Support is obtained, solely by execution of Orders. Each Order is deemed to be a discrete contract, separate from each other Order, unless expressly stated otherwise therein, and in the event of a direct conflict between any Order and the terms of this

Press <Enter> to continue or <S> to skip: S

Do you accept and agree to the terms of this Software License Agreement (Y/N)?Y
```

11. Press **Enter** to dismiss the **Usage Collection** notification.

NOTE:

Control-M automatically collects anonymous information on your product usage patterns. This information helps BMC to identify trends, enhance Control-M capabilities, and improve the quality.

BMC does not collect any of your personal or organizational identifiable data. Your participation in the usage collection is optional. You can opt-out at any time by changing the values of the UsageCollectionDisabled system parameter to 1 as described in the Control-M Help (CMS parameters).

== <Enter> Continue ==

12. On the **Product Settings : Installation Options** page, use option **3** to select **Additional Installations**.
13. Select option **2 - Control-M/Enterprise Manager**.

```
==== Control-M 9.0.21.200 Installation ====

==== Product Settings : Installation Options ===

1 : ( ) Control-M 9.0.21.200 - Full Installation
      Use custom settings (y/n)?
      Install trial version with all optional components (y/n)?

2 : ( ) Control-M Agent

3 : (x) Additional Installations
      ( ) Control-M/Server
      (x) Control-M/Enterprise Manager
      ( ) Secondary installation for High-Availability

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==
Enter command or item number you wish to change: █
```

14. Press **Enter** to move to the next panel.
15. We want to install a Control-M/Enterprise Manager using the **Default installation** (which is the default option). Press **Enter** to move to the next panel.

```
== Control-M/Enterprise Manager 9.0.21.200 Installation ==

== Product Settings : Setup Type ==

1 : (x) Default installation
2 : ( ) Custom installation
3 : ( ) Additional distributed installation

== <C> Cancel <N>/<Enter> Next Panel ==

Enter command or item number you wish to change:  
```

16. From the **Product Settings : Dedicated Database Properties** page, select **2** to set the **Database admin (postgres) password**. Set it to **Passw0rd** and confirm.
17. Select **3** to set the **Database owner (emuser) password**. Set it to **Passw0rd** and confirm.

```
== Product Settings : Dedicated Database Properties ==

1 : Database size
    ( ) Small - Less than 1,000 jobs per day
    (x) Medium - 1,001-10,000 jobs per day
    ( ) Large - More than 10,000 jobs per day
2 : Database admin (postgres) password: *****
3 : Database owner (emuser) password:

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==
Enter command or item number you wish to change: 3
Enter a new value for Database owner (emuser) password: *****
Confirm the password: ***** 
```

18. Press **Enter** to move to the next panel.
19. Review the settings on the **Summary** page, and when ready press **Enter** to begin the installation (which takes approximately 15 minutes).

```
Apache Zookeeper Leader Election port number: 3994  
Database Server Type: PostgreSQL  
Database Server Name: linserver  
Database Server Port Number: 5433  
Control-M/Enterprise Manager Database Owner Username: emuser  
Control-M/Enterprise Manager Database Name: emdb  
Database Size: Medium  
== <C> Cancel <P> Previous Panel <I>/<Enter> Install <G> Generate an automatic i  
nstallation configuration file ==  
Enter command: █
```

20. Verify the installation completes successfully.

```
==== Control-M/Enterprise Manager 9.0.21.200 Installation ====  
  
==== Installation Result - Success ====  
  
Installation has completed successfully.  
  
Note:  
  
To start working with Control-M/Enterprise Manager, you must close  
the current session and open a new one.  
  
To download the Control-M client and view the latest help and videos,  
see the Control-M Welcome page  
https://linserver:8446  
linserver% █
```

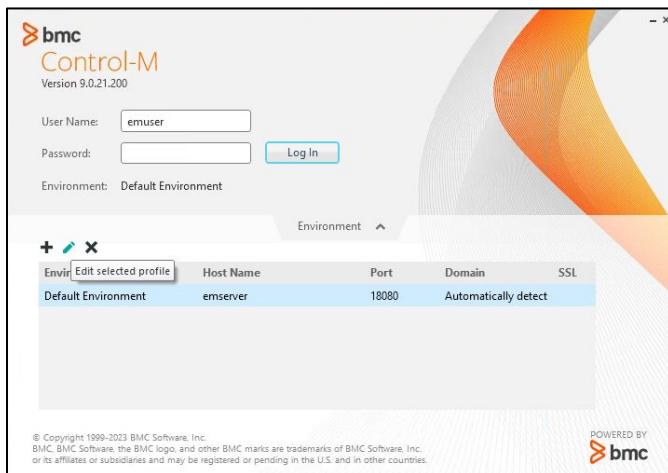
21. When the installation completes, the automatic startup file should be configured. In this environment the service file has already been defined, it simply needs enabling. To do so type **su** to switch to the **root** user and enter the password: **password**.
22. Type **systemctl daemon-reload**.
23. Type **systemctl enable EM.service**.

```
linserver% su  
Password:  
[root@linserver emuser]# systemctl daemon-reload  
[root@linserver emuser]# systemctl enable EM.service  
[root@linserver emuser]# █
```

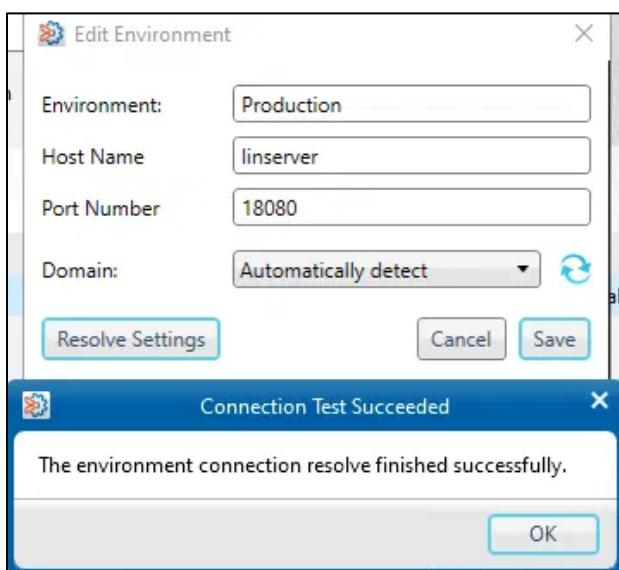
24. Type **exit** to logout from the **root** account.

Task 2: Verify the Availability of the New Control-M/EM Components**Steps:**

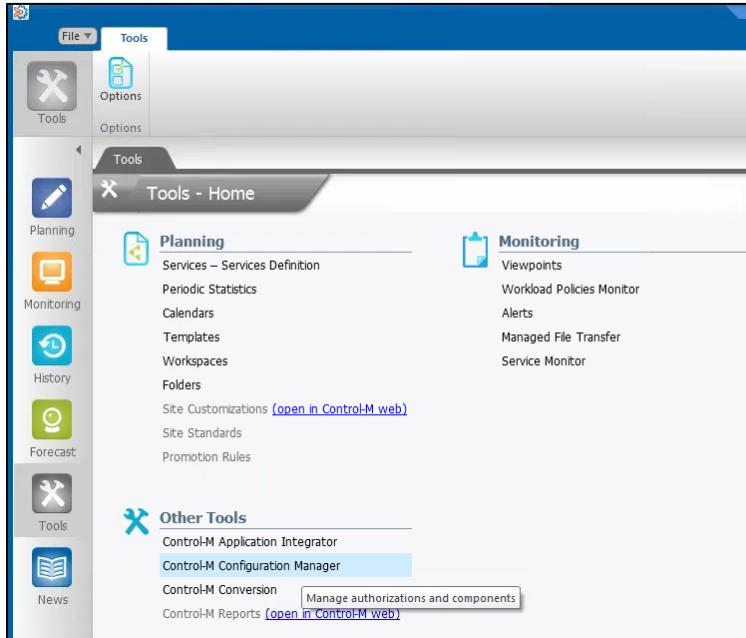
1. From the landing server (**ctmserver**) desktop, open the **Control-M GUI** by double-clicking on **Control-M CTMSERVER_0**.
2. Expand **Environment**.
3. Use the pencil icon to edit the **Default Environment**.



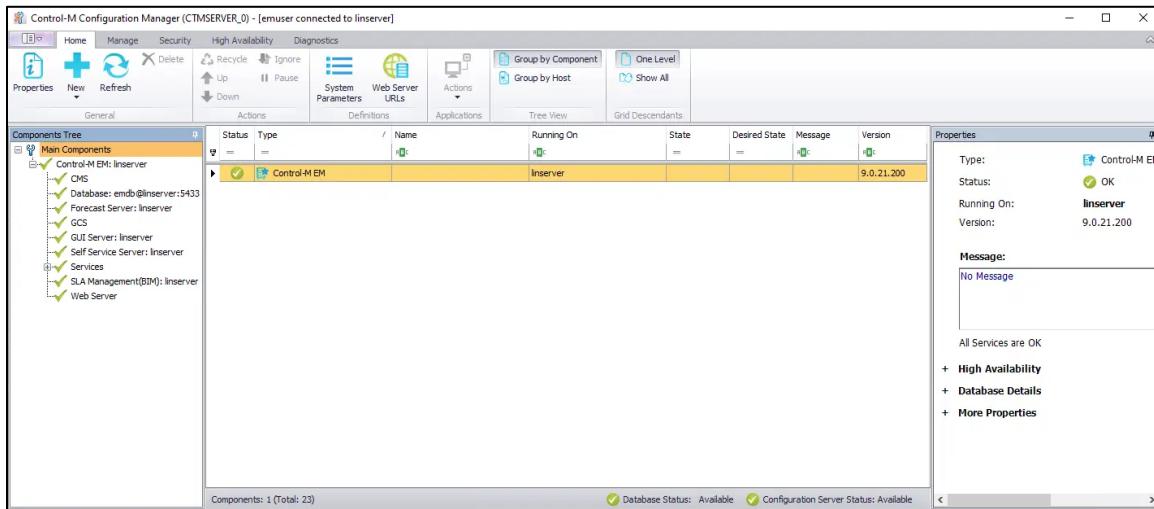
4. Set the **Environment** name to **Production**.
5. Set the **Host Name** to **linserver**.
6. Click **Resolve Settings** to verify connectivity.



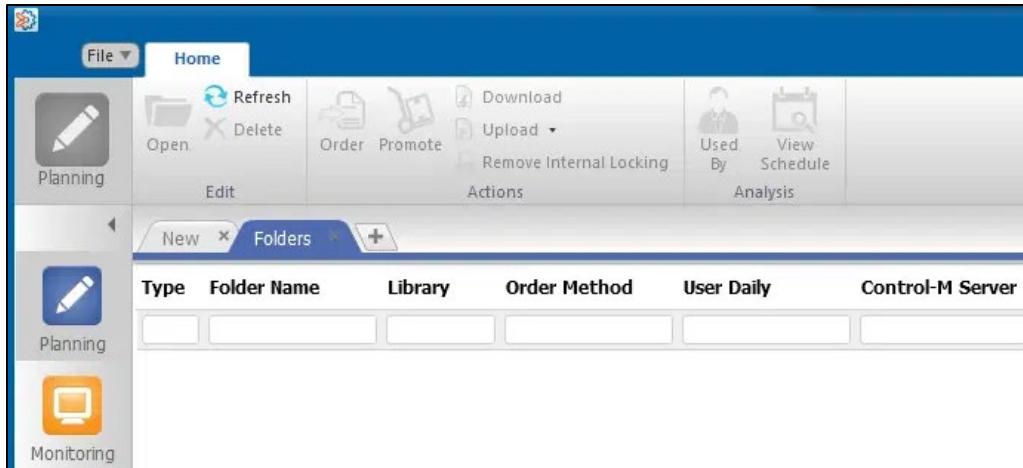
7. Click **Save**.
8. Login as **emuser** with the password: **Passw0rd**.
9. Open the **Tools** domain, then select **Control-M Configuration Manager**.



10. When the **Control-M Configuration Manager (CCM)** opens, verify that all components show as available.



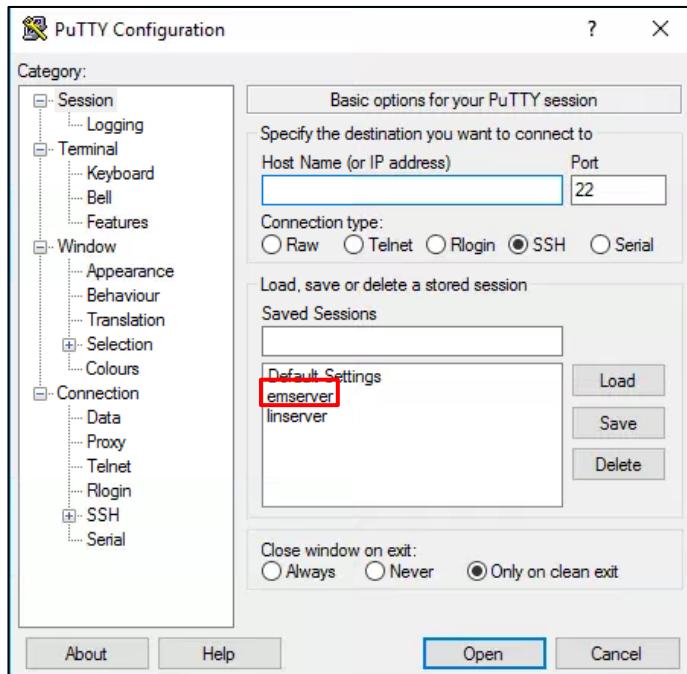
11. Return to the **Control-M GUI**. Select the **Planning** domain.
12. From the ribbon, click **Folders**. As this environment is new, no folders are defined.



Task 3: Export the Control-M/EM Data from emserver

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **PuTTY**.
2. Double-click **emserver** from the **Saved Sessions** section.



3. A **PuTTY Security Alert** window will open, click **Accept**.
4. Sign in as **emuser** with the password: **Passw0rd**.

The Control-M/EM processes are set to start up automatically when the **emserver** host starts up. This needs to be disabled. In the next lab we will migrate the Control-M/Server from the **emserver** host, so we will also disable the automatic startup procedure for this component at the same time.

5. Enter **su** to switch to the **root** user and enter the password: **password**.
6. Run the command: **systemctl disable EM.service CTM.service**.

```
login as: emuser
emuser@emserver's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Apr 11 11:35:06 2024 from 192.168.1.5
emserver% su
Password:
[root@emserver emuser]# systemctl disable EM.service CTM.service
Removed /etc/systemd/system/multi-user.target.wants/EM.service.
Removed /etc/systemd/system/multi-user.target.wants/CTM.service.
[root@emserver emuser]# 
```

7. Enter **exit** to logout as the root user.

```
[root@emserver emuser]# exit
exit
emserver% 
```

8. Run the following upgrade command: **ctm_em/Upgrade_Export/upgrade**
9. Enter **1** to **Export**.

```
emserver% ctm_em/Upgrade_Export/upgrade

Upgrade (Export)

Select one of the following options:

1) Export.
2) Exit Menu

Enter option number---> [] : 1 
```

10. When prompted, enter the Control-M/EM database owner credentials, and then enter the database system administrator password.
 - **Control-M/EM DB owner username:** emuser
 - **Control-M/EM DB owner password:** Passw0rd

- Database System Administrator password: Passw0rd

```
Enter Control-M/EM DB owner user name:  
emuser
```

```
Enter Control-M/EM DB owner password:
```

```
Enter Database System Administrator password:
```

11. To Shutdown local Control-M/EM components before proceeding, enter 2.

emserver(192.168.1.6)	47778
emserver(192.168.1.6)	53582
emserver(192.168.1.6)	45108
emserver(192.168.1.6)	53244
emserver(192.168.1.6)	53260
emserver(192.168.1.6)	39488

If this is your final upgrade, shut down all open connections before continuing.
If you are testing the export process, continue, as long as no database changes
are made during the export.

Select one of the following options:

- 1) Continue with export
- 2) Shutdown local Control-M/EM components
- 3) Display database connections
- 4) Exit

Enter option number---> []:

2

12. When prompted to export Forecast history (**Would you like to export Forecasting Job History data?**), enter y.
13. When prompted to export job history data (**Would you like to export job history data?**), enter y.
14. When prompted for the number of job history days to retain (**Enter the number of days back, you wish to upgrade**) enter 2:

```
Exporting the Forecast historical data may require a significant amount of time.  
Note that scheduling forecasts will be accurately generated  
even if you choose not to export this data.
```

```
Would you like to export Forecasting Job History data [n]?  
Y
```

```
Would you like to export jobs history data [n]?  
Y
```

```
Note that upgrade of archived jobs may take a long time. Enter the number of days  
you wish to upgrade [4]:  
2
```

- Once the data is exported successfully, press **Enter** to continue.

The export files are stored in the following location:
/home/emuser/ctm_em/Upgrade_Export/EMExportForUpgrade.tar

```
Export ended successfully.  
=====
```

```
The export files are stored in the following locations:  
Unix: "Upgrade_Export/EMExportForUpgrade.tar"  
Windows: "Upgrade_Export/data/*".
```

```
To proceed with the upgrade process, copy or replace the  
export output pack/files to the 9.0.21.200 machine/account as follows:  
o In Unix, copy to <EM_HOME>/Upgrade/Import directory.  
o In Windows, copy the <EM_HOME>\Upgrade\Import\data folder.
```

```
For more information, see the Upgrade Guide.
```

```
Press ENTER to continue.
```

Task 4: Import the Control-M/EM Data from the Source (**emserver**) to the Target (**linserver**)

Steps:

- Log out of any active **Control-M GUI** and **CCM** sessions.
- From the landing server (**ctmserver**) desktop, double-click the **PuTTY** icon.
- Double-click **linserver** from the **Saved Sessions** section.
- Sign in as **emuser** with the password: **Passw0rd**.
- Copy the exported file from the source (**emserver**) to the target (**linserver**) host by running:

```
scp  
emuser@emserver:/home/emuser/ctm_em/Upgrade_Export/EMExportForUpgrade.tar  
/home/emuser/ctm_em/Upgrade/Import/
```

- When prompted, state **yes** to continue connecting:

```
linserver% scp emuser@emserver:/home/emuser/ctm_em/Upgrade_Export/EMExportForUpgrade.tar /home/emuser/ct  
m_em/Upgrade/Import/  
The authenticity of host 'emserver (192.168.1.6)' can't be established.  
ECDSA key fingerprint is SHA256:+v7GOOX7eWrkqzT3Nm6jwG+4YyDgFqYGIhrGXc5lfeq.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

- When prompted, enter **emuser**'s password: **Passw0rd**.
- Verify the file is successfully transferred.

```
emuser@emserver's password:  
EMExportForUpgrade.tar  
linserver% 100% 2100KB 141.4MB/s 00:00
```

- Run the migration command:
ctm_em/Upgrade/Import/upgrade

```
linserver% ctm_em/Upgrade/Import/upgrade
```

- Enter **1** for **Import**.

```
Upgrade (Import)  
  
Before Import, make sure that:  
* The exported upgrade data is placed under <EM_HOME>/Upgrade/Import/data.  
* There are no open connections to Control-M/EM database.  
* All Control-M/EM components are down.  
* The Control-M/EM database server is up and running.  
  
Select one of the following options:  
1) Import  
2) Exit Menu.  
  
Enter option number--> []: 1
```

- When prompted, enter your Control-M/EM database credentials:

- Enter **Control-M/EM DB owner user name**: emuser
- Enter **Control-M/EM DB owner password**: Passw0rd
- Enter **Database System Administrator password**: Passw0rd

12. Enter 1 to Shutdown local Control-M/EM components.

```
linserver(192.168.1.8) | 57308
linserver(192.168.1.8) | 57322
linserver(192.168.1.8) | 57334
linserver(192.168.1.8) | 36044

NOTE:
You may need to manually stop non-local Control-M/EM
components or any other database connections.

Select one of the following options:
1) Shutdown local Control-M/EM components
2) Continue Import
3) Exit
Enter option number---> []:
Select an option: 1
```

13. Once all connections are shut down, enter Y to proceed with the import.

```
Getting export data information ...

Export data time: Thu Apr 11 12:34:43 2024

Export data host: emserver

Proceed with data import? (y/n):
y
```

14. Once the data is imported successfully, press **Enter to continue.**

```
-----  
Importing C001_RUNINFO ... (1 tables)  
  Table C001_RUNINFO                      ==> No Data  
-----  
Importing C002_RUNINFO ... (1 tables)  
  Table C002_RUNINFO                      ==> No Data  
-----  
Importing C001_ARCINFO ... (1 tables)  
  Table C001_ARCINFO                      ==> No Data  
-----  
Importing C002_ARCINFO ... (1 tables)  
  Table C002_ARCINFO                      ==> No Data  
  
Forecast historical data import ended successfully  
  
Old components data may exist in Control-M Configuration Manager for topology information.  
These components may be manually removed or redefined.  
  
The Import procedure ended successfully.  
  
Press ENTER to continue.
```

15. Once the data has been migrated, type **start_all** to start up the Control-M/EM components and enter the password **Passw0rd** when prompted.

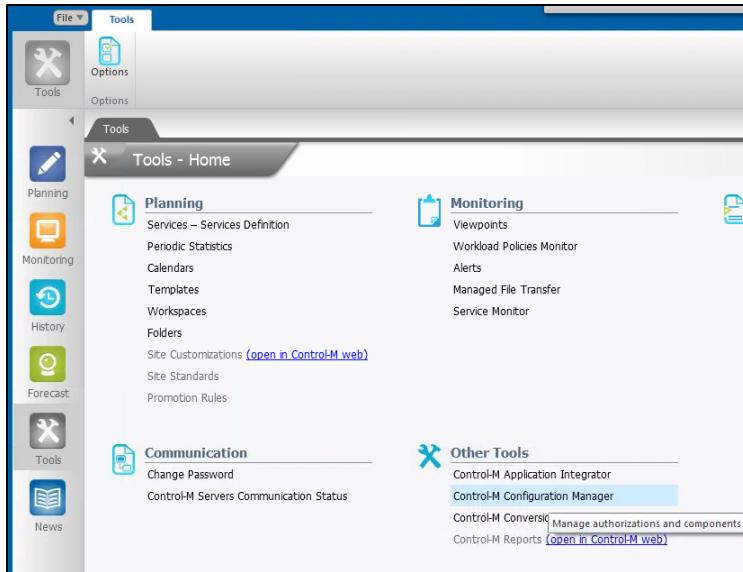
```
linserver% start_all  
Server is already running  
Enter the CONTROL-M/EM DBO password:  
CONTROL-M Configuration Server started successfully !  
  
CONTROL-M/EM Configuration Agent started successfully!  
linserver%
```

Note: If the command doesn't work, it's because the **emuser** hasn't logged out and back in since installing the Control-M/EM. Logout and log back in then run the command once more.

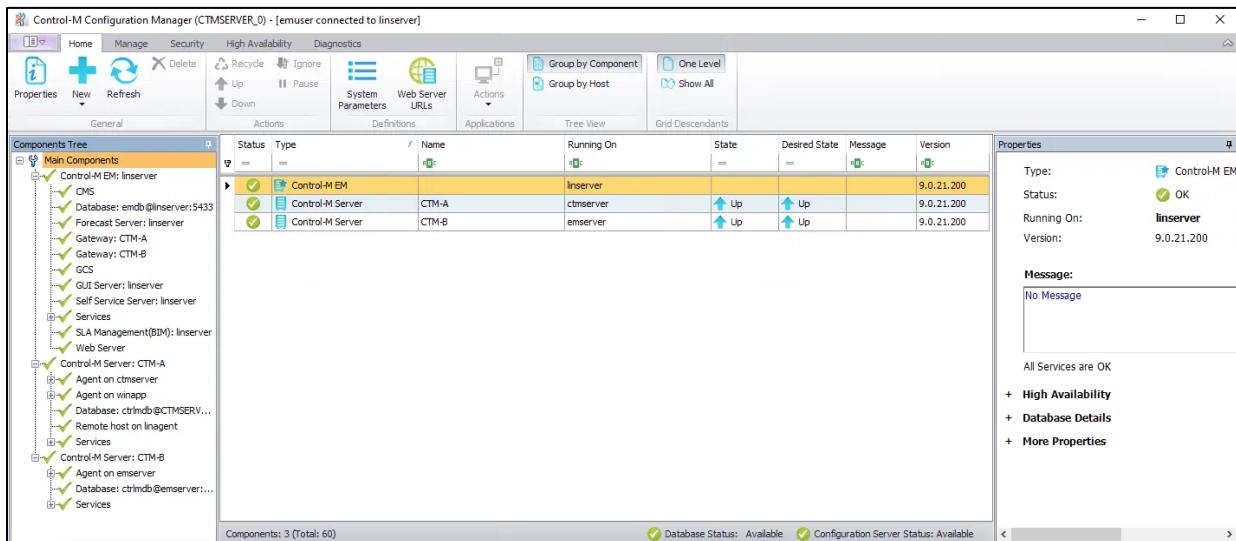
Task 5: Verify the Status of the Control-M/EM Components and the Migrated Job Data

Steps:

1. From the **ctmserver** desktop, open the **Control-M GUI** by double-clicking on **Control-M CTMSERVER_0**.
2. Login as **emuser** with the password: **Passw0rd**.
3. Open the **Tools** domain, then select **Control-M Configuration Manager**.



- When the **CCM** opens verify that all components show as available, noting the inclusion of the Control-M/Servers:

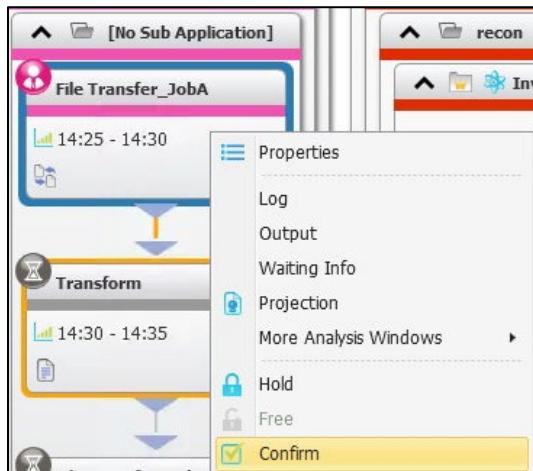


- Return to the **Control-M GUI** and open the **Planning** domain.
- Select **Folders** from the ribbon.

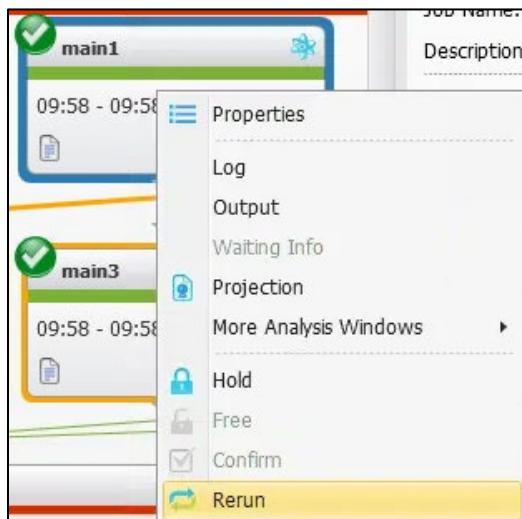
Check if all folders from the source Control-M/EM (**emserver**) are migrated to the target Control-M EM (**linserver**) and synchronized with the Control-M/Servers by observing the **Synchronization State** column. All folders should be synchronized:

Type	Folder Name	Library	Order Method	User Daily	Control-M Server	Checked out by	Synchronization State	Synchronization...	Last Synchroniz...
Inventory			None (Manual Ord...		CTM-B		Synchronized		2/19/2024 1:38 PM
Lab2-1			Automatic (Daily)		CTM-B		Synchronized		2/19/2024 1:39 PM
TransferFiles			None (Manual Ord...		CTM-A		Synchronized		2/19/2024 12:00...

7. Go to the **Monitoring** domain and open the **All Active jobs** viewpoint.
8. Right-click the **File Transfer_JobA** job (under the **CTM-A Control-M/Server**) and **Confirm** it.



9. Verify the job flow runs successfully.
10. Right-click the **main1** job (under the **CTM-B Control-M/Server**) and **Rerun** it.



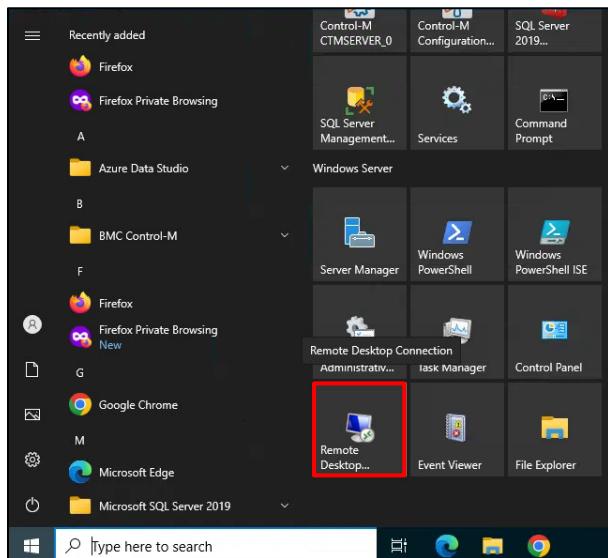
11. Verify the job reruns and completes successfully.

Lab 1.3: Migrating the CTM-B Control-M/Server Automatically

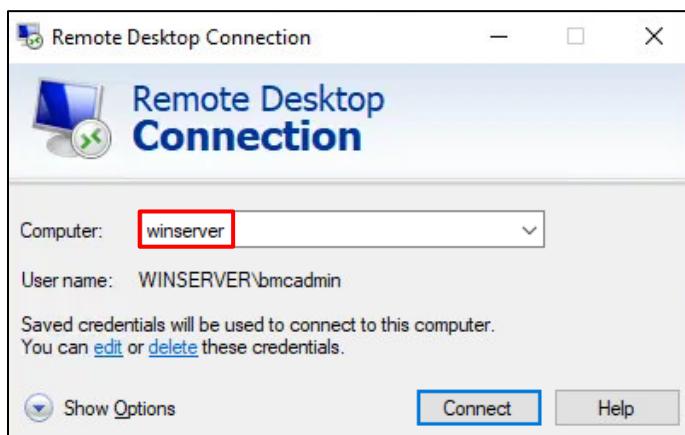
Task 1: Install the Target Control-M/Server onto winserver

Steps:

1. From the landing server (**ctmserver**), click **Start**.
2. Scroll down on the application tiles section to find **Remote Desktop**. Click the **Remote Desktop Connection** icon.



3. From the **Remote Desktop Connection** window that opens, enter **winserver** into the **Computer** field.

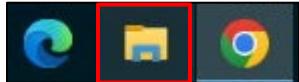


4. Click **Connect**.
5. Enter the password: **Passw0rd**.

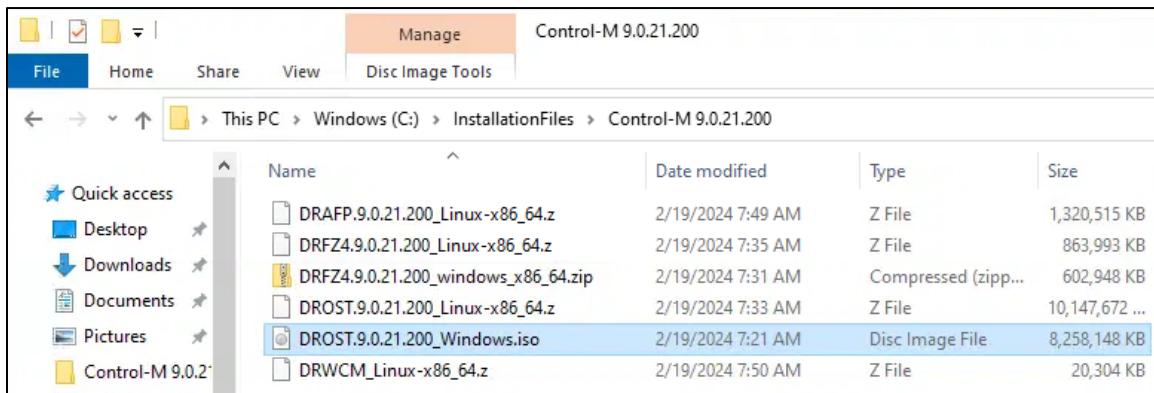
- From the popup that appears, check the **Don't ask me again for connections to this computer** box and click **Yes**.



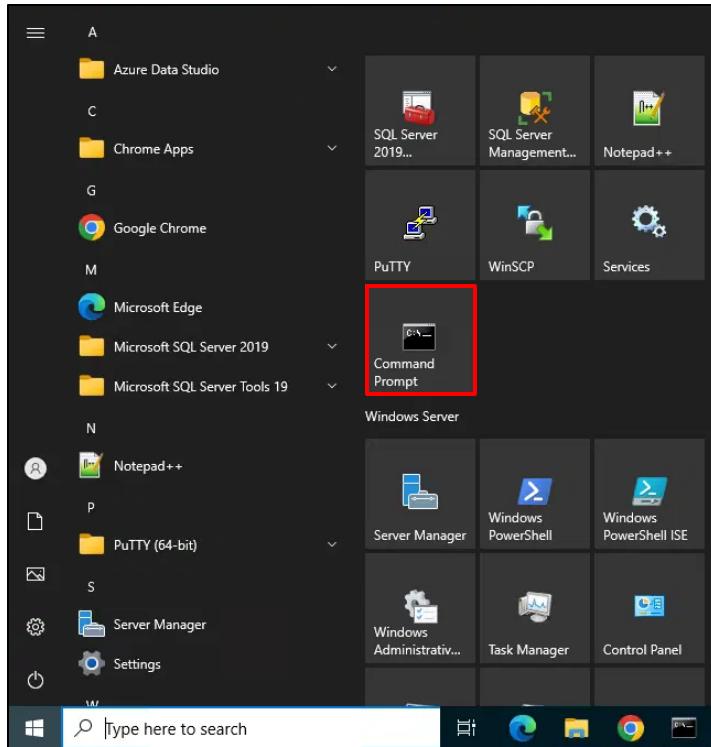
- From the **winserver** host taskbar, open **File Explorer**.



- Browse to **C:\InstallationFiles\Control-M 9.0.21.200**.
- Double-click **DROST.9.0.21.200_Windows.iso** to mount it.



- Open **Start > Command Prompt**.



11. The installation requires Java, which has been installed into the directory **C:\Program Files\Eclipse Adoptium\jre-11.0.20.101-hotspot**. To direct the installer to use this directory, the **BMC_INST_JAVA_HOME** environment variable must be defined. To do so, run the command:

```
set BMC_INST_JAVA_HOME="C:\Program Files\Eclipse Adoptium\jre-11.0.20.101-hotspot"
```

12. Verify the variable is correctly defined by running:

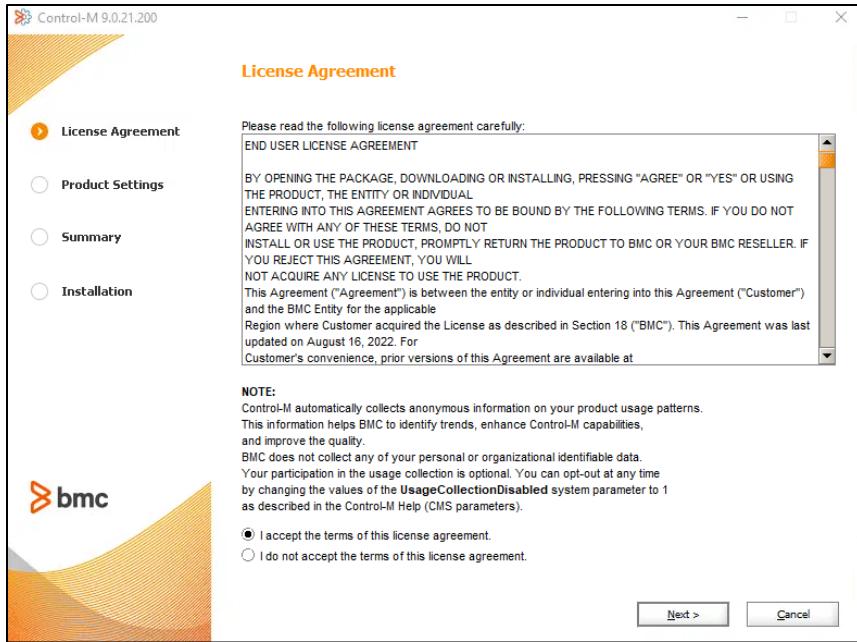
```
echo %BMC_INST_JAVA_HOME%
```

```
C:\Users\bmcadmin>set BMC_INST_JAVA_HOME="C:\Program Files\Eclipse Adoptium\jre-11.0.20.101-hotspot"
C:\Users\bmcadmin>echo %BMC_INST_JAVA_HOME%
"C:\Program Files\Eclipse Adoptium\jre-11.0.20.101-hotspot"
C:\Users\bmcadmin>
```

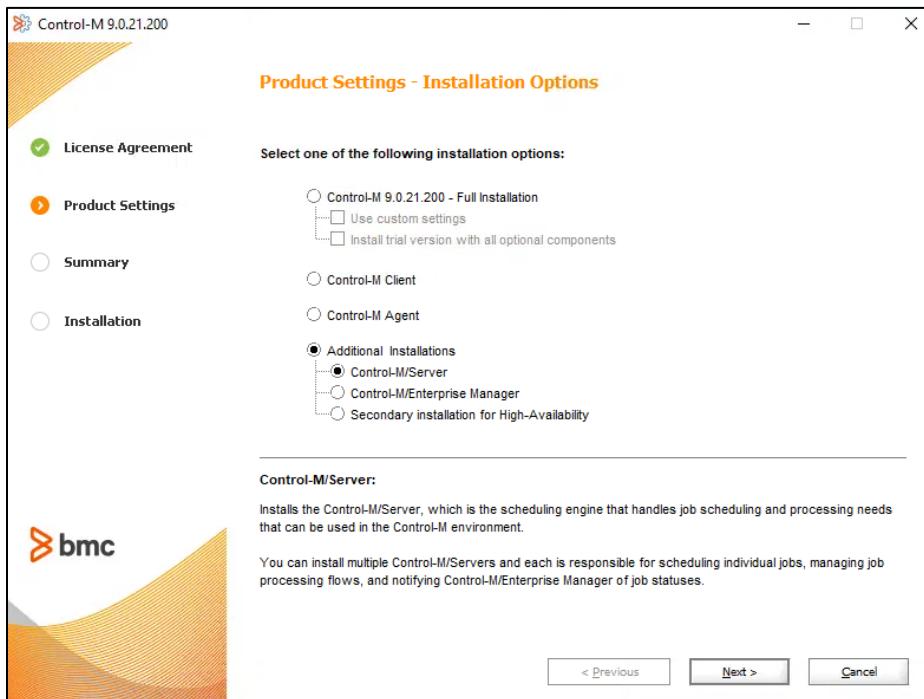
13. Type **E:\setup.exe** to run the installer.

```
C:\Users\bmcadmin>E:\setup.exe
```

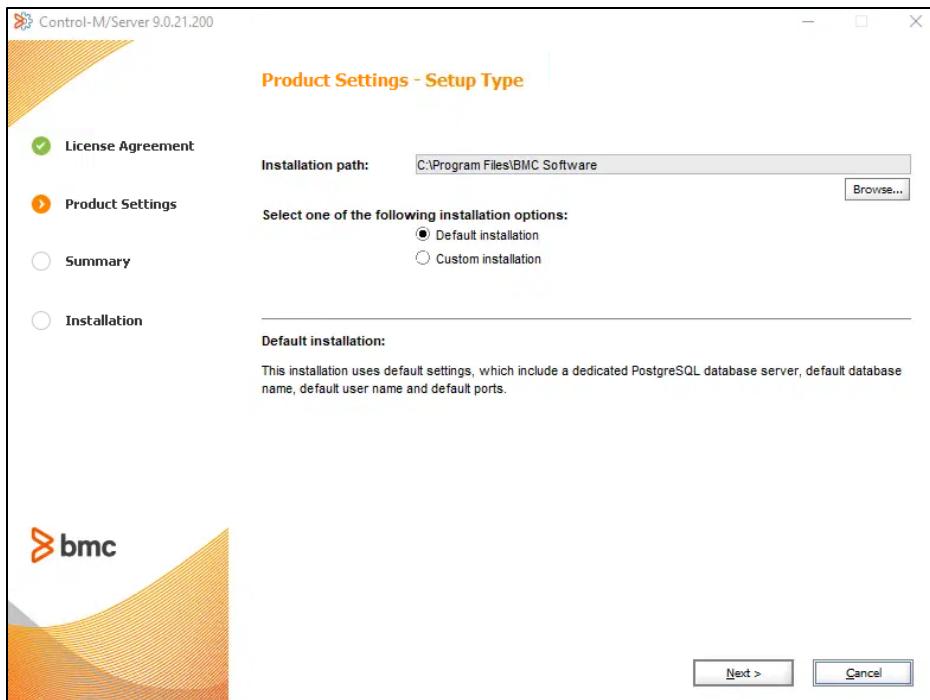
14. Accept the terms of the license agreement and click **Next**.



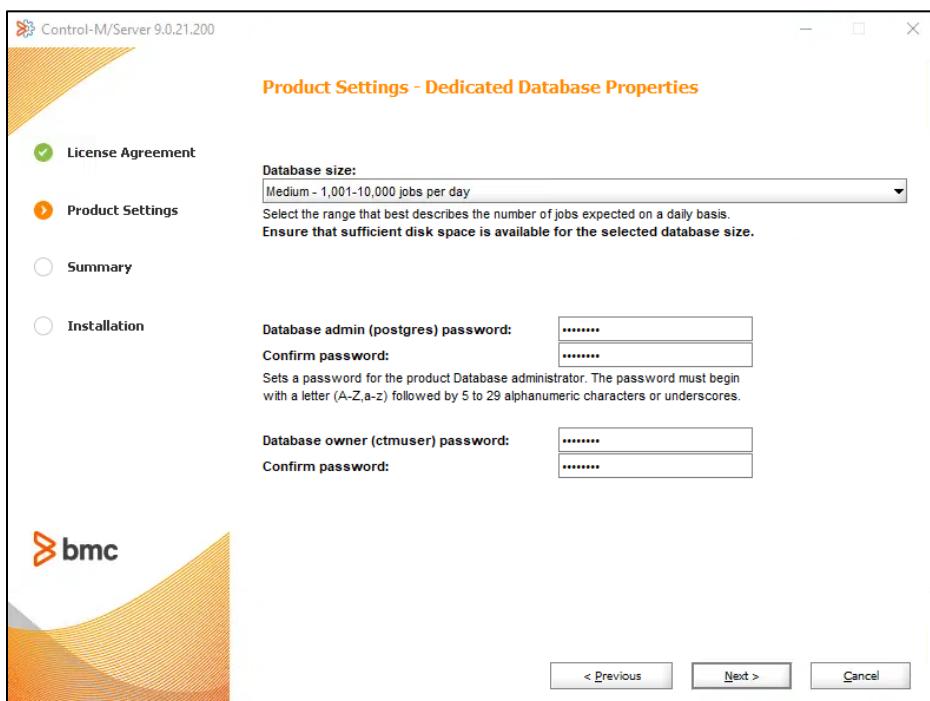
15. From the **Product Settings - Installation Options** page, select **Additional Installations > Control-M/Server** and click **Next**.



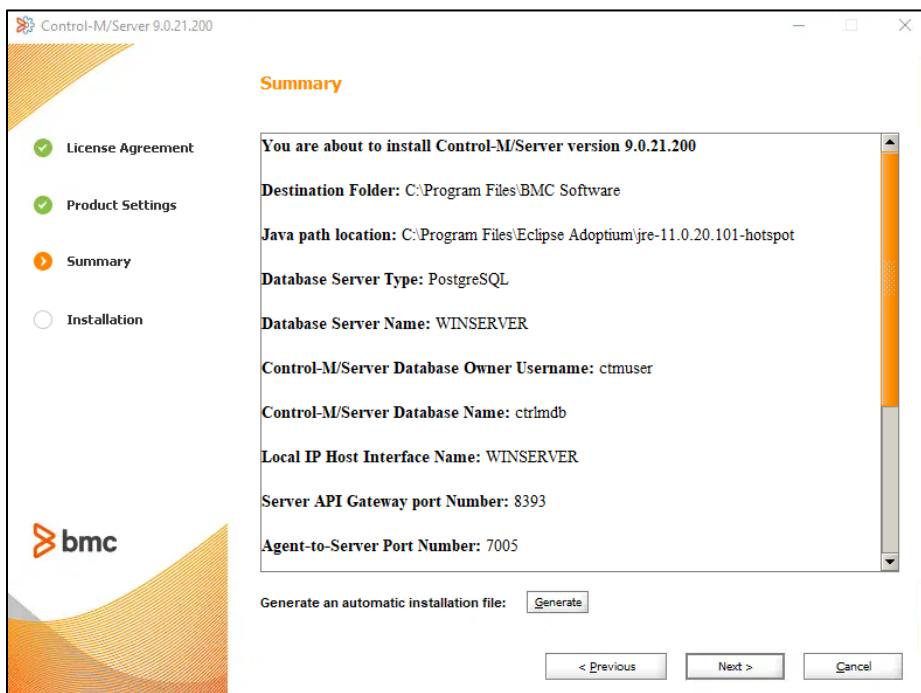
16. From the **Product Settings - Setup Type** page, keep the default values and click **Next**.



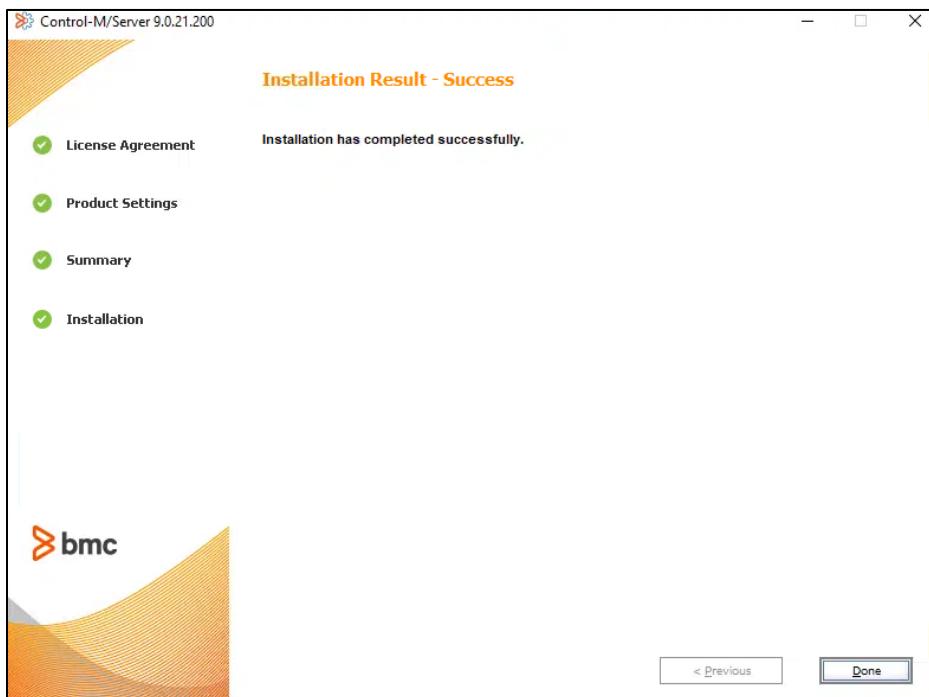
17. From the **Product Settings - Dedicated Database Properties** page, set the **Database admin (postgres)** password to **Passw0rd** and confirm.
18. Set the **Database owner (ctmuser)** password to **Passw0rd** and confirm.
19. Click **Next**.



20. Review the configuration in the **Summary** page and click **Next** to begin the installation.



21. Verify the installation completes successfully and click **Done** to close the window.



Task 2: Migrate the CTM-B Control-M/Server Automatically**Steps:**

1. Remaining on the **winserver** host, click **Start > Command Prompt**.

Note: It is essential to use a new command prompt session and not reuse the same session used to install the Control-M/Server.

2. Switch to the migration directory by typing:

```
cd "C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade\import"
```

3. Run the migration command: **upgrade**.

```
C:\Users\bmcadmin>cd "C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade\import"  
C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade>upgrade
```

4. From the **Control-M/Server Upgrade Menu**, select **1 (Automatic Upgrade)**.

```
=====  
Control-M/Server Upgrade Menu  
=====  
  
1) Automatic Upgrade: Enables you to run the whole upgrade process from the destination Control-M/Server.  
This uses Control-M agentless technology to connect to the source environment to export, transfer and import the Control-M/Server data to the destination.  
With the automatic upgrade you do not have to log on to the source environment to perform the upgrade.  
  
2) Manual Upgrade: Enables you to upgrade by first exporting the source environment, transferring the export file to the destination environment and then running the import from the destination environment.  
With the manual upgrade, you must log on to the source environment to perform the export and then log on to the destination environment to perform the import.  
  
q) Quit  
  
Select an Option:
```

5. Set the parameter values as below:

- **Host Name:** emserver
- **User:** ctmuser
- **Password:** Passw0rd
- **Platform Type:** UNIX
- **Home Directory(location of installed-versions.txt file):** /home/ctmuser/
- **Connection Protocol:** SSH (default)
- **SSH Server Port:** 22 (default)

```
=====
Control-M/Server Upgrade - Automatic Upgrade Settings
=====

Enter the source environment connection parameters:

1) Host Name [emserver]
2) User [ctmuser]
3) Password [*****]
4) Platform Type (UNIX/WINDOWS) [UNIX]
5) Home Directory(location of installed-versions.txt file) [/home/ctmuser/]
6) Connection Protocol (SSH/WMI(WINDOWS only)) [SSH]
7) SSH server port(SSH only) [22]
8) WMI shared directory on source environment(WMI only) []
9) Test connection settings and continue.

r) Return to main menu
q) Quit

Select an Option:9
```

6. Once all details are updated enter **9** to **Test connection settings and continue.**
7. Once the test completes, press **Enter** to continue.

```
Defining "emserver" as source environment...completed successfully
Waiting for source environment to become available(180 seconds timeout)...source environment available
Defining "ctmuser" as source environment owner...completed successfully
Testing connection to source environment...completed successfully
Testing remote execution on source environment.....completed successfully
Testing file transfer from source environment.....completed successfully
Press ENTER to continue.
```

8. To start the **Automatic Migration**, enter **1**.

```
=====
Control-M/Server Automatic Upgrade menu
=====

1) Automatic Migration -
   Migrates historical, definitions, and active data.

r) Return to settings menu.

q) Quit

Select an option:1
```

9. If one or more Control-M/Agents are in an available state on the source Control-M/Server, then you will be prompted to add the target Control-M/Server host to the Authorized Server list for those Agents.

Enter **YES** and press **Enter**.

```
Validation will not be executed.
No validation required when upgrading from version 9.0.21

.....
.....
.....
one or more agents were found available and have version 640 FP4 or above.
You can find the agents list at "C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade\import\remote_files\rh_emserverAuthorized_agents.txt".
Updating agents may take a long time.
Do you want to add the destination environment name to the authorized Server for those agents?<YES/NO>YES
```

10. When prompted, **When do you plan to upgrade active environment**, enter **NOW** to import the active data immediately.

```
Security definitions for BIM/GCS/CTMSYNC users updated successfully.
Importing Keys ended successfully.
Remedy parameters updated successfully.
Configuring new parameters ended successfully.
Update fields for constraint ended successfully.
Delete invalid rows from DB ended successfully.
Import of TimeZone.dat file ended successfully.

.....
.....
When do you plan to upgrade active environment(requires source environment shut down)?<NOW|LATER|NEVER>NOW
```

11. When prompted **Would you like to shut down the source Control-M Server** to enable the migration of active data, enter **YES**.

```
For export of active environment Control-M Server on source(production) environment must be down.
Would you like to shut down the Control-M Server ?<YES/NO>YES
```

12. Once the import completes, press **Enter** to continue.

```
=====
Upgrade process summary.
=====

Upgrade process Start time(Starting of upgrade toolkit): 2024\04\11 10:51
Upgrade process End time: 2024\04\11 11:10
Source environment CONTROL-M/Server downtime: 00:03:38

***Upgrade completed successfully
***All data from source environment transferred successfully.
***Control-M/Server on source environment is down.
***Control-M/Server on destination environment is down and waiting for startup.
***Destination environment machine name added to list of authorized servers on Control-M/Agents version 6.4.01.400 and above.
  You can find a list of updated Control-M/Agents version 6.40 FP4 and above in 'upgrade/import/output/definition/data/authorized_agents' file
***Please verify that destination environment machine name added to list of authorized servers on the Control-M/Agents version lower than 6.4.01.400
***Local agent could be unavailable if default Server to Agent port was different between source and destination environments.
***For more information,please see the CONTROL-M/Server Upgrade Guide.

Press ENTER to continue.
```

13. Run the command **start_ctm && start_ca** to start the Control-M/Server and Control-M/Server Configuration Agent services.

```
C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade\import>start_ctm && start_ca
-----
Starting CONTROL-M.
-----
CONTROL-M/Server Pause mode is N
-----
Starting CONTROL-M Configuration Agent
-----
C:\Program Files\BMC Software\Control-M Server\ctm_server\upgrade\import>
```

14. Return to the **ctmserver** host by, minimizing or closing the **Remote Desktop** window from the blue **Remote Desktop Connection** bar at the top of the screen.

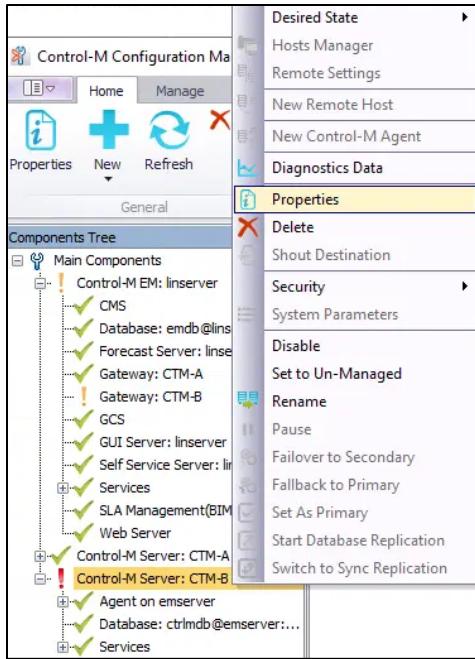
Note, this may be partially or totally obstructed by the gray **ReadyTech Access** bar. Click and drag either bar (**ReadyTech Access** or the **Remote Desktop Connection**) to display both side-by-side:



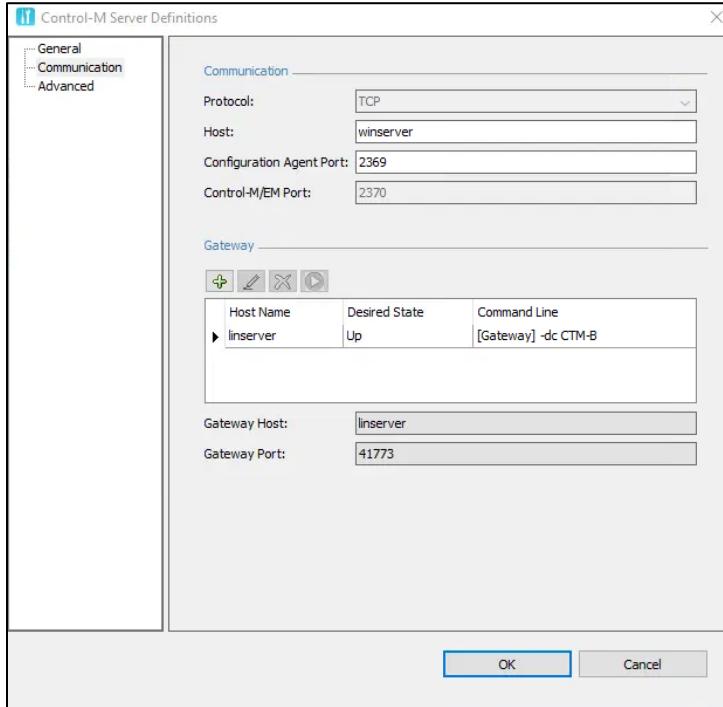
Task 3: Connect the Gateway to the New Control-M/Server

Steps:

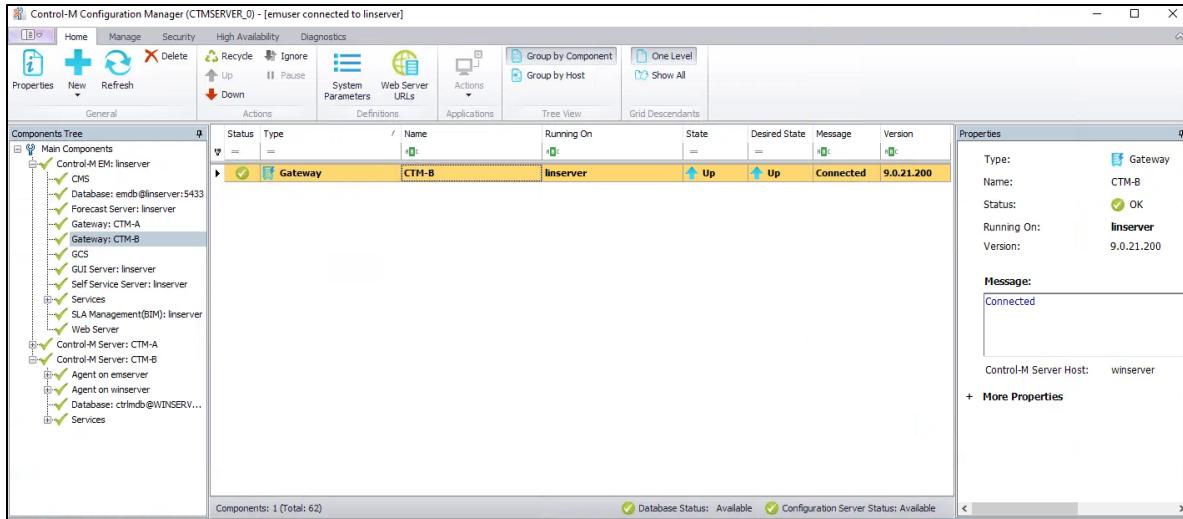
1. From the landing server (**ctmserver**) desktop, double-click the **Control-M Configuration Manager** icon.
2. Sign in as **emuser** with the password: **Passw0rd**.
3. From the **Components Tree**, right-click the **Control-M Server: CTM-B** and select **Properties**.



4. From the **Control-M Server Definitions** dialog box that appears, select **Communication**.
5. Update the **Host** value from **emserver** to **winserver**, and then click **OK**.



6. Recycle the gateway.

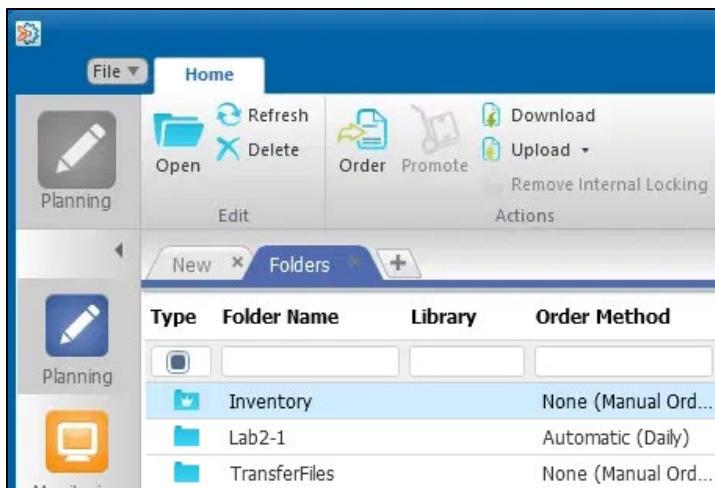


Task 4: Verify the Control-M/Server Jobs on CTM-B Run

In Lab 1.1 the Inventory folder on the CTM-B server was ordered and verified. As the OS platform has changed, the jobs need updating before verifying.

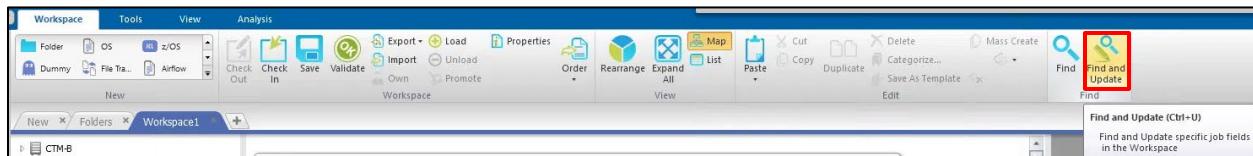
Steps:

- From the **ctmserver** desktop, open the **Control-M GUI** by double-clicking on **Control-M CTMSERVER_0**.
- Login as **emuser** with the password: **Passw0rd**.
- Select the **Planning** domain and open **Folders** from the ribbon.

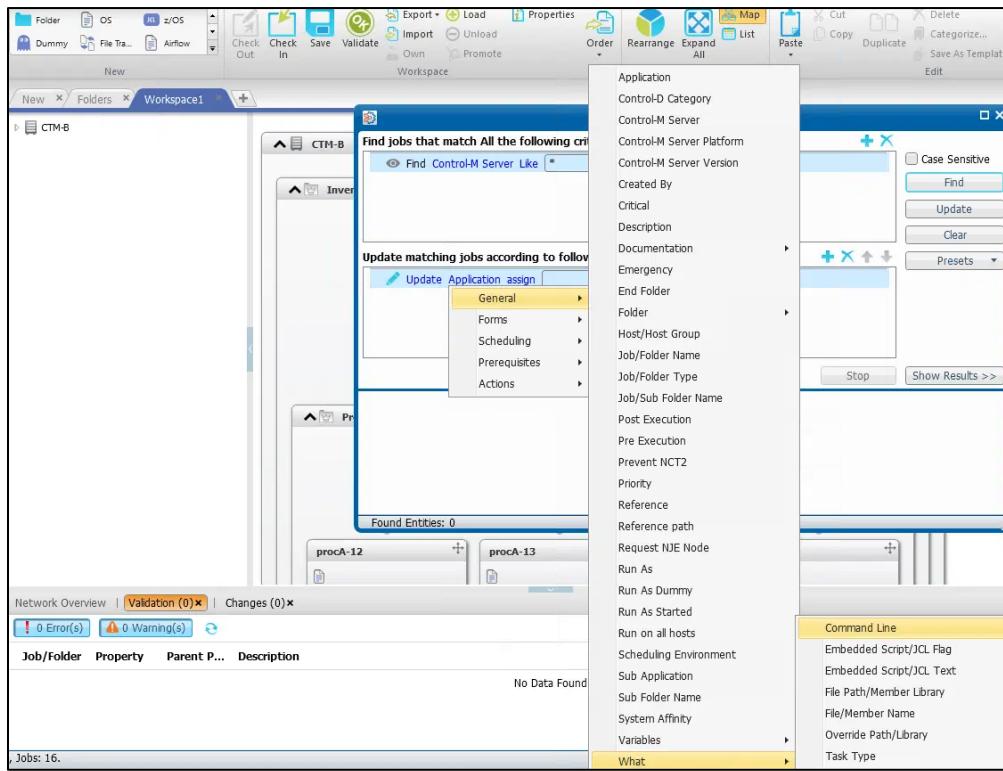


- Double-click the **Inventory** folder to open it into a workspace.
- Click **Check Out** from the ribbon.

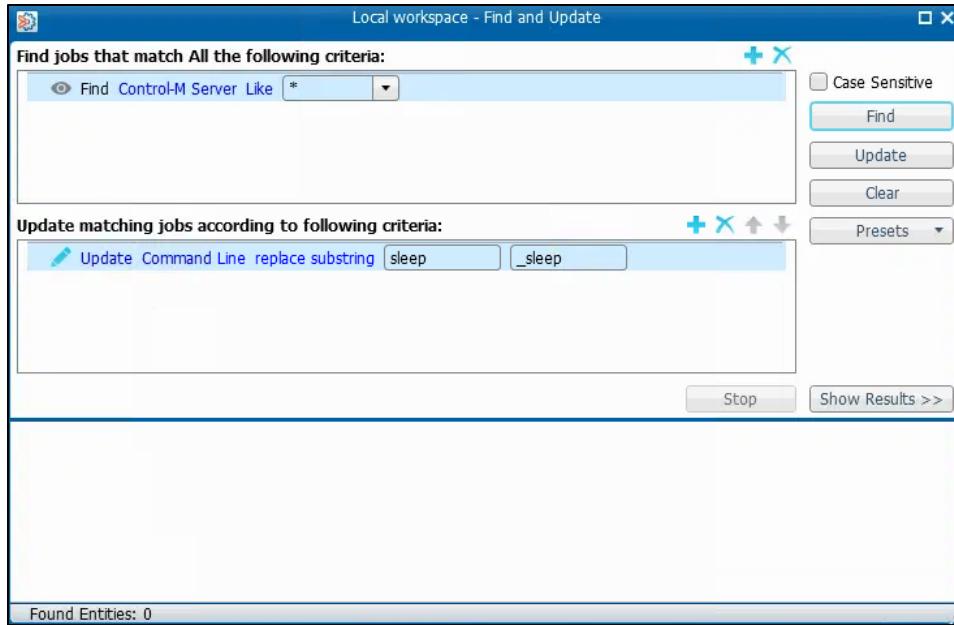
6. Open **Find and Update** from the **Workspace** tab on the ribbon.



7. From the **Update matching jobs according to following criteria** section, click the **New (+)** icon.
8. Click **Application** and change it to **General > What > Command Line**.



9. Change **assign** to **replace substring**.
10. Set the first value to **sleep** and the second value to **_sleep**.



11. Click **Update**, then close the **Find and Update** window.

The screenshot shows the 'Local workspace - Find and Update' window with the 'Find' and 'Update' sections visible. To the right, a detailed configuration panel for a job named 'procA-12' is open. The 'General' tab is selected, showing the following details:

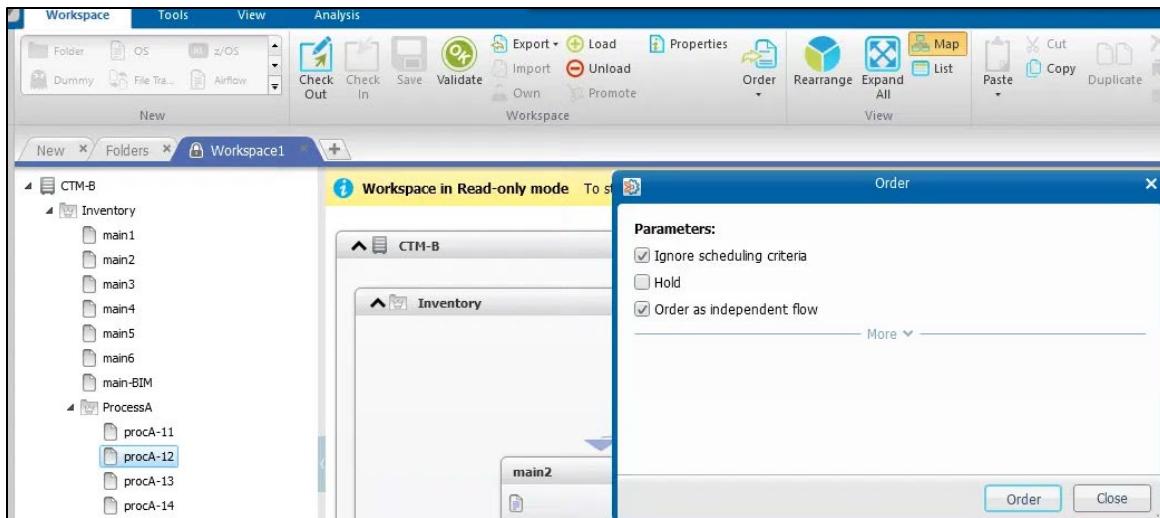
- Job Type:** OS
- Job Name:** procA-12
- Description:** (empty)
- Run as Dummy:** (unchecked)
- What:** Command
- Command:** _sleep 10
- Host/Host Group:** (empty)
- Control-M Server:** CTM-B
- Run As:** emuser
- Parent Folder:** Inventory/ProcessA
- Application:** Inventory
- Sub Application:** recon

At the bottom left of the main window, the 'Update Results' section shows the following statistics:

- Found Entities: 19
- Updated Entities: 15
- Invalid Entities: 0
- Skipped Entities: 4

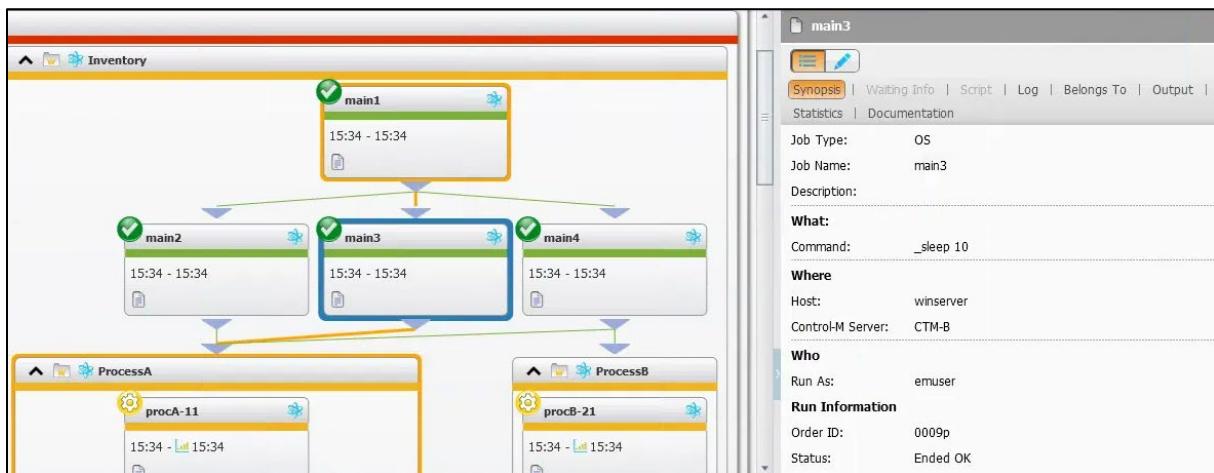
12. From the ribbon, **Check In** the workspace.

13. **Order** the workspace.



14. Switch to the **Monitoring** domain and open the **All Active Jobs** viewpoint.

15. Verify the updated jobs run successfully.



Task 5: Uninstall the Control-M/Enterprise Manager on emserver

Once the target Control-M/EM has been verified, the source environment can be removed. The reason for doing so in the labs is due to this host being used as a Distributed Control-M/EM in Module 2.

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **PuTTY**.
2. Double-click **emserver** in the **Saved Sessions** section.
3. Login as **emuser**, with the password: **Passw0rd**.
4. Execute the uninstallation script by typing:
/home/emuser/BMCINSTALL/uninstall/DRNFT.9.0.21.200/uninstall.sh

```
login as: emuser
emuser@emserver's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Apr 11 11:27:55 2024 from 192.168.1.5
emserver% /home/emuser/BMCINSTALL/uninstall/DRNFT.9.0.21.200/uninstall.sh
```

5. Type Y to confirm the uninstaller should continue in non-graphical mode.

```
emserver% /home/emuser/BMCINSTALL/uninstall/DRNFT.9.0.21.200/uninstall.sh
[ Starting Control-M Managed File Transfer Deployment Package 9.0.21.200 uninstall ]
[ Control-M Managed File Transfer Deployment Package 9.0.21.200 uninstall completed successfully ]
Starting graphical user interface...

The $DISPLAY environment variable is not defined.

Uninstall will continue in non graphical mode.
Are you sure you want to continue?
== <N> No  <Y> Yes ==

Enter command:
Y
```

6. Type Y to confirm the uninstallation of the Control-M/EM.

```
emserver% /home/emuser/BMCINSTALL/uninstall/DRNFT.9.0.21.200/uninstall.sh
[ Starting Control-M Managed File Transfer Deployment Package 9.0.21.200 uninstall ]
[ Control-M Managed File Transfer Deployment Package 9.0.21.200 uninstall completed successfully ]
Starting graphical user interface...

The $DISPLAY environment variable is not defined.

Uninstall will continue in non graphical mode.
Are you sure you want to continue?
== <N> No  <Y> Yes ==

Enter command:
Y
[ Starting Control-M/Enterprise Manager 9.0.21.200 uninstall ]
Warning: sql_out=`echo "select datname from pg_database where datname not like 'template%'" | InstallRunCommand -t -q | tr -d " " | grep -v '^postgres$' | grep -v "^${ECS_DATABASE}\$"`
There are additional databases on this server: ctrlmdb
Are you sure you want to proceed? (Yes/No) [N]:Y
```

7. Verify the uninstallation completes successfully.

```
[ Control-M/Enterprise Manager 9.0.21.200 uninstall completed successfully ]  
emserver% [REDACTED]
```

Module 2: Installing an Additional Distributed Control-M/Enterprise Manager

Objective:

- Install a Distributed Control-M/Enterprise Manager on emserver

Lab 2.1: Installing a Distributed Control-M/EM on emserver

Task 1: Install a Distributed Control-M/Enterprise Manager on emserver

Steps:

1. From the landing server (**ctmserver**) desktop, double-click the **PuTTY** icon.

Note: As the configuration has changed, use a new **PuTTY** session.
2. Double-click **emserver** from the **Saved Sessions** section.
3. Sign in as **emuser** with the password: **Passw0rd**.
4. The installation files have been unpacked and placed into the **InstallationFiles/DROST.9.0.21.200_Linux** directory. Switch into it by running the command:
cd InstallationFiles/DROST.9.0.21.200_Linux

```
login as: emuser  
[emuser@emserver ~]$ cd InstallationFiles/DROST.9.0.21.200_Linux  
[emuser@emserver DROST.9.0.21.200_Linux]$ [REDACTED]
```

5. The installation requires **Java**, which has been installed into the directory **/home/emuser/OpenJDK/jdk-11.0.19+7-jre/**. To direct the installer to use this directory,

the **BMC_INST_JAVA_HOME** environment variable must be defined. To do so, run the command:

```
setenv BMC_INST_JAVA_HOME /home/emuser/OpenJDK/jdk-11.0.19+7-jre/
```

- Verify the variable is correctly defined by running:

```
echo $BMC_INST_JAVA_HOME
```

```
[emuser@emserver DROST.9.0.21.200_Linux]$ setenv BMC_INST_JAVA_HOME /home/emuser/OpenJDK/jdk-11.0.19+7-jre/  
[emuser@emserver DROST.9.0.21.200_Linux]$ echo $BMC_INST_JAVA_HOME  
/home/emuser/OpenJDK/jdk-11.0.19+7-jre/  
[emuser@emserver DROST.9.0.21.200_Linux]$ █
```

- Type **./setup.sh** to run the installer:

```
[emuser@emserver DROST.9.0.21.200_Linux]$ ./setup.sh  
Starting graphical user interface...  
  
The $DISPLAY environment variable is not defined.  
  
Install will continue in non graphical mode.  
Are you sure you want to continue?  
== <N> No <Y> Yes ==  
  
Enter command:  
█
```

- Confirm the installation should continue in non-graphical mode by typing **Y**.
- Type **S** to skip the **License Agreement** section.
- Type **Y** to agree to the **License Agreement**.

```
"Territory" means the country(ies) where Customer is licensed to install the Product as specified in the Order.  
2. SCOPE. Licenses are granted, and Support is obtained, solely by execution of Orders. Each Order is deemed to be a discrete contract, separate from each other Order, unless expressly stated otherwise therein, and in the event of a direct conflict between any Order and the terms of this  
  
Press <Enter> to continue or <S> to skip: S  
  
Do you accept and agree to the terms of this Software License Agreement (Y/N) ?Y█
```

- Press **Enter** to dismiss the **Usage Collection** notification.

NOTE:
Control-M automatically collects anonymous information on your product usage patterns. This information helps BMC to identify trends, enhance Control-M capabilities, and improve the quality.
BMC does not collect any of your personal or organizational identifiable data. Your participation in the usage collection is optional. You can opt-out at any time by changing the values of the UsageCollectionDisabled system parameter to 1 as described in the Control-M Help (CMS parameters).
== <Enter> Continue ==

12. On the **Product Settings : Installation Options** page, use option 3 to select **Additional Installations**.

13. Select option 2 - **Control-M/Enterprise Manager**.

```
==== Control-M 9.0.21.200 Installation ====  
  
==== Product Settings : Installation Options ====  
  
1 : ( ) Control-M 9.0.21.200 - Full Installation  
      Use custom settings (y/n)?  
      Install trial version with all optional components (y/n)?  
2 : ( ) Control-M Agent  
3 : (x) Additional Installations  
      ( ) Control-M/Server  
      (x) Control-M/Enterprise Manager  
      ( ) Secondary installation for High-Availability  
  
== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==  
Enter command or item number you wish to change: █
```

14. Press **Enter** to move to the next panel.

15. On the **Product Settings : Setup Type** page, select option 3 - **Additional distributed installation**.

```
==== Control-M/Enterprise Manager 9.0.21.200 Installation ====

==== Product Settings : Setup Type ===

1 : ( ) Default installation
2 : ( ) Custom installation
3 : (x) Additional distributed installation

== <C> Cancel <N>/<Enter> Next Panel ==

Enter command or item number you wish to change: █
```

16. Press **Enter** to move to the next panel.
17. As the primary Control-M/EM database server is PostgreSQL, which is already selected under **Database Server Type**, press **Enter** to move to the next panel.
18. Select option **1 - Host interface name** and set the value to **linserver**.
19. Select option **2 - DB server Port number** and set the value to **5432**.

```
==== Control-M/Enterprise Manager 9.0.21.200 Installation ===

==== Product Settings : BMC Software Database Advanced Parameters ===

1 : Host interface name: linserver
2 : DB server Port number: 5432

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==

Enter command or item number you wish to change: █
```

20. Press **Enter** to move to the next panel.
21. Select option **2 - Database owner password** and set the value to **Passw0rd**.

```
==== Control-M/Enterprise Manager 9.0.21.200 Installation ====

==== Product Settings : Database Properties ===

1 : Database owner username: emuser
2 : Database owner password: *****
3 : SSL certificate path (required only for TLS):

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==

Enter command or item number you wish to change: █
```

22. Press **Enter** to move to the next panel.
23. Review the details on the **Summary** page, and when ready to start the installation, press **Enter**.
24. Verify the installation completes successfully.

```
==== Control-M/Enterprise Manager 9.0.21.200 Installation ====

==== Installation Result - Success ===

Installation has completed successfully.

Note:

To start working with Control-M/Enterprise Manager, you must close
the current session and open a new one.

[emuser@emserver DROST.9.0.21.200_Linux]$ █
```

25. When the installation completes, the automatic startup file should be configured.
In this environment the service file has already been defined, it simply needs enabling. To do so type **su** to switch to the **root** user and enter the password: **password**.
26. Type **systemctl daemon-reload**.
27. Type **systemctl enable EM.service**.

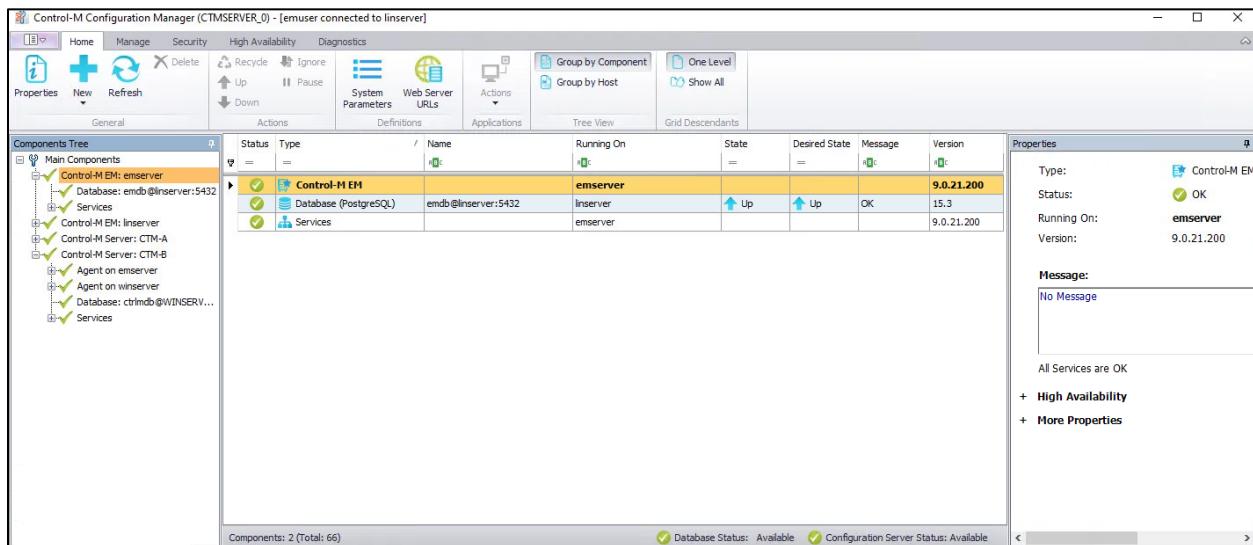
```
[emuser@emserver DROST.9.0.21.200_Linux]$ su
Password:
[root@emserver DROST.9.0.21.200_Linux]# systemctl daemon-reload
[root@emserver DROST.9.0.21.200_Linux]# systemctl enable EM.service
Created symlink /etc/systemd/system/multi-user.target.wants/EM.service → /etc/systemd/system/EM.service.
[root@emserver DROST.9.0.21.200_Linux]#
```

28. Type **exit** to logout from the **root** account.
29. Type **logout** to logout from the **PuTTY** session.

Task 2: Verify the Distributed Control-M/Enterprise Manager Installation

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **Control-M Configuration Manager CTMSERVER_0**.
2. Log in as **emuser** with the password: **Passw0rd**.
3. Verify that two Control-M/Enterprise Managers appear in the **Components Tree**, and all components show as **Up**.



Module 3: Workload Archiving Installation

Objectives:

- Install the Control-M Workload Archiving Server onto the Distributed Control-M/Enterprise Manager: emserver
- Define a Workload Archiving Policy
- Search for Archive Data in the Control-M GUI

Lab 3.1: Installing Control-M Workload Archiving on emserver

Task 1: Install the Control-M Workload Archiving Add-On

Steps:

1. From the landing server (**ctmserver**) **Desktop**, double-click **PuTTY**.
2. From the **Saved Sessions** section, double-click **emserver**.
3. Sign in as **emuser** with the password: **Passw0rd**
4. The installation files have been unpacked and placed into the **InstallationFiles/DRARB_Linux/** directory. Switch into it by running the command:
cd InstallationFiles/DRARB_Linux/

```
login as: emuser
[emuser@emserver ~]$ emuser@emserver's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Apr 11 14:30:21 2024 from 192.168.1.5
emserver% cd InstallationFiles/DRARB_Linux/
emserver%
```

5. Type **./setup.sh** to run the installer:

```
emserver% ./setup.sh
Starting graphical user interface...

The $DISPLAY environment variable is not defined.

Install will continue in non graphical mode.
Are you sure you want to continue?
== <N> No  <Y> Yes ==

Enter command:
Y
```

6. Confirm the installation should continue in non-graphical mode by typing **Y**.
7. Type **S** to skip the **License Agreement** section.
8. Type **Y** to agree to the **License Agreement**.

```
"Territory" means the country(ies) where Customer is licensed to install the Product as specified in the Order.
2. SCOPE. Licenses are granted, and Support is obtained, solely by execution of Orders. Each Order is deemed to be a discrete contract, separate from each other Order, unless expressly stated otherwise therein, and in the event of a direct conflict between any Order and the terms of this

Press <Enter> to continue or <S> to skip: S

Do you accept and agree to the terms of this Software License Agreement (Y/N)? Y
```

9. On the **Product Settings : Database Server Type** page, retain the default database server (**PostgreSQL**) and press **Enter** to move to the next panel.

```
== Control-M Workload Archiving Installation ===

== Product Settings : Database Server Type ===

1 : Database Server Type
  (x) PostgreSQL
  ( ) Oracle

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==
Enter command or item number you wish to change: Y
```

10. From the **Product Settings: Database Server Setup Type** page, again retain the default setting (**Install a BMC-supplied PostgreSQL database server dedicated to Control-M Workload Archiving**) and press **Enter** to move to the next panel.

```
==== Control-M Workload Archiving Installation ====  
  
==== Product Settings : Database Server Setup Type ====  
  
1 : Database Server Setup Type  
  
(x) Install a BMC-supplied PostgreSQL database server dedicated to  
     Control-M Workload Archiving  
  
( ) Install a new database on an existing PostgreSQL  
     database server  
  
== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==  
  
Enter command or item number you wish to change: █
```

11. Select option 4 - **Database admin password**, set the value to **Passw0rd** and confirm.
12. Select option 5 - **Database owner (archive) password**, set the value to **Passw0rd** and confirm.

```
==== Control-M Workload Archiving Installation ===

==== Product Settings : BMC Control-M Workload Archiving ===

Host interface name: emserver

1 : Database server Port number: 5432

2 : Database size

    (x) Large database (recommended)

    ( ) Small database

System directory full path: /home/emuser/ctm_em/archive/pgsql/data

3 : Database admin name: postgres

4 : Database admin password: *****

5 : Database owner (archive) password: *****

== <C> Cancel <P> Previous Panel <N>/<Enter> Next Panel ==

Enter command or item number you wish to change: █
```

13. Press **Enter** to move to the next panel.
14. Review the details from the **Summary** page and when ready press **Enter** to begin the installation.
15. Verify the installation completes successfully.

```
==== Control-M Workload Archiving Installation ===

==== Installation Result - Success ===

Installation has completed successfully.

Note:

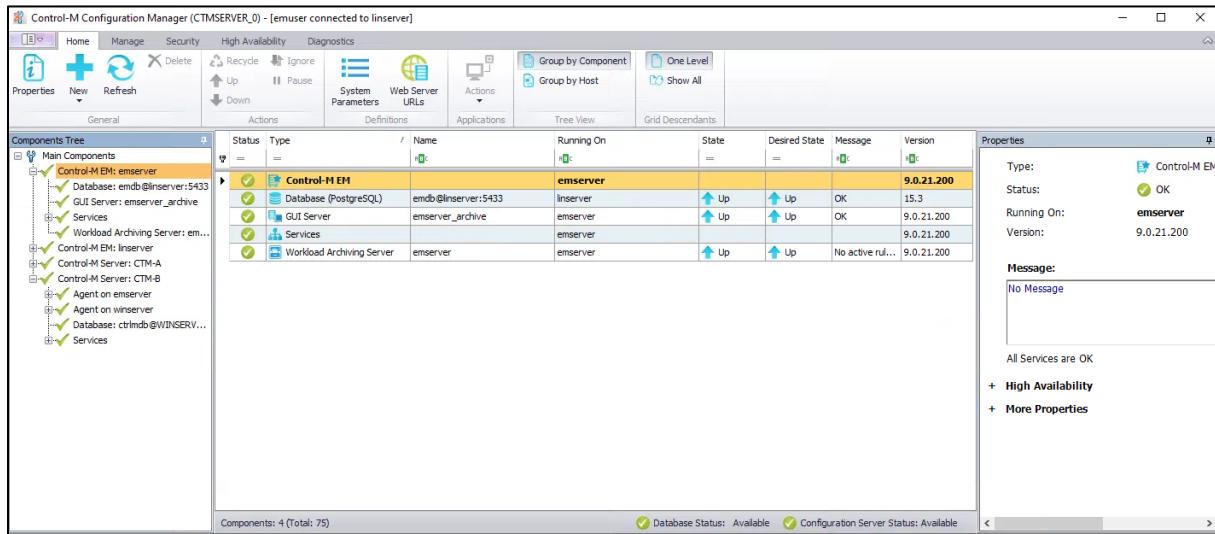
To start working with Control-M Workload Archiving you must
close the current session and open a new one.

emserver% █
```

Task 2: Verify the Workload Archiving Installation

Steps:

- From the landing server (**ctmserver**), double-click **Control-M Configuration Manager CTMSERVER_0**.
- Log in as **emuser** with the password: **Passw0rd**.
- Verify that the **Control-M EM: emserver** host now contains a **GUI Server** and **Workload Archiving Server**, with both components set to **Up**.



Task 3: Update the Automatic Startup and Shutdown Procedure for the Workload Archiving Server Host

With the Control-M Workload Archiving Server installed, the automatic startup/shutdown procedure needs to be updated so that the PostgreSQL database that is dedicated to Workload Archiving is started up and shut down automatically.

Steps:

- From the landing server (**ctmserver**) **Desktop**, double-click **PuTTY**.
- From the **Saved Sessions** section, double-click **emserver**.
- Sign in as **root** with the password: **password**
- Edit the service file by typing:
vi /etc/systemd/system/EM.service

```

login as: root
root@emserver's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed May 22 10:54:43 2024
[root@emserver ~]# vi /etc/systemd/system/EM.service

```

5. Use the arrow keys to move to the **ExecStart** line, then across to the text **start_server**.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c start_server;start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown; /home/emuser/bin/stop_
server
[Install]
WantedBy=multi-user.target
~
```

6. Use the **x** key repeatedly (12 times) to delete the text **start_server**.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown; /home/emuser/bin/stop_
server
[Install]
WantedBy=multi-user.target
~
```

Note: If you make a mistake, use the **i** key to enter **insert mode**, and type the deleted text.

7. Ensure the cursor has the semicolon (;) before the **start_config_agent** command highlighted. Use the **i** key to enter **insert mode**.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown; /home/emuser/bin/stop_
server
[Install]
WantedBy=multi-user.target
~
~
~
-- INSERT --
```

8. Insert the following text:

'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart'

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart';start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown; /home/emuser/bin/stop_server
[Install]
WantedBy=multi-user.target
~
~
-- INSERT --
```

9. Use the arrow keys to move to the **ExecStop** line, then across to the text **/home/emuser/bin/stop_server**.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart';start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown; /home/emuser/bin/stop_server
[Install]
WantedBy=multi-user.target
~
~
-- INSERT --
```

10. Use the **delete** key to delete the text **/home/emuser/bin/stop_server**.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart';start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em ctl -mcs -C Config_Agent -M emserver -cmd shutdown;
[Install]
WantedBy=multi-user.target
~
~
-- INSERT --
```

11. Insert the following text (after the semicolon next to the **shutdown** command):
'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStop'

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart';start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em_ctl -mcs -C Config_Agent -M emserver -cmd shutdown; 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStop'
[Install]
WantedBy=multi-user.target
~
-- INSERT --
```

12. Exit insert mode by pressing the **escape** key.
13. Type **:wq!** to write and quit the file.

```
[Unit]
Description=Control-M/EM
After=systemd-user-sessions.service multi-user.target network.target
[Service]
ExecStart=/bin/sudo -u emuser /bin/csh -c 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStart';start_config_agent
Type=forking
RemainAfterExit=yes
ExecStop=/bin/sudo -u emuser /bin/csh -c /home/emuser/bin/em_ctl -mcs -C Config_Agent -M emserver -cmd shutdown; 'arc /home/emuser/ctm_em/archive/bin/DBUtils/DBUStop'
[Install]
WantedBy=multi-user.target
~
:wq!
```

14. As the configuration has changed, the file needs reloading. Type the command:
systemctl daemon-reload
15. Test the updated service file works by running:
systemctl restart EM.service

```
[root@emserver ~]# systemctl daemon-reload
[root@emserver ~]# systemctl restart EM.service
[root@emserver ~]#
```

16. If no errors are produced, the service file has been correctly updated. If not, compare the above screenshots to your configuration and adjust accordingly.

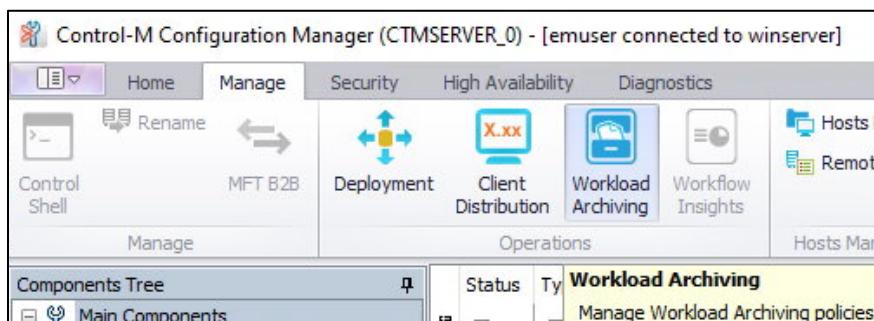
Lab 3.2: Defining Workload Archiving Policies

Task 1: Define an Archiving Policy

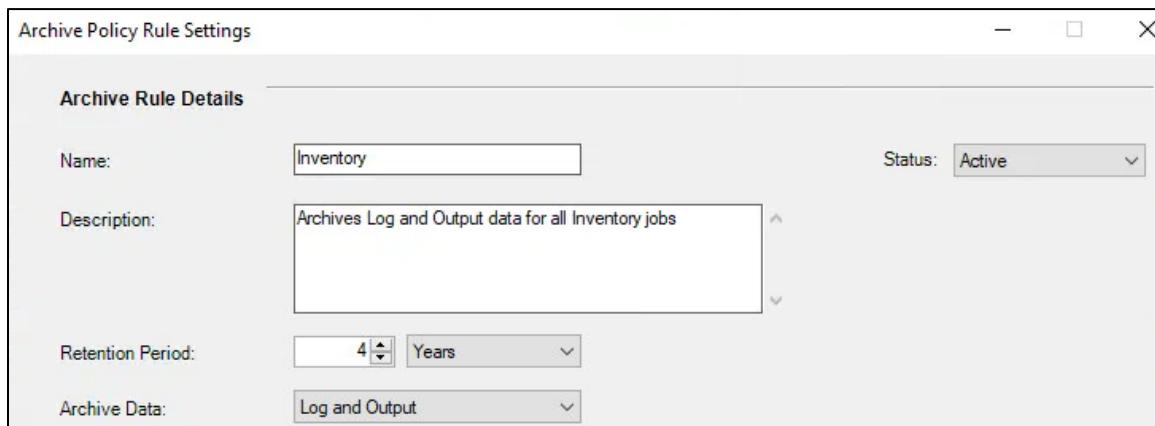
Steps:

1. Sign into the **CCM** as **emuser** with the password: **Passw0rd**.
2. From the **Manage** tab, click **Workload Archiving**. The **Workload Archiving Configuration** window is displayed.

If the window does not show, either log out and back into the **CCM**, or right-click the **Workload Archiving Server** component and select **Configuration** to open the **Workload Archiving Configuration** window.

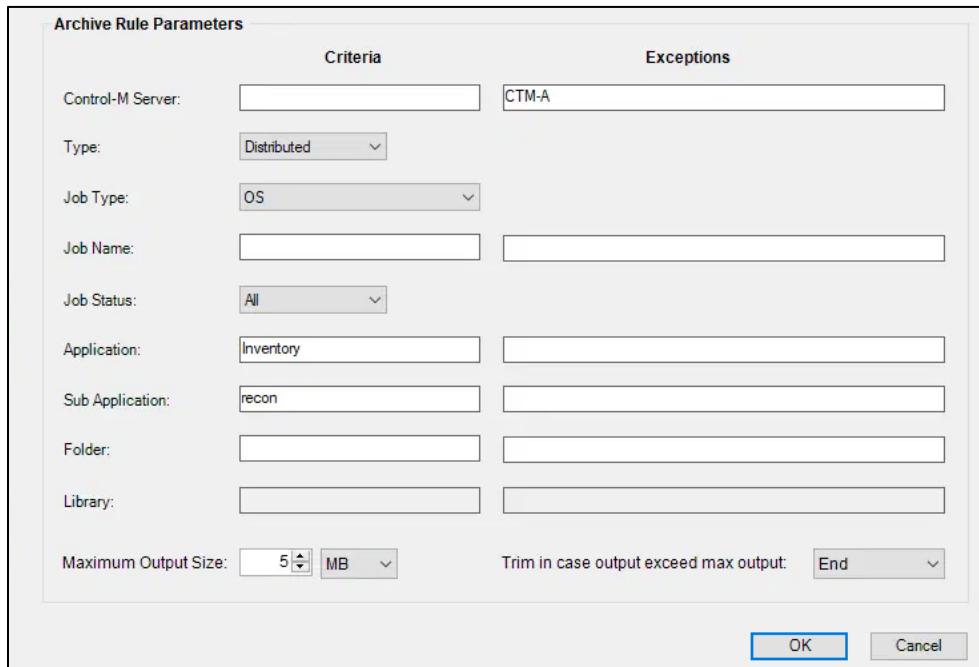


3. From the **Workload Archiving Configuration** window > **Archive Policy** tab, Click the **Add (+)** icon.
4. In the **Archive Rule Details** section, set the following values:
 - **Name:** Inventory
 - **Status:** Active
 - **Description:** Archives Log and Output data for all Inventory jobs
 - **Retention Period:** 4 Years
 - **Archive Data:** Log and Output



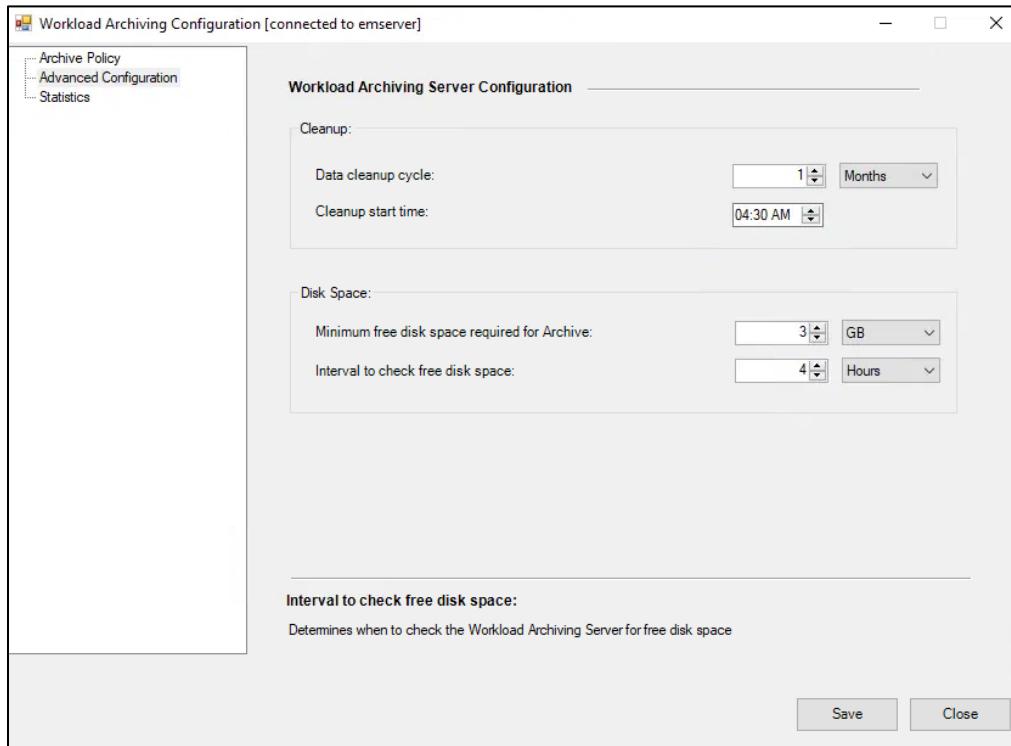
5. In the **Archive Rule Parameters** section, set the following values:

- **Control-M/Server:**
 - **Exceptions:** CTM-A
- **Type:** Distributed
- **Job Type:** OS
- **Job Name:** none (blank)
- **Job Status:** All
- **Application:** Inventory
- **Sub Application:** recon
- **Folder:** none (blank)
- **Maximum Output Size:** 5 MB
- **Trim in case output exceed max output:** End



6. Click **OK**.
7. From the **Workload Archiving Configuration** window, select the **Advanced Configuration** tab.
8. Set the **Cleanup** parameters to:
 - **Data cleanup cycle:** 1 Months
 - **Cleanup start time:** 04:30 AM
9. Set the **Disk Space** parameters to:

- **Minimum free disk space required for Archive:** 3 GB
- **Interval to check free disk space:** 4 Hours

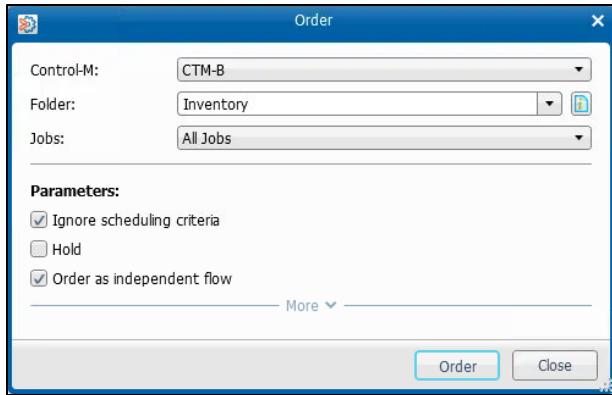


10. Click **Save** and **Close** the Workload Archiving Configuration window.

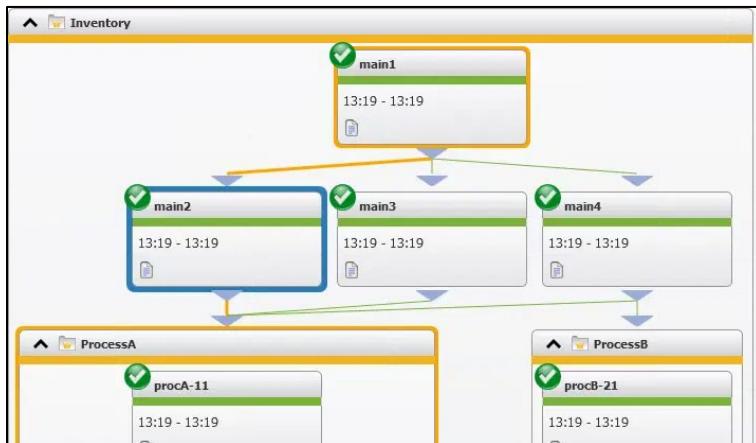
Task 2: Order Inventory Jobs for the CTM-B Control-M/Server

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **Control-M CTMSERVER_0**.
2. Log in as **emuser** with the password: **Passw0rd**.
3. Click **Monitoring** to display the **Monitoring** domain.
4. Open the **All Active Jobs** viewpoint from the **All ViewPoints** tab.
5. From the ribbon, click **Order** (from the **Viewpoint** tab).
6. In the **Order** dialog box, specify the following:
 - Control-M: **CTM-B**
 - Folder: **Inventory**
 - Jobs: **All Jobs**
7. Ensure that the **Ignore scheduling criteria** and **Order as independent flow** options are selected.



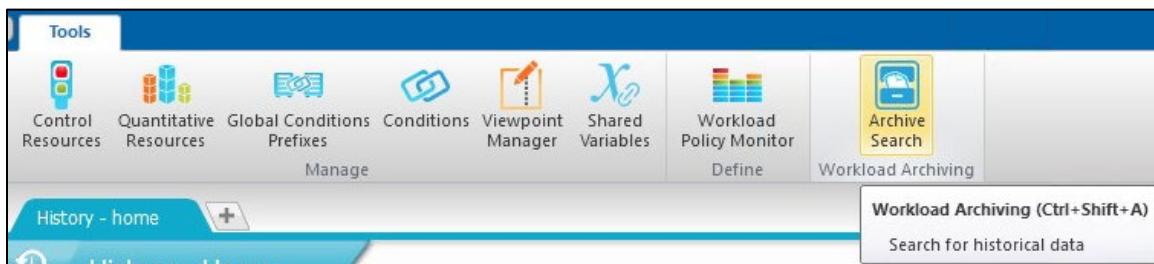
8. Click **Order**.
9. From the ribbon, click **Expand All** (from the **Viewpoint** tab).
10. Verify that the ordered jobs appear in the interface:



Task 3: Search the History Domain for Archive Data

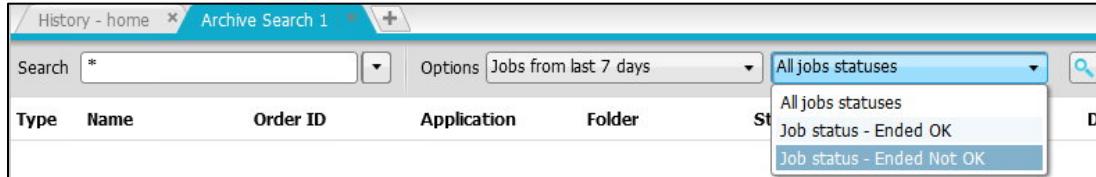
Steps:

1. From the **History** domain of the **Control-M GUI**, in the **Tools** menu, select **Archive Search**.
The **Archive Search** will open in a separate tab.



Note: If **Archive Search** is grayed out, then you need to log out and log back into the **Control-M GUI** (the GUI needs refreshing after Workload Archiving is installed).

2. In the **Search** field, type *.
3. From the **All jobs statuses** drop-down list, select the **Job Status - Ended Not OK**.

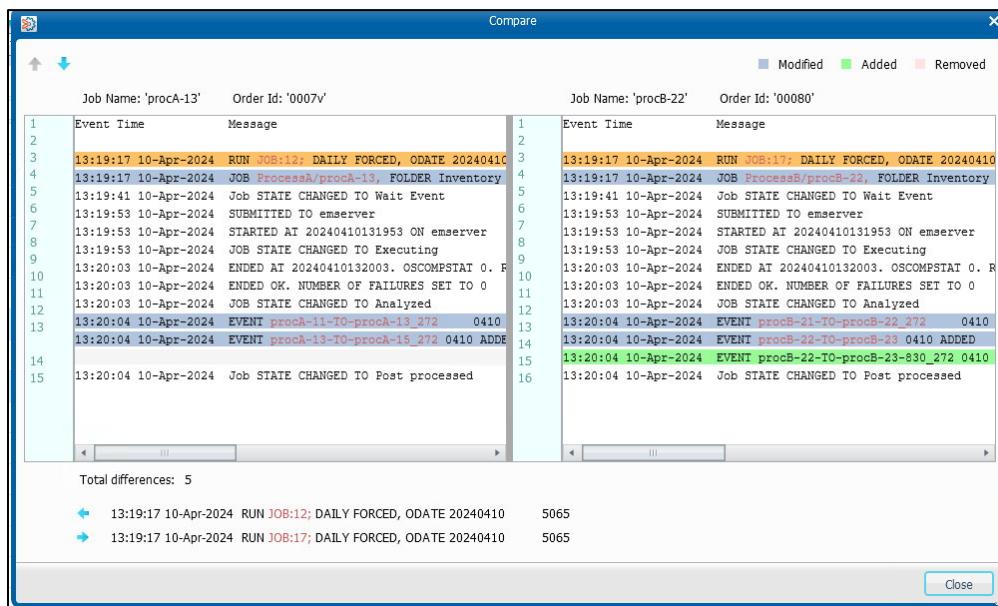


4. Click the **Search** (🔍) icon.

The archived jobs list with jobs that ended **Not OK** will be displayed.

Note: If the **Search** icon is not visible, then scroll to the right of the search bar.

5. From the **Job status - Ended Not OK** drop-down list, select **All job statuses**.
6. Click the **Search** (🔍) icon.
7. Select any two jobs and click **Compare**.
8. Select **Log**.
9. The **Compare** window appears highlighting the differences between the two job logs.



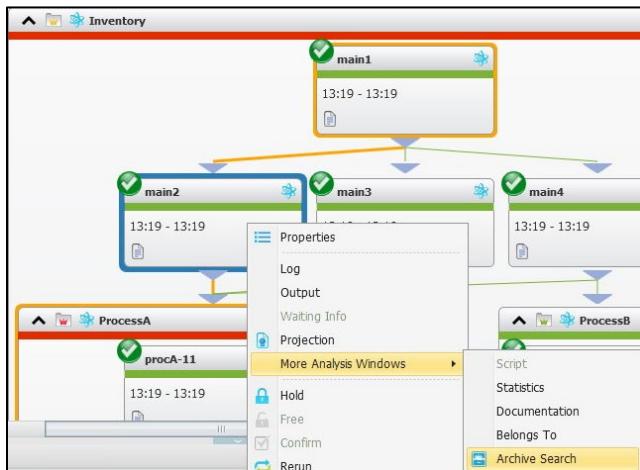
10. Close the **Compare** window.

Task 4: Perform an Archive Search from the Monitoring Domain

Steps:

1. From the **Monitoring** domain of the **Control-M GUI**, open the **All Active Jobs** viewpoint.

2. Identify and right-click the **main2** job, then select **More Analysis Windows > Archive Search**.



3. A confirmation message appears. Click **Yes**.

The archive search results appear in the **History** domain in an **Archive Search** tab.

Module 4: Role-Based Administration

Objectives:

- Add a new user and verify their access without using Role-Based Administration
- Add a Host Tag
- Add Host Groups with and without the Host Tag
- Update a Role to include Role-Based Administration Authorization
- Verify the user's access when using Role-Based Administration

Lab 4.1: Assigning Role-Based Administration Privileges

Task 1: Create a Role for Control-M Schedulers

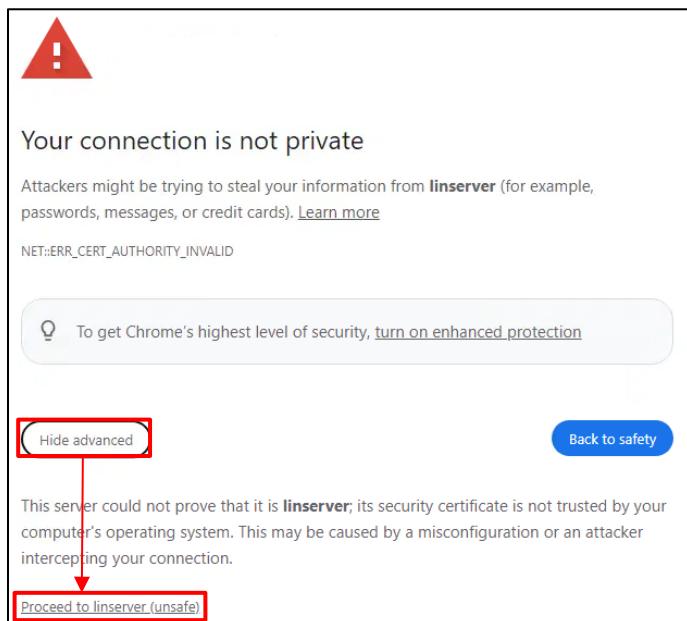
Steps:

1. From the landing server (**ctmserver**) desktop, double-click on **Google Chrome**.
2. To get to the **Control-M Configuration** window, type into the address bar:

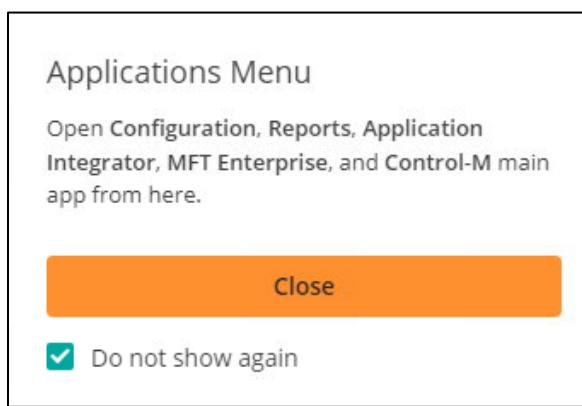
<https://linserver:8446/Configuration>

Note: The text **Configuration** is case-sensitive.

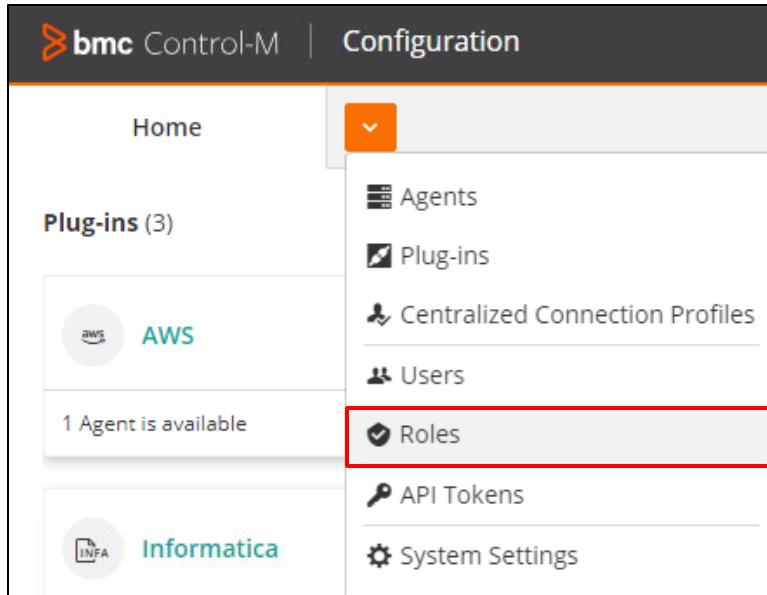
3. As the environment is using self-signed certificates, a warning appears in the web browser stating the connection is not private (the certificate signing party isn't recognized by the browser). Click **Advanced** and then **Proceed to linserver (unsafe)**.



4. Sign in as **emuser** with the password: **Passw0rd**.
5. Optionally, dismiss the **Applications Menu** dialog box by selecting **Do now show again** and **Close**.



6. Use the orange drop-down to open **Roles**.



7. Select the **Viewer** role and from the ribbon, click **Duplicate**.

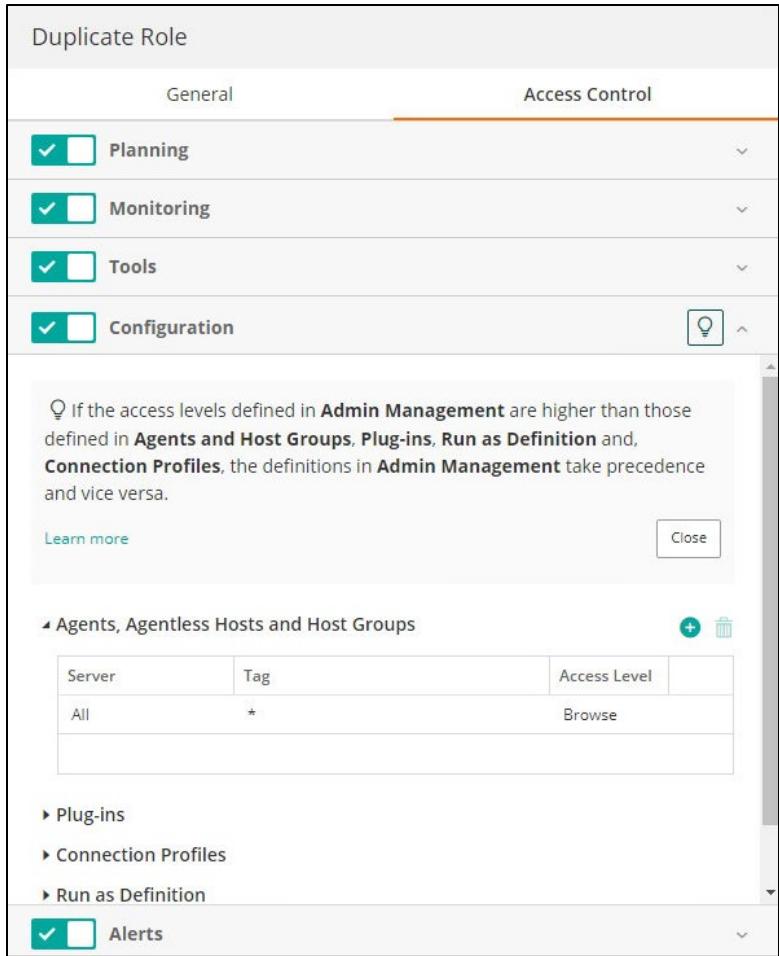
Role Name ↑		Description
Admin		Full access to all functionality
Students		
TeamLeader		Partial access with the ability to manage permissions for each member of the team
Viewer		View access

8. In the **Duplicate Role** pane, enter the following:
- Role Name:** Schedulers
 - Description:** Schedules Control-M jobs
 - Associated With Organizational Groups:** blank (default)
 - Associated With Organizational Users:** blank (default)
 - Interface Access:** Control-M Web

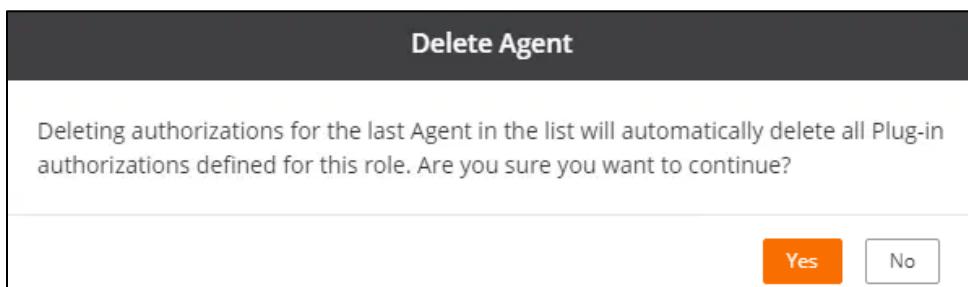
Duplicate Role

General	Access Control
Role Name (Required) Schedulers	
Description Schedules Control-M jobs	
Associated With Organizational Groups	<input type="button" value="▼"/>
Associated With Organizational Users	<input type="button" value="▼"/>
Interface Access (Required) Control-M Web	<input type="button" value="X"/> <input type="button" value="▼"/>

9. Click on the **Access Control** tab.
10. Expand **Configuration**.
11. Expand **Agents, Agentless Hosts and Host Groups**.



12. Delete the existing permission.
13. A dialog box appears stating all associated **Plug-in** permissions will also be removed. Confirm this action by clicking **Yes**.



14. Verify both the **Agents, Agentless Hosts and Host Groups** and **Plug-ins** sections are now blank (empty).

The screenshot shows a table with columns for Server, Tag, and Access Level. A note at the bottom says "Start by adding Agents permissions".

Server	Tag	Access Level
Start by adding Agents permissions		

The screenshot shows a table with columns for Server, Agent Tag, Plug-in Type, and Access Level. A note at the bottom says "You must first define authorizations for at least one Agent".

Server	Agent Tag	Plug-in Type	Access Level
You must first define authorizations for at least one Agent.			

15. Expand the **Connection Profiles** section.
16. Delete the existing permission.
17. Repeat steps 15 and 16 to delete the existing **Run as Definition** permission.
18. Verify that the **Connection Profiles** and **Run as Definition** sections are now blank (empty).

The screenshot shows two sections. The first section, 'Connection Profiles', has a table with columns for Server, Agent Tag, Name, Plug-in Type, and Access Level. A note at the bottom says "Start by adding connection profiles permissions". The second section, 'Run as Definition', has a table with columns for Server and Access Level. A note at the bottom says "Start by adding Run as definition permissions".

Server	Agent Tag	Name	Plug-in Type	Access Level
Start by adding connection profiles permissions				

Server	Access Level
Start by adding Run as definition permissions	

19. Expand the **Admin Management** section.
20. Verify the **Access Level** for **Authorizations/Users & Roles** is **Browse**, and all other categories are set to **None**.
21. Click **Duplicate**.

The screenshot shows the Control-M Configuration interface. At the top, there are two checkboxes: one checked for 'Configuration' and one unchecked for 'Alerts'. Below these are sections for 'Agents, Agentless Hosts and Host Groups', 'Plug-ins', 'Connection Profiles', 'Run as Definition', and 'Admin Management'. The 'Admin Management' section contains a table with the following data:

Admin Management	Access Level
Authorizations/Users & Roles	Browse
Configuration	None
Database Maintenance	None
Operation	None
Promotion Rules	None
Security	None

Below this are sections for 'Alerts' (unchecked) and 'Workflow Insights' (checked). At the bottom right are 'Duplicate' and 'Cancel' buttons.

Task 2: Create a User and Assign Them to the Schedulers Role

Steps:

1. Remaining in the **Control-M Web, Configuration** domain, use the orange drop-down to open **Users**.

The screenshot shows the Control-M Configuration interface with the 'Roles' dropdown menu open. The menu items are: Agents, Plug-ins, Centralized Connection Profiles, **Users** (which is highlighted with a red box), Roles, API Tokens, and System Settings.

2. Next, **Add User**.

The screenshot shows the 'Users' configuration page. At the top, there's a search bar labeled 'Search by user' and a 'Delete' button. Below the header, there's a table with columns: 'User Name', 'Full Name', and 'Roles'. Two rows are visible: one for 'emuser' (Full Name: emuser, Roles: Admin) and another for 's01' (Full Name: Students). At the bottom right of the table area, there's a blue 'Add User' button with a plus sign, which is also highlighted with a red box.

3. In the **Add User** pane, enter the following:
 - a. **User Name:** ssched
 - b. **Full Name:** Sandy Scheduler
 - c. **Description:** Senior Control-M Scheduler
 - d. **Assigned Roles:** Schedulers
 - e. **Enable external authentication only:** Untoggled (default)
 - f. **LDAP User and Domain:** Blank (default)
 - g. **Password:** Passw0rd
 - h. **Password Expiration:** Never expires
 - i. **User must change password at next login:** Disabled (default)
 - j. **Lock account:** Untoggled (default)

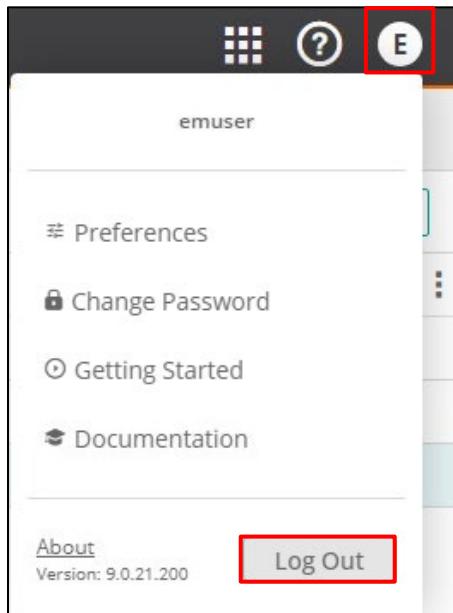
The 'Add User' dialog box is shown. It has several input fields and dropdowns:

- User Name (Required):** ssched
- Full Name:** Sandy Scheduler
- Description:** Senior Control-M Scheduler
- Assigned Roles (Required):** A dropdown menu is open, showing 'Schedulers' selected.
- Enable external authentication only:** An unchecked checkbox.
- LDAP User and Domain:** An empty text input field.
- Password (Required):** A password field containing 'Passw0rd'.
- Password Expiration:** A dropdown menu set to 'Never expires'.
- User must change password at next login:** A checked checkbox.
- Lock account:** An unchecked checkbox.

 At the bottom, there are 'Add' and 'Cancel' buttons.

4. Click **Add**.

5. From the upper-right hand corner of the screen, click **E** (for emuser, the username) and **Log Out**.



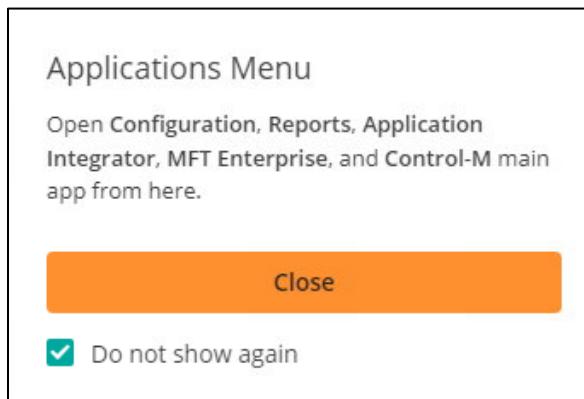
Task 3: Verify the ssched User's Access With No Role-Based Administration Privileges Defined

Steps:

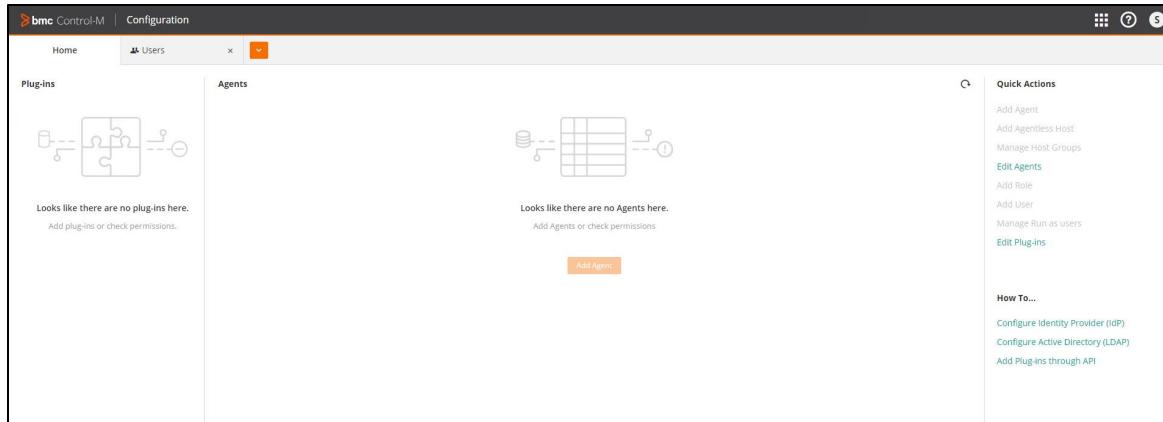
1. From the **Control-M Web** login screen, login as **ssched** with the password: **Passw0rd**.

Note: If the login screen is not displayed, open **Google Chrome** from the desktop and enter <https://linserver:8446/Configuration> into the address bar.

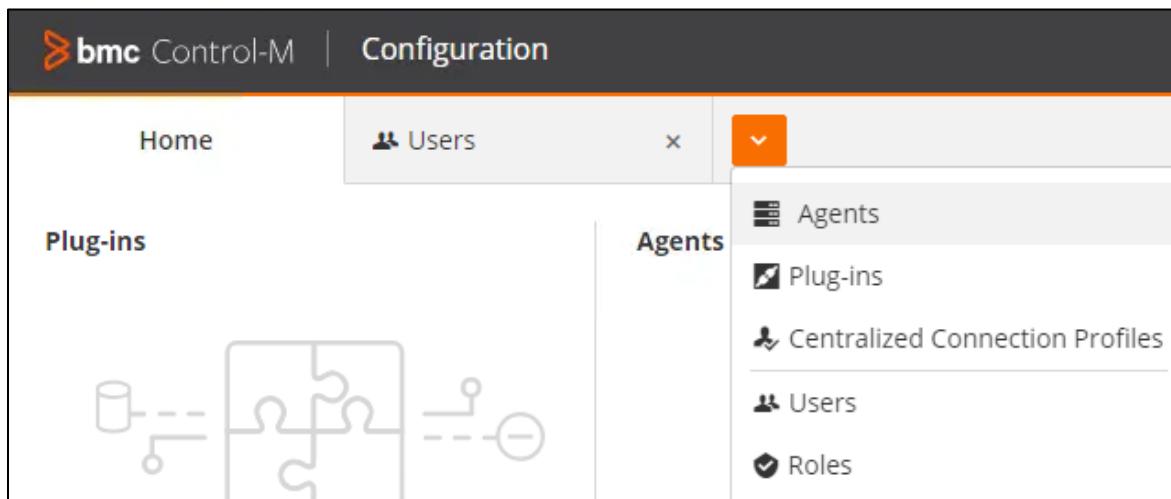
2. Dismiss the **Applications Menu** dialog box by selecting **Do now show again** and **Close**.



3. Click on the **Home** tab. Verify no **Agents** or **Application Plug-ins** appear.



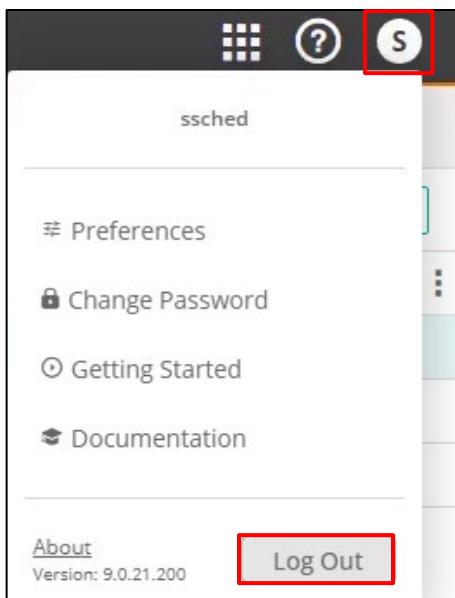
4. Use the orange drop-down to open **Agents**.



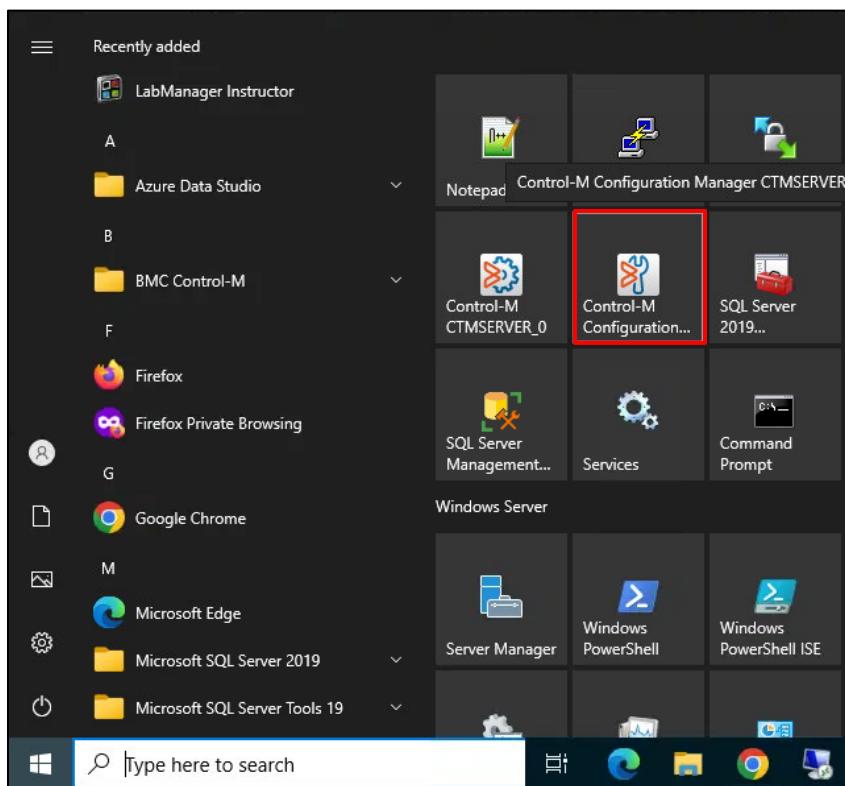
5. Observe the options available on the ribbon. Only the refresh, search and export options should be available.



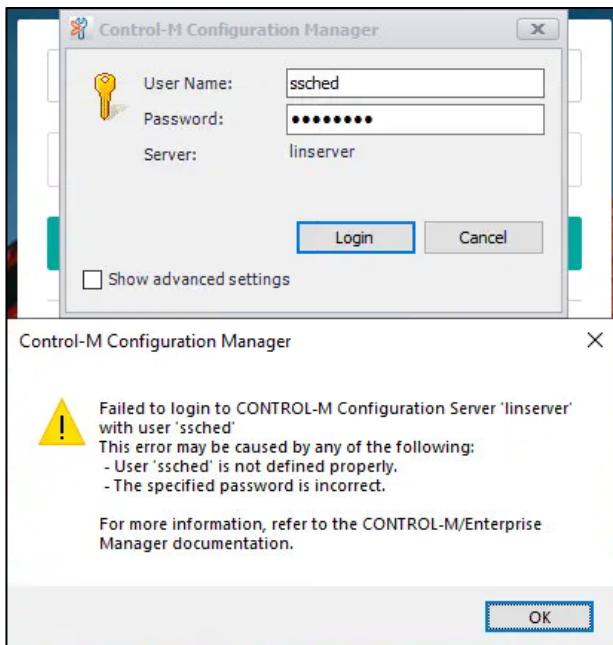
6. From the upper-right hand corner of the screen, click **S** (for ssched, the username) and **Log Out**.



7. Click on the **Start** menu and open the **Control-M Configuration Manager**.



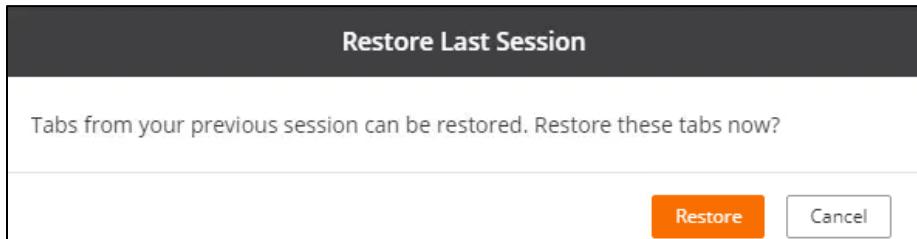
8. Attempt to sign in as **ssched** with the password: **Passw0rd**. The user is denied access to the CCM.



Task 4: Add a Host Tag and Define Host Groups

Steps:

1. From the **Control-M Web** login screen, sign in as **emuser** with the password: **Passw0rd**.
2. If the **Restore Last Session** dialog box appears, click **Cancel** to close it.



3. From the **Agents** tab (or use the orange drop-down to open **Agents**), select **winapp** from the **Name** column.

The screenshot shows the 'Agents' table in the Control-M Configuration interface. The table has columns: Name, Status, Status Message, Tag, Host, Host Groups, and Version. The rows show agents named ctmserver, emserver, winapp, and winserver, all marked as 'Available'. The 'winapp' row is highlighted with a red box. The 'Tag' column for winapp contains a dropdown menu with an asterisk (*) selected.

Name	Status	Status Message	Tag	Host	Host Groups	Version
ctmserver	Available			ctmserver		9.0.21.200
emserver	Available			emserver		9.0.21.200
winapp	Available		*	winapp		9.0.21.200
winserver	Available			winserver		9.0.21.200

4. From the **Tag** drop-down select *.

Edit Agent winapp

General Advanced

Server
CTM-A

Agent Name
winapp

Server to Agent Port
7007 ^
Changes to this field effects connectivity. [Test](#) before save.

Secure Socket Layer
Default server setting

Tag [Learn More](#)

*
*
Tags

Manage restrictions on this agent in the [Restrictions Manager](#)

5. In the **Enter tag that matches the pattern above** field, enter AWS.

Edit Agent winapp

General Advanced

Server
CTM-A

Agent Name
winapp

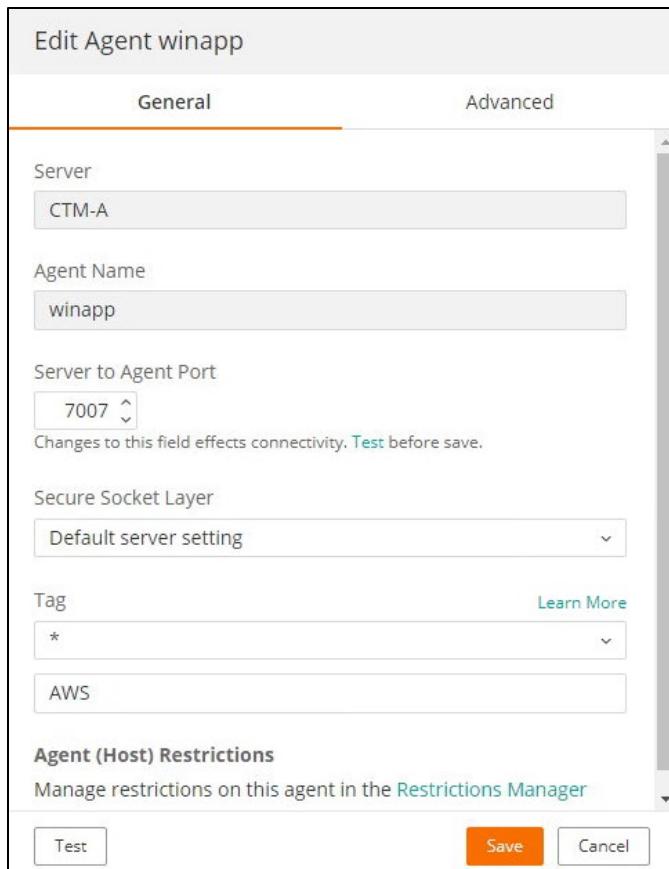
Server to Agent Port
7007 ^
Changes to this field effects connectivity. [Test](#) before save.

Secure Socket Layer
Default server setting

Tag
*
AWS

Agent (Host) Restrictions
Manage restrictions on this agent in the [Restrictions Manager](#)

[Test](#) [Save](#) [Cancel](#)



6. Click **Save**.
7. From the ribbon, click **Manage > Host Groups**.

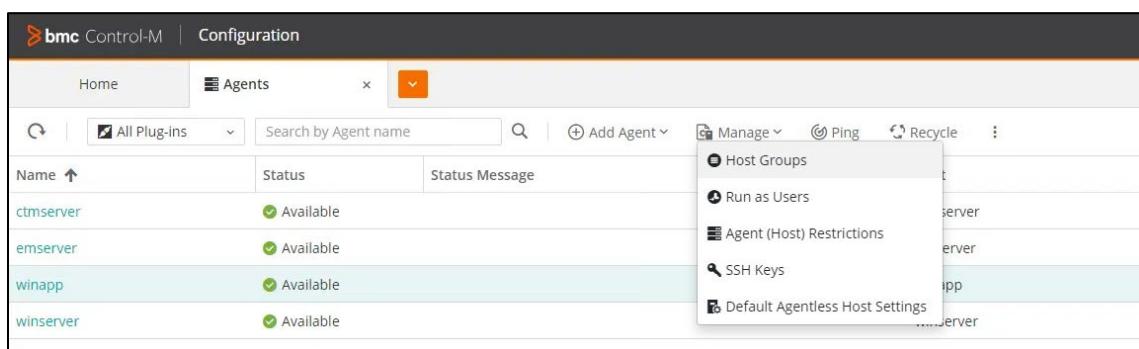
bmc Control-M | Configuration

Home Agents x

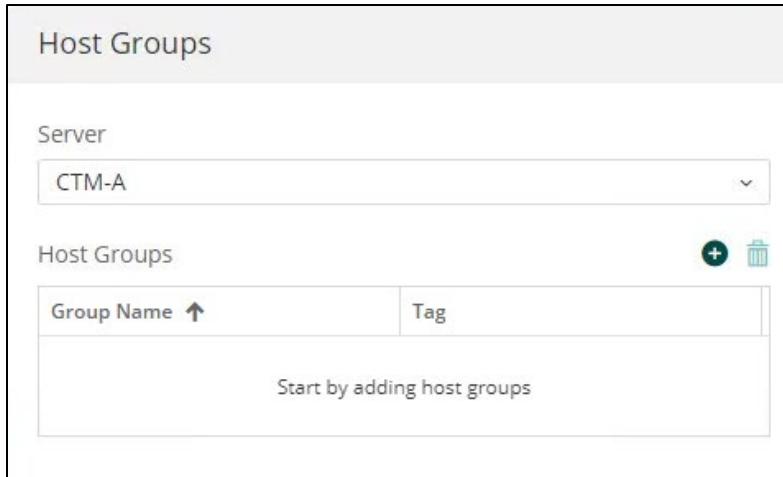
All Plug-Ins Search by Agent name Add Agent

Manage Host Groups Run as Users Agent (Host) Restrictions SSH Keys Default Agentless Host Settings

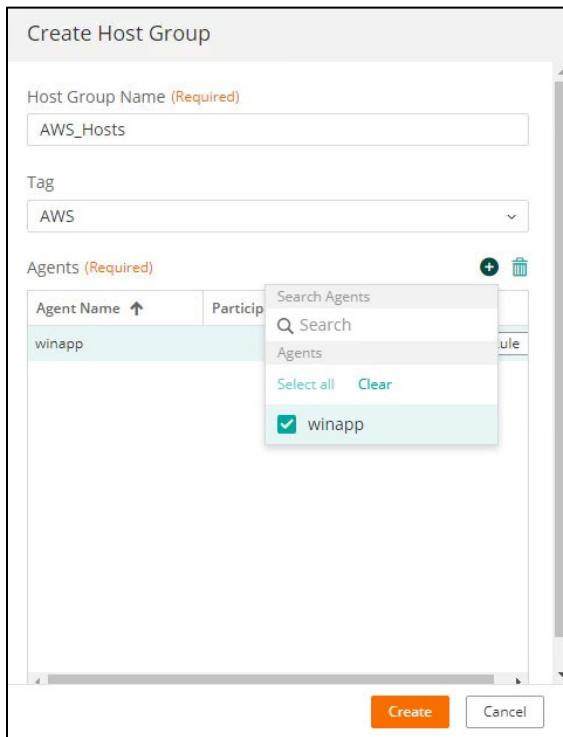
Name	Status	Status Message
ctmserver	Available	
emserver	Available	
winapp	Available	
winserver	Available	



8. From the **Host Groups** pane, set the **Server** to **CTM-A**.
9. Next to the **Host Groups** section, click **Add (+)**.



10. In the **Create Host Group** pane, set the following:
 - a. **Host Group Name:** AWS_Hosts
 - b. **Tag:** AWS
11. Next to **Agents**, click **Add (+)**. As the AWS tag is set, only hosts that have the **AWS Host Tag** defined are displayed.
12. Check the box next to **winapp**.



13. Click **Create**.
14. Add another Host Group with the following details:
 - a. **Host Group Name:** Backups
 - b. **Tag:** none
 - c. **Agents:** ctmserver, winapp

Create Host Group

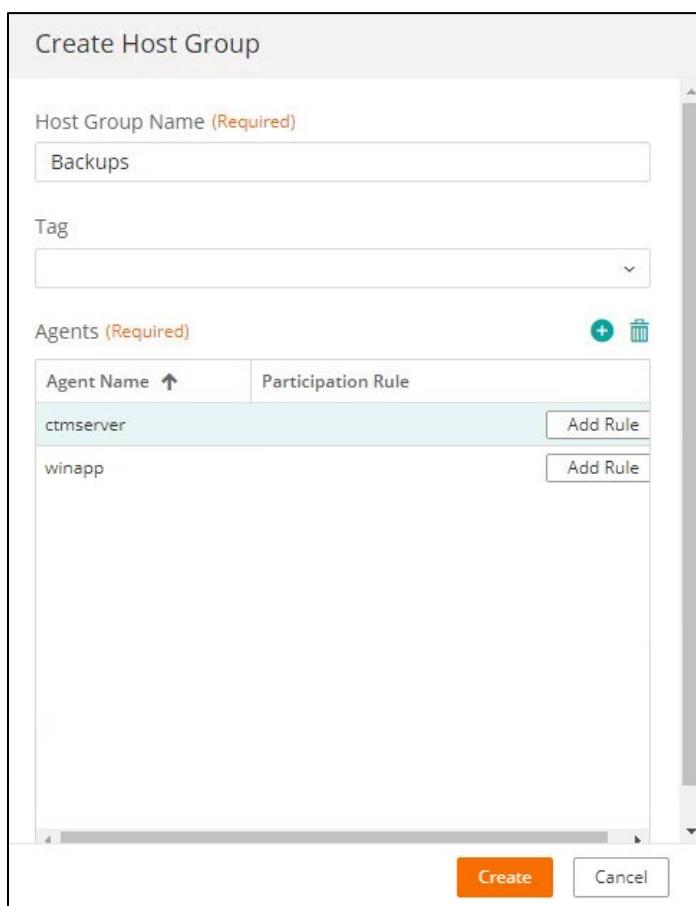
Host Group Name (Required)
Backups

Tag

Agents (Required)

Agent Name ↑	Participation Rule
ctmserver	Add Rule
winapp	Add Rule

Create **Cancel**

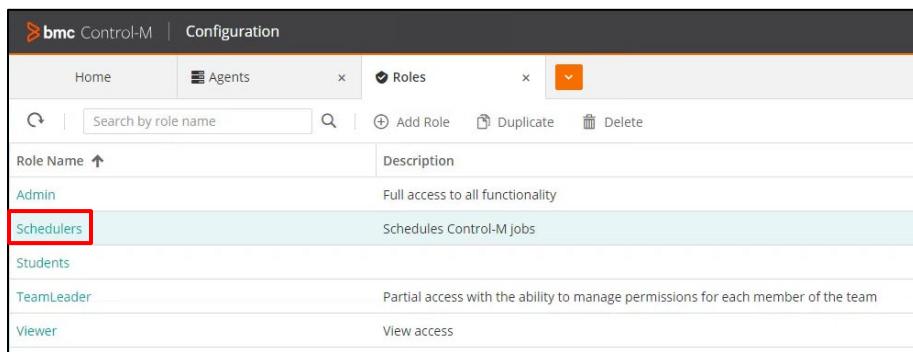


15. Click **Create**.
16. Close the **Host Groups** pane.

Task 5: Update the Schedulers Role to Include Role-Based Administration Authorization

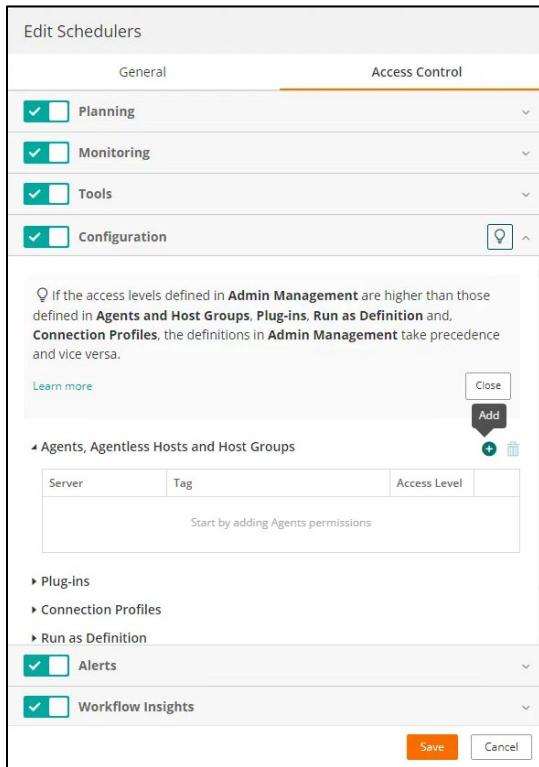
Steps:

1. Use the orange drop-down to open **Roles**.
2. Click on the **Schedulers** role from the **Role Name** column.



Role Name ↑	Description
Admin	Full access to all functionality
Schedulers	Schedules Control-M jobs
Students	
TeamLeader	Partial access with the ability to manage permissions for each member of the team
Viewer	View access

3. From the **Edit Schedulers** pane, click on the **Access Control** tab.
4. Expand **Configuration**.
5. Expand **Agents, Agentless Hosts and Host Groups**.



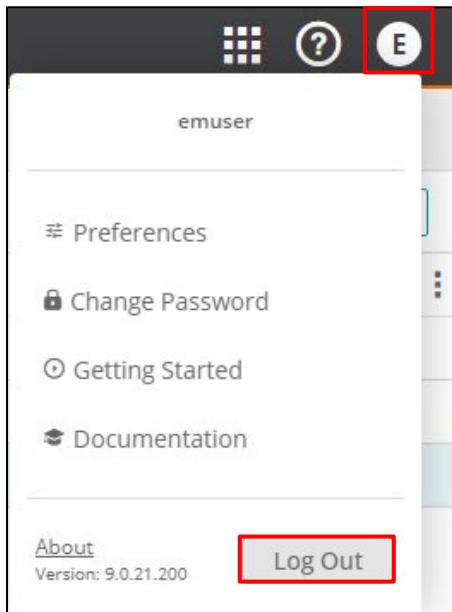
6. Click **Add** (+) to add a new permission. Set the following:
 - a. **Server:** CTM-A
 - b. **Tag:** AWS
 - c. **Access Level:** Full

Agents, Agentless Hosts and Host Groups		
Server	Tag	Access Level
CTM-A	AWS	Full

7. Expand **Plug-ins**.
8. Click **Add** (+) to add a new permission. Set the following:
 - a. **Server:** CTM-A
 - b. **Agent Tag:** AWS
 - c. **Plug-in Type:** AWS
 - d. **Access Level:** Update

Plug-ins				
Server	Agent Tag	Plug-in Type	Access Level	
CTM-A	AWS	AWS	Update	

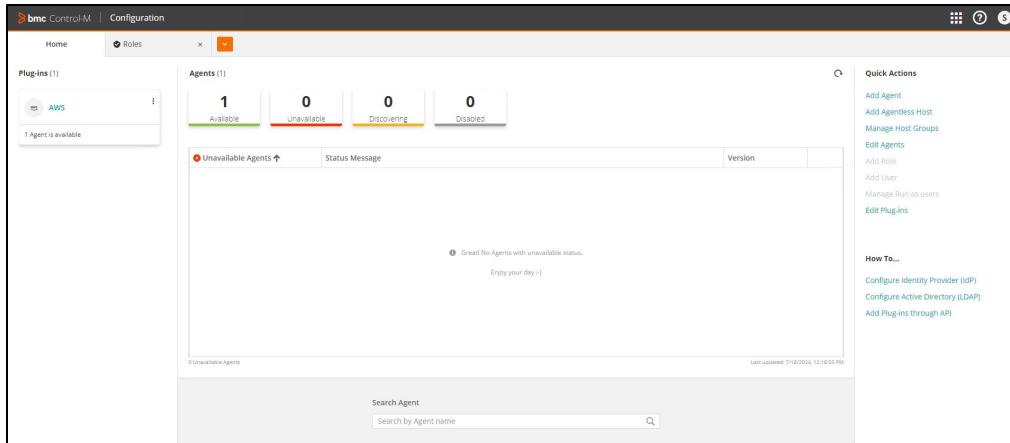
9. Click **Save**.
10. From the upper-right hand corner of the screen, click **E** (for emuser, the username) and **Log Out**.



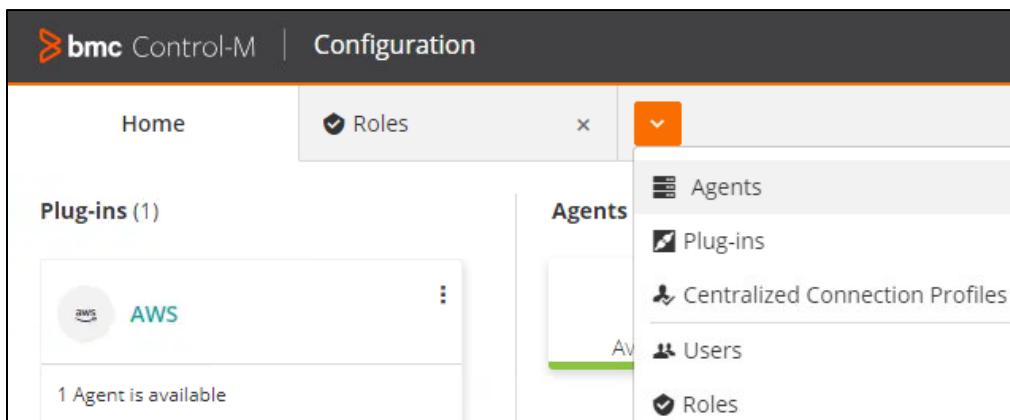
Task 6: Verify the ssched User's Access With Role-Based Administration Privileges Defined

Steps:

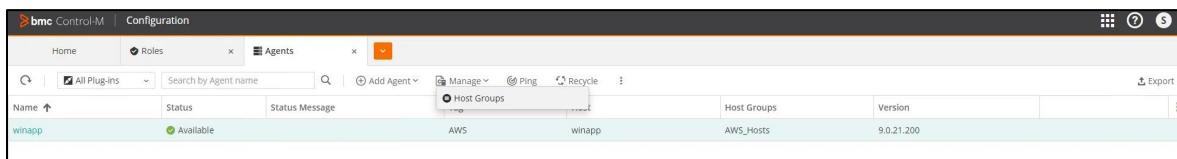
1. From the **Control-M Web** login screen, login as **ssched** with the password: **Passw0rd**.
2. If the **Restore Last Session** dialog box appears, click **Cancel** to close it.
3. Click on the **Home** tab. This time, one **Agent** and one **Plug-in (AWS)** should appear.



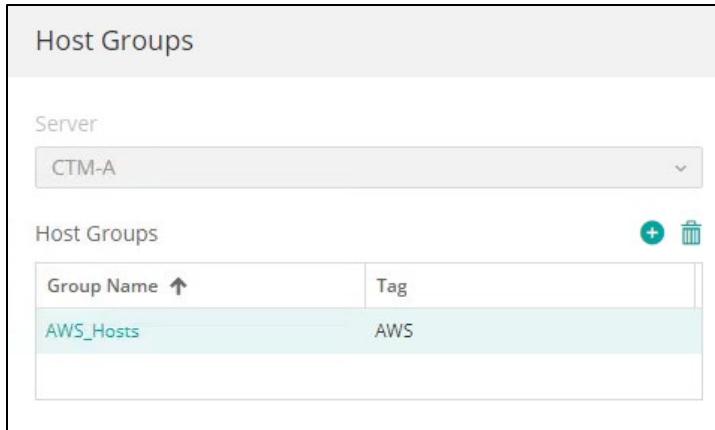
- Click the orange drop-down and open **Agents**.



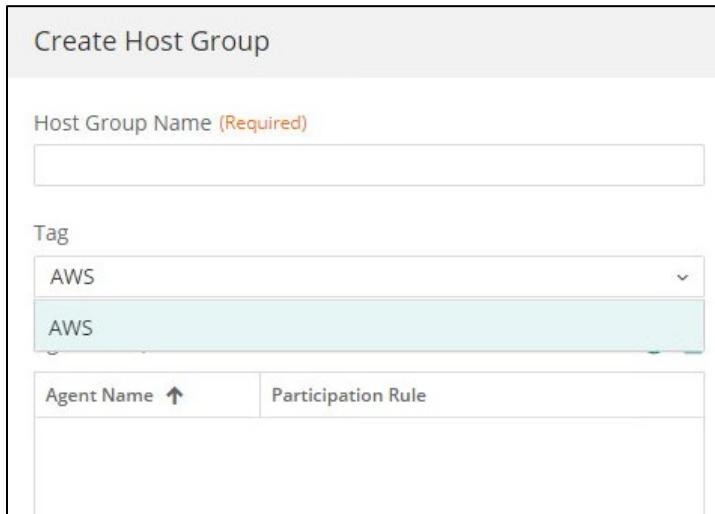
- Click **Manage > Host Groups**.



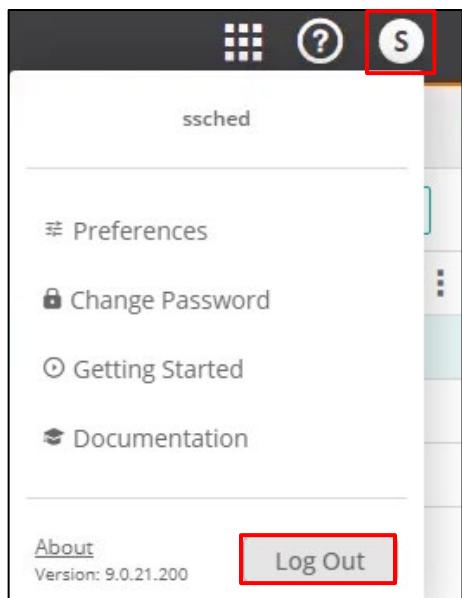
- Verify only the **AWS_Hosts** Host Group is available, and the **Server** drop-down field is not selectable.



7. Click **Add** to add a new Host Group.
8. In the **Tag** drop-down field, verify only **AWS** is selectable.



9. Click **Cancel**.
10. Close the **Host Groups** pane.
11. From the upper-right hand corner of the screen, click **S** (for ssched, the username) and **Log Out**.



Module 5: Administering Control-M Using Automation API

Objectives:

- Install the Control-M Automation API on the Control-M/Enterprise Manager Server
- Create an API Token
- Configure an Automation API Command Line Interface environment
- Use the Authentication Service to update the expiration date for an API Token

Lab 5.1: Installing the Automation API on the Control-M/Enterprise Manager Server

Task 1: Download the Latest Automation API

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **Google Chrome**.
2. When the web browser opens, type the following into the address bar:
<https://controlm.github.io>
3. Under the **Automation API CLI** section, click the text **installation guide**.

© Copyright 2005-2022 BMC Software, Inc. Use of this site signifies your acceptance of BMC's [Terms of Use](#), [Privacy Policy](#) and [Cookie Notice](#). BMC, BMC Software, the BMC logo, and other BMC marks are trademarks or registered trademarks of BMC Software, Inc. in the U.S. and/or certain other countries.

4. Scroll down to the **Installing Control-M REST API from Amazon S3 Storage** section and click the **Linux S3 Link** to download the latest Automation API for Linux.

Note
During an upgrade, the API process (the emrestsrv process) is stopped and automatically restarted.

Begin

- 1 Create a temporary directory to save downloaded files.
- 2 Click one of the following S3 links:
 - Linux: https://controlm-apidev.s3.us-west-2.amazonaws.com/release/v9.21.310/output/Unix/PADEV.9.0.21.310_Linux-x86_64_INSTALL.BIN
 - AIX: https://controlm-apidev.s3.us-west-2.amazonaws.com/release/v9.21.310/output/Unix/PADEV.9.0.21.310_AIX_INSTALL.BIN
 - Windows: https://controlm-apidev.s3.us-west-2.amazonaws.com/release/v9.21.310/output/Windows/PADEV.9.0.21.310_windows_x86_64.exe
- 3 Save the PADEV.9.0.21.310 file in the temporary directory.
- 4 (UNIX only) Type the following command for the copied installation file to ensure that it has the necessary authorizations:
`chmod +x <full name of PADEV.9.0.21.310 file>`
- 5 Ensure that you are logged in with the same user account that is used to install Control-M/EM and run the .bin or .exe file.

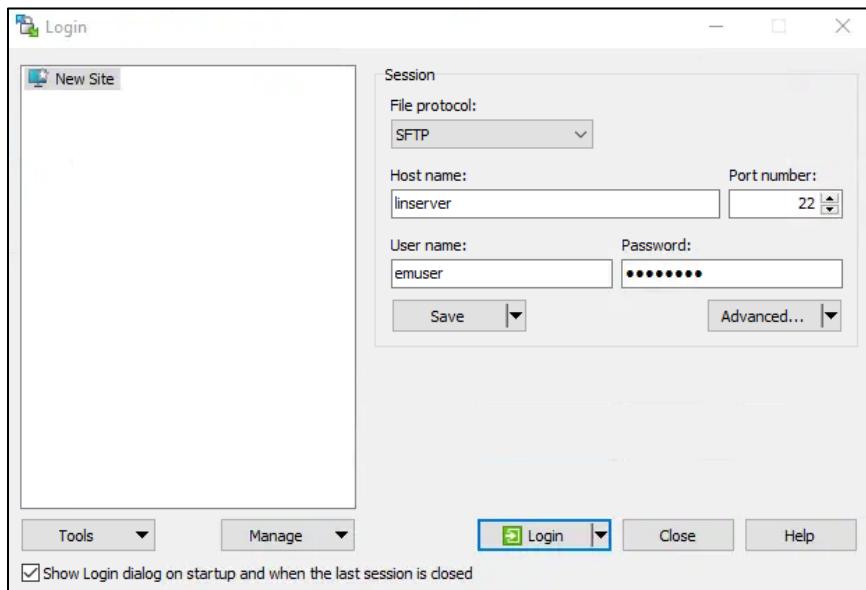
Task 2: Transfer and Install Automation API on the Control-M/Enterprise Manager Steps

1. When the installation file has downloaded, from the landing server (**ctmserver**) desktop

double-click **WinSCP**.

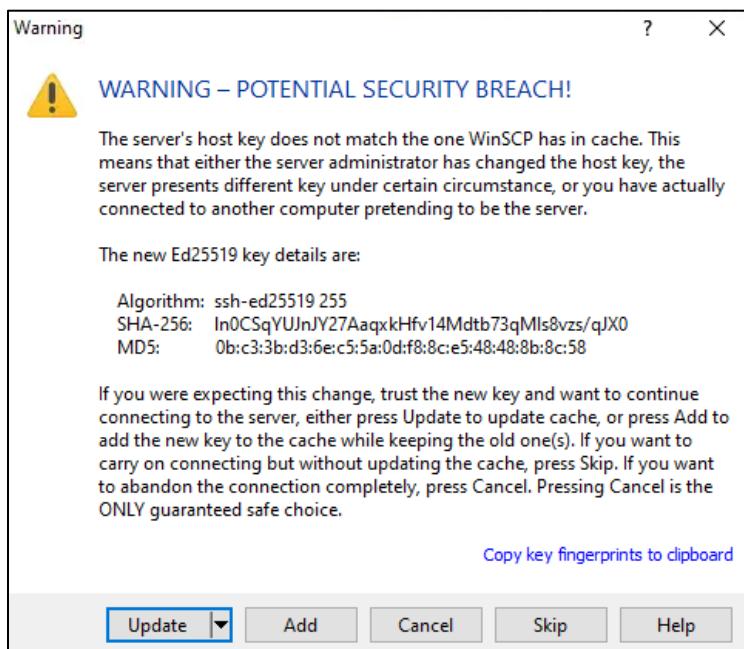
2. From the **Login** dialog box enter the following details:

- **Host name:** linserver
- **User name:** emuser
- **Password:** Passw0rd

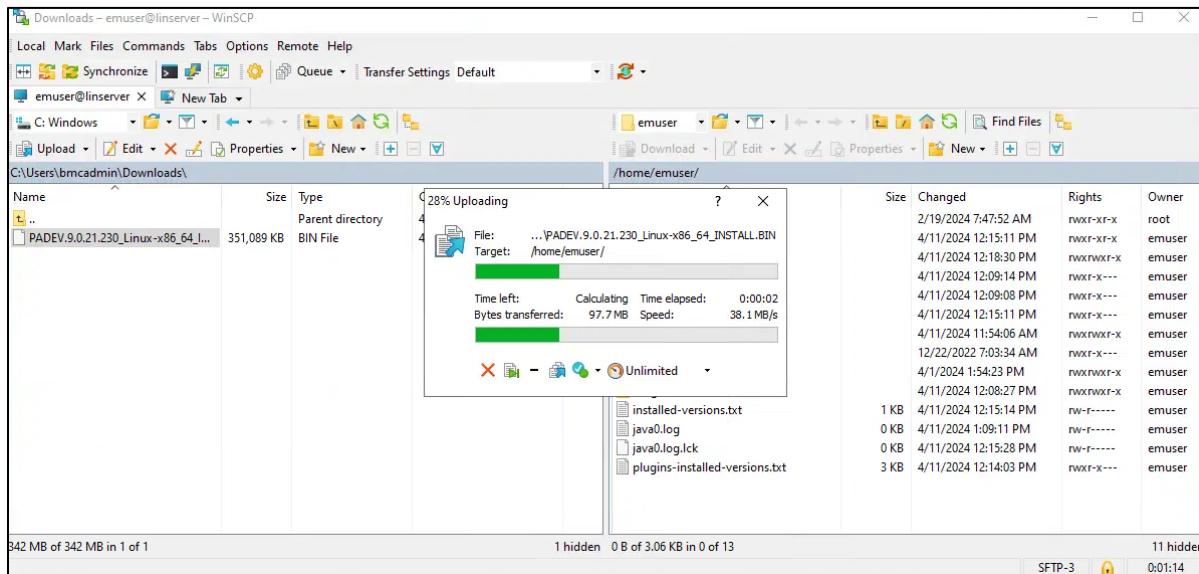


3. Click **Login**.

4. A **Warning** dialog box appears. Click **Update**.

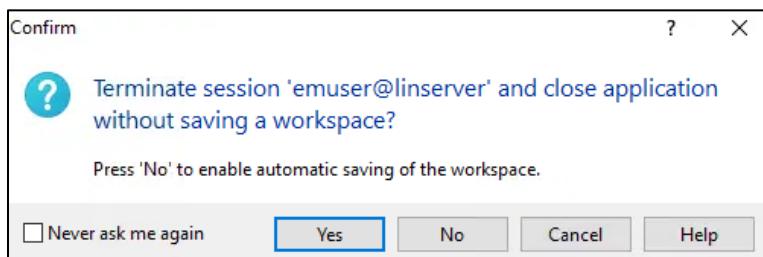


5. To change the directory of the left host (**ctmserver**), click the **Open Directory** (📁) icon and select the following directory:
- C:\Users\BmcAdmin\Downloads**
6. With the directory selected, click **OK** on the **Open Directory** window.
7. Drag the **PADEV.9.0.2x.xxx_Linux-x86_64_INSTALL.BIN** file from the left (**ctmserver**) to the right (**linserver**) host so that the Automation API installer is copied to the Control-M/Enterprise Manager server.



Note: The x characters in the **PADEV.9.0.2x.xxx_Linux-x86_64_INSTALL.BIN** file name represent numerical characters (e.g. **PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN**). As this file is updated monthly this value changes, and the S3 link will always contain the most recent version of the API.

8. Close **WinSCP** and state **Yes** in the dialog box to confirm.



9. From the landing server (**ctmserver**) desktop, open **PuTTY**.
10. Double-click **linserver** from the **Saved Sessions** section.
11. Login as **emuser** with the password: **Passw0rd**.

12. First, we need to make the Automation API installation file executable. To do this, type:

```
chmod +x PADEV.9.0.2x.xxx_Linux-x86_64_INSTALL.BIN
```

```
login as: emuser
emuser@linserver's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Apr 11 11:23:03 2024 from 192.168.1.5
linserver% chmod +x PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN
linserver%
```

Tip: Type the first few characters of the file name (case sensitive) and press tab to automatically complete the name, e.g., type **chmod +x PAD** and press the tab key.

Note: The x characters in the **PADEV.9.0.2x.xxx_Linux-x86_64_INSTALL.BIN** file name represent numerical characters (e.g. **PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN**)

13. Run the Automation API installation file by typing:

```
./PADEV.9.0.2x.xxx_Linux-x86_64_INSTALL.BIN
```

14. Confirm the installation by typing y and pressing enter.

```
linserver% ./PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN
Extracting files...
Succeeded in extracting files to /tmp/PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN
emuser.

Initiating installer, please wait...

Starting installation of Control-M Automation API (version 9.0.21.230)
Are you sure you want to install Control-M Automation API (version 9.0.21.230)?
[y/n]: y
```

15. The installer will stop the Automation API server but the rest of the Control-M/EM processes remain up. Verify the installation completes successfully

```
Copying files...
Updating settings...
Setting installation type (upgrade or new install)
Create a temporary file, so that tomcat will stop emrestsrv
Stopping Control-M Automation API Server
Stopping Control-M Automation API Configuration Server
Confirming Control-M Automation API Server is not running
Check for automation-api properties
Check for configuration-api properties
Deleting files...
Verify webapps automation-api is deleted
Waiting for extracted gateway.war to be deleted ...Copying files...
Updating settings...
Delete soft link to emrestsrv script
Create a soft link to start/stop script
Delete soft link to handle_emweb_ssl_port script
Create a soft link to handle_emweb_ssl_port script
Delete link to automation_api_config script
Create a soft link to automation_api_config script
Check for configuration server properties
Update the configuration files
Setting ports for config api server

Control-M Automation API (version 9.0.21.230) installation completed successfully.

Log file:
/home/emuser/ctm_em/install/PADEV.9.0.21.230/trace.log
linserver%
```

Lab 5.2: Configuring an Automation API Environment

Task 1: Create an API Token

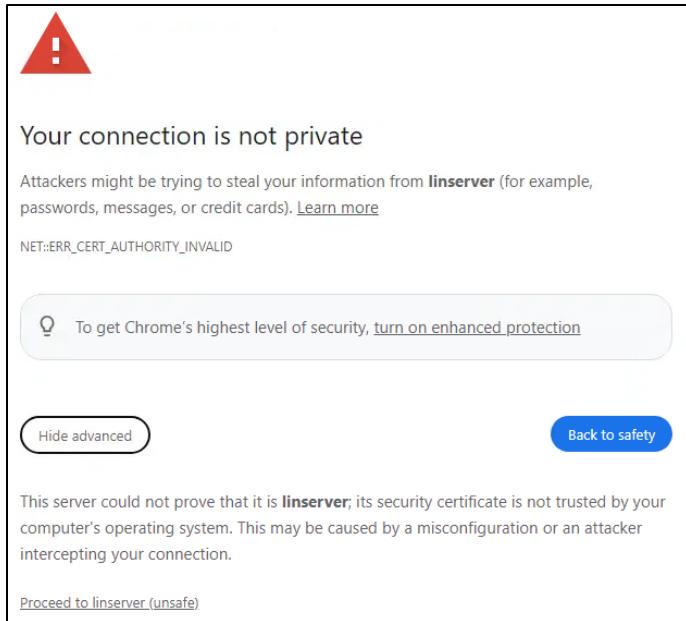
Before configuring the Control-M environment, we need to create an API Token that will be used to authenticate the AAPI CLI requests. We will do this from inside of the Control-M Web interface.

Steps:

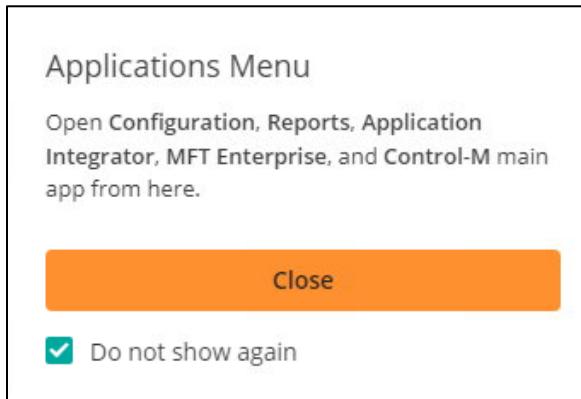
1. From the landing server (**ctmserver**) desktop, double-click **Google Chrome**.
2. To get to the **Control-M Configuration** window, type into the address bar:
https://linserver:8446/Configuration

Note: The text **Configuration** is case-sensitive.

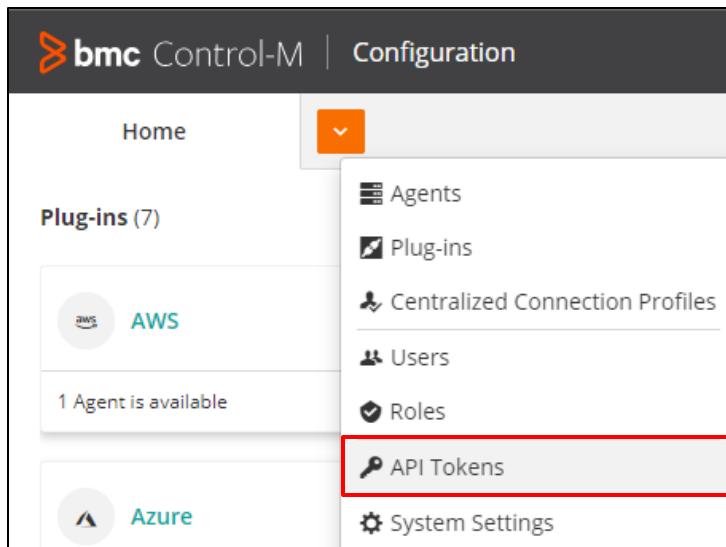
3. As the environment is using self-signed certificates, a warning appears in the web browser stating the connection is not private (the certificate signing party isn't recognized by the browser). Click **Advanced** and then **Proceed to linserver (unsafe)**.



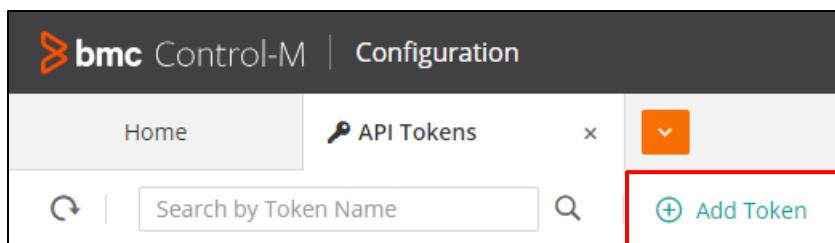
4. Sign in as **emuser** with the password: **Passw0rd**.
5. Optionally, dismiss the **Applications Menu** dialog box by selecting **Do now show again** and **Close**.



6. Use the orange drop-down to open **API Tokens**.



7. Next, **Add Token**.



8. Set the **Token Name** to **emuser_AAPI_Token** and expand the **Roles** section.
9. Click **Clear All** on the **Roles** and then click **Admin**. Click the **Roles** arrow again to close the drop-down window.

Add API Token

Token Name **(Required)**

Roles **(Required)**

Admin

Search

Search

Roles

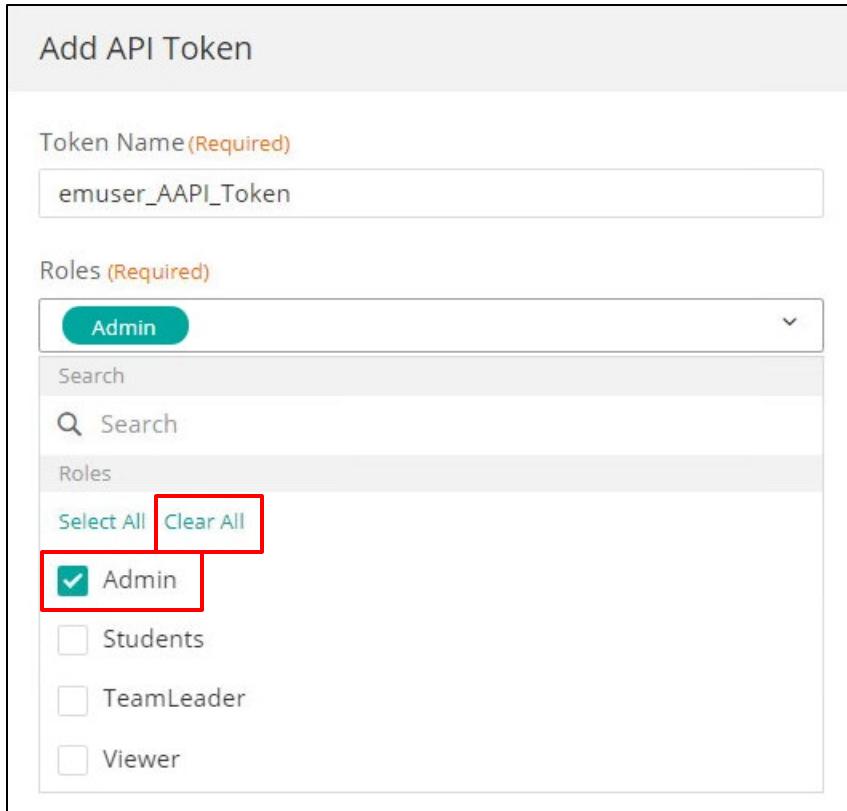
Select All

Admin

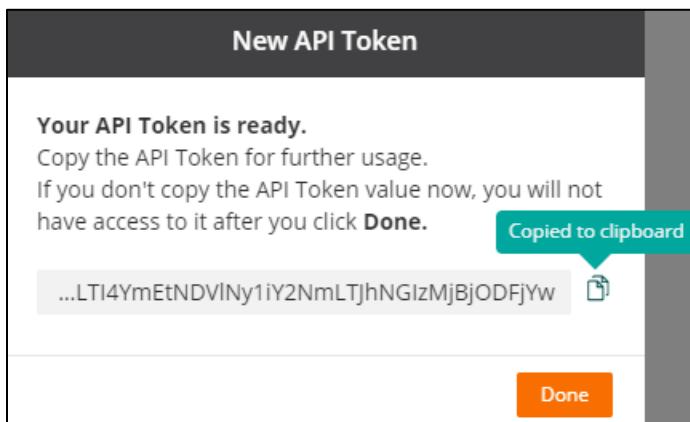
Students

TeamLeader

Viewer



10. Leave the **Expiration Date** as **Indefinitely** and click **Generate**.
11. Copy the **API Token**.



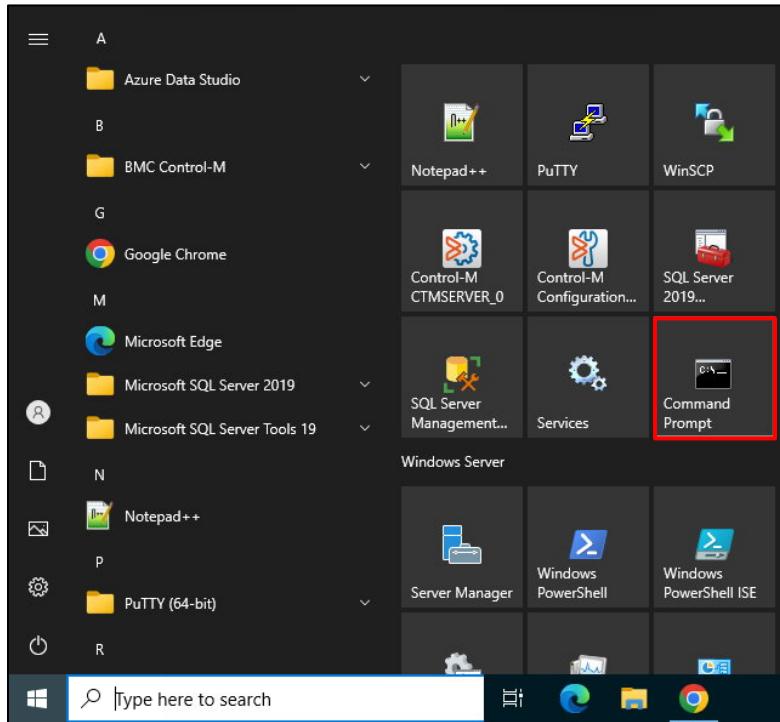
12. With the **API Token** copied, click **Done** to close the window.

Task 2: Configure the Control-M Production Environment as an Automation API Command Line Interface Environment

With the API Token generated, we can now add the Control-M environment to the AAPI CLI.

Steps:

- From the landing server (**ctmserver**), click the **Start** menu and select **Command Prompt**.



- Enter the following command, substituting <API_Token> for the API Token as copied in **Task 1**:
ctm environment add prod https://linserver:8446/automation-api <API_Token>
- Press **Enter** to add the environment.

```
C:\Users\bmcadmin>ctm environment add prod https://linserver:8446/automation-api b25QcmVtOjkyODM3NTY3LWQyNGItNGYwNS1iZmRjLTMONzU0Y2I5NThiOA==  
Environment 'prod' was created  
prod: {"endPoint":"https://linserver:8446/automation-api"}  
C:\Users\bmcadmin>
```

Lab 5.3: Using the Authentication Service

Task 1: Listing Defined API Tokens Through the Control-M Automation API Command Line Interface

Steps:

- Remaining in the command prompt, run the following command to list all defined tokens for the current user:

ctm authentication tokens::get

2. Notice that before listing the **emuser_AAPI_Token**, the Automation API CLI installation detects the new Automation API version installed on the Control-M/Enterprise Manager server and automatically updates itself.

```
C:\Users\bmcadmin>ctm authentication tokens::get
info:   Server version 9.21.235 is different from client version 9.21.100
info:   Starting download of server version 9.21.235 from https://linserver:8446/automation-api/ctm-cli.tgz
info:   Download finished in 0.271 sec.
info:   Installing version 9.21.235 to C:\Users\bmcadmin\.ctm\node_modules\ctm-cli-9.21.235
info:   Install finished in 21.482 sec.
{
  "tokens": [
    {
      "tokenName": "emuser_AAPI_Token",
      "tokenType": "user",
      "user": "emuser",
      "roles": [
        "Admin"
      ],
      "createdDate": "2024-04-17T10:41:41.083075Z",
      "lastUpdatedDate": "2024-04-17T10:41:41.083083Z"
    }
  ]
}
C:\Users\bmcadmin>
```

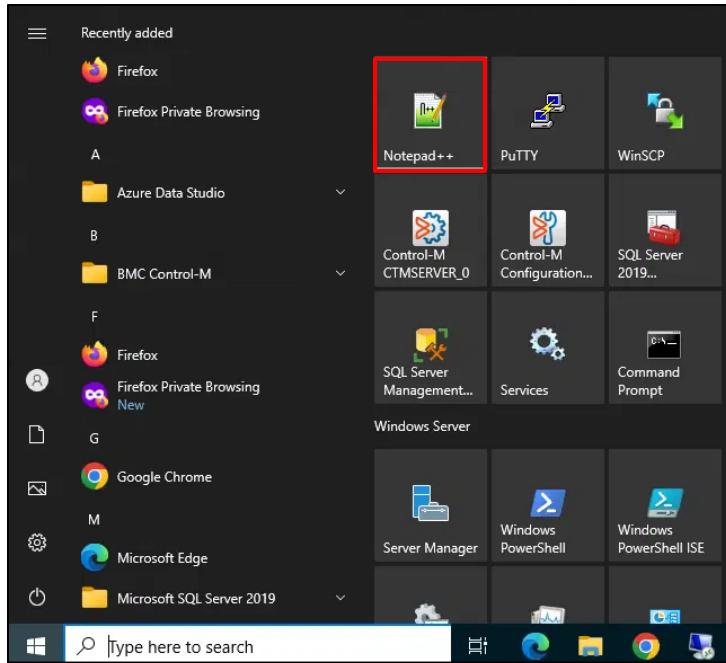
Task 2: Create a JSON Configuration File That Will Update the Expiration Date for the emuser API Token

When listing the API tokens we can see that the **emuser_AAPI_Token** doesn't have an expiration date. This goes against company security policy, so we need to update the token with a defined expiration date. To do so, we'll create a JSON configuration file that states the token name and a fixed expiration date.

Important Note: This lab, and other labs that follow require inputting text into a JSON configuration file. Please be careful when copying text from the lab guide as it may be incorrectly interpreted (for example, quotation marks may appear in the wrong format and should be manually entered).

Steps:

1. Click the **Start** menu and select **Notepad++**.



2. On the first line, add an open curly brace:

```
1 | {
```

3. On the second line, type:

"tokenName" : "emuser_AAPI_Token",

```
1 | {
2 | "tokenName" : "emuser_AAPI_Token",
```

4. On the third line, type:

"expirationDate" : "2026-12-31",

```
1 | {
2 | "tokenName" : "emuser_AAPI_Token",
3 | "expirationDate" : "2026-12-31",
```

5. On the fourth line, type:

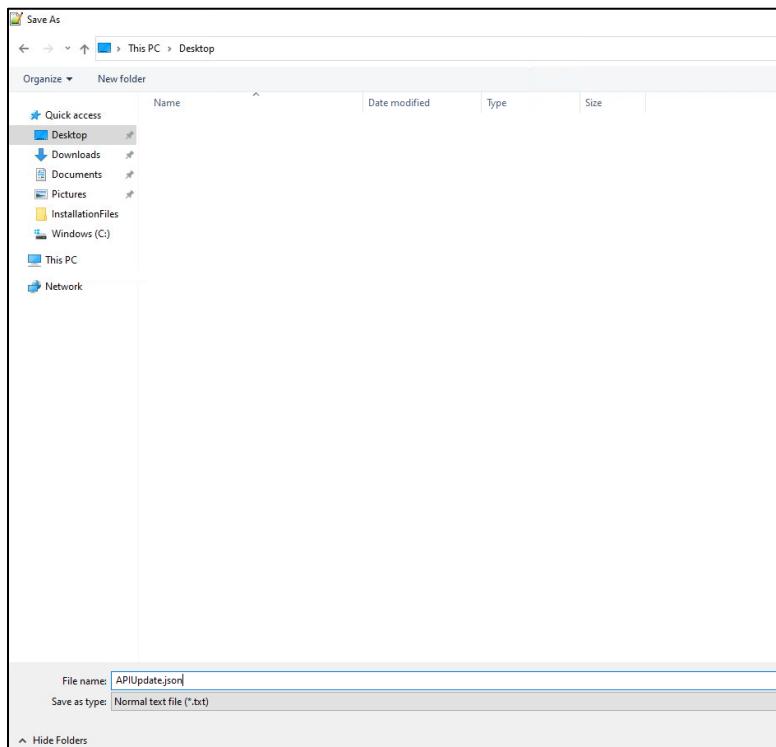
"roles" : ["Admin"]

```
1 {  
2 "tokenName" : "emuser_AAPI_Token",  
3 "expirationDate" : "2026-12-31",  
4 "roles" : ["Admin"]
```

6. On the fifth line, state a closed curly brace.

```
1 {  
2 "tokenName" : "emuser_AAPI_Token",  
3 "expirationDate" : "2026-12-31",  
4 "roles" : ["Admin"]  
5 }
```

7. Save the file to the **Desktop** with the name **APIUpdate.json**.



Task 3: Update the Expiration Date for the emuser API Token

With the JSON configuration file created, we can issue a command that applies the configuration details to the **emuser_AAPI_token**, thereby fixing its expiration date.

Steps:

1. Return to the **Command Prompt**, or open a new **Command Prompt** window.
2. Issue the following command:

```
ctm authentication token::update -f C:\Users\BmcAdmin\Desktop\APIUpdate.json
```

```
C:\Users\bmcadmin>ctm authentication token::update -f C:\Users\BmcAdmin\Desktop\APIUpdate.json
{
  "tokenName": "emuser_AAPI_Token",
  "tokenType": "user",
  "user": "emuser",
  "roles": [
    "Admin"
  ],
  "expirationDate": "2026-12-31",
  "createdDate": "2024-04-10T14:31:08.322734600Z",
  "lastUpdatedDate": "2024-04-10T14:48:37.413206700Z"
}
C:\Users\bmcadmin>
```

3. Verify the token is updated correctly.

Module 6: Using the Automation API Config Service

Objectives:

- Use the Automation API Config Service to:
 - Configure an agentless host
 - Generate an SSH Key
 - Analyze, enable and disable a Control-M/Agent
 - Add a host restriction
 - Add and test a Run As user
 - Set Control-M/Enterprise Manager, Control-M/Server and Control-M/Agent system parameters
 - List and define Control-M Roles and Users

Lab 6.1: Configuring an Agentless Host Using the API

Task 1: Create an Agentless Host Configuration File

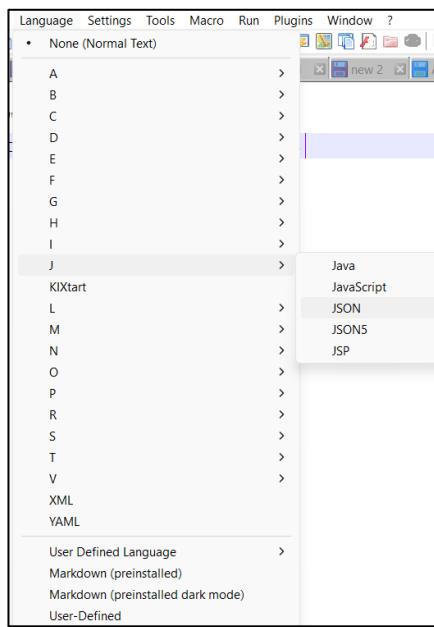
Steps:

1. From the landing server (**ctmserver**) desktop, open **Notepad++**.
2. In a new file, enter the following text:

```
{  
  "agents" : ["ctmserver", "winapp"],  
  "compression" : true  
}
```

```
1 | {  
2 |   "agents" : ["ctmserver", "winapp"],  
3 |   "compression" : true  
4 | }
```

Tip: From the toolbar, select **Language > J > JSON** to change the language to JSON, thereby making the text editing simpler.



-
3. Save the file to the **Desktop** as **AgentlessHost.json**.

Task 2: Add linagent as an Agentless Host

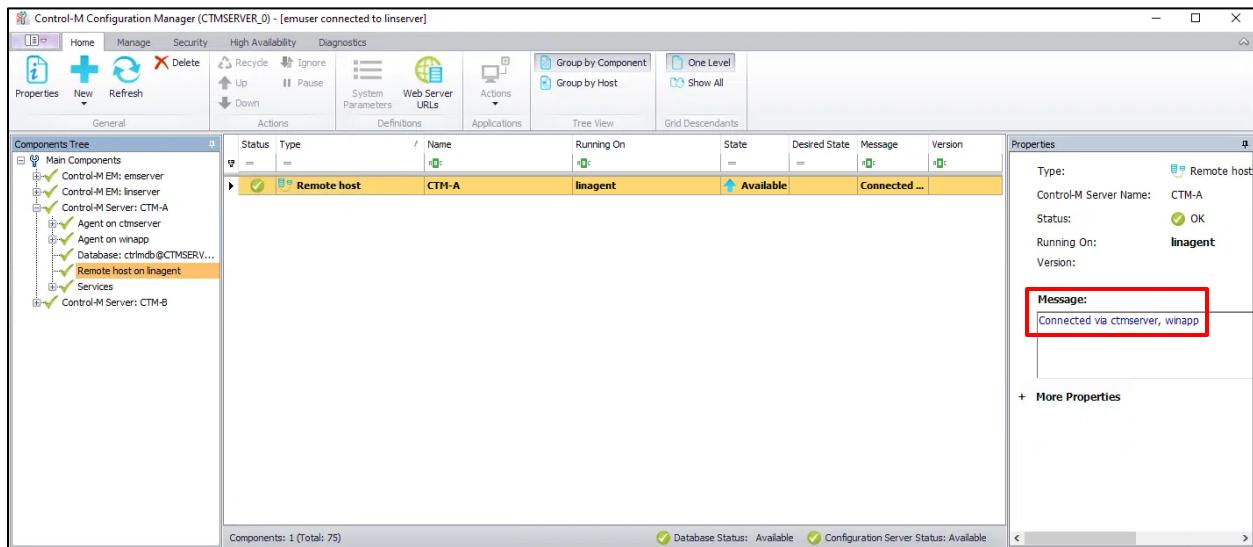
Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the agentless host, issue the following command:

```
ctm config server:agentlesshost::add CTM-A linagent -f  
C:\Users\BmcAdmin\Desktop\AgentlessHost.json
```

```
C:\Users\bmcadmin>ctm config server:agentlesshost::add CTM-A linagent -f C:\Users\BmcAdmin\Desktop\AgentlessHost.json  
{  
    "message": "Successfully added Agentless Host linagent to CTM-A"  
}  
C:\Users\bmcadmin>
```

3. From the landing server (**ctmserver**) desktop, double-click **Control-M Configuration Manager CTMSERVER_0**.
4. Log in as **emuser** with the password: **Passw0rd**.
5. From the **Components Tree**, expand **Control-M Server: CTM-A** and select the **Remote host on linagent**.
6. Verify the host is available and is connected through both **ctmserver** and **winapp**, as specified in the configuration file.



Lab 6.2: Generating an SSH Key Using the API

Task 1: Add an SSH Key to the CTM-A Control-M/Server

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the SSH Key, issue the following command:

ctm config server:sshkey::add CTM-A linagentkey Passw0rd

```
C:\Users\bmcadmin>ctm config server:sshkey::add CTM-A linagentkey Passw0rd
{
  "message": "SSH Key 'linagentkey' created successfully for ctm: CTM-A"
}

C:\Users\bmcadmin>
```

Task 2: Get the Public SSH Key for linagent

Steps:

1. To locally download the previously generated SSH Key, issue the following command:

ctm config server:sshkey::get CTM-A linagentkey Passw0rd

```
C:\Users\bmcadmin>ctm config server:sshkey::get CTM-A linagentkey Passw0rd
{
  "key": "ssh-rsa AAAAB3NzaC1yc2EAAAQABJQAAIAEAmcCnF5a8frs1+gGDdSqIDZkpqoIQFZYJ7EI95PpkQibU5c48uTF5AZHyPOpazuOa/+xT3tcUKG
oFOR9T52qnBpInJrHfrEhGsjAym/qQHPc0dvJtLotLB12wXqalKXk5XZXpxy0NvWCkEAijC0q/4heo/Qti2jk8aek/ixcQ/1s= rsa-key-20240410\n"
}

C:\Users\bmcadmin>
```

2. Highlight the text **ssh-rsa <key>** and right-click to copy it (the highlight will disappear but there will be no confirmation. This is expected and indicates the text is copied). Where **<key>** represents the key value **excluding** the **\n** value as per the below screenshot:

```
C:\Users\bmcadmin>ctm config server:sshkey::get CTM-A linagentkey Passw0rd
{
    "key": "ssh-rsa AAAAB3NzaC1yc2EAAAQAAIEAmdCnF5a8frsl+gGDdSqIDZkpqoIQFZYJ7EI95PpkQibU5c48uTF5AZHyPOpazuOa/+xT3tcUKG
oF0K9T52gnBpInJrHfrEhGsjaYm/qQHPc0dvJtLotLB12wXgalKXk5XZXpxy0NvWCkEAijC0q/4heo/Qti2jK8aek/ixcQ/is= rsa-key-20240410\n"
}
C:\Users\bmcadmin>
```

Task 3: Add the Public SSH Key to the linagent Host

Steps:

1. From the landing server (**ctmserver**) desktop, open **PuTTY**.
2. In the **Host Name (or IP address)** field, type: **linagent**.
3. Click **Open**.
4. From the **PuTTY Security Alert** window, click **Accept**.
5. Sign in as **emuser** with the password: **Passw0rd**.
6. Enter the command: **mkdir -p ~/.ssh**
7. To create the SSH public key store on the **linagent** host, type:
vi ~/.ssh/authorized_keys

```
login as: emuser
[...] emuser@linagent's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Apr 10 12:12:33 2024 from 192.168.1.5
linserver% mkdir -p ~/.ssh
linserver% vi ~/.ssh/authorized_keys
```

8. Type **i** to enter insert mode, then right-click to paste the SSH key copied in Task 2.

Note: If you enter other text by mistake hold down the shift key and use the backspace key to delete the text.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQAAIEAmcCnF5a8frsl+gGDdSqIDZkpqoIQFZYJ7EI95PpkQibU  
5c48uTF5AZHyPOpazuOa/+xT3tcUKGoFOK9T52qnBpInJrHfrEhGsjAym/qQHPc0dvJtLotLB12wXqal  
KXk5XZXpxy0NvWCkEAijC0q/4heo/QtI2jK8aek/ixcQ/1s= rsa-key-20240410
```

9. Press the **Escape** key to exit insert mode.
 10. Type **:wq!** followed by **Enter** to write and quit the file.

Lab 6.3: Analyzing, Enabling and Disabling Control-M/Agents Using the API

Task 1: Analyze the Status of a Host

Steps:

1. If not already open, from the landing desktop (**ctmserver**), click the **Start** menu and select **Command Prompt**.
2. To analyze the status of a specific host, issue the following command:
ctm config server:agent::analysis CTM-A linagent

```
C:\Users\bmcadmin>ctm config server:agent::analysis CTM-A linagent
{
  "basicInfo": {
    "serverListenPortNumber": 7006,
    "agentToServerPortNumber": 7005,
    "persistentConnection": "transient",
    "tcpsslServerMode": "Default",
    "protocolVersion": "14",
    "agentStatus": "available",
    "ipAddressesList": [
      ""
    ],
    "ctmagentCtmTestsType": [
      {
        "title": "Host Resolve",
        "result": "Failure",
        "message": "Failed to resolve host linagent",
        "userAction": "Check that hostname is spelled correctly.\r\nIf it is the correct host, run nslookup linagent to see the problem.\r\nContact your Network administrator to check the problem.",
        "command": "nslookup linagent",
        "commandOutput": "*** Unknown can't find linagent: Non-existent domain\r\nServer: UnKnown\r\nAddress: 168.63.129.16\r\n*** UnKnown can't find linagent: Non-existent domain\r\nServer: UnKnown\r\nAddress: 168.63.129.16"
      },
      {
        "title": "CTMPing",
        "result": "Failure",
        "message": "Command line timed out after 60 seconds.",
        "userAction": "",
        "command": "ctmping -hostid linagent -discover N",
        "commandOutput": ""
      }
    ]
  }
}
```

Note: This command works for agentless hosts as well as Control-M/Agents. The **linagent** host referenced here is the agentless host that was added in Lab 5.1.

Task 2: Disable a Control-M/Agent

Steps:

1. Remaining in the command line, issue the following command:
ctm config server:agent::disable CTM-A winapp

```
C:\Users\bmcadmin>ctm config server:agent::disable CTM-A winapp
{
  "message": "Successfully disabled agent winapp in CTM-A"
}

C:\Users\bmcadmin>
```

2. Verify the Agent has been disabled by running the analysis command:

ctm config server:agent::analysis CTM-A winapp

```
C:\Users\bmcadmin>ctm config server:agent::analysis CTM-A winapp
{
  "basicInfo": {
    "serverToAgentPortNumber": 7007,
    "agentToServerPortNumber": 7005,
    "persistentConnection": "transient",
    "tcpsslServerMode": "Default",
    "protoColVersion": "1.4",
    "agentStatus": "Disabled",
    "ipAddressesList": [
      ""
    ]
  },
  "ctmagentCtmTestsType": [
    {
      "title": "Host Resolve",
      "result": "Failure",
      "message": "Failed to resolve host winapp",
      "userAction": "Check that hostname is spelled correctly.\r\nif it is the correct host, run nslookup winapp to see the problem.\r\nContact your Network administrator to check the problem.",
      "command": "nslookup winapp",
      "commandOutput": "*** Unknown can't find winapp: Non-existent domain\r\nServer: UnKnown\r\nAddress: 168.63.129.16\r\n"
    },
    {
      "title": "CTMPing",
      "result": "Success",
      "message": "Agent : winapp is alive",
      "userAction": "",
      "command": "ctmping -hostid winapp -discover N",
      "commandOutput": "\nAgent : winapp is alive\r\n"
    }
  ],
  "ctmagentStatesChangedType": [
    {
      "timestamp": "1218 06:22:51",
      "status": "Unavailable",
      "message": "failure to connect to agent: java.net.ConnectException: Connection refused: no further information, by service winapp/000718400004 Availability Request"
    }
  ]
}
```

Task 3: Enable a Control-M/Agent**Steps:**

1. Again, from the command line, issue the following command:

ctm config server:agent::enable CTM-A winapp

```
C:\Users\bmcadmin>ctm config server:agent::enable CTM-A winapp
{
  "message": "Successfully enabled agent winapp in CTM-A"
}

C:\Users\bmcadmin>
```

2. Verify the Agent has been enabled by running the analysis command (scrolling through the command output to find the “agentStatus” : “Available” line):

ctm config server:agent::analysis CTM-A winapp

```
C:\Users\bmcadmin>ctm config server:agent::analysis CTM-A winapp
{
  "basicInfo": {
    "serverToAgentPortNumber": 7007,
    "agentToServerPortNumber": 7005,
    "persistentConnection": "transient",
    "tcpsslServerMode": "Default",
    "protoColVersion": "1.4",
    "agentStatus": "Available",
    "ipAddressesList": [
      ""
    ]
  },
  "ctmagentCtmTestsType": [
    {
      "title": "Host Resolve",
      "result": "Failure",
      "message": "Failed to resolve host winapp",
      "userAction": "Check that hostname is spelled correctly.\r\nif it is the correct host, run nslookup winapp to see the problem.\r\nContact your Network administrator to check the problem.",
      "command": "nslookup winapp",
      "commandOutput": "*** Unknown can't find winapp: Non-existent domain\r\nServer: UnKnown\r\nAddress: 168.63.129.16\r\n"
    },
    {
      "title": "CTMPing",
      "result": "Success",
      "message": "Agent : winapp is alive",
      "userAction": "",
      "command": "ctmping -hostid winapp -discover N",
      "commandOutput": "\nAgent : winapp is alive\r\n"
    }
  ],
  "ctmagentStatesChangedType": [
    {
      "timestamp": "1218 06:22:51",
      "status": "Available",
      "message": "Agent : winapp is alive"
    }
  ]
}
```

Lab 6.4: Adding a Host Restriction Using the API

Task 1: Add a Host Restriction for winapp

The **winapp** Control-M/Agent instance needs updating so that it can run an unlimited number of jobs concurrently, but jobs cannot be submitted to it if the CPU usage is over 80%. We can add this through the API by following the below steps.

Steps:

1. If not already open, from the landing server (**ctmserver**), click the **Start** menu and select **Command Prompt**.
2. To add a host restriction, issue the following command:

```
ctm config server:hostRestriction::add CTM-A winapp UNLIMITED 80
```

```
C:\Users\bmcadmin>ctm config server:hostRestriction::add CTM-A winapp UNLIMITED 80
{
  "message": "The Host Restriction has been successfully added"
}

C:\Users\bmcadmin>
```

3. Verify the host restriction is successfully added as indicated by the text **the Host Restriction has been successfully added**.

Task 2: Add a Second Host Restriction for ctmserver

The **ctmserver** Control-M/Agent instance needs updating so that it can run up to 5 jobs concurrently, so long as the CPU usage does not exceed 75%. We can add this through the API by following the below steps.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add a host restriction, issue the following command:

```
ctm config server:hostRestriction::add CTM-A ctmserver 5 75
```

```
C:\Users\bmcadmin>ctm config server:hostRestriction::add CTM-A ctmserver 5 75
{
  "message": "The Host Restriction has been successfully added"
}

C:\Users\bmcadmin>
```

3. Verify the host restriction is successfully added.

Note: Host Restrictions may be viewed in the **CCM** (from the ribbon **Manage > Hosts Manager > Host Restrictions**), or from the **Control-M Web** (**Configuration > Agents > Manage > Agent (Host) Restrictions**).

Task 3: List the Defined Host Restrictions

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list all defined host restrictions for Control-M/Agents managed by the CTM-A Control-M/Server, issue the following command:

ctm config server:hostRestrictions::get CTM-A

```
C:\Users\bmcadmin>ctm config server:hostRestrictions::get CTM-A
[
  {
    "nodePrefix": "ctmserver",
    "maxJobsAllowed": "5",
    "maxCPUPct": "75"
  },
  {
    "nodePrefix": "winapp",
    "maxJobsAllowed": "UNLIMITED",
    "maxCPUPct": "80"
  }
]

C:\Users\bmcadmin>
```

Task 4: Update the winapp Host Restriction

The **winapp** Control-M/Agent instance should be updated to allow up to 4 jobs to run on it concurrently, with the same 80% CPU threshold.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add a host restriction, issue the following command:

ctm config server:hostRestriction::update CTM-A winapp 4 80

```
C:\Users\bmcadmin>ctm config server:hostRestriction::update CTM-A winapp 4 80
{
  "message": "The Host Restriction has been successfully updated"
}

C:\Users\bmcadmin>
```

- Verify the host restriction is successfully updated.

Task 5: List the Defined Host Restrictions

Steps:

- If not already open, click the **Start** menu and select **Command Prompt**.
- To list all defined host restrictions for Control-M/Agents managed by the CTM-A Control-M/Server, issue the following command:

ctm config server:hostRestrictions::get CTM-A

```
C:\Users\bmcadmin>ctm config server:hostRestrictions::get CTM-A
[
  {
    "nodePrefix": "ctmserver",
    "maxJobsAllowed": "5",
    "maxCPUPct": "75"
  },
  {
    "nodePrefix": "winapp",
    "maxJobsAllowed": "4",
    "maxCPUPct": "80"
  }
]
C:\Users\bmcadmin>
```

Lab 6.5: Adding and Testing a Run As User Using the API

The SSH Key for the **linagent** agentless host has been added to the Control-M/Server and its public key added to the **linagent** host. We will now add a Run As user to the Control-M/Server, enabling a login to the **linagent** host using the SSH Key.

Task 1: Add a Run As User's SSH Key Passphrase to the Secrets Vault

Sensitive information (such as passwords) can be securely stored in the secrets vault. Information once added to the secrets vault can then be referenced without having to specify the secret's value. Here you will add the passphrase of an SSH Key to the secrets vault.

Steps:

- If not already open, click the **Start** menu and select **Command Prompt**.
- To add a host restriction, issue the following command:

ctm config secret::add linagentsshkey Passw0rd

```
C:\Users\bmcadmin>ctm config secret::add linagentsshkey Passw0rd
{
    "message": "Successfully added secret linagentsshkey"
}

C:\Users\bmcadmin>
```

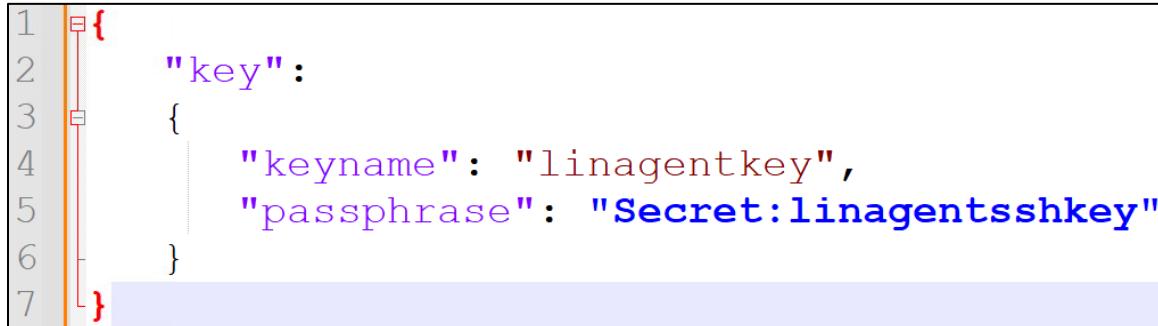
Task 2: Create a Run As User Configuration File

As we are using an SSH Key, we need to create a Run As User configuration file which will contain a reference to the SSH Key name as well as a reference to the passphrase stored in the secrets vault.

Steps:

1. From the landing server (**ctmserver**) desktop, open **Notepad++**.
2. In a new file, enter the following text:

```
{
  "key": {
    "keyname": "linagentkey",
    "passphrase": "Secret:linagentsshkey"
  }
}
```



```
1 {  
2   "key":  
3     {  
4       "keyname": "linagentkey",  
5       "passphrase": "Secret:linagentsshkey"  
6     }  
7 }
```

3. Save the file to the **Desktop** as **RunAs.json**.

Task 3: Test the Run As User

Before adding the Run As User, we should check to ensure the credentials are valid.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add a test the Run As user credentials are valid, issue the following command:

```
ctm config server:runasuser::test CTM-A linagent emuser -f  
C:\Users\BmcAdmin\Desktop\RunAs.json
```

```
C:\Users\bmcadmin>ctm config server:runasuser::test CTM-A linagent emuser -f C:\Users\BmcAdmin\Desktop\RunAs.json  
{  
    "message": "Run-as user 'emuser:linagent' credentials are valid"  
}  
C:\Users\bmcadmin>
```

Task 4: Add the Run As User

Now the credentials have been successfully validated, the user can be added to the Control-M/Server.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the Run As user, issue the following command:

```
ctm config server:runasuser::add CTM-A linagent emuser -f  
C:\Users\BmcAdmin\Desktop\RunAs.json
```

```
C:\Users\bmcadmin>ctm config server:runasuser::add CTM-A linagent emuser -f C:\Users\BmcAdmin\Desktop\RunAs.json  
{  
    "message": "user emuser:linagent created successfully"  
}  
C:\Users\bmcadmin>
```

Task 5: Add a Second Run As User

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add a Run As user using a username and password for the **winapp** host, issue the following command:

```
ctm config server:runasuser::add CTM-A winapp bmcadmin Passw0rd
```

```
C:\Users\bmcadmin>ctm config server:runasuser::add CTM-A winapp bmcadmin Passw0rd  
{  
    "message": "user bmcadmin:winapp created successfully"  
}  
C:\Users\bmcadmin>
```

Note: This time we stated the password directly in the command line, eliminating the need to create a Run As User configuration file.

Task 6: List the Defined Run As Users

There are two list options for Run As Users: list one specific Run As User or list all defined Run As Users. Here you will run both commands and compare the two.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list the details for one specific Run As User, issue the following command:

ctm config server:runasuser::get CTM-A linagent emuser

```
C:\Users\bmcadmin>ctm config server:runasuser::get CTM-A linagent emuser
{
  "agent": "linagent",
  "user": "emuser",
  "key": {
    "keyname": "linagentkey"
  }
}

C:\Users\bmcadmin>
```

3. To list all defined Run As Users, issue the following command:

ctm config server:runasusers::get CTM-A

```
C:\Users\bmcadmin>ctm config server:runasusers::get CTM-A
[
  {
    "agent": "winapp",
    "user": "bmcadmin"
  },
  {
    "agent": "linagent",
    "user": "emuser",
    "key": {
      "keyname": "linagentkey"
    }
  }
]

C:\Users\bmcadmin>
```

4. The **ctm config server:runasusers::get** command can also be filtered by using a search string. Filter for all Run As Users defined for all Control-M/Agents that start “win” by running the following command:

ctm config server:runasusers::get CTM-A -s “agent=win”

```
C:\Users\bmcadmin>ctm config server:runasusers::get CTM-A -s "agent=win*"
[
  {
    "agent": "winapp",
    "user": "bmcadmin"
  }
]

C:\Users\bmcadmin>
```

Lab 6.6: Setting System Parameters Using the API

Control-M system parameters can be listed and set for all three tiers (Control-M/EM, Control-M/Server and the Control-M/Agent). In this lab you will list system parameters for each tier and update some key system parameters.

Task 1: List Control-M/Enterprise Manager System Parameters

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list the Control-M/Enterprise Manager system parameters that can be modified using the API, issue the following command:

ctm config systemsettings::get

```
c:\Users\bmcadmin>ctm config systemsettings::get
{
  "saml2IdentityProvider": {
    "metadataUrl": "",
    "enabled": false,
    "serviceProviderInformation": {
      "entityID": "Control-M_appId",
      "ssoUrls": [
        "https://linserver:8446/services-proxy/idpcallback"
      ]
    },
    "forceAuthentication": true
  },
  "ldapSettings": {
    "ldapEnabled": false,
    "defaultDomain": ""
  },
  "enforceSiteStandards": {
    "value": "true"
  },
  "strictnesslevel": {
    "value": "non-strict"
  },
  "cmsCommMode": {
    "value": "tcp"
  },
  "userAuditAnnotation": {
    "value": "false"
  },
  "additionalParameters": [
    {
      "name": "EnableLoadBalancerRouter",
      "value": "false"
    },
    {
      "name": "WorkflowInsightsDataRetention",
      "value": "16"
    }
  ],
}
```

Task 2: Update the CmsCommMode Control-M/Enterprise Manager System Parameter

After listing the Control-M/EM system parameters, observe the value for the cmsCommMode parameter. cmsCommMode refers to the Control-M/EM to Control-M/Server communication, which is currently set to TCP. We want this to be able to automatically switch between TCP and SSL, so this should be set to AUTO.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. Set the **CmsCommMode** parameter value to **AUTO** by issuing the following command:

```
ctm config em:param::set CmsCommMode AUTO
```

```
C:\Users\bmcadmin>ctm config em:param::set CmsCommMode AUTO
{
    "message": "CmsCommMode successfully set to AUTO"
}

C:\Users\bmcadmin>
```

Note: The parameter name (**CmsCommMode**) is case-sensitive.

Task 3: List Control-M/Server System Parameters

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list the Control-M/Server system parameters for the CTM-A Control-M/Server, issue the following command:

ctm config systemsettings:server::get CTM-A

```
C:\Users\bmcadmin>ctm config systemsettings:server::get CTM-A
[
    {
        "name": "COMM_TRACE",
        "value": "0",
        "defaultValue": "0"
    },
    {
        "name": "CTM_RT_PORT_NUMBER",
        "value": "6005",
        "defaultValue": "N/A"
    },
    {
        "name": "CTMS_PORT_NUM",
        "value": "7005",
        "defaultValue": "N/A"
    },
    {
        "name": "WD_ALIVE_MSG",
        "value": "",
        "defaultValue": "N/A"
    },
    {
        "name": "CTM_CONFIG_AGENT_PORT_NUMBER",
        "value": "2369",
        "defaultValue": "N/A"
    },
    {
        "name": "CTM_PRM_ENABLE_UE",
        "value": "Y",
        "defaultValue": "Y"
    }
],
```

3. Search through the results to find three parameters and their values:

- **IOALOGLM**

- This parameter states the number of Control-M/Server log file days to retain in the database
- **OS_DIAG_LIMIT_LOG_FILE_SIZE**
 - This parameter states the maximum size in MB a Control-M/Server process log file can reach
- **OS_DIAG_LIMIT_LOG VERSIONS**
 - This parameter states the number of log file generations to retain

```
{  
    "name": "C2",  
    "value": "N",  
    "defaultValue": "N"  
},  
{  
    "name": "OUTPUTRETN",  
    "value": "1",  
    "defaultValue": "1"  
},  
{  
    "name": "IOALOGLM",  
    "value": "2",  
    "defaultValue": "2"  
},  
{  
    "name": "SWEET",  
    "value": "2",  
    "defaultValue": "2"  
},  
{  
    "name": "OUTPUT_WINDOW_SIZE",  
    "value": "",  
    "defaultValue": "80"  
},
```

```
{
  "name": "CTM_DB_TIMEOUT",
  "value": "",
  "defaultValue": "300"
},
{
  "name": "OS_DIAG_LIMIT_LOG_FILE_SIZE",
  "value": "15",
  "defaultValue": "15"
},
{
  "name": "OS_DIAG_LIMIT_LOG VERSIONS",
  "value": "20",
  "defaultValue": "20"
},
{
  "name": "CTM_CONFIG_AGENT_MODE",
  "value": "",
  "defaultValue": "2"
},
```

Task 4: Update the IOALOGLM, OS_DIAG_LIMIT_LOG_FILE_SIZE and OS_DIAG_LIMIT_LOG_VERSIONS Control-M/Server System Parameters

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. Retain a maximum of 4 days of Control-M/Server logs for the CTM-A Control-M/Server by issuing the following command:

ctm config systemsettings:server::set IOALOGLM 4 CTM-A

```
C:\Users\bmcadmin>ctm config systemsettings:server::set IOALOGLM 4 CTM-A
{
  "message": "System Parameter 'IOALOGLM' was updated successfully."
}

C:\Users\bmcadmin>
```

3. Configure Control-M/Server log files to reach a maximum of 15MB for the CTM-B Control-M/Server by issuing the following command:

ctm config systemsettings:server::set OS_DIAG_LIMIT_LOG_FILE_SIZE 15 CTM-B

```
C:\Users\bmcadmin>ctm config systemsettings:server::set OS_DIAG_LIMIT_LOG_FILE_SIZE 15 CTM-B
{
  "message": "System Parameter 'OS_DIAG_LIMIT_LOG_FILE_SIZE' was updated successfully."
}

C:\Users\bmcadmin>
```

4. Allow a maximum of 10 generations of log files per-process for the CTM-B Control-M/Server by issuing the following command:

```
ctm config systemsettings:server::set OS_DIAG_LIMIT_LOG VERSIONS 10 CTM-B
```

```
C:\Users\bmcadmin>ctm config systemsettings:server::set OS_DIAG_LIMIT_LOG VERSIONS 10 CTM-B
{
  "message": "System Parameter 'OS_DIAG_LIMIT_LOG VERSIONS' was updated successfully."
}
C:\Users\bmcadmin>
```

Task 5: List Control-M/Agent System Parameters

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list the system parameters for the **winapp** Control-M/Agent, issue the following command:

```
ctm config server:agent:params::get CTM-A winapp
```

```
C:\Users\bmcadmin>ctm config server:agent:params::get CTM-A winapp
[
  {
    "name": "AGENT_DIR",
    "value": "C:\\\\Program Files\\\\BMC Software\\\\Control-M Agent\\\\winapp\\\\",
    "defaultValue": "N/A"
  },
  {
    "name": "ATCMNDATA",
    "value": "7005",
    "defaultValue": "N/A"
  },
  {
    "name": "CTMSHOST",
    "value": "CTMSERVER",
    "defaultValue": "N/A"
  },
  {
    "name": "CTMPERMHOSTS",
    "value": "ctmserver",
    "defaultValue": "N/A"
  },
  {
    "name": "PROTOCOL_VERSION",
    "value": "14",
    "defaultValue": "13"
  },
]
```

Task 6: Update the LOGKEEPDAYS and MEASURE_USAGE_DAYS Control-M/Agent System Parameters on the WinApp Control-M/Agent

The LOGKEEPDAYS system parameter states the number of days to retain Control-M/Agent log files (default value is 1 day). The MEASURE_USAGE_DAYS system parameters states the number of days to retain Control-M Daily Log files, if the daily log file is enabled (default is 7 days).

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. Retain a maximum of 2 days of Control-M/Agent log files for the **winapp** Control-M/Agent by issuing the following command:

```
ctm config server:agent:param::set CTM-A winapp LOGKEEPDAYS 2
```

```
C:\Users\bmcadmin>ctm config server:agent:param::set CTM-A winapp LOGKEEPDAYS 2
{
    "name": "LOGKEEPDAYS",
    "value": "2",
    "defaultValue": "N/A"
}

C:\Users\bmcadmin>
```

3. Retain a maximum of 4 days of Control-M/Agent daily logs for the **winapp** Control-M/Agent by issuing the following command:

```
ctm config server:agent:param::set CTM-A winapp MEASURE_USAGE_DAYS 4
```

```
C:\Users\bmcadmin>ctm config server:agent:param::set CTM-A winapp MEASURE_USAGE_DAYS 4
{
    "name": "MEASURE_USAGE_DAYS",
    "value": "4",
    "defaultValue": "7"
}

C:\Users\bmcadmin>
```

Lab 6.7: Listing and Defining a Role Using the API

In this lab you will list the existing roles that have been defined. After observing the list of roles, you will export the TeamLeader role to a file. This file will then serve as a template to define another role: SAP_Developers. You will then add the SAP_Developers role to the Control-M environment.

Optionally, you will then use Control-M Web to export a role, modify it through Notepad++, and import the modified file back into Control-M.

Task 1: List All Roles and Export the Settings for the TeamLeader Role

First, let's get a list of all the roles that are available and then export the details of the TeamLeader role. This will be used as a template to build a new role in the next task.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list all available roles, issue the following command:

```
ctm config authorization:roles::get
```

```
C:\Users\bmcadmin>ctm config authorization:roles::get
[
  {
    "name": "Admin",
    "description": "Full access to all functionality"
  },
  {
    "name": "Viewer",
    "description": "View access"
  },
  {
    "name": "TeamLeader",
    "description": "Partial access with the ability to manage permissions for each member of the team"
  },
  {
    "name": "Students",
    "description": ""
  }
]

C:\Users\bmcadmin>
```

By reviewing the description of the TeamLeader role, it seems a suitable role to use as a template for creating another role. We will export the settings for the TeamLeader role with the next command.

3. To export the details for the TeamLeader role, issue the following command:

```
ctm config authorization:role::get TeamLeader > C:\Users\BmcAdmin\Desktop\TeamLeader.json
```

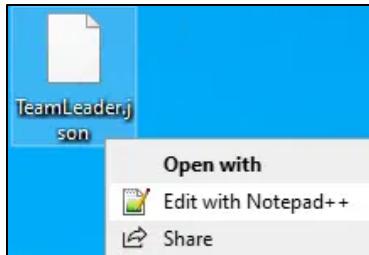
```
C:\Users\bmcadmin>ctm config authorization:role::get TeamLeader > C:\Users\BmcAdmin\Desktop\TeamLeader.json
C:\Users\bmcadmin>
```

Task 2: Use the TeamLeader JSON Template to Create a SAP Developers Role

In this task you will create a new role, based on the TeamLeader role. While changing many privileges may be more efficient programmatically (or manually through the interface), the purpose of this task is to familiarize yourself with the role definitions file format.

Steps:

1. From the landing server (**ctmserver**) desktop, right-click **TeamLeader.json** and select **Edit with Notepad++**.



2. The role should be called **SAP_Developers**. Modify the **Name** parameter to the value **SAP_Developers**:

```
1  {
2    "Name": "SAP_Developers",
```

3. The role's **Description** should be updated accordingly. Modify the **Description** to **Develops SAP Jobs**:

```
1  {
2    "Name": "SAP_Developers",
3    "Description": "Develops SAP Jobs"
4    "AllowedJobs": {
```

4. SAP Developers should only be able to see jobs within folders that begin **SAP**. On line 8, change **JobName** to **Folder**:

```
1  {
2    "Name": "SAP_Developers",
3    "Description": "Develops SAP Jobs",
4    "AllowedJobs": {
5      "Included": [
6        [
7          [
8            "Folder",
9            "like",
10           "*"
11          ]
12        ]
13      ],
14    },
```

5. Underneath the **like** operator, set the value to **SAP*** so that the role members can only view folders in the **Monitoring** domain that begin **SAP**:

```
1  {
2      "Name": "SAP_Developers",
3      "Description": "Develops SAP Jobs",
4      "AllowedJobs": {
5          "Included": [
6              [
7                  [
8                      "Folder",
9                      "like",
10                     "SAP*"
11                 ]
12             ]
13         ]
14     },
15 }
```

6. The **AllowedJobActions** object states the actions that role members can perform in the Monitoring domain. SAP Developers should be able to perform all actions *except Kill, Delete and Set to OK*. Set the associated parameters to false:

```
15  {
16      "AllowedJobActions": {
17          "ViewProperties": true,
18          "Documentation": true,
19          "Log": true,
20          "Statistics": true,
21          "ViewOutputList": true,
22          "ViewJcl": true,
23          "Why": true,
24          "Hold": true,
25          "Free": true,
26          "Confirm": true,
27          "Rerun": true,
28          "React": true,
29          "Restart": true,
30          "Kill": false,
31          "Bypass": true,
32          "Delete": false,
33          "Undelete": true,
34          "SetToOK": false,
35          "EditProperties": true,
36          "EditJcl": true
37      },
38 }
```

7. Inside the **Privileges** object, delete the **UtilitiesAccess** line:

```
37   "Privileges": {  
38     "ClientAccess": {  
39       "ControlMWebClientAccess": "Full",  
40  
41       "ApplicationIntegratorAccess": "Update",  
42       "AutomationAPIAccess": "Full",  
43       "WorkflowInsightsAccess": "Full"  
44     },
```

Note: UtilitiesAccess grants access to the Control-M desktop GUI and Control-M/Server utilities.

8. Inside the **Monitoring** object, modify the **Alert** permission to **Full**:

```
48   "Monitoring": {  
49     "Alert": "Full",  
50     "ViewpointArchive": "Full"  
51   },
```

9. Inside the **Planning** object, remove the **PromoteAction** line:

```
52   "Planning": {  
53     "PeriodicalStatistics": "Full",  
54     "ForecastOrBatchImpactManagerConfig": "Full"  
55   },  
56 }
```

Note: As the **PromoteAction** parameter was the final parameter in the **Planning** object, remember to remove the comma from the previous parameter (**ForecastOrBatchImpactManagerConfig**).

10. Scroll down to the **Folders** array. Modify the **Privilege** to **Full** and set the **Folder** value to **SAP***:

```
71   "Folders": [
72     {
73       "Privilege": "Full",
74       "Folder": "SAP*",
75       "Run": true
76     }
]
```

11. In the **Calendars** array, set the **Privilege** to **Browse**:

```
78   "Calendars": [
79     {
80       "Privilege": "Browse",
81       "Name": "*"
82     }
83   ],
```

12. Similarly, set the **WorkloadPolicies**, **SiteStandard** and **SiteCustomization** **Privilege** parameters to **Browse**:

```
89     "WorkloadPolicies": [
90       {
91         "Privilege": "Browse",
92         "Name": "*"
93       }
94     ],
95     "SiteStandard": [
96       {
97         "Privilege": "Browse",
98         "Name": "*"
99       }
100    ],
101   "SiteCustomization": [
102     {
103       "Privilege": "Browse",
104       "Name": "*"
105     }
106   ],
```

Note: Site Customizations are known as User Views in Control-M Web

13. The SAP Developers should only be able to view and modify **Services** that begin with **SAP**. Under the **Services** section, remove the comma at the end of the **Name** parameter line and on a line underneath add a closed curly brace followed by a comma:

```
107     "Services": [
108       {
109         "Privilege": "Update",
110         "Name": "*"
111       },
112       {
113         "AllowedActions": {
114           "DrillDown": true,
115           "Run": true,
116           "Resume": true,
117           "ViewOrderableService": true
118         }
119       }
120     ],
121   ],
122 ]
```

14. Underneath that line use an open curly brace to open a new object and set the following parameters:

```
{
  "Privilege": "None",
  "Name": "SAP*",
```

```
107     "Services": [
108       {
109         "Privilege": "Update",
110         "Name": "*"
111       },
112       {
113         "Privilege": "None",
114         "Name": "SAP*",
115         "AllowedActions": {
116           "DrillDown": true,
117           "Run": true,
118           "Resume": true,
119           "ViewOrderableService": true
120         }
121       }
122     ],
```

15. Finally, update the **Events** section **Privilege** parameter to **Full**:

```
123     "Events": [
124       {
125         "Privilege": "Full",
126         "Name": "*"
127       }
128     ],
```

16. Save the file to the **Desktop** as **SAPDevs.json**.

Task 3: Add the SAP_Developers Role to the Control-M Environment

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the **SAP_Developers** role to the Control-M environment, issue the following command:
ctm config authorization:role::add C:\Users\BmcAdmin\Desktop\SAPDevs.json

```
C:\Users\bmcadmin>ctm config authorization:role::add C:\Users\BmcAdmin\Desktop\SAPDevs.json
{
  "message": "Role was created successfully."
}

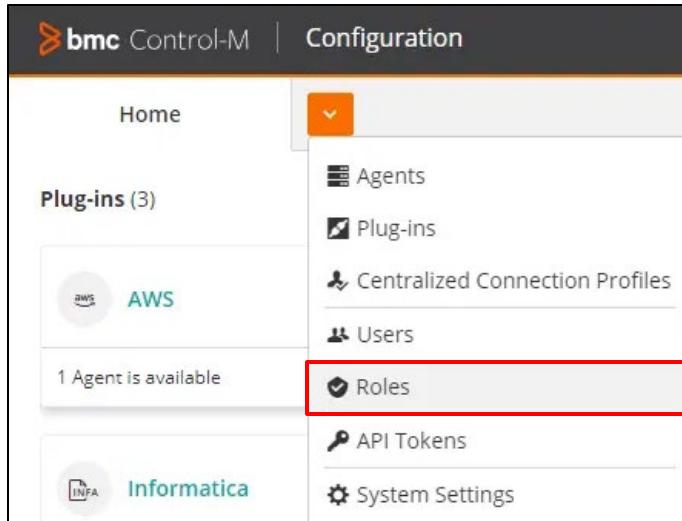
C:\Users\bmcadmin>
```

Task 4: Review the Defined Permissions in Control-M Web

In the previous tasks, we modified the TeamLeader role to fit the requirements of SAP Developers then added the role to the Control-M environment. In this task you will open Control-M Web and identify the modified permissions.

Steps:

1. From the landing server (**ctmserver**) desktop, double-click **Google Chrome**.
2. To get to the **Control-M Configuration** window, type into the address bar:
https://linserver:8446/Configuration
3. Sign in as **emuser** with the password: **Passw0rd**.
4. Use the orange drop-down to open **Roles**.



5. Click **SAP_Developers** to open the **SAP_Developers** role.

Role Name ↑		Description
Admin		Full access to all functionality
SAP_Developers		Develops SAP Jobs
Students		
TeamLeader		Partial access with the ability to manage permissions for each member of the team
Viewer		View access

6. When the **Edit SAP_Developers** window opens, verify the **Interface Access**, **Automation API** and **Control-M Web** should be allowed, **Control-M client (Desktop)**, **Utilities** and **EM API** should not be allowed. This is due to removing the **UtilitiesAccess** line from the JSON.

Edit SAP_Developers

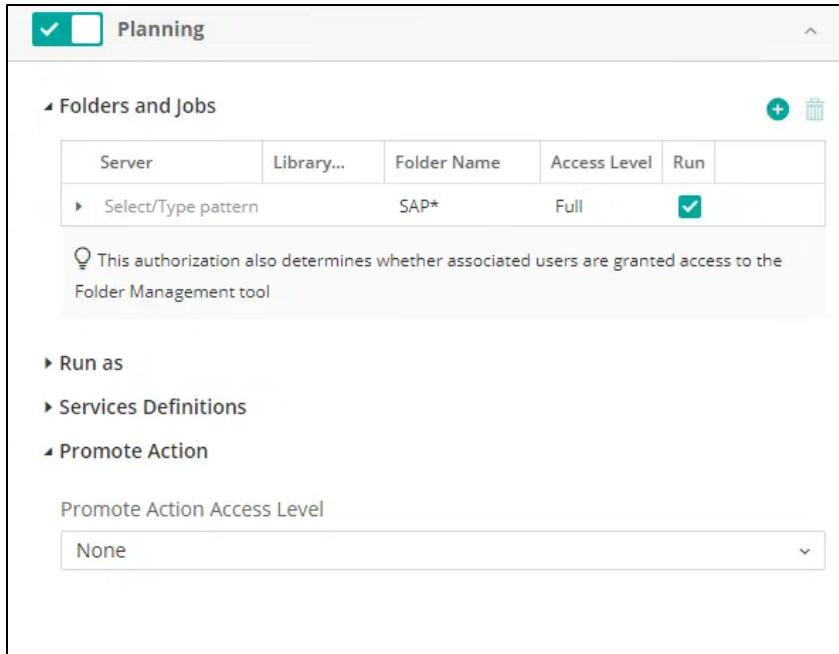
General	Access Control
Role Name (Required) SAP_Developers	
Description Develops SAP Jobs	
Associated With Organizational Groups	
Associated With Organizational Users	
Interface Access (Required)	<input type="checkbox"/> Automation API <input checked="" type="checkbox"/> Control-M Web

7. Switch to the **Access Control** tab and expand **Planning**.
8. Expand **Folders and Jobs**. Role members should have **Full** access to folders that begin **SAP**.

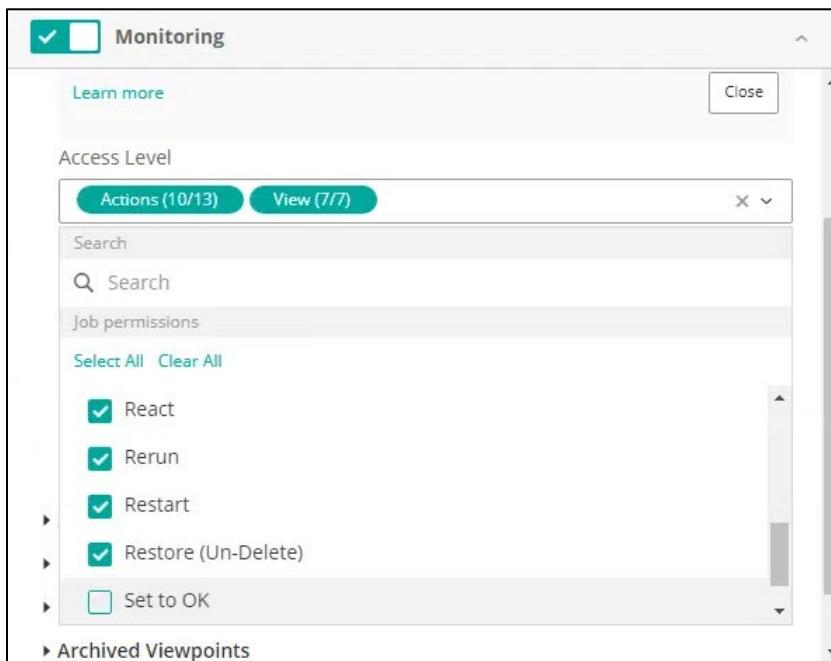
Edit SAP_Developers

General	Access Control												
<input checked="" type="checkbox"/> <input type="checkbox"/> Planning													
Folders and Jobs													
<table border="1"><thead><tr><th>Server</th><th>Library...</th><th>Folder Name</th><th>Access Level</th><th>Run</th><th></th></tr></thead><tbody><tr><td>▶ Select/Type pattern</td><td>SAP*</td><td>Full</td><td><input checked="" type="checkbox"/></td><td></td><td></td></tr></tbody></table>		Server	Library...	Folder Name	Access Level	Run		▶ Select/Type pattern	SAP*	Full	<input checked="" type="checkbox"/>		
Server	Library...	Folder Name	Access Level	Run									
▶ Select/Type pattern	SAP*	Full	<input checked="" type="checkbox"/>										
<small>💡 This authorization also determines whether associated users are granted access to the Folder Management tool</small>													

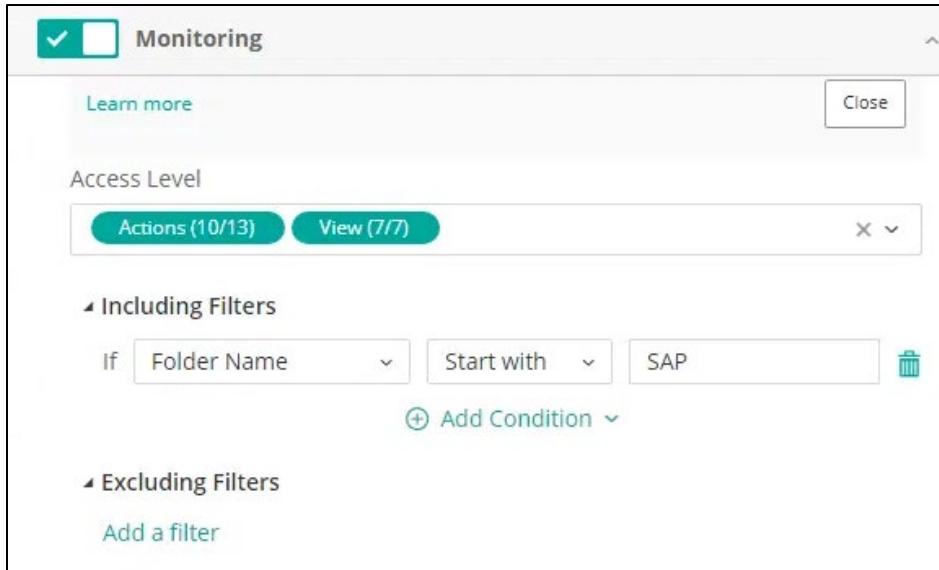
9. Expand **Promote Action**. This should be set to **None**.



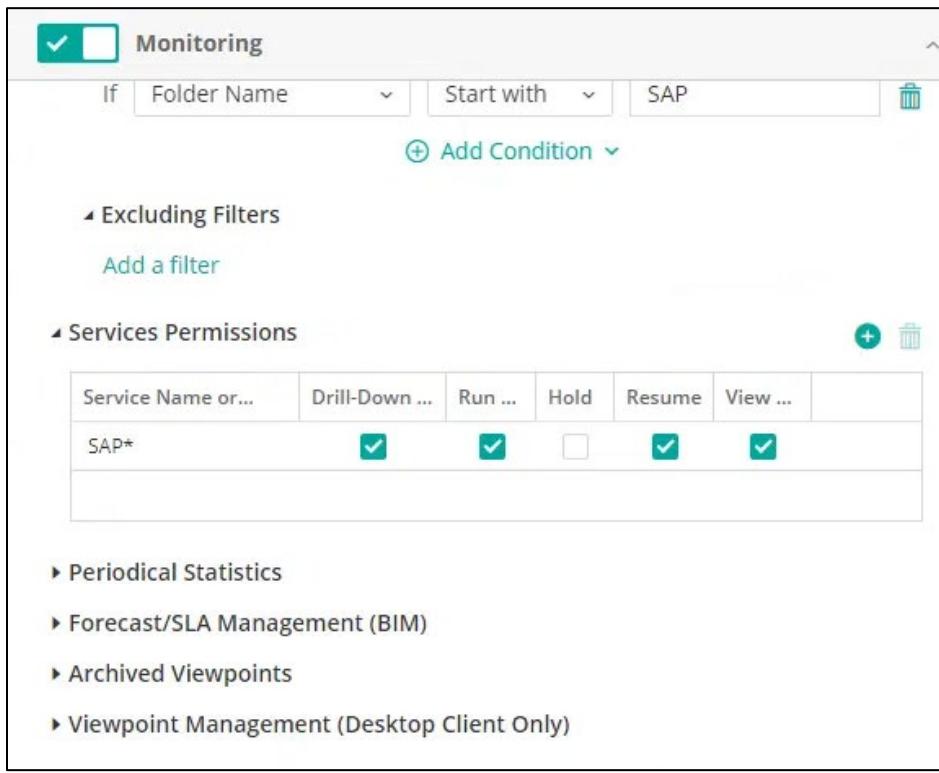
10. Expand Monitoring > Job Permissions.
11. Expand Access Level. All View and Actions should be permitted except Kill, Delete and Set to OK.



12. The permitted Actions and View options should be restricted to Folders that begin SAP, as denoted by the Including Filters line:



13. Remaining in **Monitoring**, expand **Services Permissions**. Verify that role members can only view services that begin **SAP**.



14. Expand **Tools**. Verify that **Calendars**, **Site Standards**, **User Views** (known as **Site Customizations** in the JSON) and **Workload Policies** are all set to **Browse**.

The screenshot shows the SAP Control-M Tools interface. At the top, there are two checkboxes: one checked (blue) and one unchecked (white). The title bar says "Tools". Below the title bar, there are two sections: "User Views" and "Workload Policies". Each section has a table with columns for "Name" and "Access Level". In the "User Views" section, there is one row with a name starting with an asterisk (*) and an "Access Level" of "Browse". In the "Workload Policies" section, there is also one row with a name starting with an asterisk (*) and an "Access Level" of "Browse". Each section has a green "+" button and a green trash can icon.

15. Remaining in **Tools**, expand **Events** and verify the **Access Level** is set to **Full**.

The screenshot shows the SAP Control-M Tools interface with the "Events" section expanded. The title bar says "Tools". Below the title bar, there are three sections: "Application Integrator", "Calendars", and "Events". The "Events" section is expanded, showing a table with columns for "Server", "Name", and "Access Level". There is one row with a "Select/Type pattern" of "*" and an "Access Level" of "Full". The "Events" section has a green "+" button and a green trash can icon.

16. Finally, expand the **Alerts** section and verify the **Alerts Access Level** is set to **Full**.

The screenshot shows the SAP Control-M Tools interface with the "Alerts" section expanded. The title bar says "Tools". Below the title bar, there is one section labeled "Alerts". Under "Alerts", there is a label "Alerts Access Level" followed by a dropdown menu. The dropdown menu is open and shows the option "Full".

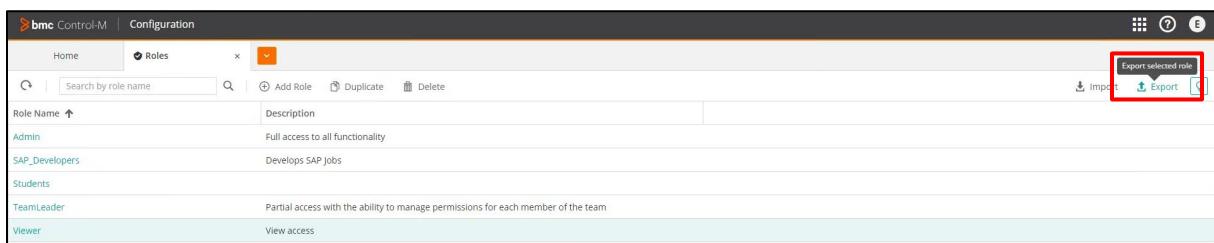
17. Close the **Edit SAP_Developers** window.

(Optional) Task 5: Export the Viewer Role

Control-M role definition configuration files can be exported from Control-M Web. In this task we'll export the Viewer role, before modifying and importing it in the next task.

Steps:

1. Remaining in the **Roles** tab from the last task, select the **Viewer** role, and from the upper-right of the screen select **Export**.

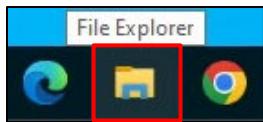


(Optional) Task 6: Modify the Viewer Role and Import it via Control-M Web

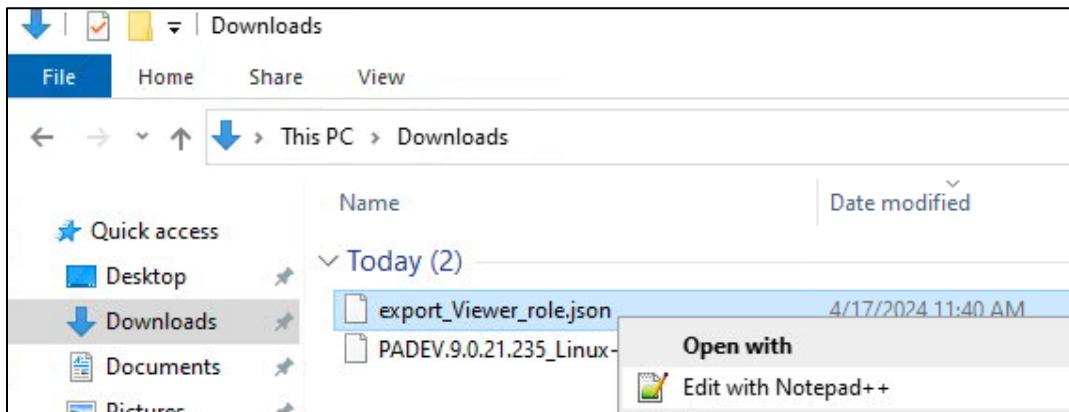
In this task you will modify the exported **Viewer** role in **Notepad++**, creating a new role. You will then import the role into Control-M using **Control-M Web**.

Steps:

1. From the taskbar, click **File Explorer**.



2. Browse to **Downloads**.
3. Right-click **export_Viewer_role.json** and **Edit with Notepad++**.



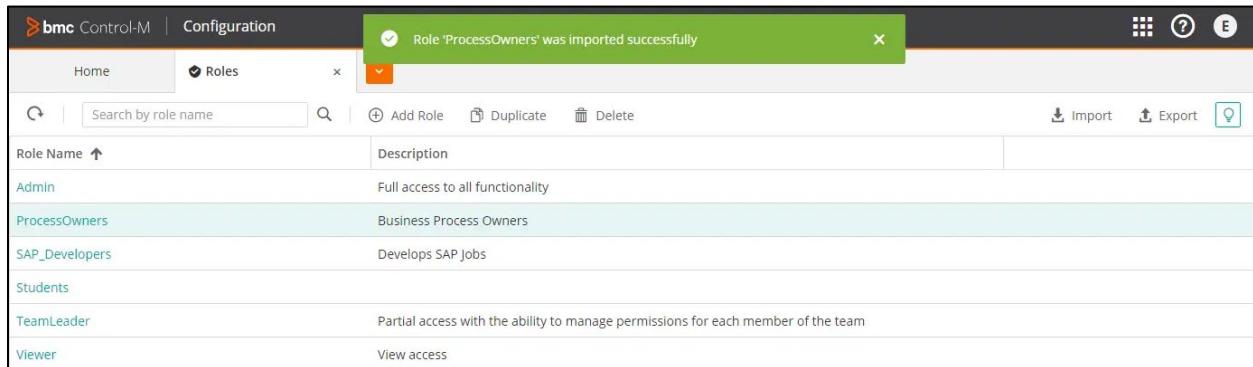
4. The role should be called **ProcessOwners**. Modify the **Name** parameter to the value **ProcessOwners**:

```
1 | { "Name": "ProcessOwners",
```

5. Change the **Description** to the value **Business Process Owners**:

```
1 | { "Name": "ProcessOwners", "Description": "Business Process Owners",
```

6. Save the file to the **Desktop** as **ProcessOwners.json**.
 7. Returning to **Control-M Web**, open the **Roles** tab in the **Configuration** domain, if it isn't already.
 8. Click **Import** and select the **ProcessOwners.json** file.



The screenshot shows the Control-M Configuration interface with the 'Roles' tab selected. A green success message at the top right states 'Role 'ProcessOwners' was imported successfully'. The main table lists various roles with their descriptions:

Role Name	Description
Admin	Full access to all functionality
ProcessOwners	Business Process Owners
SAP_Developers	Develops SAP Jobs
Students	
TeamLeader	Partial access with the ability to manage permissions for each member of the team
Viewer	View access

Lab 6.8: Defining a Control-M User Using the API

In this lab you will create a new user and assign the Viewer role to them. You will then use the simulate command to simulate their user authorizations. Next, you will assign the SAP_Developers role to them, in addition to the Viewer role, and again simulate their authorizations to compare. Following this, you will review the existing users and assign the SAP_Developers role to an existing user.

Task 1: Create a User Definitions File

Steps:

1. From the landing server (**ctmserver**) start menu, open **Notepad++**.
2. Create a new file.
3. Set the user's **Name** and **Description** parameters as follows:

```
{  
  "Name": "sdev",  
  "Description": "SAP Developer",
```

```
1 |  {  
2 |    "Name": "sdev",  
3 |    "Description": "SAP Developer",
```

4. Set the user's **FullName** to **Sally Developer**:

```
1 |  {  
2 |    "Name": "sdev",  
3 |    "Description": "SAP Developer",  
4 |    "FullName": "Sally Developer",
```

5. Add an **Authentication** object, setting the authentication method to **ControlM**, and the password to **Passw0rd**, by inputting the following:

```
"Authentication": {  
  "ControlM": {  
    "Password": "Passw0rd"  
  }  
},
```

```
1 | {  
2 |     "Name": "sdev",  
3 |     "Description": "SAP Developer",  
4 |     "FullName": "Sally Developer",  
5 |     "Authentication": {  
6 |         "ControlM": {  
7 |             "Password": "Passw0rd"  
8 |         }  
9 |     },
```

6. Finally, add the **Viewer** role and close the JSON by inputting the following:

```
"Roles": ["Viewer"]  
}
```

```
1 | {  
2 |     "Name": "sdev",  
3 |     "Description": "SAP Developer",  
4 |     "FullName": "Sally Developer",  
5 |     "Authentication": {  
6 |         "ControlM": {  
7 |             "Password": "Passw0rd"  
8 |         }  
9 |     },  
10 |     "Roles": ["Viewer"]  
11 | }
```

7. Save the file to the **Desktop** as **sdev.json**.

Task 2: Add the sdev User to the Control-M Environment

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the **sdev** user to the Control-M environment, issue the following command:
ctm config authorization:user::add C:\Users\BmcAdmin\Desktop\sdev.json

```
C:\Users\bmcadmin>ctm config authorization:user::add C:\Users\BmcAdmin\Desktop\sdev.json
{
  "message": "User was created successfully."
}

C:\Users\bmcadmin>
```

Task 3: Simulate sdev's Authorizations

With the user created and added, we can test the user's authorizations by using the simulate command.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To simulate **sdev**'s authorizations with their assigned role (**Viewer**), run:
ctm config authorization:user::simulate sdev

```
C:\Users\bmcadmin>ctm config authorization:user::simulate sdev
{
  "Name": "sdev",
  "Description": "SAP Developer",
  "FullName": "Sally Developer",
  "Authentication": {
    "ControlM": {
      "Password": "KEEP_EXISTING"
    }
  },
  "Roles": [
    "Viewer"
  ],
  "Authorization": {
    "AllowedJobs": {
      "Included": [
        [
          [
            "JobName",
            "like",
            "*"
          ]
        ]
      ]
    },
    "AllowedJobActions": {
      "ViewProperties": true,
      "Documentation": true,
      "Log": true,
      "Statistics": true,
      "ViewOutputList": true,
      "ViewJcl": true,
      "Why": true
    },
    "Privileges": {
      "ClientAccess": {
        "ControlmWebClientAccess": "Full",
        "UtilitiesAccess": "Full",
        "ApplicationIntegratorAccess": "Browse",
        "AutomationAPIAccess": "None",
        "WorkflowInsightsAccess": "Full"
      }
    }
  }
}
```

Task 4: Assign the SAP_Developers Role to the sdev User

Permissions are additive. We will assign the SAP_Developers role to the sdev user, in addition to the Viewer role they are currently assigned. In the next task, we will test the combined permissions.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To add the **SAP_Developers** role to the **sdev** user, run:

```
ctm config authorization:user:role::add sdev SAP_Developers
```

```
C:\Users\bmcadmin>ctm config authorization:user:role::add sdev SAP_Developers
{
  "message": "Role 'SAP_Developers' was successfully added to user 'sdev'."
}

C:\Users\bmcadmin>
```

Task 5: Simulate sdev's Modified Authorizations

With the SAP_Developers role added, let's again simulate and compare the user's permissions.

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To simulate **sdev**'s authorizations with their assigned roles (**Viewer** and **SAP_Developer**), run:

```
ctm config authorization:user::simulate sdev
```

Note: The below screenshot shows just a small portion of the output. Notice the **AllowedJobs** section. Both SAP folders and all jobs are referenced due to the combined roles.

```
C:\Users\bmcadmin>ctm config authorization:user::simulate sdev
{
  "Name": "sdev",
  "Description": "SAP Developer",
  "FullName": "Sally Developer",
  "Authentication": {
    "ControlM": {
      "Password": "KEEP_EXISTING"
    }
  },
  "Roles": [
    "SAP_Developers",
    "Viewer"
  ],
  "Authorization": {
    "AllowedJobs": {
      "Included": [
        [
          [
            [
              "Folder",
              "like",
              "SAP*"
            ]
          ],
          [
            [
              [
                "JobName",
                "like",
                "*"
              ]
            ]
          ]
        ]
      ],
      "Excluded": []
    }
  },
  "AllowedJobActions": {
    "ViewProperties": true,
    "Documentation": true,
    "Log": true,
    "Statistics": true,
    "ViewOutputList": true,
    "ViewJcl": true,
    "Why": true,
    "Hold": true,
    "Free": true,
    "Confirm": true
  }
}
```

Task 6: Get a List of All Defined Users and Assign the SAP_Developers Role to the s01 User

The **ctm config authorization:users::get** command produces a list of all defined Control-M users and their assigned roles. We will review the list and assign the **SAP_Developers** role to any relevant user(s).

Steps:

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To list the defined Control-M users, run:

ctm config authorization:users::get

```
C:\Users\bmcadmin>ctm config authorization:users::get
[
  {
    "name": "s01",
    "fullName": "",
    "description": "",
    "accountLockedOnDate": "",
    "memberOf": [
      "Students"
    ]
  },
  {
    "name": "emuser",
    "fullName": "emuser",
    "description": "super user - belongs to AdminGroup",
    "accountLockedOnDate": "",
    "memberOf": [
      "Admin"
    ]
  },
  {
    "name": "sdev",
    "fullName": "Sally Developer",
    "description": "SAP Developer",
    "accountLockedOnDate": "",
    "memberOf": [
      "Viewer",
      "SAP_Developers"
    ]
  }
]
C:\Users\bmcadmin>
```

3. The **s01** user should be a member of the **SAP_Developers** role. To assign the role to them, run:
ctm config authorization:user:role::add s01 SAP_Developers

```
C:\Users\bmcadmin>ctm config authorization:user:role::add s01 SAP_Developers
{
  "message": "Role 'SAP_Developers' was successfully added to user 's01'."
}
C:\Users\bmcadmin>
```

4. Run the **ctm config authorization:users::get** command a second time to verify the authorizations are now correct for all users.

```
C:\Users\bmcadmin>ctm config authorization:users::get
[
  {
    "name": "s01",
    "fullName": "",
    "description": "",
    "accountLockedOnDate": "",
    "memberOf": [
      "Students",
      "SAP_Developers"
    ]
  },
  {
    "name": "emuser",
    "fullName": "emuser",
    "description": "super user - belongs to AdminGroup",
    "accountLockedOnDate": "",
    "memberOf": [
      "Admin"
    ]
  },
  {
    "name": "sdev",
    "fullName": "Sally Developer",
    "description": "SAP Developer",
    "accountLockedOnDate": "",
    "memberOf": [
      "Viewer",
      "SAP_Developers"
    ]
  }
]
C:\Users\bmcadmin>
```

Module 7: Using Automation API Provision and Usage Services

Objectives:

- Install the Automation API Command Line Interface
- Use the Provision Service to:
 - Provision a new Control-M/Agent
 - Upgrade a Control-M/Agent
 - Install the Application Pack on a Control-M/Agent
- Use the Usage Service to generate a task usage report.

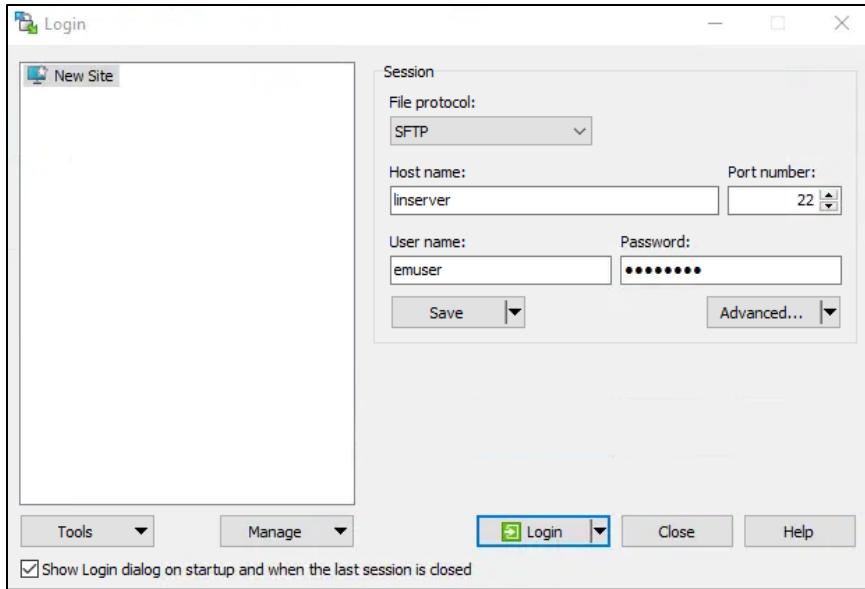
The labs for this module involve installing the Automation API CLI on the linserver host, so that the aguser UNIX user account may install the Control-M/Agent and Application Pack. The Control-M/Agent installation and upgrade packages will be transferred to the Control-M/Enterprise Manager host. We will then install the Control-M/Agent into the aguser account. Once complete we will upgrade the Agent and finally install the Application Pack on the Agent. The Usage Service will be invoked by both the command line interface and curl to provide a task license count for the current day.

Lab 7.1: Provision a Control-M/Agent Using the API

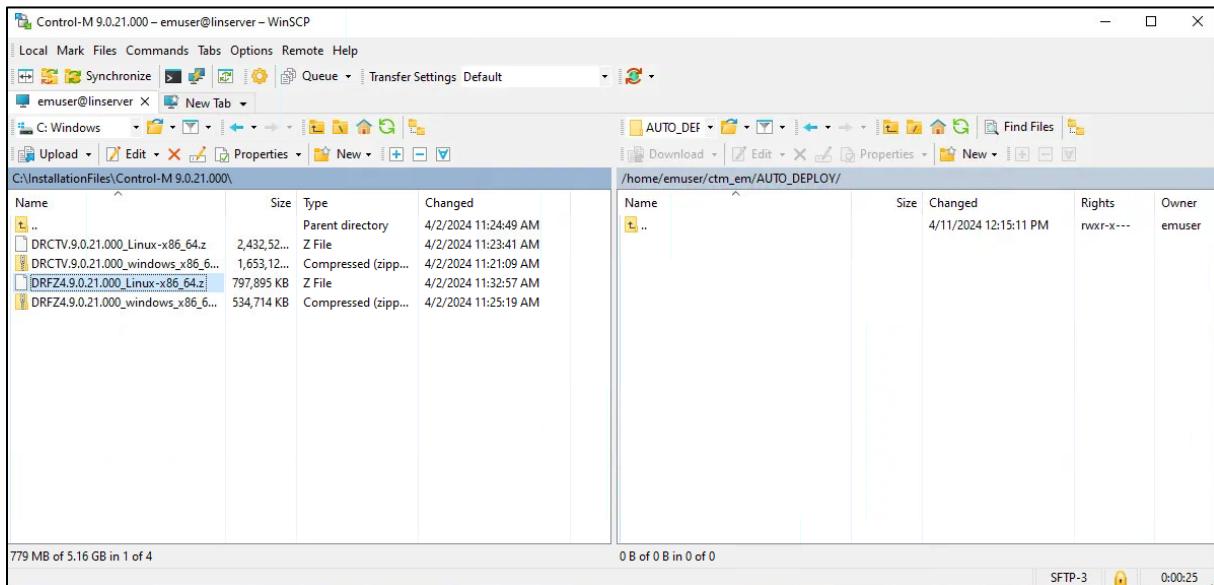
Task 1: Place the Control-M/Agent Installation Package on the Control-M/Enterprise Manager Server

Steps:

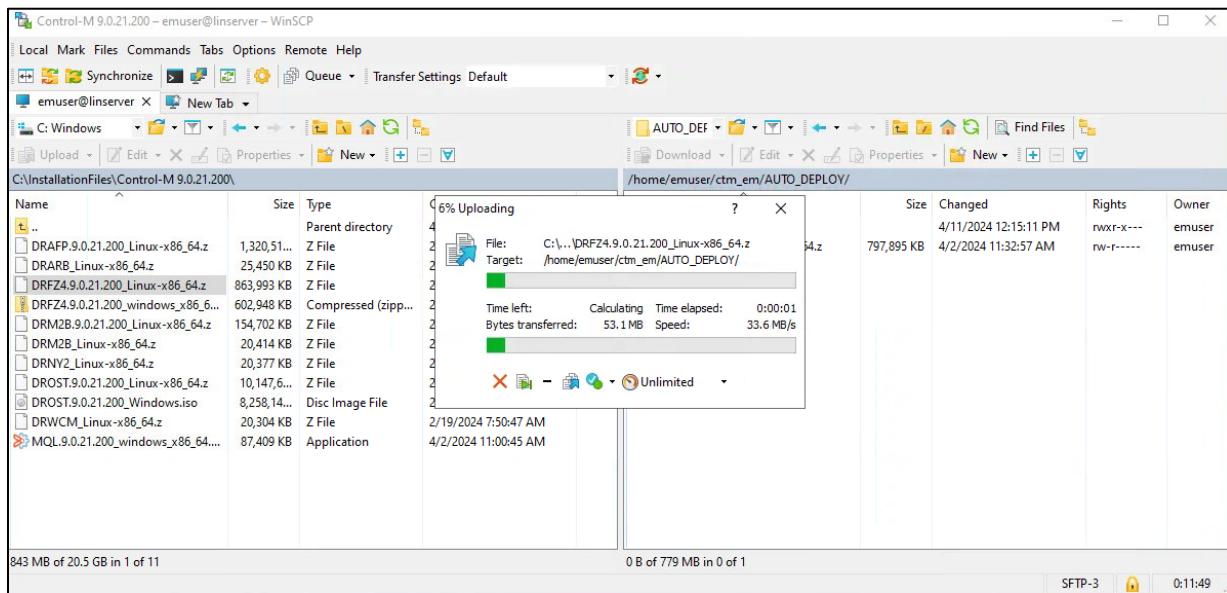
1. From the landing server (**ctmserver**) **Desktop**, open **WinSCP**.
2. From the **Login** dialog box enter the following details:
 - **Host name:** linserver
 - **User name:** emuser
 - **Password:** Passw0rd



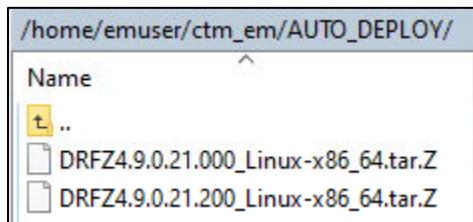
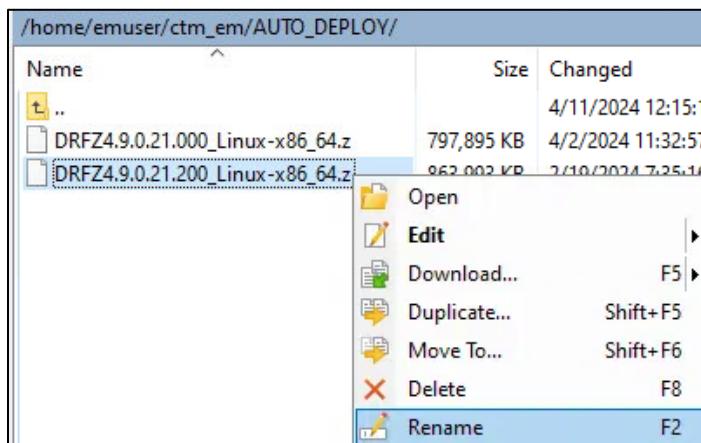
3. Click **Login**.
4. Set the left host (**ctmserver**) directory to: **C:\InstallationFiles\Control-M 9.0.21.000**.
5. Set the right host (**linserver**) directory to: **/home/emuser/ctm_em/AUTO_DEPLOY/**.
6. Drag the **DRFZ4.9.0.21.000_Linux-x86_64_.z** file from the left (**ctmserver**) to the right (**linserver**) host so that the Control-M/Agent installer is copied to the deployment directory on the Control-M/Enterprise Manager server.



7. Set the left host (**ctmserver**) directory to: **C:\InstallationFiles\Control-M 9.0.21.200**.
8. Drag the **DRFZ4.9.0.21.200_Linux-x86_64_.z** file from the left (**ctmserver**) to the right (**linserver**) host so that the Control-M/Agent upgrade file is copied to the Control-M/Enterprise Manager server.

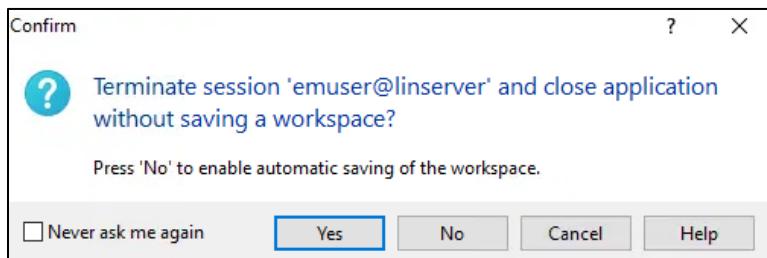


9. The Control-M/Agent packages must follow a specific name format. The current names (**DRFZ4.9.0.21.000_Linux-x86_64.z** and **DRFZ4.9.0.21.200_Linux-x86_64.z**) are not correct (.z should be .tar.Z). Right-click the Control-M/Agent installers on the **linserver** host and rename them to **DRFZ4.9.0.21.000_Linux-x86_64.tar.Z** and **DRFZ4.9.0.21.200_Linux-x86_64.tar.Z** respectively.



Note: This is how the file often appears when downloaded from the BMC EPD, so this is a typical step when placing into the deployment directory. Please note these names are case-sensitive.

10. Close **WinSCP** and state **Yes** in the dialog box to confirm.



Task 2: Install the Automation API for All Users on linserver and Create an Automation API Environment

We want to install a Control-M/Agent onto an empty account, **aguser**, on the **linserver** host. The **Provision Service** requires the **Automation API CLI** so we will first install the **Automation API CLI** for all users on this host, then add an **Environment** for the **aguser** account.

Steps:

1. From the landing server (**ctmserver**) desktop, open **PuTTY**.
2. Double-click **linserver** from the **Saved Sessions** section.
3. Login as **root** with the password: **password**.
4. The **Automation API CLI** requires **Node.js**, first enable the module stream by running **dnf module enable nodejs:18** and confirm it with **y**:

```
dnf module enable nodejs:18
```

```
[root@linserver ~]# dnf module enable nodejs:18
No such command: enable. Please use /usr/bin/dnf --help
It could be a DNF plugin command, try: "dnf install 'dnf-command(enable)'""
[root@linserver ~]# dnf module enable nodejs:18
Last metadata expiration check: 1:45:11 ago on Fri 12 Apr 2024 08:51:50 AM UTC.
Dependencies resolved.
=====
 Package           Architecture      Version       Repository      Size
=====
 Enabling module streams:
  nodejs                      18
Transaction Summary
=====
Is this ok [y/N]: y
Complete!
```

5. Next, install **Node.js** by running **dnf module install nodejs** and confirm it with **y**:

```
dnf module install nodejs
```

```
[root@linserver ~]# dnf module install nodejs
Last metadata expiration check: 1:45:41 ago on Fri 12 Apr 2024 08:51:50 AM UTC.
Dependencies resolved.

=====
Package Arch Version Repository Size
=====
Installing group/module packages:
nodejs x86_64 1:18.19.1-1.module+el8.9.0+90195+64cfbb95 ol8_appstream 14 M
npm x86_64 1:10.2.4-1.18.19.1.1.module+el8.9.0+90195+64cfbb95 ol8_appstream 2.1 M
Installing weak dependencies:
nodejs-docs
noarch 1:18.19.1-1.module+el8.9.0+90195+64cfbb95 ol8_appstream 10 M
nodejs-full-i18n
x86_64 1:18.19.1-1.module+el8.9.0+90195+64cfbb95 ol8_appstream 8.2 M
Installing module profiles:
nodejs/common

Transaction Summary
=====
Install 4 Packages

Total download size: 34 M
Installed size: 172 M
Is this ok [y/N]: y
```

6. The Automation API CLI can be pulled down from the Control-M/EM web server. To do so, run:
wget https://linserver:8446/automation-api/ctm-cli.tgz --no-check-certificate

```
[root@linserver ~]# wget https://linserver:8446/automation-api/ctm-cli.tgz --no-
check-certificate
--2024-04-12 10:38:28-- https://linserver:8446/automation-api/ctm-cli.tgz
Resolving linserver (linserver)... 192.168.1.8
Connecting to linserver (linserver)|192.168.1.8|:8446... connected.
WARNING: The certificate of 'linserver' is not trusted.
WARNING: The certificate of 'linserver' hasn't got a known issuer.
HTTP request sent, awaiting response... 200
Length: 9451969 (9.0M) [application/x-gtar]
Saving to: 'ctm-cli.tgz'

ctm-cli.tgz      100%[=====>]   9.01M  --.-KB/s   in 0.06s

2024-04-12 10:38:28 (142 MB/s) - 'ctm-cli.tgz' saved [9451969/9451969]
```

7. Finally, to install the **Automation API Command Line Interface**, run:
npm -g install ctm-cli.tgz

Note: A message may appear stating a newer version is available. Ignore the message and continue with the current version.

```
[root@linserver ~]# npm -g install ctm-cli.tgz
added 1 package in 5s
8 packages are looking for funding
  run `npm fund` for details
```

8. We'll configure the environment for the **aguser** account. Switch into the **aguser** account by running:

```
su aguser
```

9. Switch to **aguser**'s home directory by running:

```
cd /home/aguser
```

```
[root@linserver ~]# su aguser
[aguser@linserver /root]$ cd /home/aguser
[aguser@linserver ~]$ █
```

10. This is a new command line environment compared to the modules 4 and 5 labs (**ctmserver**), so we need to add a new environment to it. Run the command **ctm environment add prod https://linserver:8446/automation-api emuser -p** and when prompted enter the password: **Passw0rd** and confirm.

```
ctm environment add prod https://linserver:8446/automation-api emuser -p
```

```
[aguser@linserver ~]$ ctm environment add prod https://linserver:8446/automation-api emuser -p
Password: *****
Retype password: *****

Environment 'prod' was created
prod: {"endPoint": "https://linserver:8446/automation-api", "user": "emuser"}
[aguser@linserver ~]$ █
```

11. Verify the credentials work by typing:

```
ctm session login
```

```
[aguser@linserver ~]$ ctm session login
{
  "username": "emuser",
  "token": "4FAE3D83D4CD15F6AEC89DAEEE0263D80A0AA9D036188C0EADCEC078382E572688101F6EB5F9BE9B9D37FC1328E1
A562E4021AF99CDACA5A7CD21A0102A3FF72",
  "version": "9.21.230"
}
[aguser@linserver ~]$ █
```

Task 3: Verify the Control-M Images That Are Available to Install**Steps:**

1. Remaining in the **PuTTY** session from the last task, to verify the available Linux Control-M/Agent images that can be downloaded and installed by the API CLI, run the command:
ctm provision images Linux

```
[aguser@linserver ~]$ ctm provision images Linux
[
    "Agent.Linux",
    "Agent_18.Linux",
    "Agent_20.Linux",
    "ApplicationsAgent.Linux",
    "BigDataAgent.Linux",
    "Server.Linux",
    "Server_20.Linux"
]
[aguser@linserver ~]$ █
```

2. Note that multiple values have been returned for the Linux operating system, including multiple Control-M/Agent versions. In Task 1 we placed the version 9.0.21.000 Control-M/Agent installation file into the **AUTO_DEPLOY** directory. The **Agent.Linux** option will use this installation file when provisioned. The **ApplicationsAgent.Linux** references the **Application Pack**, which will be used in Task 7.

Task 4: Download and Prepare the Linux Agent Image**Steps:**

1. Remaining in the **PuTTY** session from the last task, as Java is used to provision images, set the **BMC_INST_JAVA_HOME** environment variable to reference the Java home directory by running the following command:

```
setenv BMC_INST_JAVA_HOME /home/aguser/OpenJDK/
```

Note: Alternatively, a JSON configuration file could be referenced that specifies javaHome as a parameter.

2. Verify the environment variable has been correctly defined by running:

```
echo $BMC_INST_JAVA_HOME
```

```
[aguser@linserver ~]$ setenv BMC_INST_JAVA_HOME /home/aguser/OpenJDK/
[aguser@linserver ~]$ echo $BMC_INST_JAVA_HOME
/home/aguser/OpenJDK/
[aguser@linserver ~]$ █
```

3. To download and prepare the Control-M/Agent image for installation, run:

ctm provision image Agent

```
[aguser@linserver ~]$ ctm provision image Agent
info: Located java at:"/home/aguser/OpenJDK//bin/java"
info: starting command: "/home/aguser/OpenJDK//bin/java" -jar "/usr/local/lib/node_modules/ctm-cli/control-m.services.provision-9.21.230.jar" -image "Agent" -agent_tag "" -server https://linserver:8446/automation-api -action image -environment prod -ctms "" -name "" -port "" -cert 0 -file "" -isSaasFromStatusRequest "false"
info: Making SSL trust all certificates and all hostnames
info: OnPrem provision delivery mode
info: image descriptor Agent was successfully downloaded and parsed
info: installing product DRFZ4.9.0.21.000_Linux-x86_64.tar.Z
info: downloading https://linserver:8446/automation-api/descriptors/ProvisionConfig.json to /home/aguser/.ctmTemp/ProvisionConfig.json
info: downloading https://linserver:8446/automation-api/DRFZ4.9.0.21.000_Linux-x86_64.tar.Z to /home/aguser/.ctmTemp/DRFZ4.9.0.21.000_Linux-x86_64.tar.Z
info: 100% (779MB/779MB) - downloading ended
```

Note: We specified **Agent** and *not Agent.Linux* when running the command. The OS platform needn't be specified as it will be automatically detected.

4. Verify the Control-M/Agent correctly downloads:

```
info: 2024-04-12 11:00:50 Tracker process stopped

info: Killing Control-M/Agent Java Process pid:141258

info: 1 seconds - 141258 is still alive

info: 2 seconds - 141258 is still alive

info: 2024-04-12 11:00:53 Java Process process stopped

info: provisioning image Agent ended successfully
info: exiting provision process with exit code (0-ok):0
info: provision image succeeded
[aguser@linserver ~]$
```

Task 5: Register the New Control-M/Agent With the Control-M/Server

Steps:

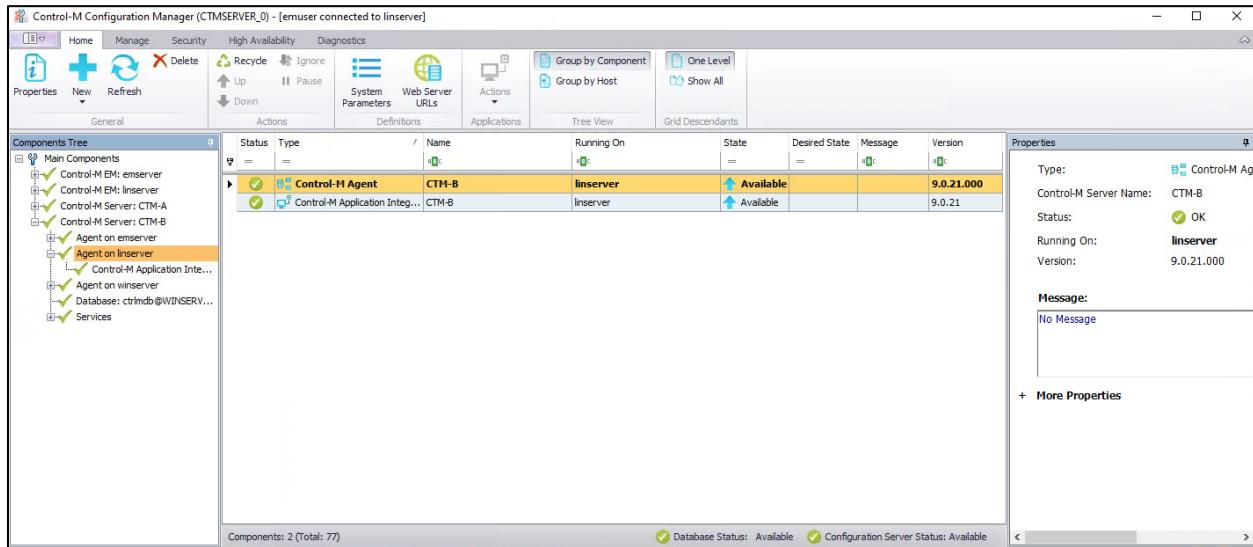
1. In the previous step, the Control-M/Agent was installed. Remaining in the PuTTY session from the last task, to configure the Control-M/Agent it and register it with the Control-M/Server run the following command:

ctm provision agent::setup CTM-B linserver

```
[aguser@linserver ~]$ ctm provision agent::setup CTM-B linserver
info: Located java at:"/home/aguser/OpenJDK//bin/java"
info: starting command: "/home/aguser/OpenJDK//bin/java" -jar "/usr/local/lib/node_modules/ctm-cli/control-m.services.provision-9.21.230.jar" -image "" -agent_tag "" -server https://linserver:8446/automation-api -action setup -environment prod -ctms "CTM-B" -name "linserver" -port "" -cert 0 -file "" -isSaaSFromStatusRequest "false"
info: Making SSL trust all certificates and all hostnames
info: OnPrem provision delivery mode
info: setting server to agent port: 7530
info: setting agent to server port: 7005
info: setting agent name (alias): linserver
info: setting primary Control-M Server: winserver
info: setting authorized Control-M Server host winserver
info: agent communication type is transient
info: agent configuration ended. restarting agent
info: adding newly active agent to Control-M Server
info: agent setup completed successfully
info: update the agent's control modules definition
info: provision setup succeeded
[aguser@linserver ~]$
```

Note: To set the Control-M/Server-to-Control-M/Agent listener port to a specific port, mention it in the command line. For example, to set 7006 as the port, the command would be: **ctm provision agent::setup CTM-B linserver 7006**

2. From the landing server (**ctmserver**) Desktop, open the **Control-M Configuration Manager** and sign in as **emuser** with the password: **Passw0rd**.
3. Verify the **linserver** Control-M/Agent appears under the **CTM-B** Control-M/Server:



4. Note the Control-M/Agent's version and the Application Plug-ins that are installed. The Agent version should be 9.0.21.000 and only the Application Integrator is installed. In the next task we will upgrade the Agent version, and then in the following task we will install the Application Pack.

Task 6: Upgrade the linserver Control-M/Agent**Steps:**

1. Remaining in the same **PuTTY** session from the last task, list available Control-M/Agent and Application Plug-in versions for the installed Control-M/Agent by running:

ctm provision upgrades::versions::get

```
[aguser@linserver ~]$ ctm provision upgrades::versions::get
[
  {
    "type": "Agent",
    "version": "9.0.21.200"
  },
  {
    "type": "Agent",
    "version": "9.0.21.000"
  },
  {
    "type": "AppPack",
    "version": "9.0.21.100"
  }
]
[aguser@linserver ~]$
```

2. The Agent can be upgraded to version **9.0.21.200**. To upgrade the Control-M/Agent, run the command:

ctm provision upgrade::install CTM-B linserver Agent 9.0.21.200

```
[aguser@linserver ~]$ ctm provision upgrade::install CTM-B linserver Agent 9.0.21.200
{
  "upgradeId": "CTM-B:1"
}
[aguser@linserver ~]$
```

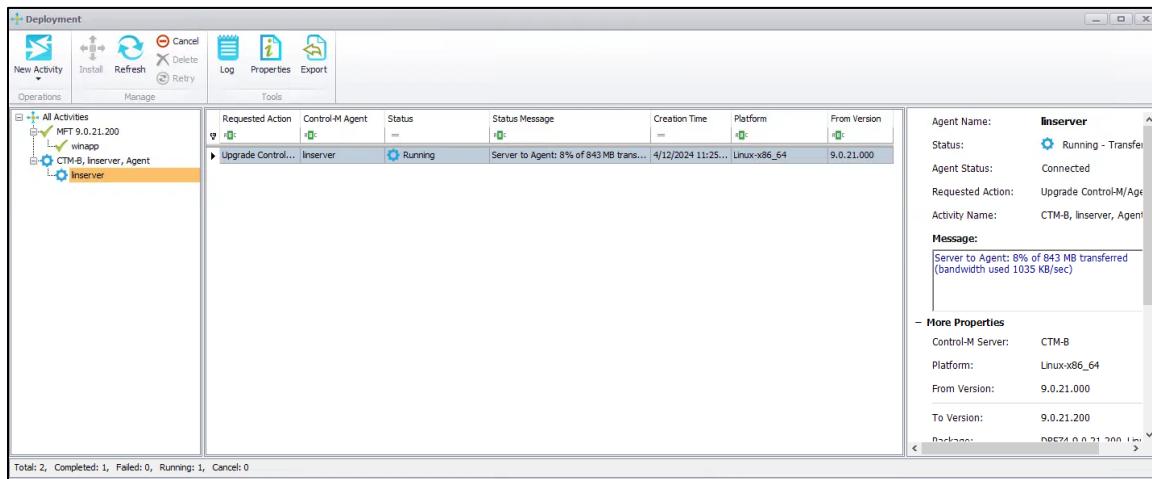
3. The command returns an **upgradeId**, that can be used to track the upgrade progress. Capture the value of the **upgradeId** and track the status by running:

ctm provision upgrade::get <upgradeID>

Note: This may take 10-15 minutes to upgrade.

```
[aguser@linserver ~]$ ctm provision upgrade::get "CTM-B:1"
{
  "upgradeId": "CTM-B:1",
  "ctm": "CTM-B",
  "agent": "linserver",
  "fromVersion": "9.0.21.000",
  "toVersion": "9.0.21.200",
  "activity": "Install",
  "status": "Running",
  "message": "Server to Agent: 4% of 843 MB transferred (bandwidth used 1040 KB/sec)",
  "creationTime": "2024-04-12T11:25:25Z",
  "transferStartTime": "2024-04-12T11:27:24Z",
  "transferEndTime": "",
  "installStartTime": "",
  "installEndTime": "",
  "activityName": "CTM-B, linserver, Agent",
  "installUser": "aguser",
  "notifyAddress": "",
  "description": "",
  "package": "DRFZ4.9.0.21.200_Linux-x86_64.tar.Z"
}
[aguser@linserver ~]$
```

4. Repeat step 3 until the upgrade completes. Alternatively, the status may be tracked from the **Manage > Deployment** window in the CCM:



```
[aguser@linserver ~]$ ctm provision upgrade::get "CTM-B:1"
{
    "upgradeId": "CTM-B:1",
    "ctm": "CTM-B",
    "agent": "linserver",
    "fromVersion": "9.0.21.000",
    "toVersion": "9.0.21.200",
    "activity": "Install",
    "status": "Completed",
    "message": "Control-M/Agent Upgrade Completed Successfully",
    "creationTime": "2024-04-12T11:25:25Z",
    "transferStartTime": "2024-04-12T11:27:24Z",
    "transferEndTime": "2024-04-12T11:46:41Z",
    "installStartTime": "2024-04-12T11:46:42Z",
    "installEndTime": "2024-04-12T11:50:56Z",
    "activityName": "CTM-B, linserver, Agent",
    "installUser": "aguser",
    "notifyAddress": "",
    "description": "",
    "package": "DRFZ4.9.0.21.200_Linux-x86_64.tar.Z"
}
[aguser@linserver ~]$
```

Task 7: Install the Application Pack on the linserver Control-M/Agent

Steps:

1. Remaining in the same **PuTTY** session from the last task, install the Application Pack on the **linserver** Control-M/Agent by running the command:

```
ctm provision upgrade::install CTM-B linserver AppPack 9.0.21.100
```

```
[aguser@linserver ~]$ ctm provision upgrade::install CTM-B linserver AppPack 9.0.21.100
{
    "upgradeId": "CTM-B:2"
}
[aguser@linserver ~]$
```

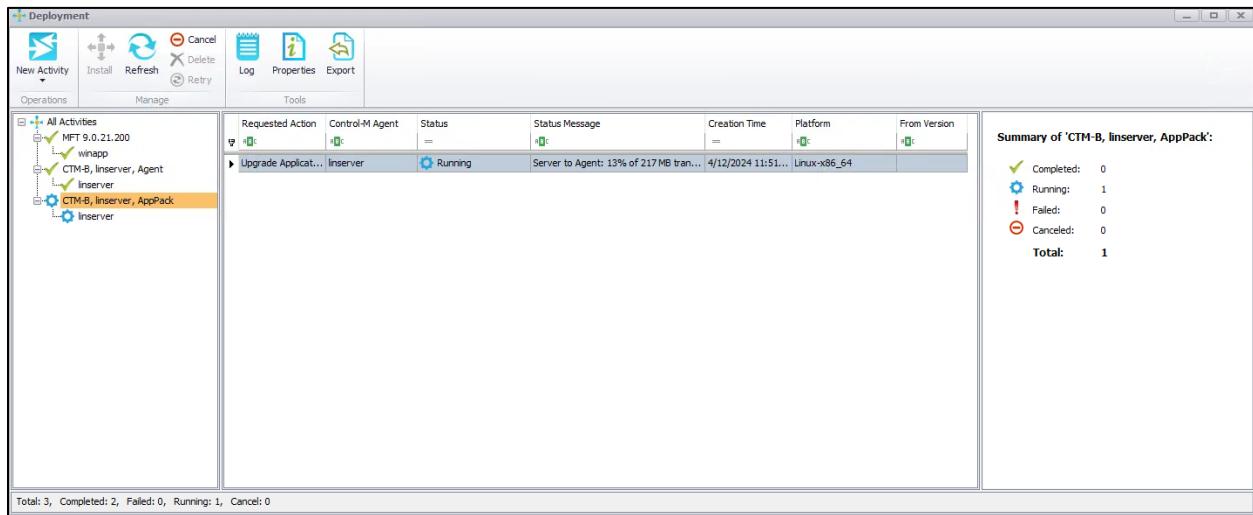
2. Again, the command returns an **upgradeId**, that can be used to track the upgrade progress. Track the status by running:

```
ctm provision upgrade::get <upgradeID>
```

Note: This may take 10-15 minutes to install.

```
[aguser@linserver ~]$ ctm provision upgrade::get "CTM-B:1"
{
  "upgradeId": "CTM-B:1",
  "ctm": "CTM-B",
  "agent": "linserver",
  "fromVersion": "9.0.21.000",
  "toVersion": "9.0.21.200",
  "activity": "Install",
  "status": "Running",
  "message": "Server to Agent: 4% of 843 MB transferred (bandwidth used 1040 KB/sec)",
  "creationTime": "2024-04-12T11:25:25Z",
  "transferStartTime": "2024-04-12T11:27:24Z",
  "transferEndTime": "",
  "installStartTime": "",
  "installEndTime": "",
  "activityName": "CTM-B, linserver, Agent",
  "installUser": "aguser",
  "notifyAddress": "",
  "description": "",
  "package": "DRFZ4.9.0.21.200_Linux-x86_64.tar.Z"
}
[aguser@linserver ~]$
```

- Repeat step 2 until the upgrade completes. Alternatively, the status may be tracked from the **Manage > Deployment** window in the CCM:



- Once the installation completes, view the installation output by running the command:

ctm provision upgrade:output::get <upgradeID>

```
[aguser@linserver ~]$ ctm provision upgrade:output::get CTM-B:2
----- Summary -----
2024/04/12 11:51:47 Determining Control-M/Agent exact platform
2024/04/12 11:51:48 Waiting for package to be transferred from Control-M/EM to Control-M/Server
2024/04/12 11:52:18 Package transferred from Control-M/EM to Control-M/Server successfully
2024/04/12 11:52:18 Transferring scripts to Control-M/Agent
2024/04/12 11:52:19 Checking pre requisites at Control-M/Agent
2024/04/12 11:52:20 Start transferring package to Control-M/Agent with size of 217 MB
2024/04/12 11:57:23 Package transferred to the Control-M/Agent successfully
2024/04/12 11:57:23 Activating Control-M Application upgrade
2024/04/12 11:57:58 Control-M Application Pack Install Completed Successfully

----- Output of preparation step (System job AutoDeployPrepare.sh (order-id tro90)) -----
++ type /home/aguser/ctm/runtime/INSTREAM_tro90_0001_AutoDeployPrepare.sh
++ awk '{print $3}'
+ SCRIPT_NAME=/home/aguser/ctm/runtime/INSTREAM_tro90_0001_AutoDeployPrepare.sh
++ dirname /home/aguser/ctm/runtime/INSTREAM_tro90_0001_AutoDeployPrepare.sh
+ SCRIPT_DIR=/home/aguser/ctm/runtime
```

Lab 7.2: Generate a Usage Report Using the API

In this lab, first you will generate a usage report using the Automation API Command Line Interface. You will then generate a usage report using curl, to illustrate that there are different ways to invoke the Automation API. Before generating a usage report using curl, an API token must be generated, as this is needed to authenticate the REST API call.

Task 1: Generate a Usage Report Using the Automation API CLI

Steps

1. From the landing server (**ctmserver**), click the **Start** menu and select **Command Prompt**.
2. To review the total number of current Active Jobs for the Control-M environment, run:
ctm usage jobs::get

```
C:\Users\bmcadmin>ctm usage jobs::get
{
  "usage": [
    {
      "server": "CTM-A",
      "jobExecution": 3
    },
    {
      "server": "CTM-B",
      "jobExecution": 72
    }
  ],
  "totalJobExecution": 75
}

C:\Users\bmcadmin>
```

Note: Feel free to experiment with ordering(/running) new jobs and re-running the command. This command will always return the current task count in the active environment (which contrasts with **Usage Alerts**, which reports on the previous day).

Task 2: Create an API Token Using the Authentication Service

Steps

1. From the landing server (**ctmserver**) **Desktop**, right-click the **APIUpdate.json** file and select **Edit with Notepad++**.
2. Modify the **tokenName** value from **emuser_AAPI_Token** to **emuser_AAPI_Token2**.

```
1  {
2    "tokenName" : "emuser_AAPI_Token2",
3    "expirationDate" : "2026-12-31",
4    "roles" : [ "Admin" ]
5 }
```

Note: This is an alternative to regenerating the API Token for the **emuser_AAPI_Token** created earlier.

3. Save the file.
4. If not already open, click the **Start** menu and select **Command Prompt**.
5. To create a new API Token, run:

ctm authentication token::create -f C:\Users\BmcAdmin\Desktop\APIUpdate.json

```
C:\Users\bmcadmin>ctm authentication token::create -f C:\Users\BmcAdmin\Desktop\APIUpdate.json
{
  "tokenName": "emuser_AAPI_Token2",
  "tokenType": "user",
  "tokenValue": "b25QcmVtOmVhNDAxZDBhLWYxNGMtNGJiYi05OWIyLWU2MDc2MnEwNTg4OQ==",
  "user": "emuser",
  "roles": [
    "Admin"
  ],
  "expirationDate": "2026-12-31",
  "createdDate": "2024-04-12T12:04:50.398207Z",
  "lastUpdatedDate": "2024-04-12T12:04:50.398210Z"
}
```

6. Copy the **tokenValue** by selecting the token and then right-clicking.

```
C:\Users\bmcadmin>ctm authentication token::create -f C:\Users\BmcAdmin\Desktop\APIUpdate.json
{
  "tokenName": "emuser_AAPI_Token2",
  "tokenType": "user",
  "tokenValue": "b25QcmVtOmVhNDAxZDBhLWYxNGMtNGJiYi05OWIyLWU2MDc2MmEwNTg4OQ==",
  "user": "emuser",
  "roles": [
    "Admin"
  ],
  "expirationDate": "2026-12-31",
  "createdDate": "2024-04-12T12:04:50.398207Z",
  "lastUpdatedDate": "2024-04-12T12:04:50.398210Z"
}
```

Task 3: Generate a Usage Report using Curl

Steps

1. If not already open, click the **Start** menu and select **Command Prompt**.
2. To run a usage report via curl, run (substituting <API Token> for the API token copied in the previous task):

```
curl -H "x-api-key: <API Token>" -X GET https://linserver:8446/automation-api/usage/jobs -k
```

```
C:\Users\bmcadmin>curl -H "x-api-key: b25QcmVtOmVhNDAxZDBhLWYxNGMtNGJiYi05OWIyLWU2MDc2MmEwNTg4OQ==" -X GET https://linserver:8446/automation-api/usage/jobs -k
{
  "usage" : [ {
    "server" : "CTM-A",
    "jobExecution" : 0
  }, {
    "server" : "CTM-B",
    "jobExecution" : 90
  } ],
  "totalJobExecution" : 90
}
C:\Users\bmcadmin>
```

Module 8: SSL Configuration

Objectives:

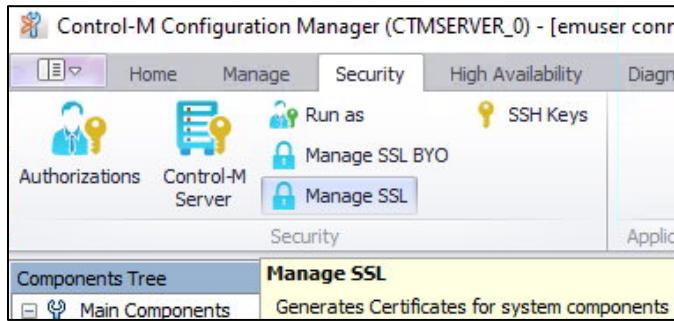
- Generate self-signed certificates
- Configure SSL in Zones 1, 2 and 3

Lab 8.1: Generating Self-Signed Certificates

Task 1: Create a Certificate Authority and Generate Self-Signed Certificates for All Control-M Components

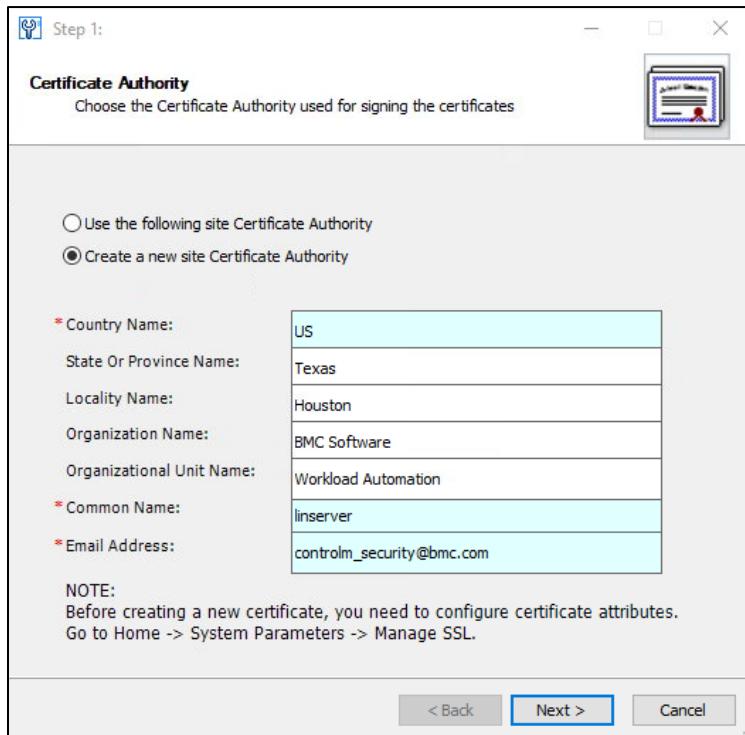
Steps:

1. From the landing server (**ctmserver**) Desktop, open the **Control-M Configuration Manager** and sign in as **emuser** with the password: **Passw0rd**.
2. Go to the **Security** tab and click **Manage SSL** from the ribbon.



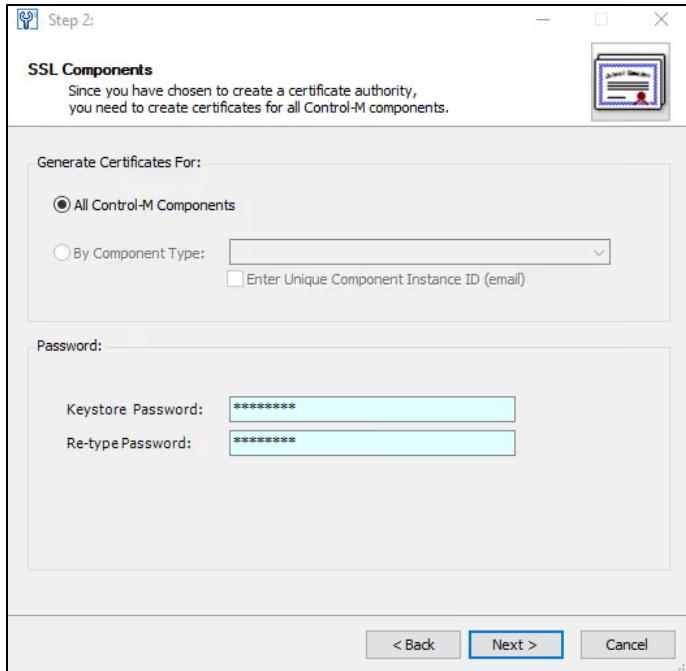
3. In Step 1, Select **Create a new site Certificate Authority**.
4. When prompted to confirm, click **Yes**.
5. Enter the following details:
 - **Country Name:** US
 - **State Or Province Name:** Texas
 - **Locality Name:** Houston
 - **Organization Name:** BMC Software
 - **Organizational Unit Name:** Workload Automation
 - **Common Name:** linserver

- **Email Address:** controlm_security@bmc.com



Note: It is imperative that the Common Name is the Fully Qualified Domain Name (FQDN) of the Enterprise Manager Server(s).

6. Click **Next**.
7. In **Step 2**, set the **Keystore Password** to **abcd1234** and confirm. Click **Next**.



8. On **Step 3**, verify the certificate path is **C:\Users\bmcadmin\Documents\Control-M Certificates**. Click **Next**.
9. On **Step 4**, verify that the certificates for all components (Control-M/Agent, Control-M/Server, Control-M for z/OS, Control-M/Enterprise Manager Servers, Control-M/Enterprise Manager Client) are listed for creation and click **Submit**.
10. Verify each certificate has been generated (denoted by the green check mark in the **Status** column). Close the **Action Result** window.

The screenshot shows the 'Action Result' window. The title bar says 'Action Result'. The main area is a table with columns: Status, Host, Time, Action, and Message. All entries show a green checkmark in the 'Status' column and 'Success' in the 'Host' column. The 'Time' column shows dates like '4/12/2024'. The 'Action' column shows actions like 'Generate SSL Certificate, batc...'. The 'Message' column contains detailed paths for each component's certificate. A status message on the right side of the window reads: 'The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_Agent. Request Time: 4/12/2024 12:18:33 PM'.

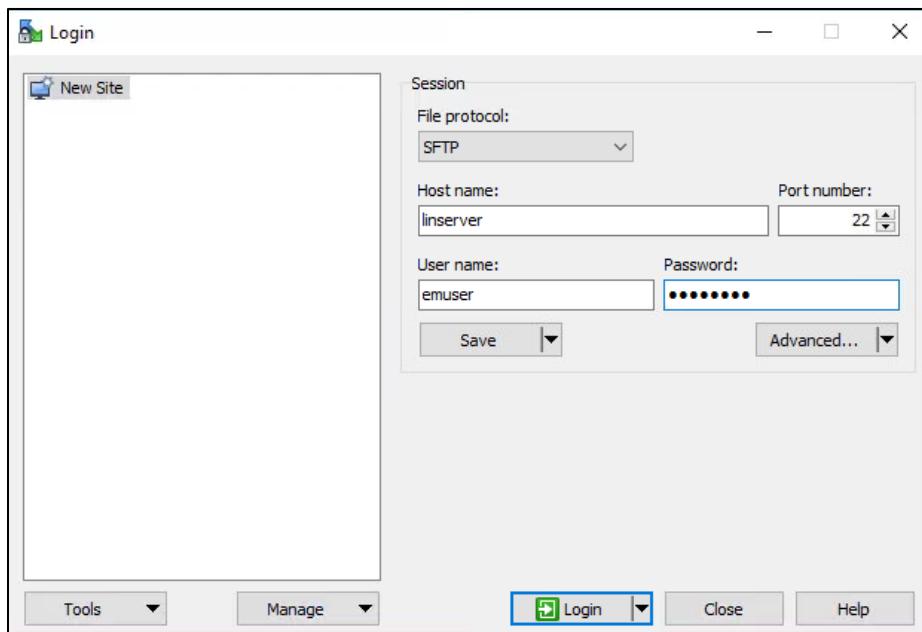
Status	Host	Time	Action	Message
Success	CONTROL-M/Agent	4/12/2024	Generate SSL Certificate, batc...	The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_Agent. Request Time: 4/12/2024 12:18:33 PM
Success	CONTROL-M/Server	4/12/2024	Generate SSL Certificate, batc...	The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_Server. Request Time: 4/12/2024 12:18:33 PM
Success	CONTROL-M for z/OS	4/12/2024	Generate SSL Certificate, batc...	The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_for_zOS. Request Time: 4/12/2024 12:18:33 PM
Success	CONTROL-M/Enterprise Manager Servers	4/12/2024	Generate SSL Certificate, batc...	The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_Enterprise_Manager_Servers. Request Time: 4/12/2024 12:18:33 PM
Success	CONTROL-M/Enterprise Manager Client	4/12/2024	Generate SSL Certificate, batc...	The certificate will be in: C:\Users\bmcadmin\Documents\Control-M Certificates\Certificate_for_CONTROL-M_Enterprise_Manager_Client. Request Time: 4/12/2024 12:18:33 PM
Success	SSL Component	4/12/2024	Generate SSL Certificate, batc...	Generated Certificate Authority controlm_securit...

Lab 8.2: Configuring SSL in Zone 1

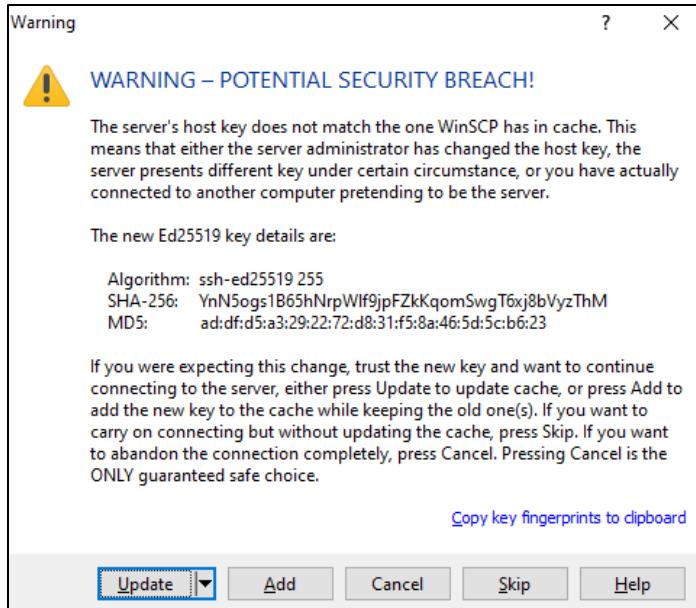
Task 1: Copy the Control-M/Enterprise Manager Server Certificate to the Control-M/Enterprise Manager Server

Steps:

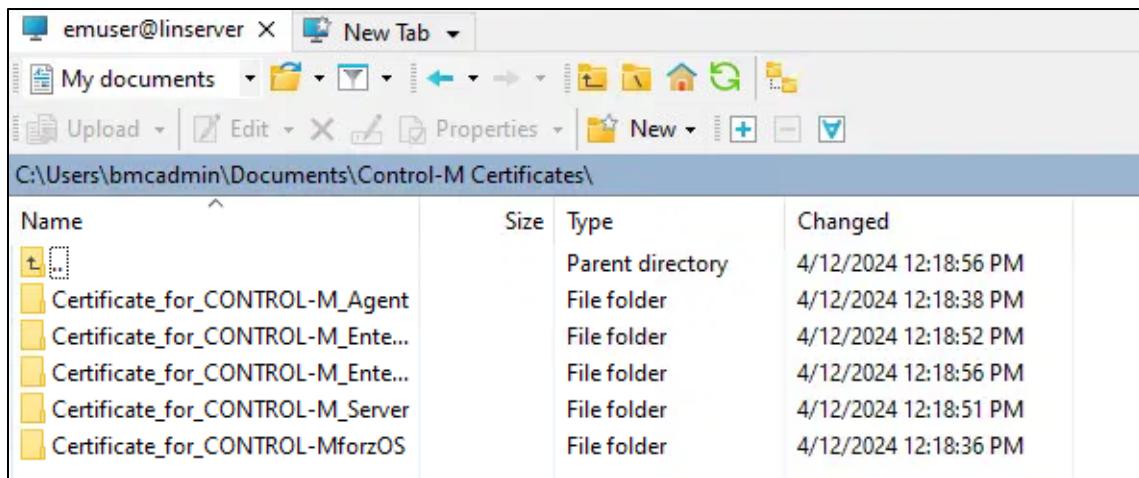
1. From the landing server (**ctmserver**) desktop, open **WinSCP**.
2. **Login** using following details:
 - **Host name:** linserver
 - **User name:** emuser
 - **Password:** Passw0rd



3. Click **Login**.
4. If a message appears warning of a potential security breach, this is due to the host key changing and is expected. Click **Update**.



- To change the directory of the left host (**ctmserver**), click the **Open Directory** (folder icon) and enter the directory name: **C:\Users\BmcAdmin\Documents\Control-M Certificates**



- Drag the **Certificate_for_CONTROL-M_EnterpriseManagerServers** directory from the left (**ctmserver**) to the right (**linserver**) host so that the Control-M/EM certificate is copied to the Control-M/EM server.

Name	Size	Changed	Rights	Owner
..		2/19/2024 7:47:52 AM	rwxr-xr-x	root
bin		4/11/2024 3:51:49 PM	rwxr-xr-x	emuser
BMCINSTALL		4/11/2024 12:18:30 PM	rwxrwxr-x	emuser
bmcperl		4/11/2024 12:09:14 PM	rwxr-x---	emuser
bmcpython		4/11/2024 12:09:08 PM	rwxr-x---	emuser
Certificate_for_CONTROL-M_EnterpriseManagerServers		4/12/2024 12:23:15 PM	rwxr-x---	emuser
ctm_em		4/11/2024 12:15:11 PM	rwxr-x---	emuser
InstallationFiles		4/11/2024 11:54:06 AM	rwxrwxr-x	emuser
kafka		12/22/2022 7:03:34 AM	rwxr-x---	emuser
OpenJDK		4/1/2024 1:54:23 PM	rwxrwxr-x	emuser
usagetool		4/11/2024 12:08:27 PM	rwxrwxr-x	emuser
installed-versions.txt	1 KB	4/11/2024 3:51:54 PM	rw-r-----	emuser
java0.log	0 KB	4/12/2024 8:09:04 AM	rw-r-----	emuser
java0.log.lck	0 KB	4/11/2024 12:15:28 PM	rw-r-----	emuser
PADEV.9.0.21.230_Linux-x86_64_INSTALL.BIN	351,089 KB	4/11/2024 3:41:54 PM	rwxr-x---	emuser
plugins-installed-versions.txt	3 KB	4/11/2024 12:14:03 PM	rwxr-x---	emuser
provision_2024-04-12_091017.log	73 KB	4/12/2024 9:10:29 AM	rw-r-----	emuser

7. Close WinSCP.
8. Click Yes in the confirmation dialogue box.

Task 2: Deploy the Certificate to the Control-M/Enterprise Manager Web Server

Steps:

1. From the landing server (ctmserver) desktop, double-click PuTTY to open a connection to linserver.
2. Sign in as emuser with the password Passw0rd.
3. First, we need to create the **tomcat.p12** file from the defined certificates. Switch to the **Certificates** directory by running the following command:
cd Certificate_for_CONTROL-M_EnterpriseManagerServers
4. To create the **tomcat.p12** file, run the following command:
openssl pkcs12 -in CertDemoU.pem -inkey CertDemoU_pk.pem -export -passout pass:abcd1234 -passin pass:abcd1234 -CAfile new_ca.pem -chain -out tomcat.p12

```
linserver% cd Certificate_for_CONTROL-M_EnterpriseManagerServers/
linserver% openssl pkcs12 -in CertDemoU.pem -inkey CertDemoU_pk.pem -export -passout pass:abcd1234 -passin pass:abcd1234 -CAfile new_ca.pem -chain -out tomcat.p12
linserver%
```

5. Change to the **ssl** directory by entering the following command:
cd .. /ctm_em /ini /ssl
6. Stop the **Web Server** and **Configuration Agent** by entering the following commands (enter the password **Passw0rd** and Y to confirm the shutdown of the Configuration Agent):
stop_web_server
stop_config_agent

```

linserver% cd ../ctm_em/ini/ssl
linserver% stop_web_server
Stopping Webserver ...
Tomcat Application name [emtomcat]
Webserver has been stopped ...
Getting Webserver status
----- EmwebStatus Begin -----
Checking Tomcat process
Tomcat Process [DOWN]
=====
[HTTP Connectors]
  Port: [18080], Status: [DOWN]
[HTTPS Connectors]
  Port: [8446], Status: [DOWN]
=====
--> Web server [DOWN]
=====

web server is not running
----- EmwebStatus End -----
linserver% stop_config_agent
Enter the CONTROL-M/EM DBO password:
Stopping the CONTROL-M/EM Configuration Agent will prevent you from managing local CONTROL-M/EM components!
Are you sure you want to stop the CONTROL-M/EM Configuration Agent ?? [y/n] : y
*****
Stop command has been issued to Config_Agent on linserver
CONTROL-M/EM Configuration Agent is DOWN !
linserver% 

```

7. Backup the existing certificate by entering the command: **mv tomcat.p12 tomcat.p12.bak**
8. Copy the new certificate into this directory by entering the command:
cp /home/emuser/Certificate_for_CONTROL-M_EnterpriseManagerServers/tomcat.p12 tomcat.p12

```

linserver% mv tomcat.p12 tomcat.p12.bak
linserver% cp /home/emuser/Certificate_for_CONTROL-M_EnterpriseManagerServers/tomcat.p12 tomcat.p12
linserver% ls
elastic_ca_key.pem elastic_ca.pem genDemoP12openssl.cfg out tomcat.ini tomcat.p12 tomcat.p12.bak
linserver% 

```

9. Next, configure the web server by entering the command: **manage_webserver**
10. Enter option **1 (Tomcat Configuration)** and press **Enter**.

```

linserver% manage_webserver
*****
***** Tomcat Configuration Manager *****
*****
***      1. Tomcat Configuration
***      2. Security Filters Configuration
***      3. Stop Web Server
***      4. Web Server Status
***      e. Exit
*****
Enter An Option Number [use 'e' to exit]: 1

```

11. From the Tomcat Configuration Manager:

- To **Backup All Configurations**, enter option 7.
- To open **SSL Mode**, enter option 4
 - To confirm you want to edit the configuration and enable SSL, Enter **Y** twice.
- To open the **Secure Connector Configuration**, enter option 3.
 - To **Edit SSL Connector**, enter option 3.
 - To edit the **https://linserver:8446/** secure connector, enter option 1.
 - To update the keystore password, enter option 9.
 - Enter the new value for password: **abcd1234**. Press **Enter**.
 - To save the configuration, enter **s**.
 - To confirm, enter **Y**.
 - Enter **b** to go back.
 - Enter **e** to exit the tool.

```

8_GCM_SHA256,TLS_EMPTY_RENEGOTIATION_INFO_SCSVF]
===
  2. SSLEnabled: [true]
  3. clientAuth: [false]
  4. compressableMimeType: [text/html,text/xml,text/plain,text/css,text/javascript,application/javascript]
  5. compression: [on]
  6. compressionMinSize: [2048]
  7. connectionTimeout: [320000]
  8. keystoreFile: [/home/emuser/ctm_em/ini/ssl/tomcat.p12]
  9. keystorePass: [abcd1234] (*)
  10. keystoreType: [PKCS12]
  11. maxHttpHeaderSize: [65536]
  12. maxIdleTime: [320000]
  13. maxThreads: [400]
  14. minSpareThreads: [20]
  15. noCompressionUserAgents: [ozilla,traviata]
  16. port: [8446]
  17. protocol: [com.bmc.ctmem.tomcat.Http]
  18. scheme: [https]
  19. secure: [true]
  20. server: [Web Server]
  21. sslEnabledProtocols: [TLSv1.2]
  22. sslProtocol: [TLSv1.2]
    s. Save
    b. Back
=====

Enter An Option Number [use 'b' to back]: s
Save the new configuration (Y/N) ? Y

```

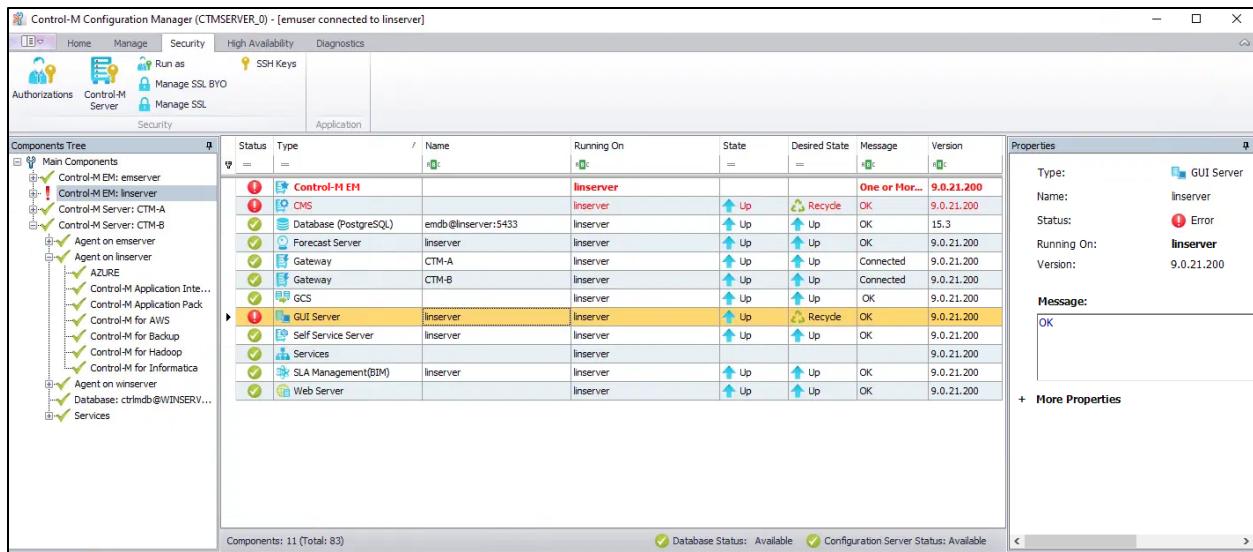
12. Start the Web Server and Configuration Agent with the following commands:

start_web_server
start_config_agent

Note: Keep the **PuTTY** session open for the next task.

13. From the landing server (ctmserver) Desktop, open Control-M Configuration Manager **CTMSERVER_0.**

14. Recycle the Control-M EM: linserver components: CMS and GUI Server.



Task 3: Extract and Install the Root CA Certificate Onto ctmserver

With the certificate installed onto the Control-M/Enterprise Manager server, next extract the Root CA Certificate from the tomcat.p12 certificate that was generated. This will allow you to connect the Control-M Client instances to the updated Web Server.

Steps:

1. Remaining on the **linserver PuTTY** session from the last task, enter the following command to extract the **Root CA** certificate:

```
openssl pkcs12 -in tomcat.p12 -cacerts -nokeys > /home/emuser/cacert.crt
```

Note: This assumes you are in the ssl directory used in the previous task. If this command does not work, switch into the directory by typing **cd /home/emuser/ctm_em/ini/ssl** and run the command again.

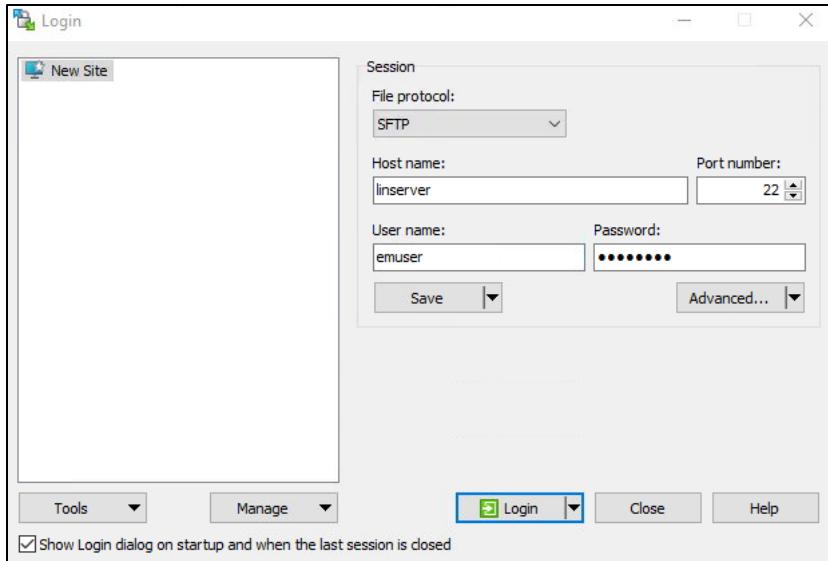
2. Enter the Import Password **abcd1234**.

```
linserver% openssl pkcs12 -in tomcat.p12 -cacerts -nokeys > /home/emuser/cacert.crt
Enter Import Password:
linserver%
```

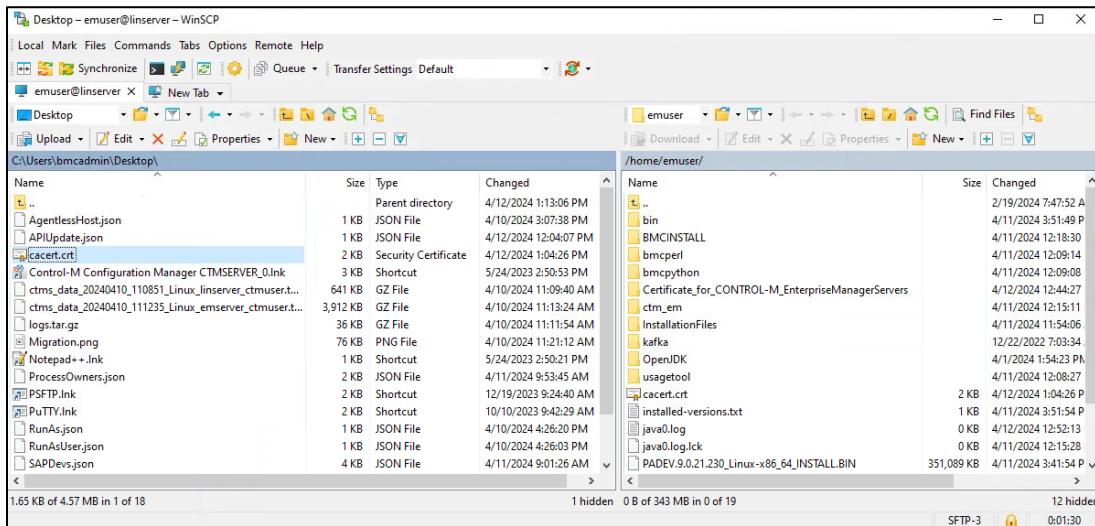
3. From the landing server (**ctmserver**) **Desktop**, open WinSCP.

4. Login using the following details:

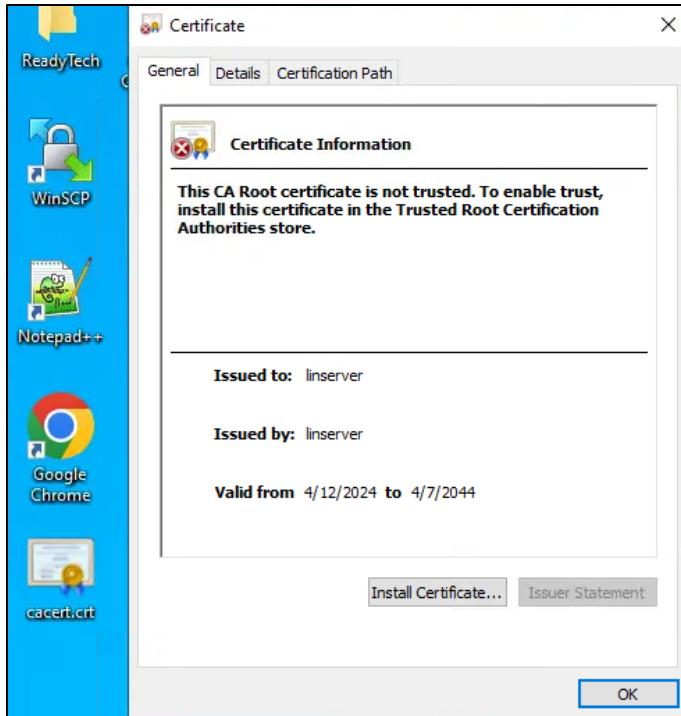
- **Host name:** linserver
- **User name:** emuser
- **Password:** Passw0rd



5. Change the left host (**ctmserver**) directory to **C:\Users\bmcadmin\Desktop**.
6. Drag the **cacert.crt** file from the right host (**linserver**) to the left host (**ctmserver**).

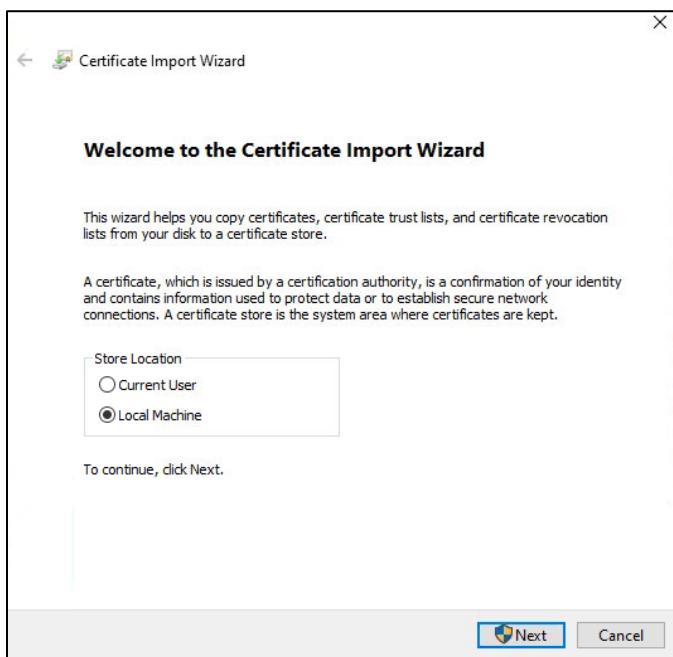


7. Close the **WinSCP** window and click **Yes** to confirm.
8. From the landing server (**ctmserver**) desktop, double-click **cacert.crt**.

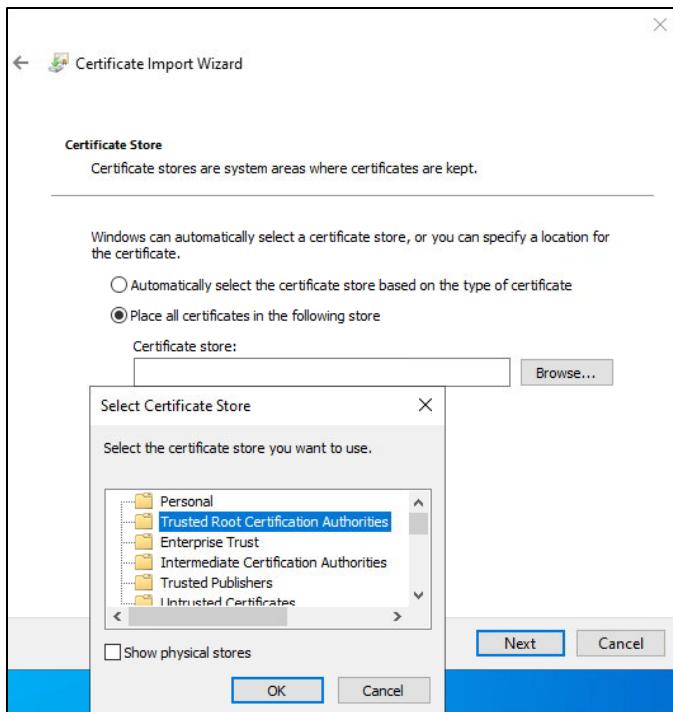


9. Click **Install Certificate....**

10. From the **Certificate Import Wizard**, select **Store Location > Local Machine** and click **Next**.

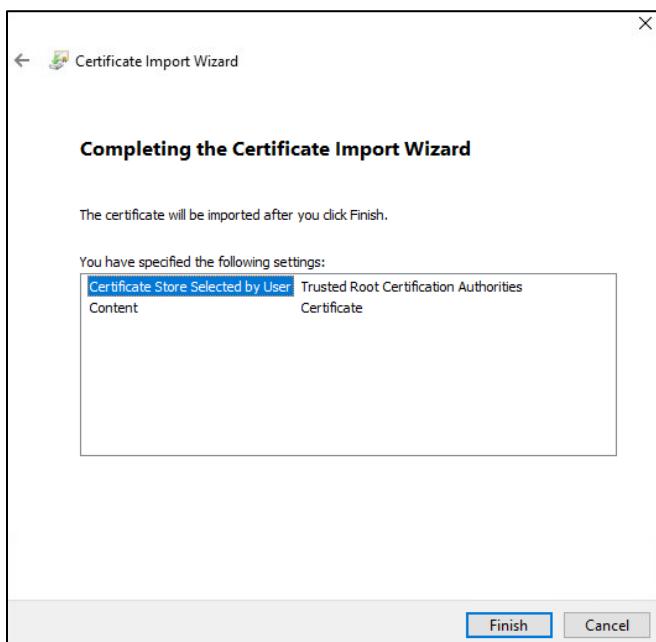


11. From the next page, select **Place all certificates in the following store** and **Browse to Trusted Root Certification Authorities**.

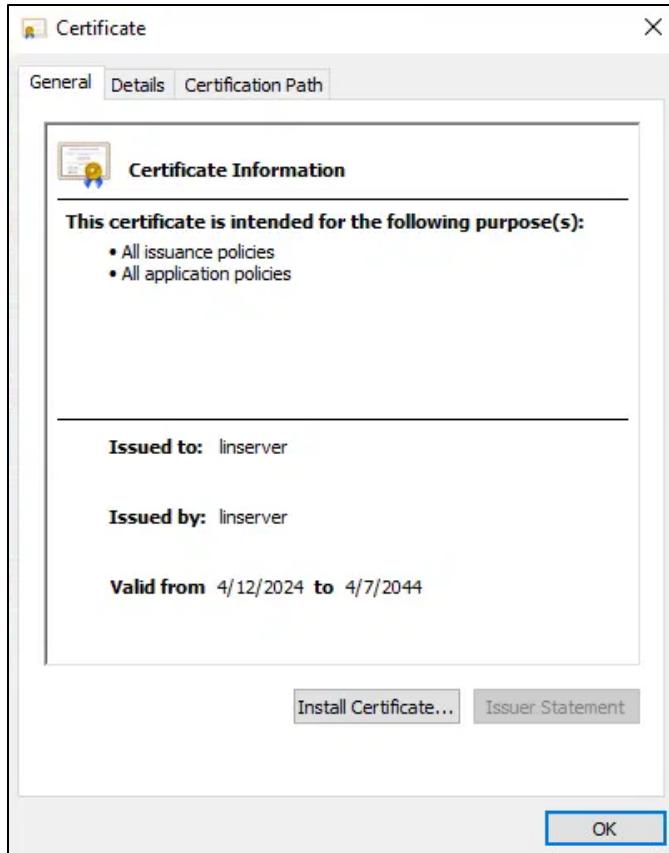


12. Click **Next**.

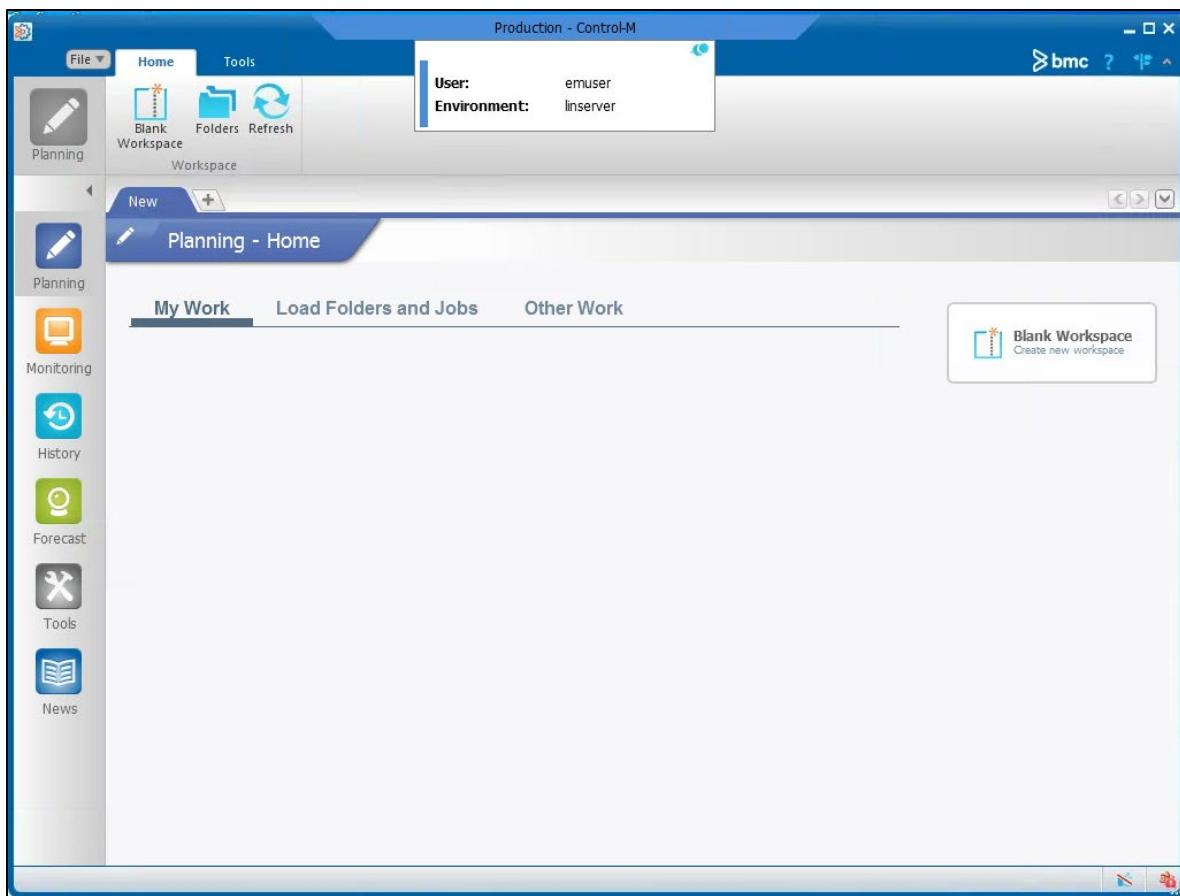
13. Click **Finish** to complete the certificate import, then **OK** to exit.



14. From the landing server (**ctmserver**) **Desktop**, once again double-click the **cacert.crt** file. Notice the details on the **General** page. The certificate is now trusted.



15. Next, we will verify we can sign in from the **Client** host. From the landing server (**ctmserver**) **Desktop**, double-click **Control-M CTMSERVER_0**.
16. Sign in as **emuser** with the password: **Passw0rd**.



Lab 8.3: Configuring SSL in Zones 2 and 3

Task 1: Deploy the SSL Certificate to the Control-M/Enterprise Manager Server (to enable Control-M/EM to Control-M/Server communication)

Steps:

1. From the landing server (**ctmserver**) Desktop, open a **PuTTY** session to **linserver**.
2. Sign in as **emuser** with the password: **Passw0rd**.
3. On the **linserver** **PuTTY** session enter the following command to enable SSL:

```
/home/emuser/ctm_em/bin/ctmkeytool -keystore  
/home/emuser/Certificate_for_CONTROL-M_EnterpriseManagerServers/gtwcert.p12 -  
password abcd1234 -passwkey  
/home/emuser/ctm_em/etc/site/resource/local/tree.bin
```

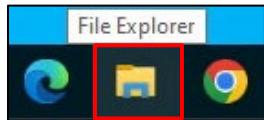
```
linserver% /home/emuser/ctm_em/bin/ctmkeytool -keystore /home/emuser/Certificate_for_CONTROL-M_Enterpris  
eManagerServers/gtwcert.p12 -password abcd1234 -passwkey /home/emuser/ctm_em/etc/site/resource/local/tre  
e.bin  
Component: Control-M/Enterprise Manager  
Importing keystore '/home/emuser/Certificate_for_CONTROL-M_EnterpriseManagerServers/gtwcert.p12'  
Keystore successfully imported to '/home/emuser/ctm_em/etc/site/resource/ssl/cert/ctmkeystore.p12'  
linserver%
```

4. Recycle the **CMS**, **GUI Server**, and **Web Server** components in the CCM. This will temporarily suspend any open Control-M Web, GUI or CCM sessions.

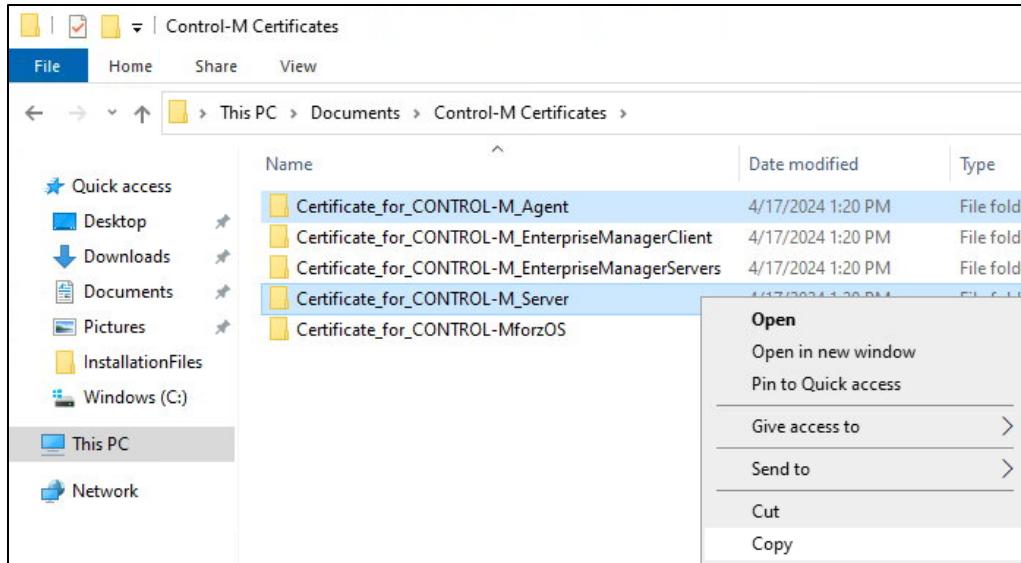
Task 2: Deploy the SSL Certificate to the CTM-B Control-M/Server

Steps:

1. From the landing server (**ctmserver**) toolbar, click **File Explorer**.



2. Browse to **C:\Users\bmcadmin\Documents\Control-M Certificates**.
3. We are going to be deploying SSL certificates onto the CTM-B Control-M/Server (**winserver**). As Control-M/Servers also contain a Control-M/Agent, select both the **Certificate_for_CONTROL-M_Server** and **Certificate_for_CONTROL-M_Agent** directories and copy them.



4. From the landing server (**ctmserver**) click Start > Remote Desktop Connection.
5. Sign into **winserver** using the password: **Passw0rd**.



6. From the **winserver** taskbar, click **File Explorer**.
7. Browse to **C:**.
8. Paste the certificates that were copied in step 3.

Name	Date modified	Type	Size
Changelogs	2/21/2024 6:33 AM	File folder	
InstallationFiles	2/20/2024 1:56 PM	File folder	
Packages	10/10/2023 9:14 AM	File folder	
PerfLogs	5/8/2021 8:20 AM	File folder	
Program Files	4/17/2024 9:24 AM	File folder	
Program Files (x86)	10/10/2023 11:32 AM	File folder	
ReadyTech	10/10/2023 9:14 AM	File folder	
SQL2019	10/10/2023 12:19 PM	File folder	
SQL2022	10/10/2023 11:22 AM	File folder	
Temp	5/5/2023 2:22 PM	File folder	
Users	5/10/2023 9:32 AM	File folder	
Windows	10/10/2023 10:00 AM	File folder	
WindowsAzure	4/17/2024 7:54 AM	File folder	
axis-install-system-agent-log.txt	4/17/2024 7:54 AM	Text Document	1 KB
axis-script-log.txt	4/17/2024 7:54 AM	Text Document	21 KB
system_agent_config.xml	4/17/2024 7:54 AM	XML Document	1 KB
Certificate_for_CONTROL-M_Server	4/17/2024 1:46 PM	File folder	
Certificate_for_CONTROL-M_Agent	4/17/2024 1:46 PM	File folder	

9. Open the **winserver** command line interface (**Start > Command Prompt**).
10. Switch to the Control-M/Server installation directory by running:
cd "C:\Program Files\BMC Software\Control-M Server"
11. Copy the certificate scripts to the **\SSL\Manage** directory by running the following command:
copy /Y "ctm_server\data\SSL\manage*\" "C:\Certificate_for_CONTROL-M_Server"

```
C:\Users\bmcadmin>cd "C:\Program Files\BMC Software\Control-M Server"
C:\Program Files\BMC Software\Control-M Server>copy /Y "ctm_server\data\SSL\manage\*\" "C:\Certificate_for_CONTROL-M_Server"
ctm_server\data\SSL\manage\README.txt
ctm_server\data\SSL\manage\setup.bat
ctm_server\data\SSL\manage\setup.pl
      3 file(s) copied.

C:\Program Files\BMC Software\Control-M Server>
```

12. Stop the **Control-M/Server Configuration Agent** and **Control-M/Server** processes by running the following command:
shut_ca && shut_ctm

```
C:\Program Files\BMC Software\Control-M Server>shut_ca && shut_ctm
-----
Shutting down CONTROL-M Configuration Agent
-----
...
CONTROL-M is running.
-----
Shutting down CTM server.
-----
Waiting ...
shutting down services...
C:\Program Files\BMC Software\Control-M Server>
```

13. Deploy the certificate by running the following command:

"C:\Certificate_for_CONTROL-M_Server\setup.bat"

```
C:\Program Files\BMC Software\Control-M Server>C:\Certificate_for_CONTROL-M_Server\setup.bat
Starting setup...
C:\Program Files\BMC Software\Control-M Server\ctm_server\data\SSL\cert\ess.txt -> C:\Program Files\BMC Software\Control-M Server\ctm_server\data\SSL\cert\ess.txt_2.bak
1 File(s) copied
updating password...
updating password completed.
running ctmkeytool...
setup completed successfully.

C:\Program Files\BMC Software\Control-M Server>
```

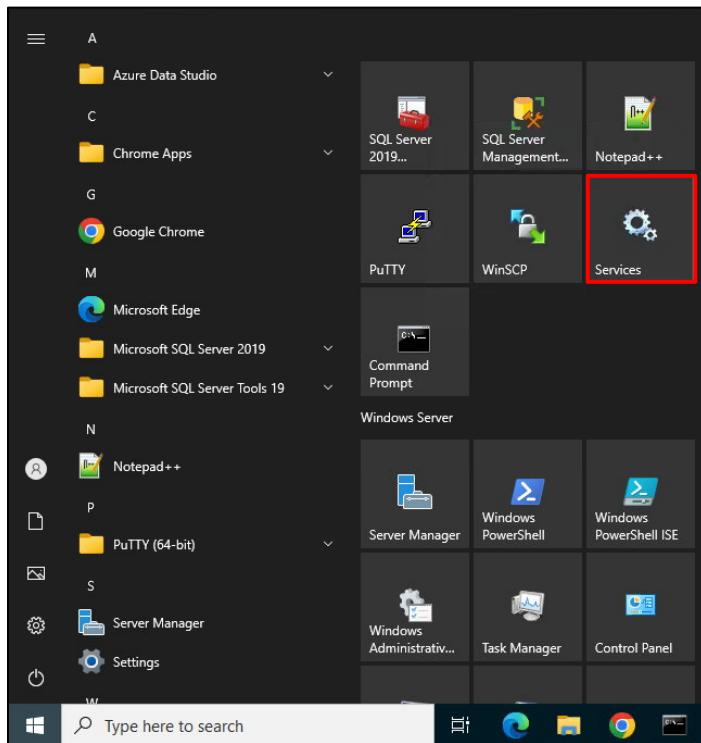
14. Start the Control-M/Server processes by running the command:

start_ctm && start_ca

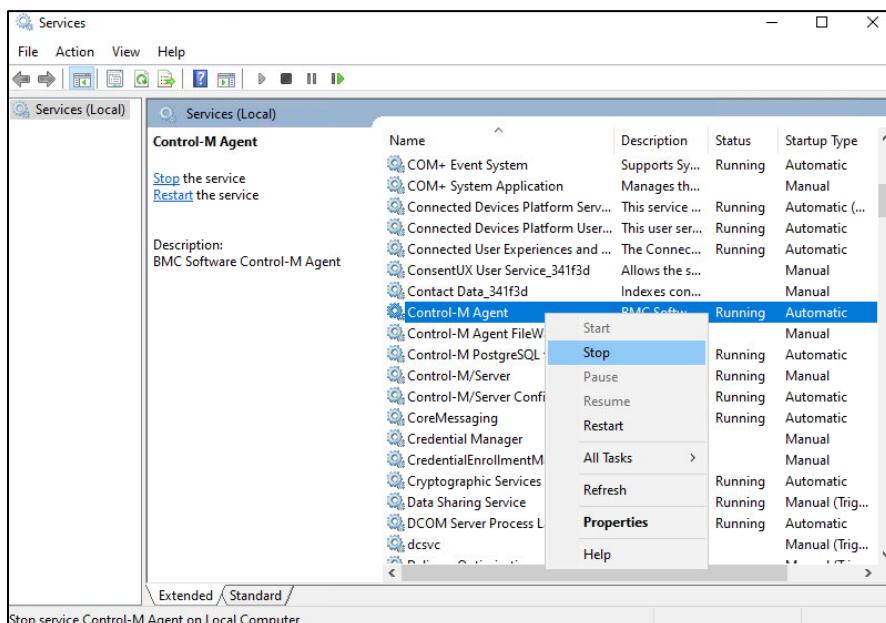
```
C:\Program Files\BMC Software\Control-M Server>start_ctm && start_ca
-----
Starting CONTROL-M.
-----
CONTROL-M/Server Pause mode is N
-----
Starting CONTROL-M Configuration Agent
-----
C:\Program Files\BMC Software\Control-M Server>
```

Task 3: Deploy the SSL Certificate to the winserver Control-M/Agent**Steps:**

1. Remaining on the **winserver** host, press **Start > Services** to open the **Windows Services** window.



2. Stop the **Control-M Agent** Windows Service. Minimize the window as it will be used later.



3. Open a command prompt window (**Start > Command Prompt**).
4. Switch to the Control-M/Agent installation directory by running:
cd "C:\Program Files\BMC Software\Control-M Agent\Default"
5. Copy the certificate scripts to the **\SSL\Manage** directory by running the following command:
copy /Y "DATA\SSL\manage*.*" "C:\Certificate_for_CONTROL-M_Agent"

```
C:\Users\bmcadmin>cd "C:\Program Files\BMC Software\Control-M Agent\Default"
C:\Program Files\BMC Software\Control-M Agent\Default>copy /Y "DATA\SSL\manage\*.*" "C:\Certificate_for_CONTROL-M_Agent"
DATA\SSL\manage\README.TXT
DATA\SSL\manage\RegistryWork.pm
DATA\SSL\manage\setup.bat
DATA\SSL\manage\setup.pl
DATA\SSL\manage\setup.sh
      5 file(s) copied.

C:\Program Files\BMC Software\Control-M Agent\Default>
```

6. Deploy the certificate by running the following command:
"C:\Certificate_for_CONTROL-M_Agent\setup.bat"

```
C:\Program Files\BMC Software\Control-M Agent\Default>"C:\Certificate_for_CONTROL-M_Agent\setup.bat"
"PERLFOUND" - C:\Program Files\BMC Software\Control-M Common\bmcperl\bmcperl_V1"
C:\Program Files\BMC Software\Control-M Agent\Default

Performing SSL certificates setup for Control-M/Agent, please wait...

Verifying component existence...

Backup all setup files and additional parameters to backup folder 'C:/Program Files/BMC Software/Control-M Agent/Default\ssl_setup\ssl_certificate_backup_202441714242'...
Backup current keystore password to backup file 'C:/Program Files/BMC Software/Control-M Agent/Default\ssl_setup\ssl_certificate_backup_202441714242\ssl_keystore.orig'...
Old keystore password to recovery file 'C:\Program Files\BMC Software\Control-M Agent\Default\data\SSL\cert\ess.txt'...

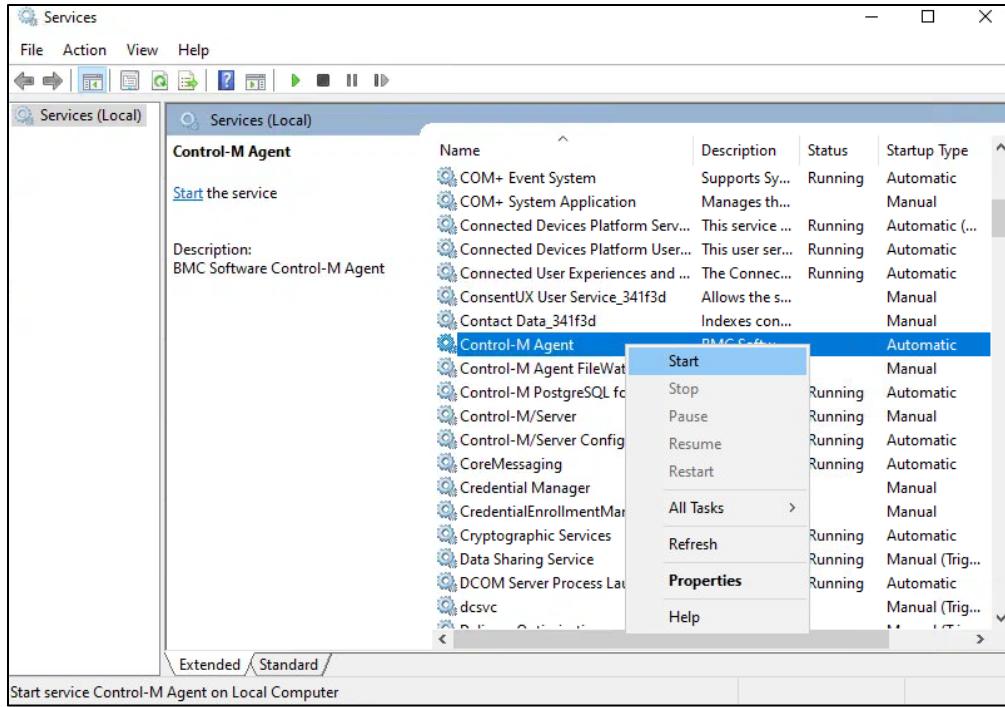
Setting up SSL certificates for Control-M Agent...

Be sure the new user has "Logon as a batch job" User Right

User '*SSL_KEYSTORE' updated successfully.
Component: Control-M/Agent
Importing keystore 'C:\Certificate_for_CONTROL-M_Agent\agcert.p12'
The operation completed successfully.
Keystore successfully imported to 'C:\Program Files\BMC Software\Control-M Agent\Default\DATA\SSL\CERT\ctmkeystore.p12'
Command completed successfully
SSL certificates for Control-M Agent successfully set up

C:\Program Files\BMC Software\Control-M Agent\Default>
```

7. From the **Windows Services** window (**Start > Services**), start the **Control-M/Agent** service.



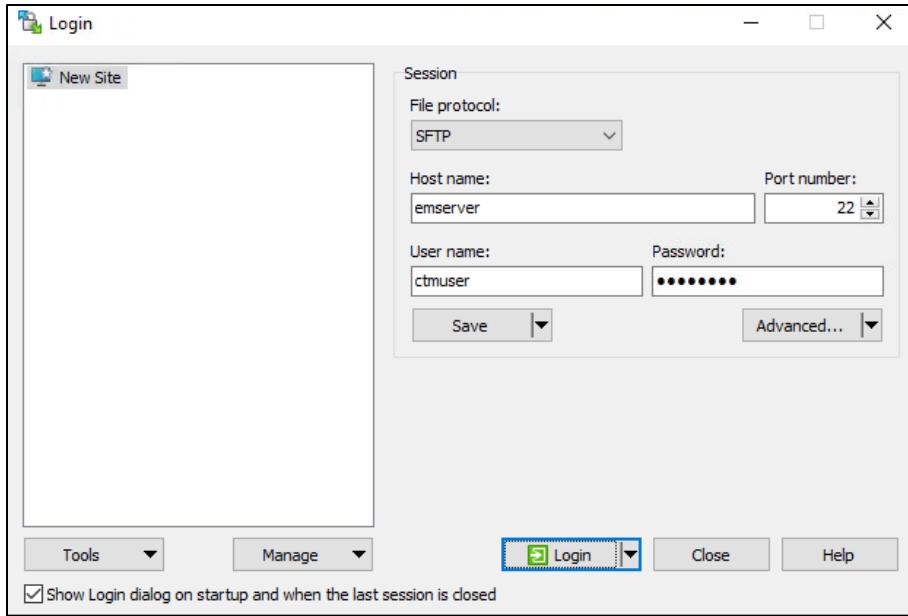
Task 4: Deploy the SSL Certificate to the emserver Control-M/Agent

Steps:

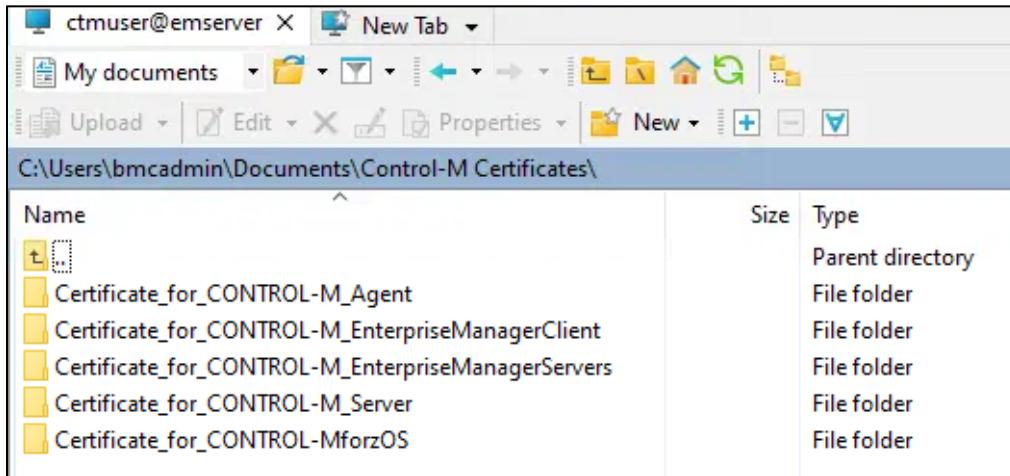
1. Return to the landing server (**ctmserver**) by minimizing the **winserver Remote Desktop Connection** window.
2. From the **Desktop**, open **WinSCP**.
3. **Login** using following details:
 - **Host name:** emserver
 - **User name:** ctmuser

Note: The user is **ctmuser**, *not emuser* as with previous logins.

- **Password:** Passw0rd



4. Click **Login**.
5. A **Warning** window may appear, click **Update**.
6. Change the directory of the left host (**ctmserver**) to:
C:\Users\bmcadmin\Documents\Control-M Certificates



7. Drag the **Certificate_for_CONTROL-M_Agent** directory from the left (**ctmserver**) to the right (**emserver**) host so that the Control-M/Agent certificate is copied to the **emserver** Control-M/Agent host.
8. Close **WinSCP** and click **Yes** in the confirmation dialog box.
9. From the landing server (**ctmserver**) **Desktop**, open a **PuTTY** session to connect to **emserver**.
10. Sign in as **ctmuser** with the password **Passw0rd**.
11. Copy the certificate setup scripts to the certificate directory by running the following command:

```
cp -p ctm_agent/ctm/data/SSL/manage/* Certificate_for_CONTROL-M_Agent/
```

```
[ctmuser@emserver ~]# cp -p ctm_agent/ctm/data/SSL/manage/* Certificate_for_CONTROL-M_Agent/  
[ctmuser@emserver ~]#
```

Note: There is whitespace between `/manage/*` and `Certificate`.

12. As this Control-M/Agent is running as root, switch to root to shut the Agent down by running `su` and entering the password: **password**.
13. To stop the Control-M/Agent UNIX daemon, run the command **shut-ag**.
14. Press **Enter** twice to verify the username (**ctmuser**) and processes (**ALL**) to stop.
15. Type **exit** to logout as root.

```
[root@emserver ~]# su  
Password:  
[root@emserver ~]# shut-ag  
  
Enter Control-M/Agent UNIX username [ctmuser]:  
  
Enter Control-M/Agent Process Name <AG|AT|AR|AGJ|AGENT|ALL> [ALL]:  
Killing Control-M/Agent Listener pid:8842  
1 seconds - 8842 is still alive  
2 seconds - 8842 is still alive  
3 seconds - 8842 is still alive  
4 seconds - 8842 is still alive  
5 seconds - 8842 is still alive  
2024-04-17 14:20:20 Listener process stopped  
Killing Control-M/Agent Tracker pid:8948  
2024-04-17 14:20:21 Tracker process stopped  
Killing Control-M/Agent Java Process pid:5653  
1 seconds - 5653 is still alive  
2 seconds - 5653 is still alive  
2024-04-17 14:20:24 Java Process process stopped  
[root@emserver ~]# exit  
exit  
[root@emserver ~]#
```

16. Run the following command to enable SSL:

Certificate_for_CONTROL-M_Agent/setup.sh

```

emserver% Certificate_for_CONTROL-M_Agent/setup.sh
Running Certificate_for_CONTROL-M_Agent/setup.pl

Performing SSL certificates setup for Control-M/Agent, please wait...

Verifying component existence...

Backup all setup files and additional parameters to backup folder '/home/ctmuser/ssl_setup/ssl_certificate_backup_2024417142135'...
Backup current keystore password to backup file '/home/ctmuser/ssl_setup/ssl_certificate_backup_2024417142135/ssl_keystore.orig'...
Old keystore password to recovery file '/home/ctmuser/ctm_agent/ctm/data/SSL/cert/.ess.txt'...

Setting up SSL certificates for Control-M Agent...

User '*SSL_KEYSTORE' updated successfully.
Component: Control-M/Agent
Importing keystore '/home/ctmuser/Certificate_for_CONTROL-M_Agent/agcert.p12'
Keystore successfully imported to '/home/ctmuser/ctm_agent/ctm/data/SSL/cert/ctmkeystore.p12'
Command completed successfully
SSL certificates for Control-M Agent successfully set up
emserver%

```

17. To start the Control-M/Agent as **ctmuser**, run the command **start-ag**, press **Enter** twice, then confirm with **Y**.

```

emserver% start-ag
Enter Control-M/Agent UNIX username [ctmuser]:
Enter Control-M/Agent Process Name <AG|AT|AR|AGJ|ALL> [ALL]:
Agent prerequisite requirements are OK.

The agent was previously running as 'root'.
You have chosen to start the agent as 'ctmuser'.

If you want to run jobs whose owner is different than 'ctmuser', perform the following steps after the
agent starts:
  1. Login as root user, execute the '/home/ctmuser/ctm_agent/ctm/scripts/set_agent_mode' script and en
able non-root mode.
  2. Define job owners passwords in Control-M using CCM or ctmsetown utility

If you upgraded the agent from a previous version and you want the agent to start as user 'ctmuser' whe
n the host
is restarted, replace the current startup script with '/home/ctmuser/ctm_agent/ctm/scripts/rc.agent_use
r'

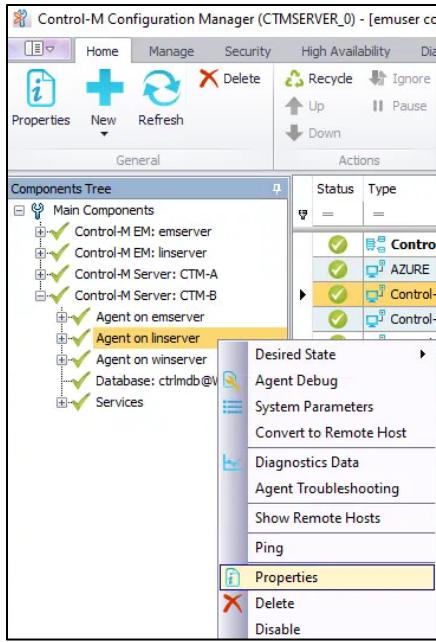
Do you want to continue ? [Y/N] : Y

```

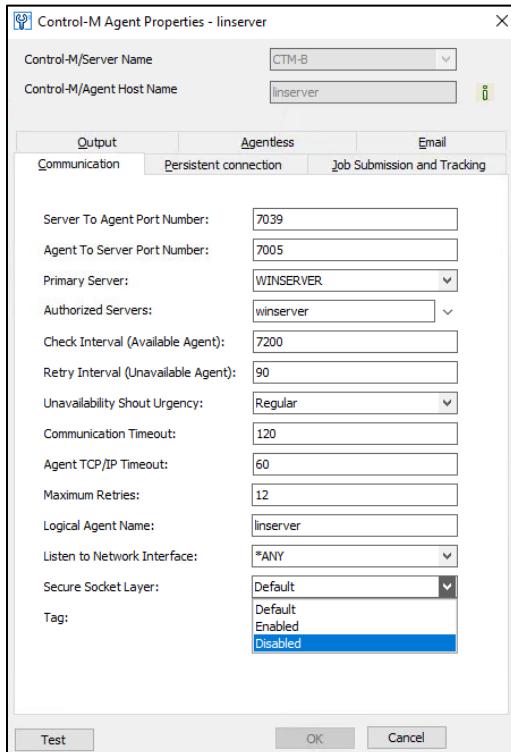
Task 5: Set the linserver Control-M/Agent SSL Mode to Disabled

Steps:

1. From the landing server (**ctmserver**) **Desktop**, open **Control-M Configuration Manager CTMSERVER_0**.
2. Sign in as **emuser** with the password: **Passw0rd**.
3. From the **Components Tree** section on the left, expand **Control-M Server: CTM-B** and right-click **Agent on linserver**. Open **Properties**.



4. When the **Control-M Agent Properties - linserver** window opens, select the **Communication** tab.
5. Change **Secure Socket Layer** from **Default** to **Disabled**.



Note: **Default** means it will inherit the SSL setting from the Control-M/Server. This will be configured in the next task.

6. Click **Test** to verify the connectivity.
7. Click **OK**.

Task 6: Enable SSL on the Control-M/Server and Control-M/Agents

Steps:

1. Return to the **winserver** host (**Start > Remote Desktop Connection**).
2. Open the command prompt (**Start > Command Prompt**).
3. Enter **ctmsys** to open the **Control-M/Server System Maintenance Utility**.
4. Enter option **2** to open **System Parameters**.
5. Enter **n** to open the next page.
6. Enter option **9**, to toggle **Secure Sockets Layer** to status **ENABLED**.
7. Press **s** to save the settings and then **q** to quit the menu.

```
Enter command, or item number you wish to change [n]:n
CONTROL-M System Parameters (Page 2/2)
-----
6) Maximum Days Retained by CONTROL-M Log :2
7) Maximum Days to Retain Output Files :1
8) Ignore New Day Conditions :N
9) Secure Sockets Layer :DISABLED

p) Previous Page
s) Save and Return to Main Menu
c) Cancel

Enter command, or item number you wish to change [p]:9
CONTROL-M System Parameters (Page 2/2)
-----
6) Maximum Days Retained by CONTROL-M Log :2
7) Maximum Days to Retain Output Files :1
8) Ignore New Day Conditions :N
9) Secure Sockets Layer :ENABLED

p) Previous Page
s) Save and Return to Main Menu
c) Cancel

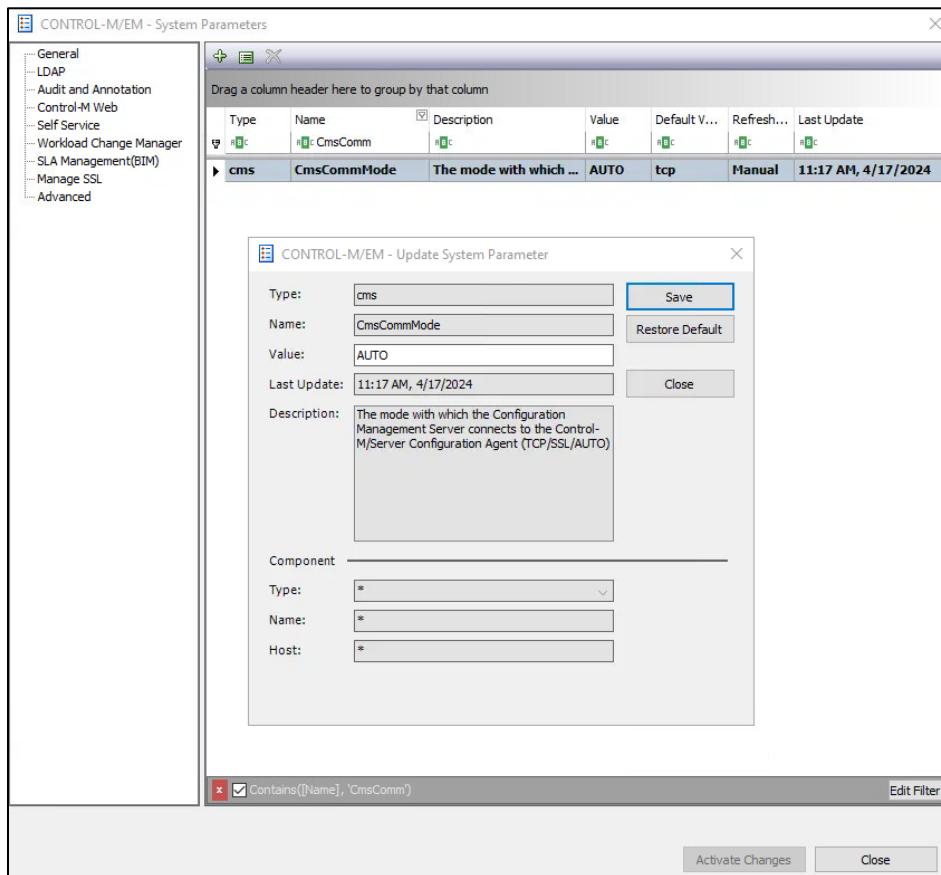
Enter command, or item number you wish to change [p]:s
+-----+
| CONTROL-M System Maintenance Utility |
| Main Menu                                |
+-----+

1) Shut Destination Tables
2) System Parameters
q) Quit

Enter Option:
```

8. Restart the Control-M/Server by entering the following commands (in order):
 - **shut_ca**
 - **shut_ctm**

- **start_ctm**
 - **start_ca**
9. Minimize the **winserver** Remote Desktop session and return to the **ctmserver** landing server host.
 10. From the landing server (**ctmserver**), login to the **CCM** as **emuser** with the password: **Passw0rd**.
 11. Right-click **Control-M EM: linserver** in the **Components Tree** and select **System Parameters**.
 12. Go to the **Advanced** tab and enter **CmsComm** in the **Name** column.
 13. Verify the **CmsCommMode** parameter is set to **AUTO**. If it needs updating double-click the parameter, set it to **AUTO** and click **Save**.



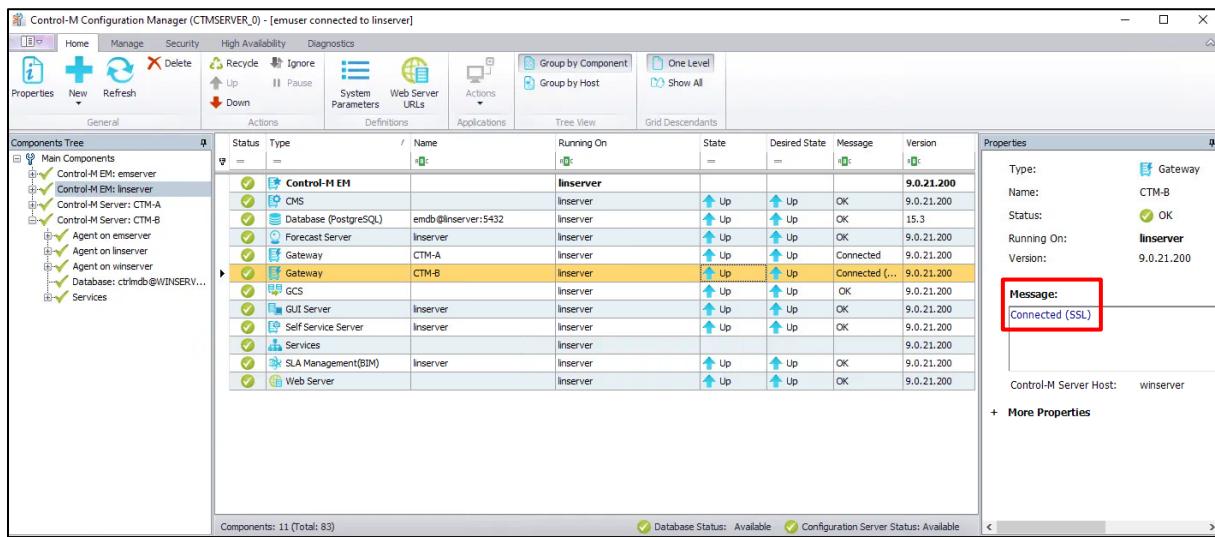
Note: This value was changed from the default (**tcp**) to **AUTO** in **Lab 5.6**.

14. Recycle the **CMS** component of the **linserver** Control-M/EM by right-clicking on the **CMS** and selecting **Desired State > Recycle**.

Task 7: Verify the SSL configuration on different components

Steps:

- From the CCM, verify that the **Gateway** component for the **CTM-B** Control-M/Server states **Connected (SSL)** in the **Message** field of the **Properties** pane. This verifies Zone 2 (Control-M/Enterprise Manager to Control-M/Server connectivity).



- Return to the **winserver** Remote Desktop session (**Start > Remote Desktop Connection**).
- From the **winserver** host, open the command prompt window (**Start > Command Prompt**).
- Verify the **CTM-B** Control-M/Server to the **winserver** Control-M/Agent connectivity by running:

ctm_diag_comm winserver

```
C:\Users\bmcadmin>ctm_diag_comm winserver
This procedure runs for about 30 seconds. Please wait
Time Stamp :
-----
04/17/2024 14:48:49
CONTROL-M/Server to CONTROL-M/Agent Communication Diagnostic Report
-----
CTMS User Name : bmcadmin: Administrator
CTMS Directory : C:\Program Files\BMC Software\Control-M Server\ctm_server\
CTMS Platform Architecture : MSWindows 6.2 (Build:9200)
CTMS Installed Version : DRCTV.9.0.21.200
CTMS Local IP Host Interface Name : WINSERVER
Server-to-Agent Port Number : 7006
Agent-to-Server Port Number : 7005
Server-Agent Comm Protocol : SSL
Server-Agent Protocol Version : 13
Server-Agent Connection mode : Transient
Agent Platform Name : winserver
Agent Status : Available
Agent Known Type : Regular
MS-Windows ping to Agent or Agentless host : Succeeded
CTMS ping to Agent or Agentless host : Succeeded
Agent IP Address : 192.168.1.7
Server-Agent Encryption Type : AES256GCM

CTMS Ping winserver as Regular Agent
=====
Agent [winserver] is available
```

5. The Server-Agent Communication Protocol should state **SSL**.
6. Verify the **CTM-B** Control-M/Server to the **emserver** Control-M/Agent connectivity by running:
ctm_diag_comm emserver

```
C:\Users\bmcadmin>ctm_diag_comm emserver

This procedure runs for about 30 seconds. Please wait

Time Stamp :
-----
04/17/2024 14:49:53

CONTROL-M/Server to CONTROL-M/Agent Communication Diagnostic Report
-----

CTMS User Name : bmcadmin: Administrator
CTMS Directory : C:\Program Files\BMC Software\Control-M Server\ctm_server\
CTMS Platform Architecture : MSWindows 6.2 (Build:9200)
CTMS Installed Version : DRCTV.9.0.21.200
CTMS Local IP Host Interface Name : WINSERVER
Server-to-Agent Port Number : 7006
Agent-to-Server Port Number : 7005
Server-Agent Comm. Protocol : SSL
Server-Agent Protocol Version : 13
Server-Agent Connection mode : Transient
Agent Platform Name : emserver
Agent Status : Available
Agent known Type : Regular
MS-Windows ping to Agent or Agentless host : Succeeded
CTMS ping to Agent or Agentless host : Succeeded
Agent IP Address : 192.168.1.6
Server-Agent Encryption Type : AES256GCM

CTMS Ping emserver as Regular Agent
=====
Agent [emserver] is available
```

7. The Server-Agent Communication Protocol should state **SSL**.
8. Remaining in the **winserver** command line, to verify **winserver** Control-M/Agent to **CTM-B** Control-M/Server connectivity run the command:

ag_diag_comm

```
C:\Users\bmcadmin>ag_diag_comm
2024-04-17 14:53:13

This procedure runs up to 120 seconds. Please wait...

Control-M/Agent communication Diagnostic Report
-----

Agent User Name : bmcadmin: Administrator
Agent Directory : C:\Program Files\BMC Software\Control-M Agent\Default\
Agent Platform Architecture : Windows-NT 6.2 (Build:9200)
Agent Version : 9.0.21.200
Agent Host Name : winserver
Logical Agent Name : winserver
Listen to Network Interface : *ANY
Server-Agent Protocol Version : 13
Server Host Name : WINSERVER
Authorized Servers Host Names : WINSERVER
Server-Agent Comm. Protocol : SSL
Server-to-Agent Port Number : 7006
Agent-to-Server Port Number : 7005
Server-Agent Connection mode : Transient (by Java)
System ping to Server Platform : Succeeded
Agent ping to Control-M/Server : Succeeded

Agent processes status:
=====
Agent Listener : Running
Agent Tracker : Running
Agent Tracker-Worker : Running (ATW000)
Java Services : Running ["ar","housekeeping","ssh-courier"] on port 53210
Agent FileWatcher : Not Running

DNS Translation of Server :
Server Host Address #1 - 192.168.1.7
--- End of Report ---
```

9. From the **emserver** PuTTY session, repeat step 8 to verify the **emserver** Control-M/Agent to **CTM-B** Control-M/Server connectivity.

```
emserver% ag_diag_comm
2024-04-17 14:54:16

This procedure runs up to 120 seconds. Please wait...

Control-M/Agent Communication Diagnostic Report
-----

Agent User Name : ctmuser
Agent Directory : /home/ctmuser/ctm_agent/ctm
Agent Platform Architecture : Linux
Agent Version : 9.0.21.200
Agent Host Name : emserver
Logical Agent Name : emserver
Listen to Network Interface : *ANY
Server Host Name : WINSERVER
Authorized Servers Host Names : winserver
Server-Agent Protocol Version : 13
Server-Agent Comm. Protocol : SSL
Server-to-Agent Port Number : 7006
Agent-to-Server Port Number : 7005
Server-Agent Connection mode : Transient (by Java)
Unix Ping to Server Platform : Succeeded
Agent Ping to Control-M/Server : Succeeded

Agent processes status
=====
Java services : ["ar","housekeeping","ssh-courier"] on port 45561
Agent Listener : Running as ctmuser (185479)
Agent Tracker : Running as ctmuser (185534)
Agent Tracker-Worker : Running as ctmuser (185536)
```

Module 9: Control-M Health Checking

Objectives

- Implement Control-M jobs to monitor Control-M/Enterprise Manager processes
- Parse the Control-M/Agent Daily Log for developing issues
- Optimize the New Day Process by implementing job statistics clean up at a time separate to the New Day Process
- Implement a Control-M job to run to compile job statistics into the Statistics Summary table
- Implement Control-M Event and Variable cleanup procedures
- Configure file system cleanup system parameters
- Use the Control-M/Agent Toolbox to monitor resource utilization

Lab 9.1: Implementing Control-M/Enterprise Manager Process Monitoring

In this lab you will create 2 jobs in Control-M. The first will monitor the availability of the Control-M/Enterprise Manager Configuration Agent and trigger an alert if it is unavailable.

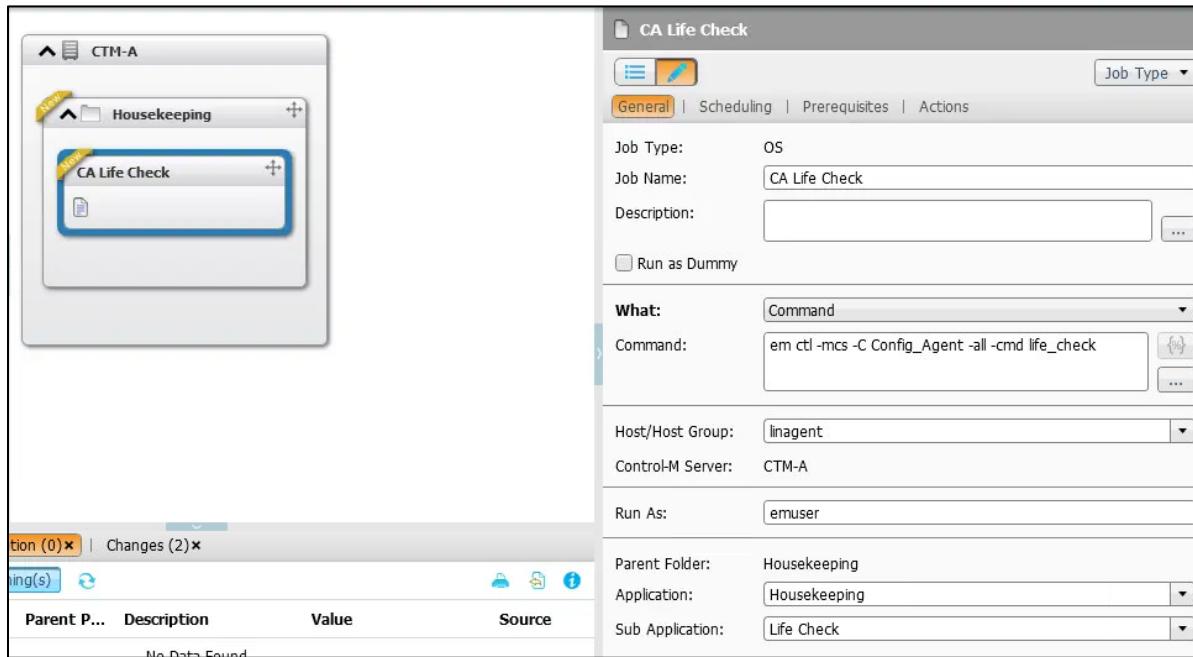
You will then repeat the process to create a cyclic job that monitors the availability of both Control-M Gateway processes. This is to show how to use the **ctl** process to monitor components. In the real world you may want to continue implementing **ctl** jobs for other processes (e.g., the CMS, SLAM).

Task 1: Implement a Cyclic Control-M Job to Verify Configuration Agent Availability

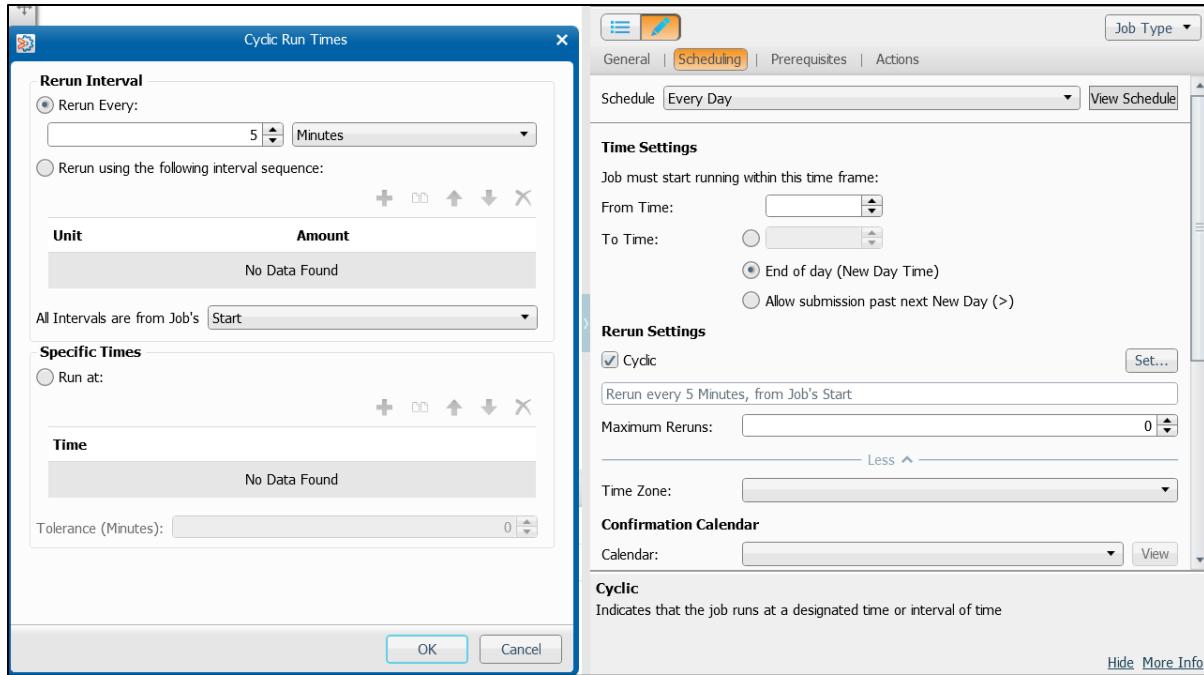
Steps:

1. From the landing server (**ctmserver**) **Desktop**, open the **Control-M GUI**.
2. Sign in as **emuser** with the password: **Passw0rd**.
3. From the **Planning** domain, open a **Blank Workspace**.
4. Drag an **OS** job down from the **Job Palette** to create a new **OS** job and folder.
5. Set the **Control-M/Server** to **CTM-A**.
6. Set the **Folder Name** to **Housekeeping**.
7. From the **General** tab of the **OS** job, set the following:
 - **Job Name:** CA Life Check
 - **What:** Command

- **Command:** em ctl -mcs -C Config_Agent -all -cmd life_check
- **Host/Host Group:** linagent
- **Run As:** emuser
- **Application:** Housekeeping
- **Sub Application:** Life Check

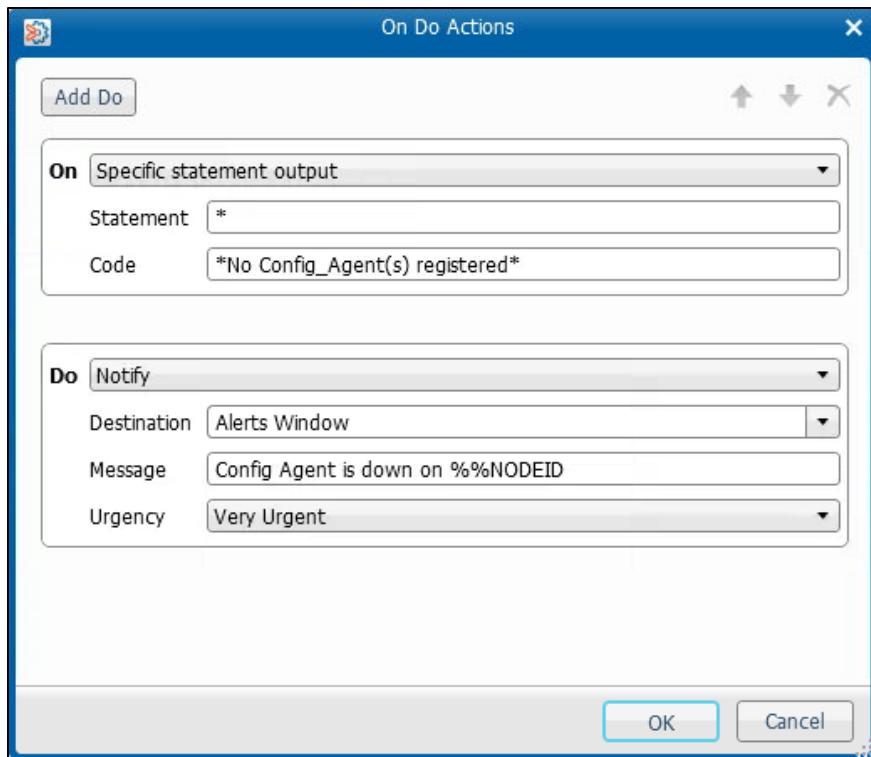


8. From the **Scheduling** tab, check the **Cyclic** box and Set the cyclic interval to **Rerun Every 5 Minutes**:

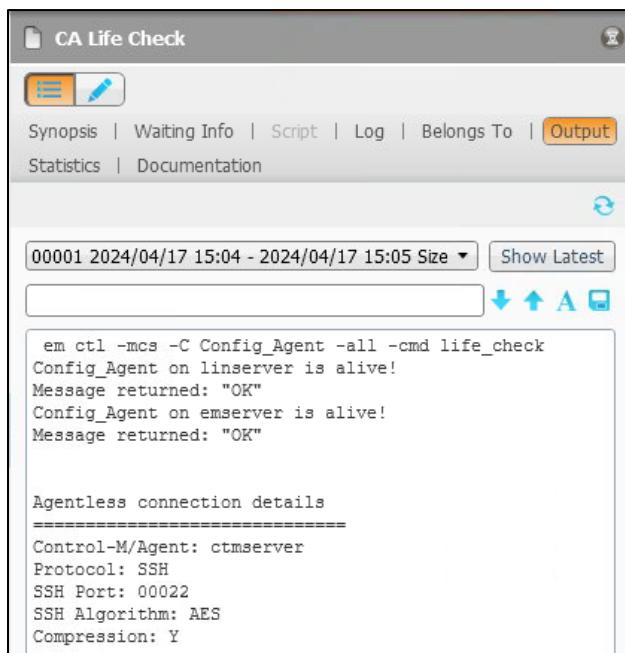


9. From the **Actions** tab, add an **On Do Action** that states the following:

- **On:** Specific Statement Output
 - **Statement:** *
 - **Code:** *No Config_Agent(s) registered*
- **Do:** Notify
 - **Destination:** Alerts Window
 - **Message:** Config Agent is down on %%NODEID
 - **Urgency:** Very Urgent



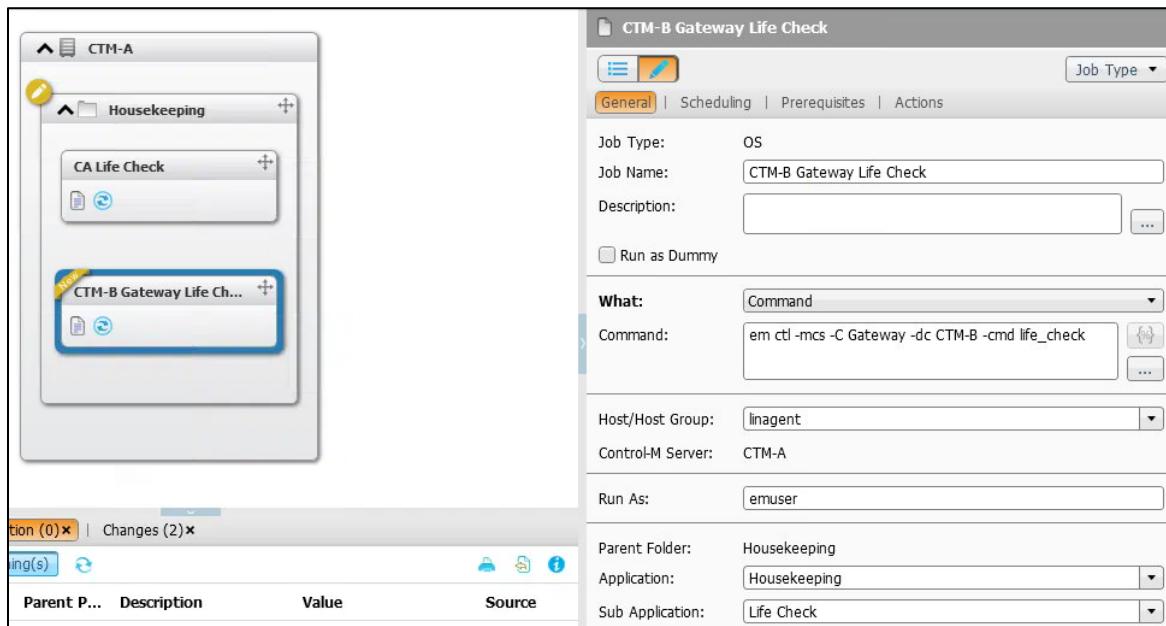
10. Check In the job and Order the workspace.
11. Switch to the **Monitoring** domain and open the **Grouped by Folder** Viewpoint (from the All ViewPoints tab).
12. Verify the job completes successfully.
13. Inspect the job's Output. Was the **Config Agent** successfully detected?



Task 2: Implement a Cyclic Control-M Job to Verify the CTM-B Gateway Availability

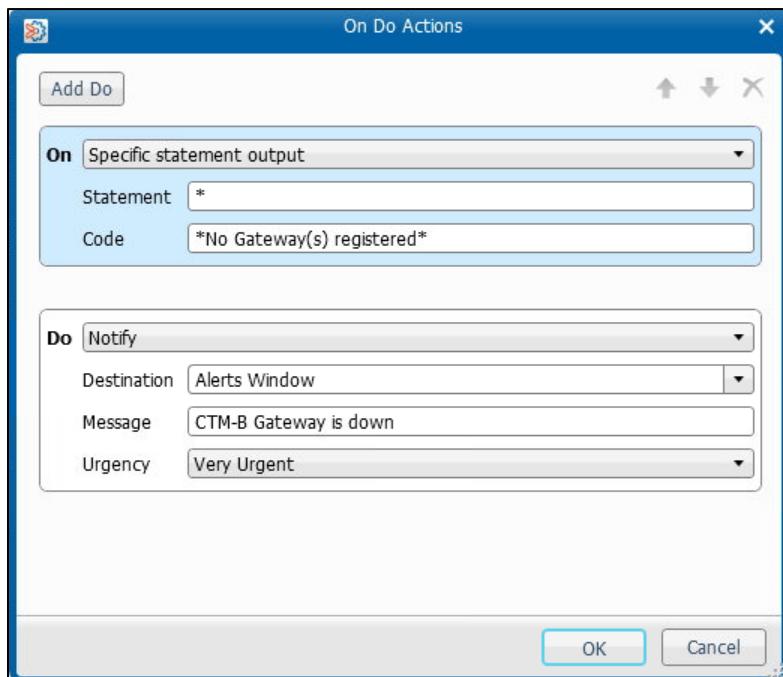
Steps:

1. Check out the workspace used in the previous task or load the **Housekeeping** folder into a new workspace.
2. Right-click the **CA Life Check** job and **Copy** it.
3. Paste it into the **Housekeeping** folder to create a duplicate.
4. From the **General** tab of the duplicated job, set the following:
 - **Job Name:** CTM-B Gateway Life Check
 - **What:** Command
 - **Command:** em ctl -mcs -C Gateway -dc CTM-B -cmd life_check
 - **Host/Host Group:** linagent
 - **Application:** Housekeeping
 - **Sub Application:** Life Check

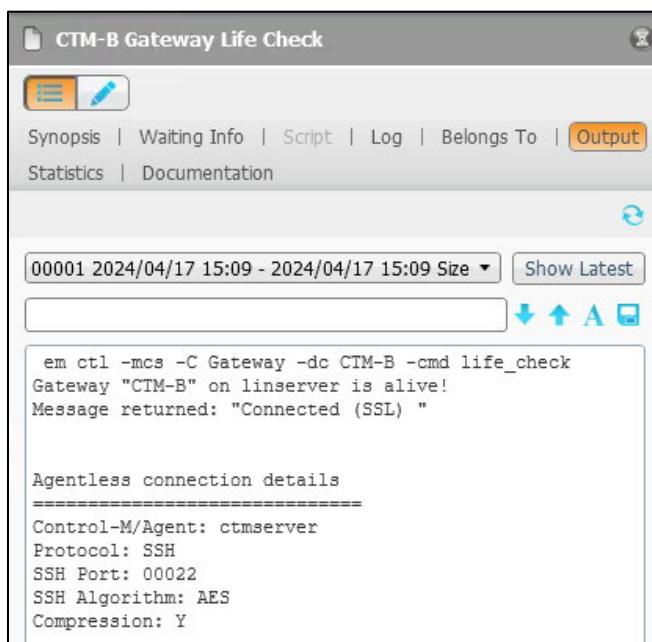


5. From the **Actions** tab, update the **On Do Action** with the following details:
 - **On:** Specific Statement Output
 - **Statement:** *
 - **Code:** *No Gateway(s) registered*
 - **Do:** Notify
 - **Destination:** Alerts Window
 - **Message:** CTM-B Gateway is down

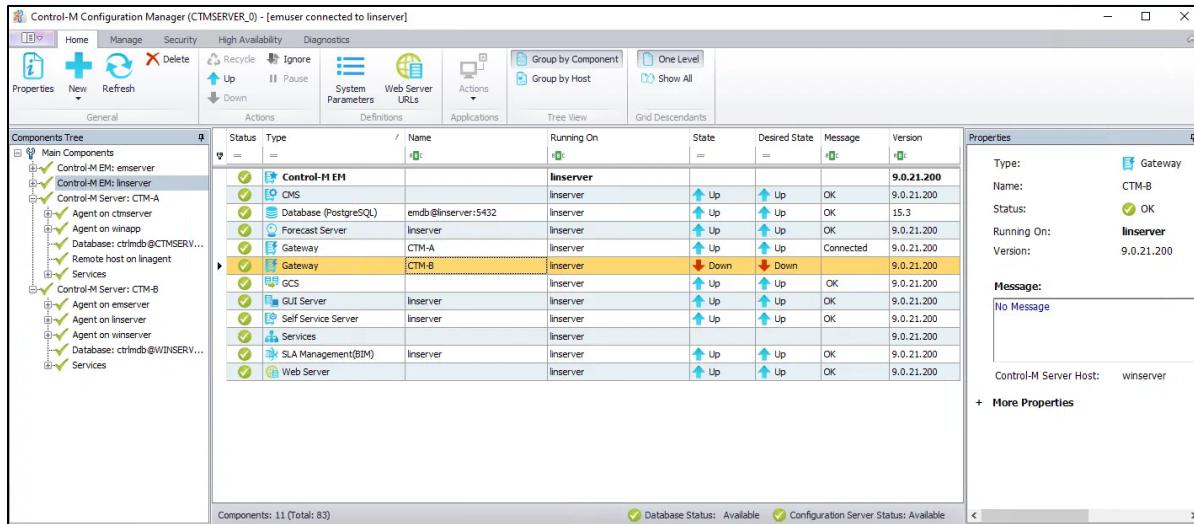
- **Urgency:** Very Urgent



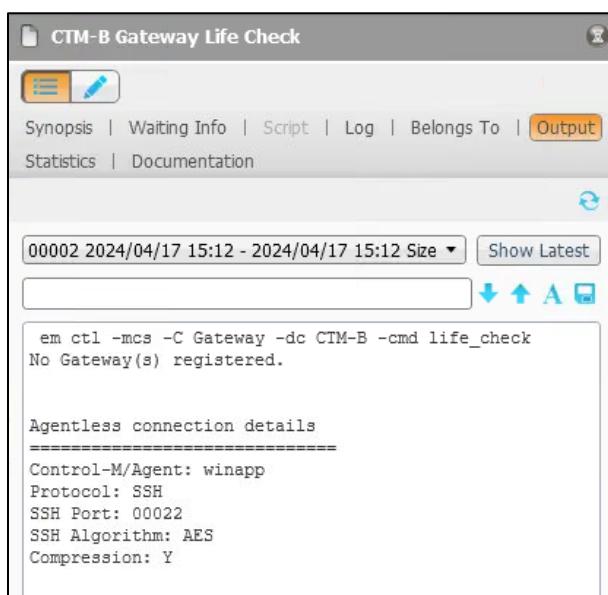
6. Check In the workspace and Order the **CTM-B Gateway Life Check** job.
7. Switch to the **Monitoring** domain and verify the job completes successfully, with the **CTM-B Gateway** being detected (viewed from the job's **Output** tab).



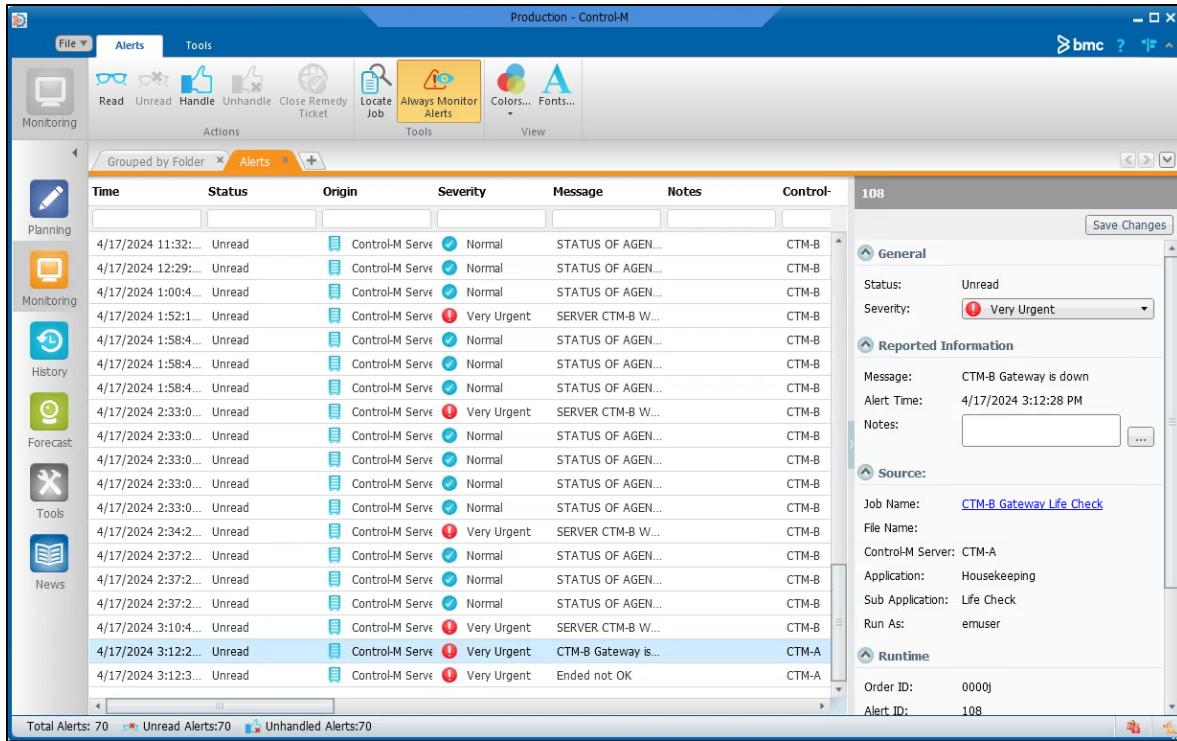
8. Remaining in the **Control-M GUI**, from the **Tools** domain, open the **Control-M Configuration Manager**.
9. When the **CCM** opens, right-click the **CTM-B Gateway** and set the **Desired State** to **Down**. Wait for the **State** to change to **Down**.



10. Return to the **Control-M GUI** and the **Monitoring** domain.
11. Wait for the next cycle of the **CTM-B Gateway Life Check** job or right-click it and **Run Now**.
12. Open the **Output** tab. The job should have failed, indicating the **Gateway** was not detected and the **Output** states **No Gateway(s) Registered**.



13. Open **Tools > Alerts**. Verify the alert was successfully posted.



14. Open the CCM, right-click the **CTM-B Gateway** and set the **Desired State** to **Up**.

Lab 9.2: Inspect the Control-M/Agent Daily Log

Task 1: Count the Jobs Submitted to a Control-M/Agent Today

Steps:

1. Open a Remote Desktop session to **winserver** (**Start > Remote Desktop Connection**).
2. From the **winserver** host, open a command prompt window (**Start > Command Prompt**).
3. Switch to the Control-M/Agent's daily log directory by running:
cd "C:\Program Files\BMC Software\Control-M Agent\Default\DEFAULTLOG"
4. List the daily log files by typing **dir**.

```
C:\Users\bmcadmin>cd "C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG"

C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>dir
Volume in drive C is Windows
Volume Serial Number is 681B-F911

Directory of C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG

04/17/2024  09:23 AM    <DIR>      .
04/17/2024  02:02 PM    <DIR>      ..
04/17/2024  02:48 PM           69,061 daily_ctmag_20240417.log
              1 File(s)       69,061 bytes
              2 Dir(s)  68,114,747,392 bytes free

C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>
```

5. Daily log files contain the date in the **yyyymmdd** format. Highlight today's **daily_ctmag_<today>.log** file, then right-click to copy it.

```
C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>dir
Volume in drive C is Windows
Volume Serial Number is 681B-F911

Directory of C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG

04/17/2024  09:23 AM    <DIR>      .
04/17/2024  02:02 PM    <DIR>      ..
04/17/2024  02:48 PM           69,061 daily_ctmag_20240417.log
              1 File(s)       69,061 bytes
              2 Dir(s)  68,114,747,392 bytes free

C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>
```

6. Count the number of jobs submitted to the Control-M/Agent today by running:
findstr /C:"ACCEPTED" "daily_ctmag_<today>.log" | find /C "ACCEPTED"

```
C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>findstr /C:"ACCEPTED" "daily_ctmag_20240417.log" | find /C "ACCEPTED"
45

C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>
```

Note: Use right-click to paste the daily log file name copied in the previous step.

7. Keep the command prompt open as it will be used in the next task.

Task 2: Search for Starvation or DEBUG DUMP Messages

The daily log being parsed will be generated on the last day of class. Depending on system performance there may be multiple messages containing Starvation or DEBUG DUMP, or none at all. This task states how to search the daily log for Starvation and DEBUG DUMP messages.

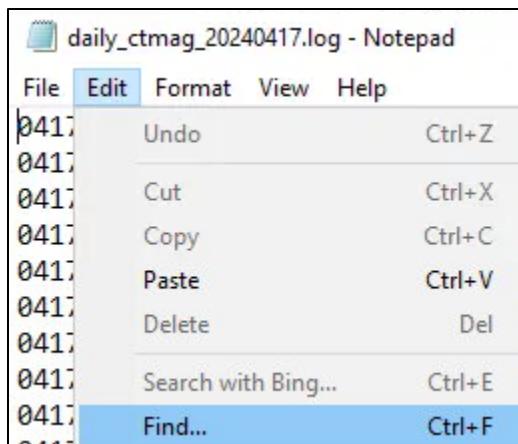
Steps:

1. Remaining in the command prompt window from the last task, open the daily log file by running:

notepad daily_ctmag_<today>.log

```
C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>notepad daily_ctmag_20240417.log
C:\Program Files\BMC Software\Control-M Agent\Default\DAILYLOG>
```

2. From the **Notepad** window, select **Edit > Find** and search for instances of **starvation**:



3. Review any messages (if any) that are displayed. Repeat step 2 to search for further instances.
4. Search for instances of **DEBUG DUMP**:

```
JOB MIK_GET_RUNTIME_FILE (ORDERID 00051, RUNNO 00001) STARTED (11004), OWNER LocalSystem, APPL TYPE WIN. More information at https://bmcsites.force.com/casemgmt/sc_KnowledgeArticle?sfid=00051000000000000000000000000000
PING SUCCESSFULLY SENT TO LOCAL AGENT wi. Find what: DEBUG DUMP
PARAMETER 'PROTOCOL_VERSION' IN TABLE 'C
PING SUCCESSFULLY SENT TO LOCAL AGENT wi. Find what: DEBUG DUMP
AGENT PROCESS 'AM' STOPPED AT 2024041709:00:00.000
JOB main1 (ORDERID 0005e, RUNNO 00001) AI
DEBUG DUMP FOR process/thread=9696. Message: Match case
Force.com/casemgmt/sc_KnowledgeArticle?sfid=0005e000000000000000000000000000
AGENT PROCESS 'AM' STARTED AT 2024041709:00:00.000
JOB main1 (ORDERID 0005e, RUNNO 00001) STARTED (11004), OWNER LocalSystem, APPL TYPE WIN. More information at https://bmcsites.force.com/casemgmt/sc_KnowledgeArti
JOB main1 (ORDERID 0005e, RUNNO 00001) EXECUTION ENDED
JOB main1 (ORDERID 0005e, RUNNO 00001) RECEIVED EVENT FROM 'WIN' CR
JOB main1 (ORDERID 0005e, RUNNO 00001) ENDED OK elapsed - 11.00 Sec cpu - 0.05 Sec sysout size - 422 bytes. More information at https://bmcsites.force.com/c
JOB main1 (ORDERID 0005e, RUNNO 00001) LONG EXIT SENT TO AGENT AR-Service
JOB main1 (ORDERID 0005e, RUNNO 00001) LONG EXIT SENT FROM AGENT AR-Service TO Control-M/SERVER
JOB main1 (ORDERID 0005e, RUNNO 00001) LONG EXIT CONFIRMATION RECEIVED FROM Control-M/SERVER 'WINSERVER'
JOB main3 (ORDERID 0005g, RUNNO 00001) ACCEPTED, OWNER emuser, APPL TYPE WIN, AGENT NAME winserver
DEBUG DUMP FOR process/thread=6420. Message is 0417 09:46:36:084 AS:ag_submit_check_existing_file: found existing file for this job 'BACKUP\0005g_0001.dsect'
```

5. Review any messages (if any) that are displayed. Repeat step 4 to search for further instances.

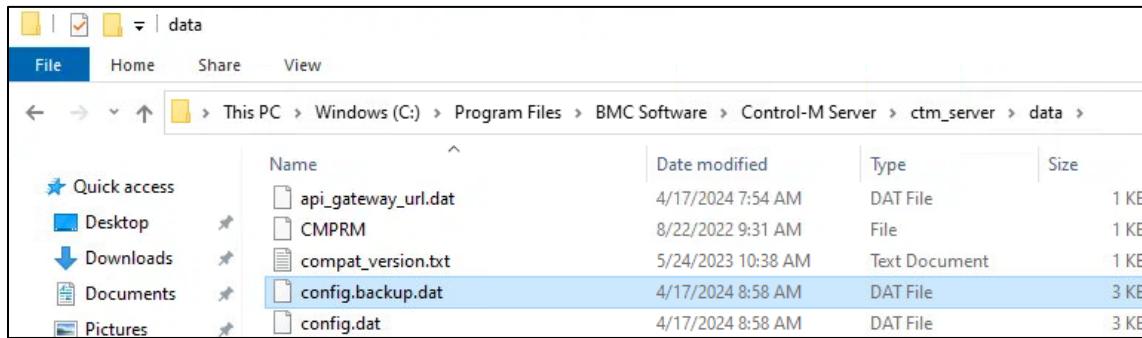
6. If no **STARVATION** or **DEBUG DUMP** messages appear in today's log, review a previous day's log. Please note these are not guaranteed so if no messages appear in any log this is considered normal (and would indicate optimal performance).

Lab 9.3: Optimizing the New Day Procedure

Task 1: Stop the Statistics Clean Up During the New Day Procedure

Steps:

1. From the landing server (**ctmserver**), open **File Explorer**.
2. Navigate to the **C:\Program Files\BMC Software\Control-M Server\ctm_server\data** directory.
3. Backup the **config.dat** file before modifying it by copying and pasting it to create a duplicate.



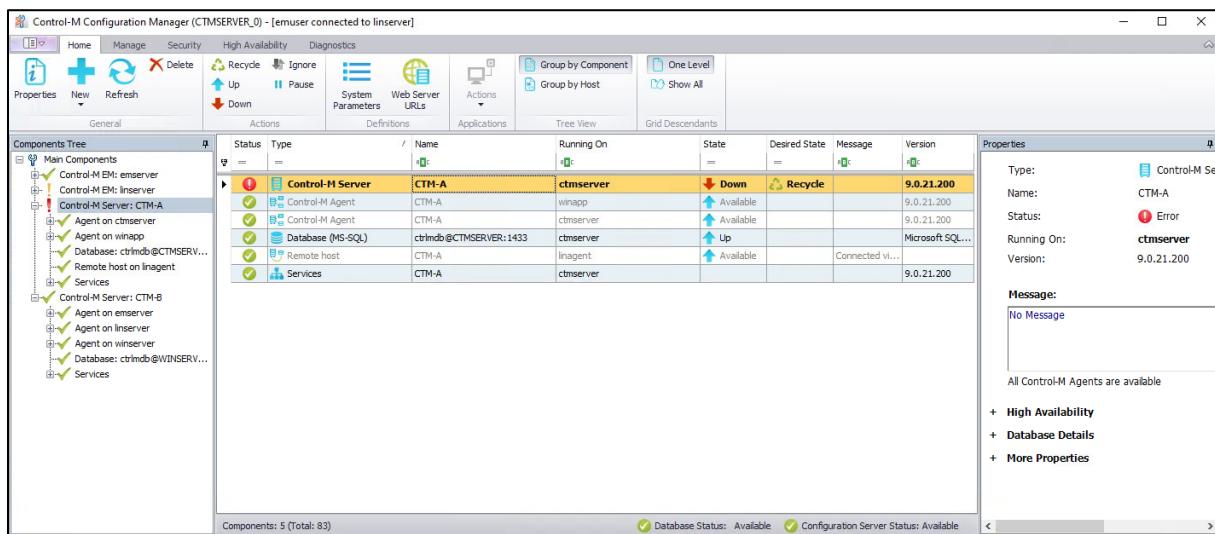
4. Right-click the **config.dat** file and **Edit with Notepad++**.
5. Add the below parameters to the end of the file:
 - **ONGOING_STATISTICS_CLEANUP N**
 - **STATISTICS_CLEANUP_IN_NEWDAY N**

```

1 APIUpdate.json 2 AgentlessHost.json 3 RunAs.json 4 SAPDevs.json 5 ProcessOwners.json 6 sdev.json 7 config.dat
95 # DUAL: Use both IPv4 and IPv6 TCP/IP families.
96
97 IPV_MODE IPV4
98 HTTPS_CTMS_PORT_NUM 10443
99 CTM_MFT_CM_IS_ACTIVATED false
100 CTMS-API-GATEWAY-SERVICE.API_GATEWAY_PORT_PROTOCOL http
101 CYCLIC_DELAY_SECS 0
102 ORDERING_THREADS_SIZE 4
103 ORDERING_MAX_CONCURRENT_JOBS 20000
104 ORDERING_PRIORITY_THREADS_SIZE 4
105 SCHEDULING_MAX_CONCURRENT_JOBS 6000
106 ONGOING_STATISTICS_CLEANUP N
107 STATISTICS_CLEANUP_IN NEWDAY N

```

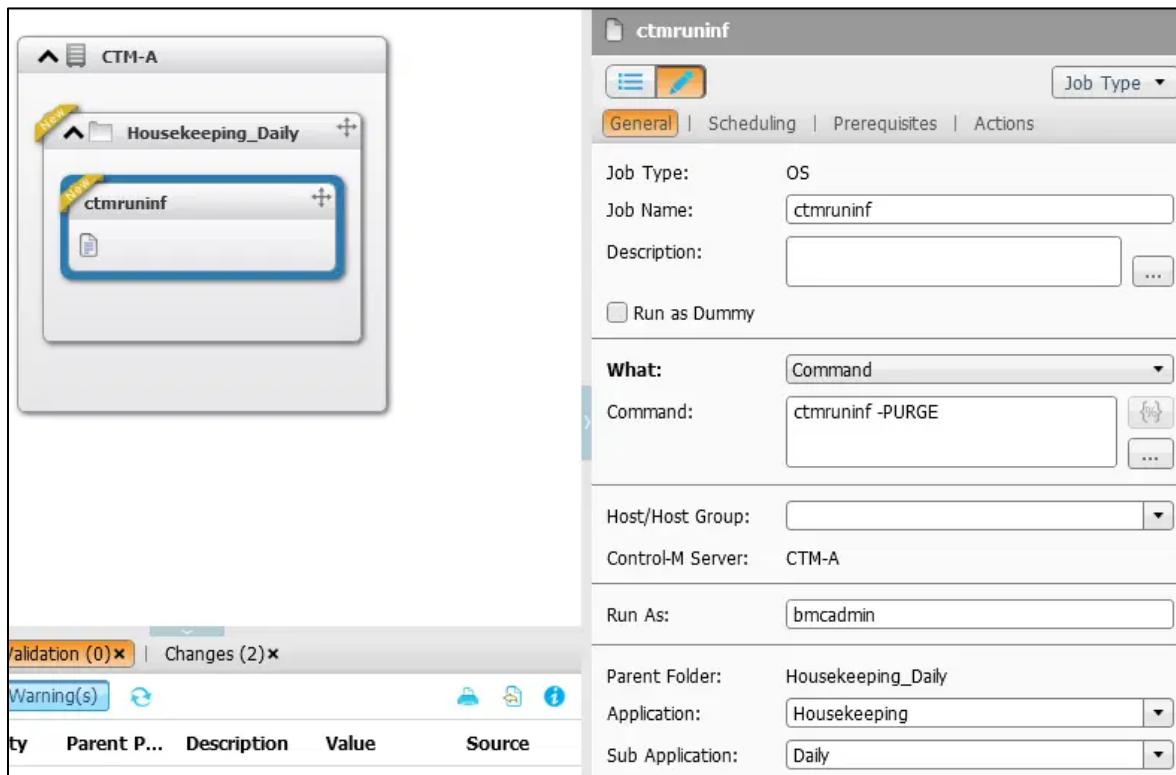
6. Save the file.
7. Recycle the **CTM-A** Control-M/Server from the CCM.



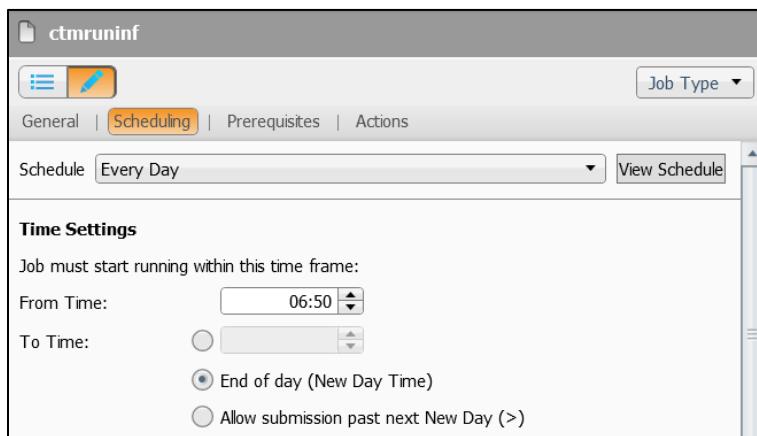
Note: Once you stop the statistics clean up during the New Day, you must carry out this process manually or by scheduling a job to run the **ctmruninf** command with the **purge** option.

8. If not already open, sign into the **Control-M GUI** as **emuser** with the password: **Passw0rd**.
9. From the **Planning** domain, open a blank workspace.
10. Define a new **OS** job. Select the **CTM-A Control-M/Server**.
11. Set the **Folder Name** to **Housekeeping_Daily**.
12. Select the job.
13. Enter the following details in the **General** tab:
 - **Job Name:** ctmruninf

- **What:** Command
- **Command:** ctmruntime -PURGE
- **Run As:** bmcadmin
- **Application:** Housekeeping
- **Sub Application:** Daily

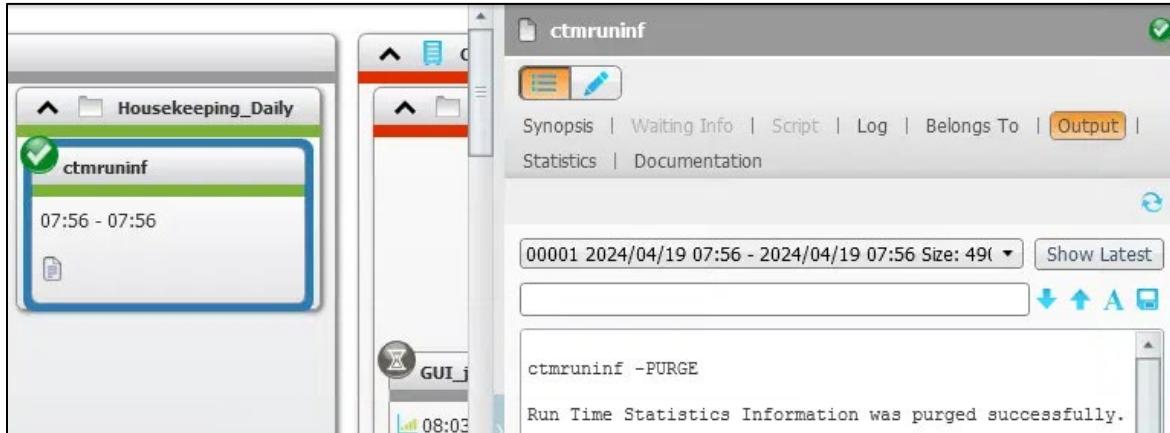


14. From the **Scheduling** tab, set the **From Time** to 06:50 (as the New Day time is set to 07:00).



15. **Check In** and **Order** the workspace.

16. Switch to the **Monitoring** domain and open the **Grouped by Folder** Viewpoint.
17. Right-click the **ctmruninf** job and **Run Now**.
18. Verify the job completes successfully.



Task 2: Change the Statistics Retention Period and Number of Retained Statistics Records in the Control-M/Server CTM-A

Steps:

1. Login to the CCM as **emuser** with the password: **Passw0rd**.
2. From the **Components Tree** section, right-click the **Control-M Server: CTM-A** and select **System Parameters**.
3. To filter the parameter name, enter **PURGE** into the **Name** column.
4. Update the values of the below parameters:
 - Statistics retention period parameters:
 - **RUNINF_PURGE_MODE: 1**
 - **RUNINF_PURGE_LIMIT: 10**
5. Click **Activate Changes** and **Close** the **System Parameters** window.
6. Press **Start** and open the **Command Prompt**.
7. Run the following command to refresh the Control-M/Server system parameters:
ctmipc -MSGID CFG -DEST ALL

```
C:\Users\bmcadmin>ctmipc -MSGID CFG -DEST ALL
message 'CFG' sent to SU successfully
message 'CFG' sent to RT successfully
message 'CFG' sent to TR successfully
message 'CFG' sent to CS successfully
message 'CFG' sent to WD successfully
message 'CFG' sent to CE successfully
message 'CFG' sent to CA successfully
message 'CFG' sent to MS successfully

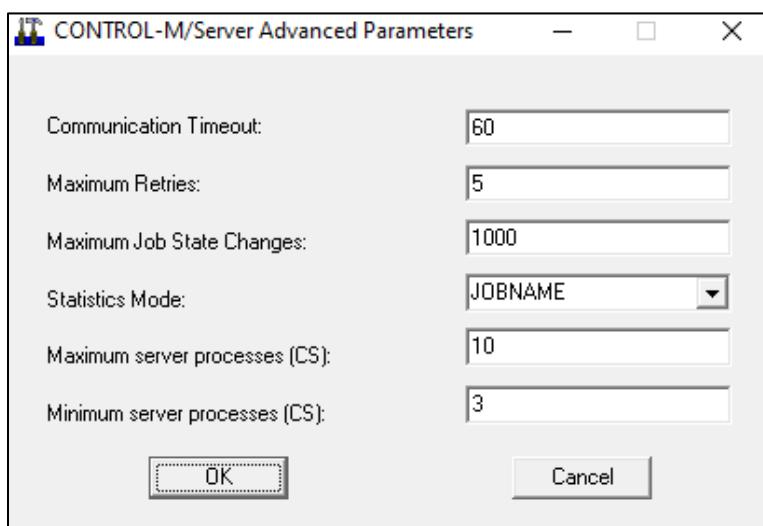
C:\Users\bmcadmin>
```

Lab 9.4: Defining a Job to Run the ctmjsa Utility

Task 1: Modify the Statistics Mode Parameter

Steps:

1. From the landing server (**ctmserver**) **Desktop**, press **Start** and open **Command Prompt**.
2. Run the command **ctm_menu**.
3. Enter **4** for **Parameter Customization**.
4. Enter **2** for **Advanced Communication and Operational Parameters**.
5. In the **Control-M/Server Advanced Parameters** window, from the **Statistics Mode** drop-down menu, select **JOBNAME**.



6. Click **OK**.
7. Press **Enter** and then **q** twice to quit.

Task 2: Define a Job to Test Statistics Gathering

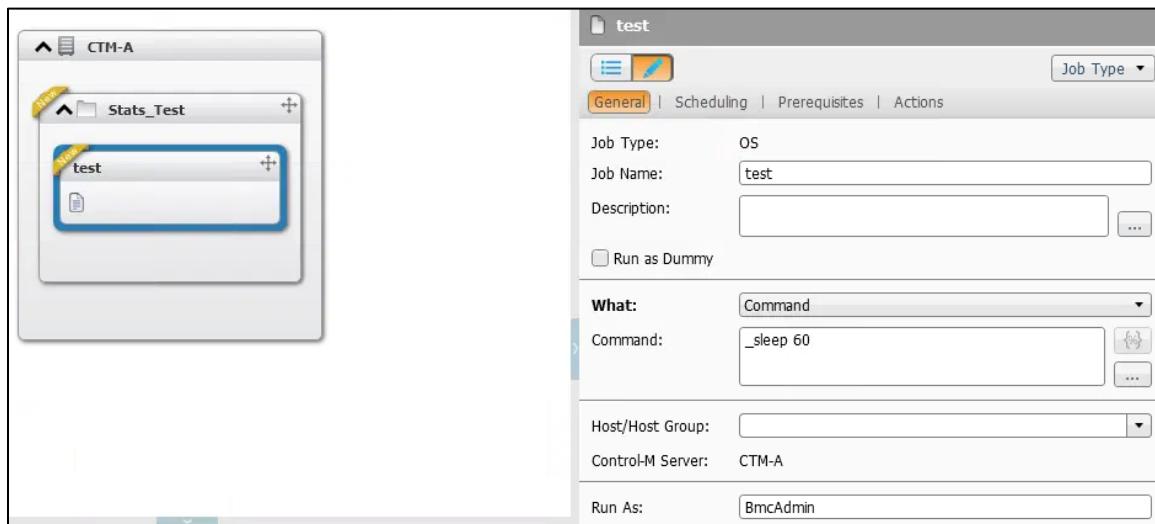
Steps:

1. If not already, sign in to the **Control-M GUI** as **emuser** with the password: **Passw0rd**.
2. From the **Planning** domain, open a **Blank Workspace**.
3. Drag an **OS** template into the workspace.
4. When prompted for to select a Control-M/Server, select **CTM-A** from the drop-down list and click **OK**.
5. Select the folder.

Add the following details:

- **Folder Name:** Stats_Test
- **Control-M Server:** CTM-A
- **Order Method:** Automatic (Daily)

6. Select the job. In the properties pane, specify the following parameters on the **General** tab:
 - **Job Name:** test
 - **What:** Command
 - **Command:** _sleep 60
 - **Run As:** BmcAdmin



7. **Check In** and then **Order** the job.
8. From the **ctmserver** command prompt, run the command **ctmjsa -list -JOBNAME test** to check the statistics of the **test** job.
9. The output of the command displays the table with no records from the **test** job, even if it has executed successfully.

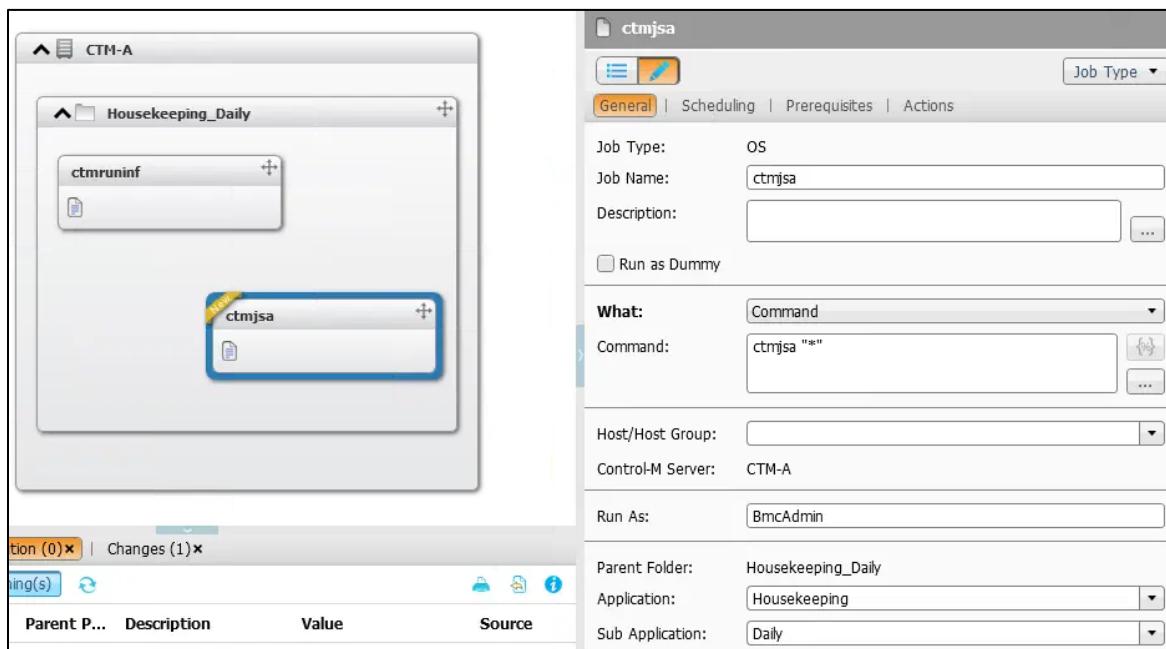
C:\Users\bmcadmin>ctmjsa -list -JOBNAME test	FILE_NAME	FILE_PATH	HOST	CPU [sec]	ELAPSED[sec]	FOLDER
JOBNAME						
--						

C:\Users\bmcadmin>

Task 3: Define a Job to Run the ctmjsa Utility

Steps:

10. From the **Control-M GUI**, access the **Planning** domain.
11. From the ribbon, click **Folders**.
12. Double-click the **Housekeeping_Daily** folder to open it into a new workspace, then **Check Out** the workspace.
13. Drag an **OS** template into the **Housekeeping_Daily** folder.
14. Select the new job. In the **Properties** pane, specify the following parameters on the **General** tab:
 - **Job Name:** ctmjsa
 - **What:** Command
 - **Command:** ctmjsa “*”
 - **Run As:** BmcAdmin
 - **Application:** Housekeeping
 - **Sub Application:** Daily



15. **Check In** and **Order** the job.
16. Once the job completes, run the command **ctmjsa -list -JOBNAME test** once again from the **ctmserver** command prompt.
17. Observe the table has updated with one record added for the test job:

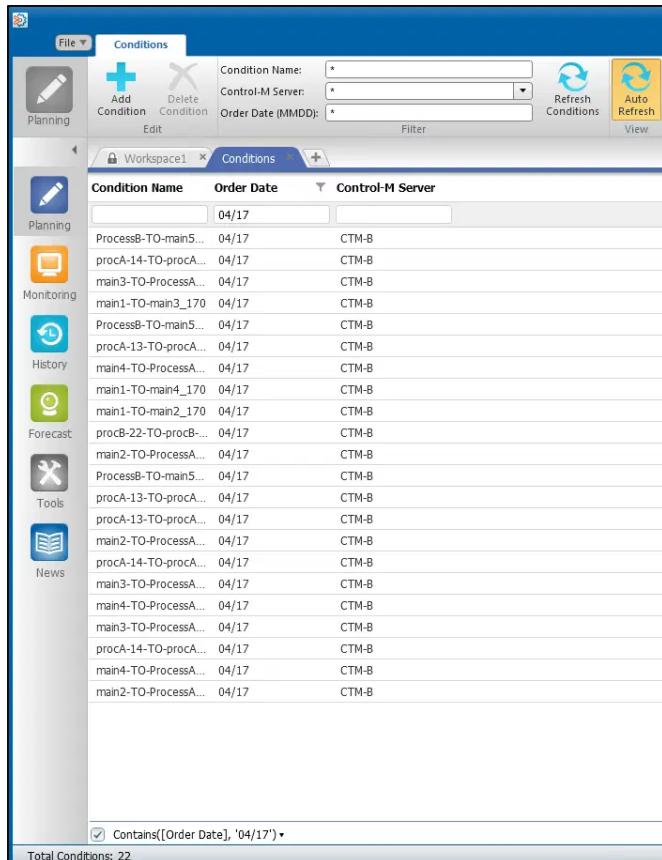
JOBNAME	FILE_NAME	FILE_PATH	HOST	CPU [sec]	ELAPSED[sec]	FOLDER
test			ctmserver	0.13	61.00	Stats_Test

Lab 8.5: Deleting Old Events (Conditions) and Global Variables

Task 1: Delete Old Events (Conditions)

Steps:

1. If not already, sign into the **Control-M GUI** as **emuser** with the password: **Passw0rd**.
2. In the **Planning** domain, from the **Tools** tab on the ribbon, go to **Conditions**.
3. Type yesterday's date in the **MM/DD** format into the **Order Date** column to filter all conditions that have been created with yesterday's date.



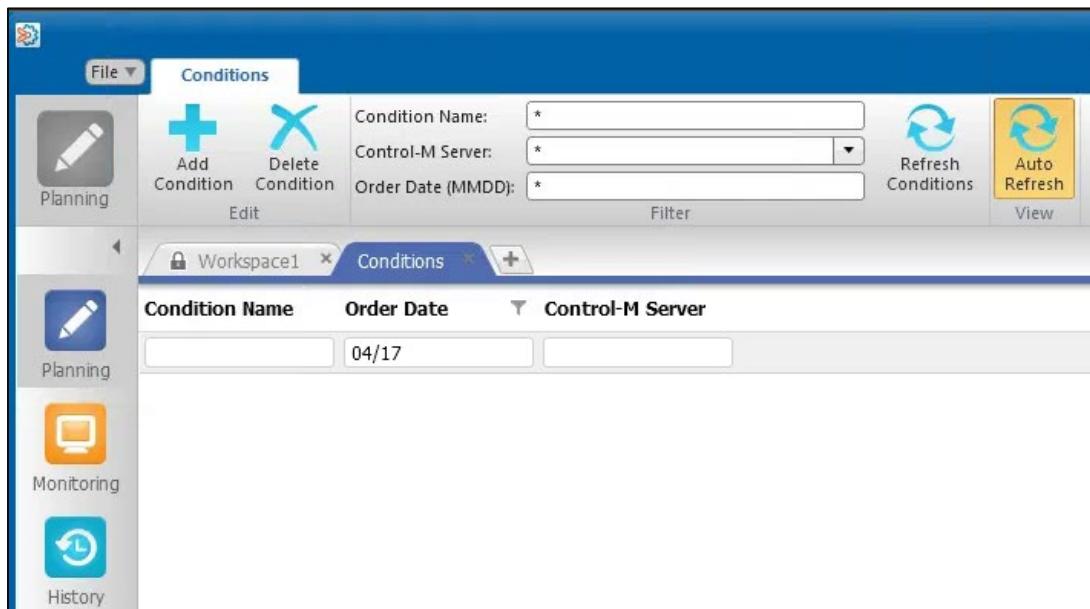
4. Click the **Refresh Conditions** button.
5. Press **Start** and open **Remote Desktop Connection** from the application tiles section.
6. Connect to the **winserver** image, using the password: **Passw0rd**.

7. On the **winserver** host, open the **Command Prompt** and run the below command to delete a range of conditions that were posted from the start of the year (0101, first of January) until yesterday.

ctmcontb -deletefrom "*" 0101 <yesterday's date in the MMDD format>

```
C:\Users\bmcadmin>ctmcontb -deletefrom "*" 0101 0417
Deleting * from 0101 to 0417
EVENT: main4-T0-ProcessA_170 ,DATE: 0417 deleted
EVENT: main3-T0-ProcessA_170 ,DATE: 0417 deleted
EVENT: main2-T0-ProcessA_170 ,DATE: 0417 deleted
EVENT: procB-22-T0-procB-23 ,DATE: 0417 deleted
EVENT: procA-13-T0-procA-15_170 ,DATE: 0417 deleted
EVENT: procA-14-T0-procA-15_170 ,DATE: 0417 deleted
EVENT: ProcessB-T0-main5_170 ,DATE: 0417 deleted
EVENT: main1-T0-main2_170 ,DATE: 0417 deleted
EVENT: main1-T0-main3_170 ,DATE: 0417 deleted
EVENT: main1-T0-main4_170 ,DATE: 0417 deleted
EVENT: main3-T0-ProcessA_193 ,DATE: 0417 deleted
EVENT: main2-T0-ProcessA_193 ,DATE: 0417 deleted
EVENT: main4-T0-ProcessA_193 ,DATE: 0417 deleted
EVENT: procA-13-T0-procA-15_193 ,DATE: 0417 deleted
EVENT: procA-14-T0-procA-15_193 ,DATE: 0417 deleted
EVENT: ProcessB-T0-main5_193 ,DATE: 0417 deleted
EVENT: main2-T0-ProcessA_216 ,DATE: 0417 deleted
EVENT: main4-T0-ProcessA_216 ,DATE: 0417 deleted
EVENT: main3-T0-ProcessA_216 ,DATE: 0417 deleted
EVENT: procA-13-T0-procA-15_216 ,DATE: 0417 deleted
EVENT: procA-14-T0-procA-15_216 ,DATE: 0417 deleted
EVENT: ProcessB-T0-main5_216 ,DATE: 0417 deleted
C:\Users\bmcadmin>
```

8. Minimize or close the **Remote Desktop Connection** window.
 9. Return to the **Control-M GUI** and refresh the **Conditions** tab.

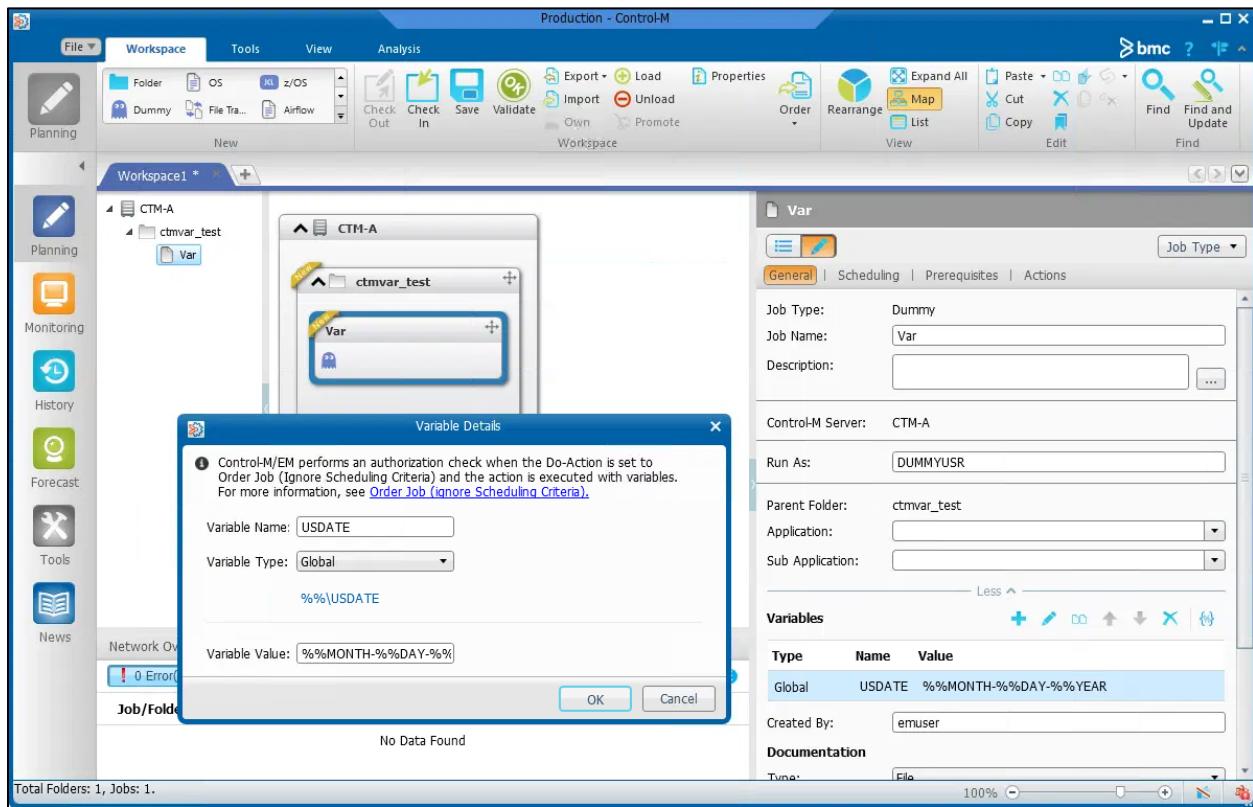


Task 2: Delete Global Variables

Steps:

1. If not already, sign in to the **Control-M GUI** as **emuser** with the password: **Passw0rd**.

2. Go to the **Planning** domain and open a **Blank Workspace**.
3. Drag a **Dummy** template into the workspace.
4. Set **CTM-A** as the Control-M/Server.
5. Set the **Folder Name** to **ctmvar_test**.
6. Select the **Dummy** job and specify the following parameters on the **General** tab:
 - **Job Name:** Var
 - **Run As:** DUMMYUSR
 - Expand **More** at the bottom of the **General** tab to reveal the variables section and click **Add (+)** to add a new variable. Enter the following details:
 - **Variable Name:** USDATE
 - **Variable Type:** Global
 - **Variable Value:** %%MONTH-%%DAY-%%YEAR
 - Click **OK**.



7. **Check In** and **Order** the job.
8. From the **ctmserver Command Prompt**, add a new global variable by running the command:
ctmvar -ACTION SET -VAR %%\UKDATE -VAREXPR %%DAY/%%MONTH/%%YEAR

```
C:\Users\bmcadmin>ctmvar -ACTION SET -VAR %%\UKDATE -VAREXPR %%DAY/%%MONTH/%%YEAR
Action SET performed successfully.

C:\Users\bmcadmin>
```

9. List the existing global variables by running the command:

ctmvar -ACTION LIST

```
C:\Users\bmcadmin>ctmvar -ACTION LIST
<<< GLOBAL >>>

VAR                                VAREXPR
-----
%%USDATE                           04-19-24
%%UKDATE                           19/04/24

C:\Users\bmcadmin>
```

10. Run the command **ctmvar -ACTION DELETE -VAR %%\USDATE** to delete the **USDATE** global variable:

```
C:\Users\bmcadmin>ctmvar -ACTION DELETE -VAR %%\USDATE
Action DELETE performed successfully.
```

```
C:\Users\bmcadmin>
```

11. Again, run the command **ctmvar -ACTION LIST** to list the global variables:

```
C:\Users\bmcadmin>ctmvar -ACTION LIST
<<< GLOBAL >>>

VAR                                VAREXPR
-----
%%UKDATE                           19/04/24

C:\Users\bmcadmin>
```

Lab 8.6: Configuring File System Clean Up Parameters

Task 1: Setup the Log Retention Parameters for the Control-M/Enterprise Manager

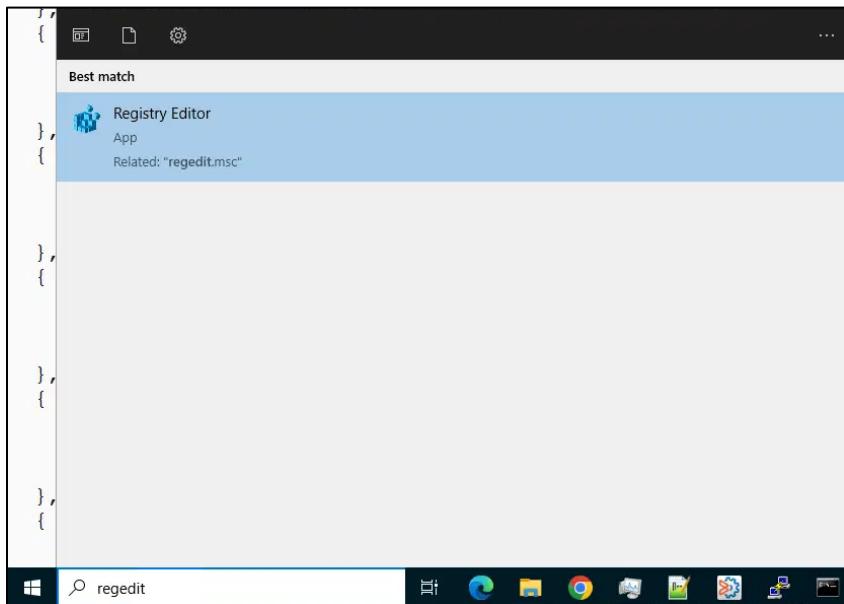
Steps:

1. Sign in to the **CCM** as **emuser** with **Passw0rd**.
2. Right-click the **Control-M EM: linserver** and select **System Parameters**.
3. Go to the **Advanced** section.
4. In the **Name** column, enter **log** to filter the system parameters.
5. Update the values of the below parameters:
 - **LogCleanInterval:** 600
 - **LogCleanLevel:** 2
 - **LogHistoryDays:** 30
 - **LogInfoLevel:** 3
6. Close the **System Parameters** window.
7. Open **PuTTY** and sign into **linserver** as **emuser** with the password: **Passw0rd**.
8. Stop the configuration agent by running the command **stop_config_agent**, entering the Control-M/EM DBO password **Passw0rd** and confirming it with **y**.
9. Start the configuration agent by running **start_config_agent**.

Task 2: Setup the Log Retention Parameters for the Control-M/Server

Steps:

1. From the landing server (**ctmserver**), click the search box and type **regedit**.
2. Open the **Registry Editor**.



3. From the **Registry Editor** window, go to **HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M/Server\SYSPRM**.
4. Find the keys **OS_DIAG_LIMIT_LOG_FILE_SIZE** and **OS_DIAG_LIMIT_LOG VERSIONS**, then double-click each parameter to update the values as below:
 - **OS_DIAG_LIMIT_LOG_FILE_SIZE:** 100
 - **OS_DIAG_LIMIT_LOG VERSIONS:** 5

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M/Server\SYSPRM

	Name	Type	Data
Computer	(Default)	REG_SZ	(value not set)
	ALWAYS_ON	REG_SZ	N
	Build	REG_SZ	B1
	Communication Protocol	REG_SZ	TCP
	CONTROLM_DATABASE	REG_SZ	ctrlmdb
	CONTROLM_SERVER	REG_SZ	C:\Program Files\BMC Software\Control-M Server...
	CTM_INSTALL_TYPE	REG_SZ	CTM
	DB Owner	REG_SZ	ctmuser
	Debug Level	REG_DWORD	0x00000000 (0)
	Debug Module Level	REG_DWORD	0x00000001 (1)
	EnvType	REG_SZ	LOCAL
	FIX_NUMBER	REG_SZ	PACTV.9.0.21.200
	Local IP Host Interface Name	REG_SZ	CTMSERVER
	OS_DIAG_LIMIT_LOG_FILE_SIZE	REG_SZ	100
	OS_DIAG_LIMIT_LOG VERSIONS	REG_SZ	5
	Product Directory	REG_SZ	C:\Program Files\BMC Software\Control-M Server\
	Product FD	REG_SZ	PACTV.9.0.21.200
	Product Version	REG_SZ	9.0.21.200
	SQLSRVRNAME	REG_SZ	ctmserver
	SQLSRVRTYPE	REG_SZ	MSSQL

Note: System Parameters are partially stored in both the **Windows Registry** (for Windows Control-M/Servers) and the **CONFIG.dat** file. For UNIX Control-M/Servers, they are stored (in their entirety) in the **CONFIG.dat** file. They can be changed from these locations, as well as the **CCM**, **ctmsys** command line utility or the **API**.

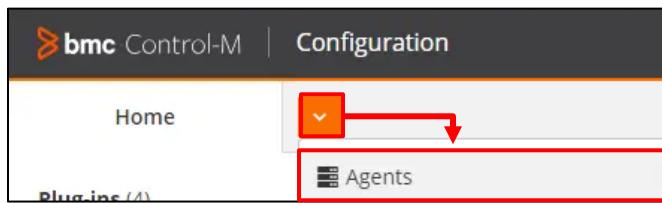
5. Close the **Registry Editor** window.
6. From the **ctmsys** Command Prompt, run the following commands to restart the Control-M/Server:
 - **shut_ctm**
 - **shut_ca**
 - **start_ctm**
 - **start_ca**
7. From the **CCM**, right-click **Control-M Server: CTM-A** and select **System Parameters**.

Note: It may take a couple of minutes for the Control-M/Server to restart and register in the CCM.

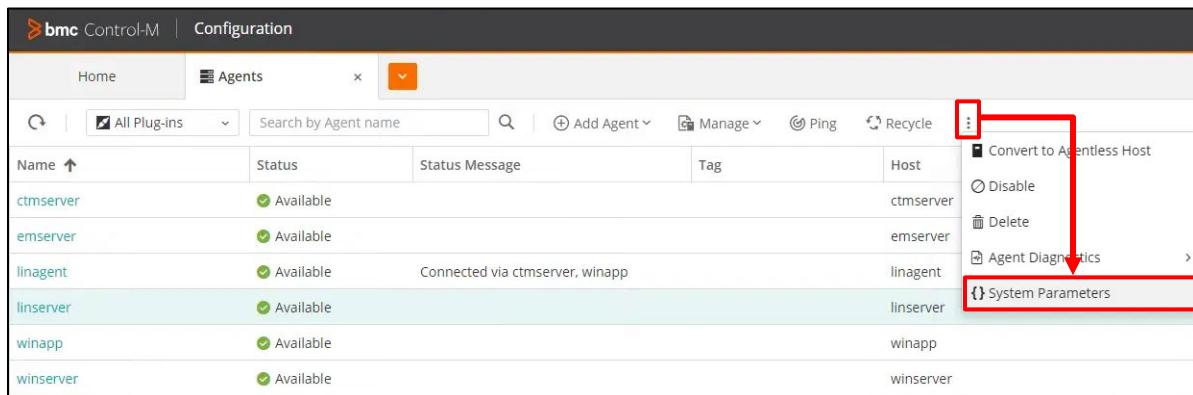
8. To filter the parameter name, enter **OS_DIAG** in the **Name** column to check the updated values.

Task 3: Setup the Log Retention Parameters for a Control-M/Agent**Steps:**

1. Control-M/Agent system parameters are now set in **Control-M Web** exclusively. From the landing server (**ctmserver**) Desktop, open **Google Chrome**.
2. Enter the following into the address bar to open the **Control-M Web Configuration** domain:
https://linserver:8446/Configuration
3. If a **Your connection is not private** window appears, click **Advanced** and then **Proceed to linserver (unsafe)**.
4. Sign in as **emuser** with the password: **Passw0rd**.
5. Once the **Configuration** domain opens, use the orange drop-down to open **Agents**.



6. When the **Agents** tab opens, select the **linserver** Control-M/Agent, then from the ribbon select the vertical ellipsis (three vertical dots) > **{ System Parameters**:



7. To filter the parameter name, hover your mouse over the **Name** column, then click the filter cog.

Editing System Parameters for 'linserver'

Name	Category	Type	Description
CMACC_AV_INTERVAL	Account Availability	Config	Interval between Account Availability checks
CMACC_UNAV_INTERVAL	Account Availability	Config	Interval between Unavailable Account checks

8. Enter **Log** as the **Name** filter value.
9. Update the values of the below parameters:
 - **LOGKEEPDAYS:** 30
 - **LIMIT_LOG_FILE_SIZE:** 50
 - **LIMIT_LOG VERSIONS:** 5

Editing System Parameters for 'linserver'

Name	Category	Type	Description	Value	Default Value
LOGICAL_AGENT_NAME	Comm	Config	Logical Agent Name	linserver	N/A
LOGKEEPDAYS	Diagnostics	Config	Days To Retain Log Files	30	N/A
AG_LOG_ON	Diagnostics	Config	Daily Log File Enabled	Y	Y
LIMIT_LOG_FILE_SIZE	Diagnostics	Config	Maximum size of log file (MB)	50	10
LIMIT_LOG_VERSIONS	Diagnostics	Config	Number of log file versions	5	10
PROCLOG_MODE	Submission	OS	Permissions of debug log files in the prolog directory	644	

10. Close the **System Parameters** tab.
11. From the **Agents** tab, recycle the **linserver** Control-M/Agent service.

Agents

Name	Status	Status Message	Tag	Host
ctmserver	Available			ctmserver
emserver	Available			emserver
linagent	Available	Connected via ctmserver, winapp		linagent
linserver	Available			linserver

Lab 8.7: Using the Control-M/Agent Toolbox

Task 1: Test the CPU Performance for the winapp Control-M/Agent

Steps:

1. From the landing server (**ctmserver**) open **Start > Command Prompt**.
2. Switch to the **winapp** Control-M/Agent directory by running:
cd C:\Program Files\BMC Software\Control-M Agent\winapp\Toolbox
3. Run the toolbox command: **toolbox.bat**.

```
C:\Users\bmcadmin>cd C:\Program Files\BMC Software\Control-M Agent\winapp\Toolbox\  
C:\Program Files\BMC Software\Control-M Agent\winapp\toolbox>toolbox.bat
```

4. Type **Y** to open the **Control-M Toolbox - Main Menu**.
5. Type **1 (CPU tests)**.

```
Control-M Toolbox - Main Menu  
-----  
Select one of the following menus:  
1 - CPU tests  
2 - System tests  
3 - Agent Help Tools 1  
4 - Agent Help Tools 2  
5 - Agent Logs Tools and Tests  
6 - Tracker tests  
7 - Tracker workers tests  
q - Quit  
  
Enter option number ---> []:1
```

6. Type **2 (CPU usage)**.

Control-M Toolbox - CPU Tests

Enter the following input:

1 - Get CPU specs
2 - CPU usage
3 - CPU and Memory monitoring
4 - CPU and Memory monitoring during changes of a directory

b - Back
q - Quit

Enter option number ---> [3]:2

7. Select **2 (Sleep between samples)** and set the value to **5 (seconds)**.
8. Type **r (Run)**.

Control-M Toolbox - Parameters

Enter the following input:

1 - Number of samples : 10
2 - Sleep between samples: 5

r - Run

b - Back
q - Quit

Enter option number ---> [2]:r

9. Monitor the CPU usage (in percent) until the test is complete.

```
Control-M Toolbox - Parameters
```

```
-----
```

```
Trying to calculate the cpu usage...
```

```
For the try: 1 cpu is: 14
```

```
For the try: 2 cpu is: 4
```

```
For the try: 3 cpu is: 8
```

```
For the try: 4 cpu is: 16
```

```
For the try: 5 cpu is: 6
```

```
For the try: 6 cpu is: 14
```

```
For the try: 7 cpu is: 5
```

```
For the try: 8 cpu is: 6
```

```
For the try: 9 cpu is: 5
```

```
For the try: 10 cpu is: 36
```

```
The cpu usage is: 11
```

```
Press enter to continue ...
```

10. Press enter, then type **b** twice to return to the **Control-M Toolbox – Main Menu**.

Task 2: Test the Disk Performance for the winapp Control-M/Agent

Steps:

1. Continuing from the last task, press **2** at the **Control-M Toolbox – Main Menu** to open **System tests**.

```
Control-M Toolbox - Main Menu
```

```
Select one of the following menus:
```

```
1 - CPU tests  
2 - System tests  
3 - Agent Help Tools 1  
4 - Agent Help Tools 2  
5 - Agent Logs Tools and Tests  
6 - Tracker tests  
7 - Tracker workers tests
```

```
q - Quit
```

```
Enter option number ---> [1]:2
```

2. Select **1** to run an **IO check**.
3. Select **1** and set the **File path** (and name) to **C:\temp\benchmark.txt**.

```
Control-M Toolbox - Parameters
```

```
Enter the following input:
```

```
1 - File path      : C:\temp\benchmark.txt  
2 - Seconds to run: 10
```

```
r - Run
```

```
b - Back
```

```
q - Quit
```

```
Enter option number ---> [1]:r
```

4. Type **r** to run the test.
5. Verify the results are below 200 milliseconds.

```
Control-M Toolbox - Parameters
```

```
5116 open/write/close in 10 seconds. Time for each write 1.954652 milliseconds
```

```
Press enter to continue ...
```