



Feature Description VMware vRealize Orchestrator

24 July 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: [Product Documentation Copyright Notice & Trademarks | Progress](#)

Table of Contents

Chapter 1: Introduction.	6
Document Purpose.	8
Intended Audience.	8
Prerequisites.	8
 Chapter 2: Install the Progress Kemp Orchestrator Plugin.	 9
 Chapter 3: Using the Progress Kemp Orchestrator Plugin.	 14
Inventory.	14
Workflows.	15
Files.	16
Delete Files.	17
Upload Files.	20
LoadMasters.	24
Add LoadMaster.	25
Add Certificate.	27
Backup Certificates.	32
Backup LoadMaster.	36
Delete Certificate.	39
Disable API.	42
Enable API.	45
Get Parameter.	48
Install Patch.	52
Reboot LoadMaster.	54
Remove LoadMaster.	56

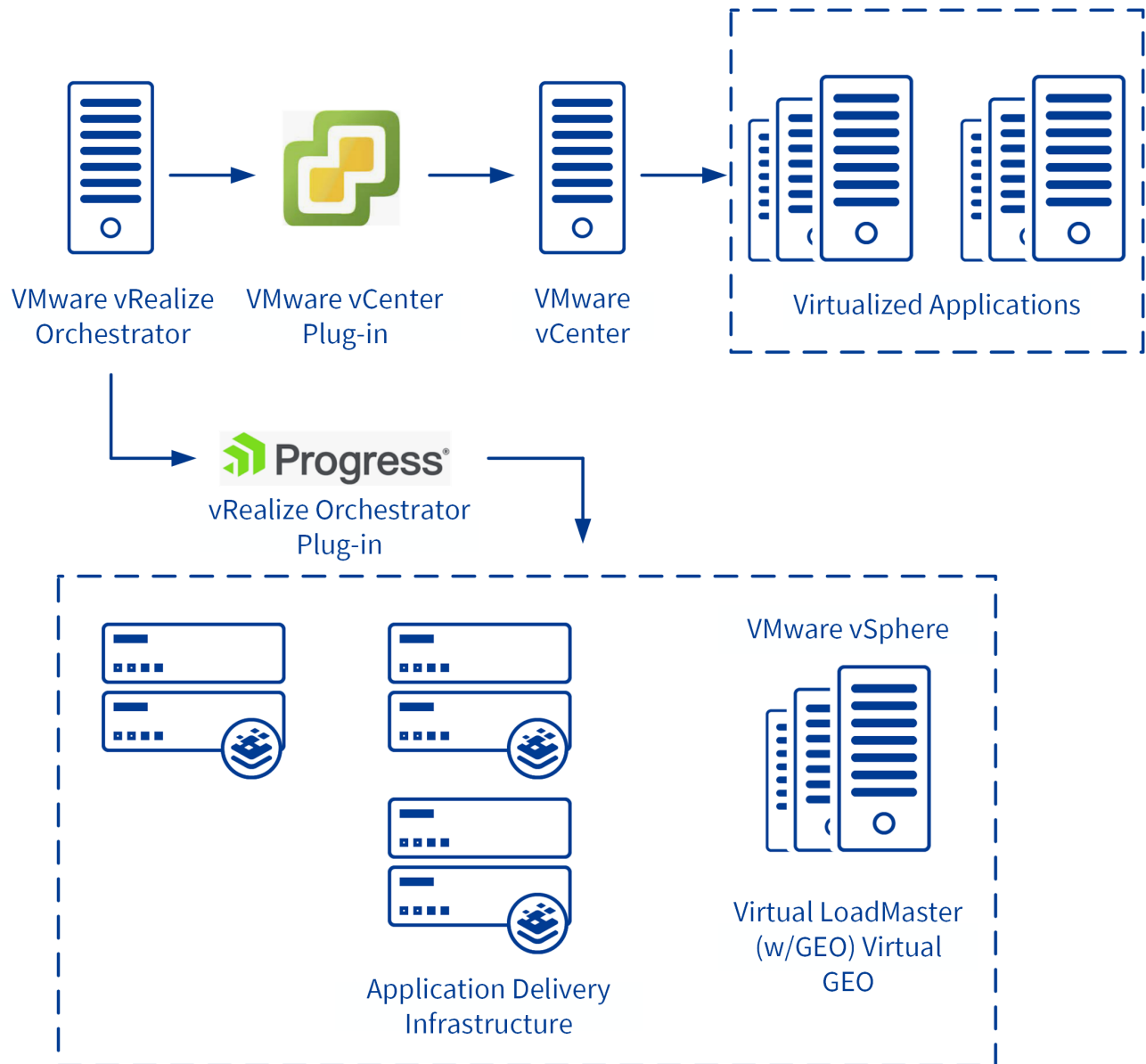
Restore Certificates.	58
Restore LoadMaster.	62
Set Credentials.	66
Set Parameter.	68
Virtual Services.	72
Add Virtual Service.	72
Assign Virtual Service Certificates.	74
Modify Virtual Service Name.	78
Remove Virtual Service.	81
Sub Virtual Services.	83
Add SubVS.	84
Modify SubVS Name.	86
Remove SubVS.	89
Real Servers.	91
Add Real Server to Sub Virtual Service.	92
Add Real Server to Virtual Service.	94
Remove Real Server.	97
 Chapter 4: Uninstall the Progress Kemp Orchestrator Plugin.	 101
Uninstall the Workflows.	101
Remove the Progress Kemp Orchestrator Plugin.	103
Restart the Service.	103
 Chapter 5: Appendix A - Get and Set Parameters.	 106
 Chapter 6: Appendix B - Memory and CPU Usage Details.	 111

Chapter 7: References.	114
---------------------------------------	------------

Introduction

Introduction

VMware vRealize Orchestrator allows administrators to develop complex automation tasks, then quickly access and launch workflows from the VMware vSphere client or various triggering mechanisms such as vROPs, vCAC, and so on.



Progress Kemp have developed a plugin for Orchestrator which acts as a front-end for the Progress Kemp Java API commands. When this plugin is installed, users can perform a number of tasks on the LoadMaster using the Orchestrator interface. The plugin allows Orchestrator to send commands (via workflows) to and receive information back from the LoadMaster and GEO products.

Related Links

- [Document Purpose](#)
- [Intended Audience](#)
- [Prerequisites](#)

Document Purpose

Document Purpose

The purpose of this document is to describe how to install and use the Progress Kemp Orchestrator plugin. The document provides step-by-step instructions on how to run the various Progress Kemp workflows which are added when the plugin is installed.

Intended Audience

Intended Audience

This document is intended to be used by anyone who would like to use Orchestrator to manage their LoadMasters.

Prerequisites

Prerequisites

Below are some prerequisites to be aware of before using the Progress Kemp Orchestrator plugin:

- If using the default self-signed certificate which is generated by the LoadMaster, please ensure it is registered properly with the systems and that it is trusted. Please refer to VMware documentation, or your Operating System documentation, for instructions on how to do this.

Note: If the certificate is not trusted there may be issues running the workflows.

- If using an FQDN as opposed to an IP address, please ensure that the DNS is properly configured.

Install the Progress Kemp Orchestrator Plugin

Install the Progress Kemp Orchestrator Plugin

Before using Orchestrator to manage a LoadMaster, the Progress Kemp Orchestrator plugin must be installed. To do that, first download the Progress Kemp Orchestrator plugin. Then, follow the steps below:

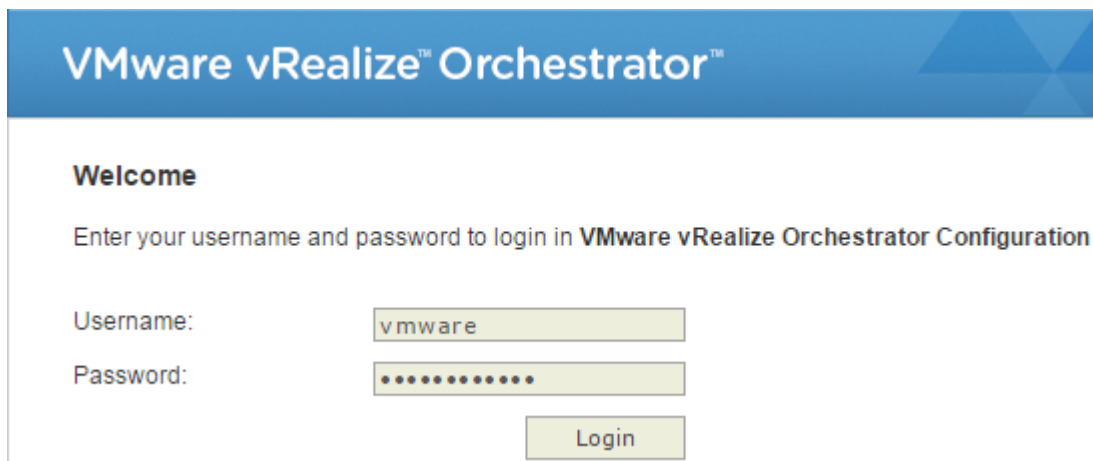
1. In a web browser, navigate to the IP address of the Orchestrator server followed by the :8281 port.

Configure the Orchestrator Server

To make additional configuration changes to the Orchestrator server, use the Orchestrator configuration interface:

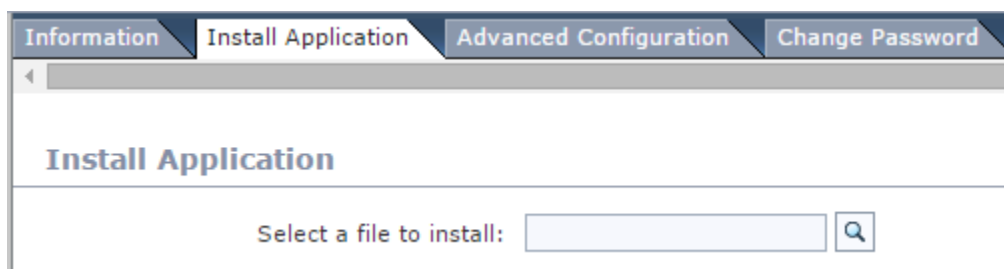
- [Orchestrator Configuration](#)
- [Orchestrator Control Center \(Beta\)](#)

2. Click the **Orchestrator Configuration** link.




The image shows the VMware vRealize Orchestrator login interface. At the top, there is a blue header with the text "VMware vRealize™ Orchestrator™". Below the header, the word "Welcome" is displayed. A message instructs the user to "Enter your username and password to login in VMware vRealize Orchestrator Configuration". There are two input fields: "Username:" with the text "vmware" entered, and "Password:" with a masked password represented by dots. A "Login" button is located below the password field.

3. Enter the Orchestrator credentials and click **Login**.



The image shows the "Install Application" tab of the VMware vRealize Orchestrator configuration interface. The tab is selected and highlighted. Below the tab, the text "Install Application" is displayed. A search bar is present with the placeholder text "Select a file to install:" and a magnifying glass icon.

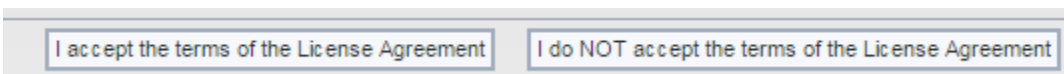
4. Select the **Install Application** tab.
5. Click the magnifying glass icon.

Install ApplicationSelect a file to install: 

6. Browse to and select the Progress Kemp Orchestrator plugin file (.vmo app file).

Note: If you cannot see the plugin file, you may need to select **All Files** in the bottom-right corner.

7. Click **Install** in the bottom-right.



Note: It might take a few seconds to upload the plugin before moving on to the next screen.

8. To accept the license agreement, click **I accept the terms of the License Agreement**.



9. The plugin is now installed, but before it can be used the Orchestrator service needs to be restarted. To do this, click **Startup Options** on the left.

Server startup options

vRO Server

Status

Running

[Refresh](#)

▶ Start service

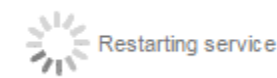
■ Stop service

⏮ Restart service

vRO Configuration Server

⏮ Restart the vRO configuration server

10. Click **Restart service**.



11. Wait for the service to restart.

Server startup options

☒ Server is restarted.

12. A message will appear when the service has been restarted.

The Progress Kemp Orchestrator plugin should now be installed and ready to use.

Using the Progress Kemp Orchestrator Plugin

Using the Progress Kemp Orchestrator Plugin

Refer to the following sections for details on how to use the Progress Kemp Orchestrator plugin.

Related Links

- [Inventory](#)
- [Workflows](#)
- [Files](#)
- [LoadMasters](#)
- [Virtual Services](#)
- [Sub Virtual Services](#)
- [Real Servers](#)

Inventory

Inventory

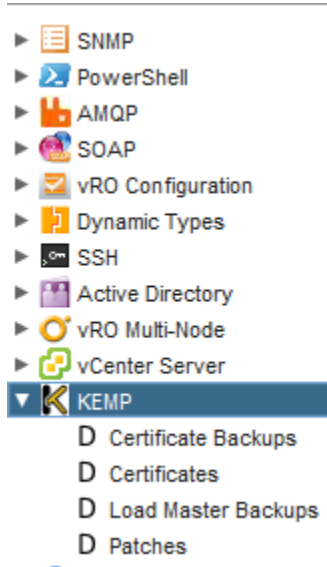
There is an **Inventory** section in Orchestrator which will list any LoadMasters that have been added to Orchestrator. There are also a number of Progress Kemp directories which are created when the Progress Kemp Orchestrator plugin is installed. To view these, follow the steps below:



1. Select the **Run** mode from the drop-down in the top-left.



2. Select the **Inventory** tab (icon of a jigsaw puzzle piece with a page behind it).



When any Progress Kemp files are uploaded to the Orchestrator, for example certificate or patch files, we recommend saving those files in the relevant Progress Kemp directories. The certificate and LoadMaster backups will automatically save into the relevant directories when the related workflows are run.

Workflows

Workflows

After the plugin has been installed, a number of Progress Kemp workflows will be available. These workflows can be used to perform various tasks in the LoadMaster.

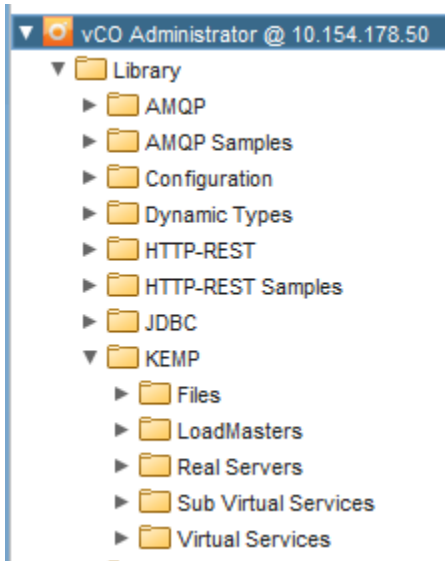
The workflows can be accessed by following the steps below:



1. Select the **Run** mode from the drop-down in the top-left.



2. Select the **Workflows** tab (blue icon).



3. Expand the **Library** directory.
4. Expand the **Kemp** directory.
5. Each of the sub-directories within the **Kemp** directory contain various workflows that can be run. To run a workflow:
 1. Expand the relevant directory.
 2. Select the relevant workflow.



1. Click the green play icon (Start workflow) in the top-left.
2. A screen will then appear which will contain relevant fields relating to that workflow. Fill out the fields and click Submit.

The steps to run each of the workflows are the same, but the fields that appear on each of the screens will differ. Refer to the sections below for more information. The section names correspond to the directory names in Orchestrator.

Files

Files

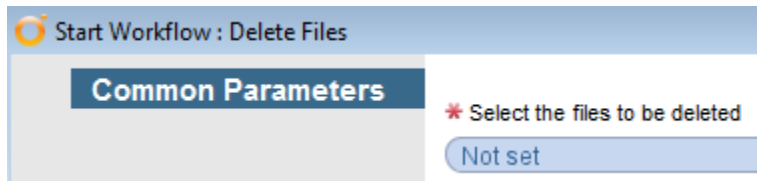
Files can be uploaded to and deleted from Orchestrator. For further details, refer to the sections below:

Related Links

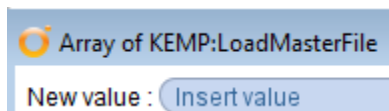
- [Delete Files](#)
- [Upload Files](#)

Delete Files

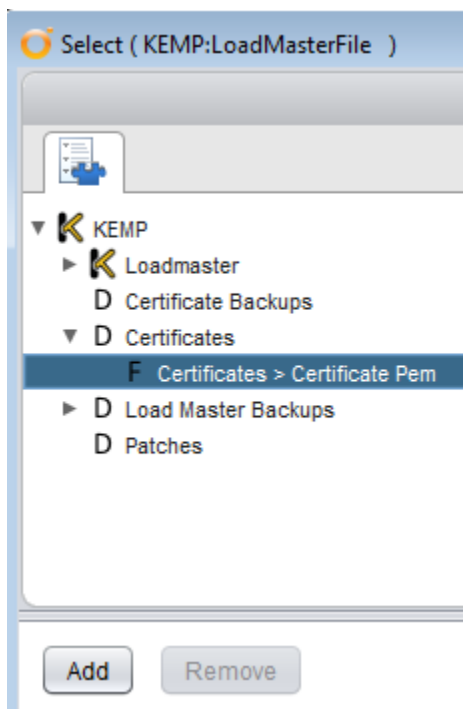
Delete Files



1. Click **Not set**.



1. Click **Insert value**.



1. Expand the **Kemp** directory.
2. Expand the relevant directory where the file is located.
3. Select the relevant file to be deleted.
4. Click **Add**.

Inventory ID	File Name
F Certificates > certificate.pem	certificate.pem

Cancel

Select

1. Click **Select**.

Array of KEMP:LoadMasterFile

New value :

✖

↑

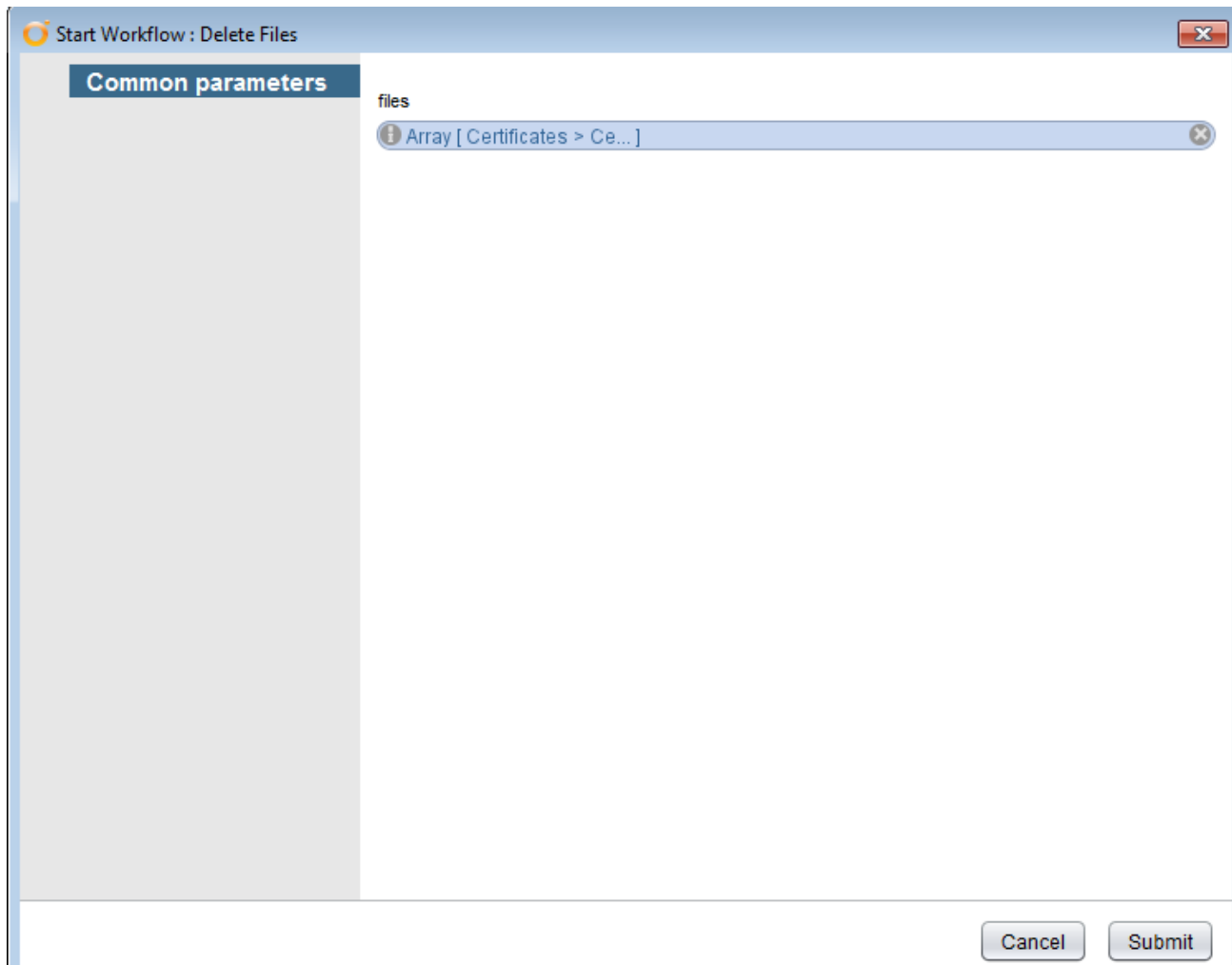
↓

Inventory ID	File Name
F Certificates > certificate.pem	certificate.pem

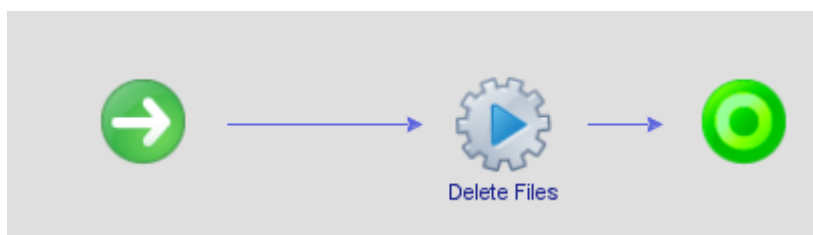
Cancel

Accept

1. Click **Accept**.



1. Click **Submit**.



1. Wait for the deletion to complete.

Upload Files

Upload Files

Start Workflow : Upload Files

Common Parameters

* Select the files to be uploaded
Not set

* Select the directory to store these files
Not set

Replace existing files with the same name?
☐ Yes ☒ No

1. Click **Not set** in the **Select files to be uploaded** field.

Array of MimeAttachment

New value : Not set

Insert value

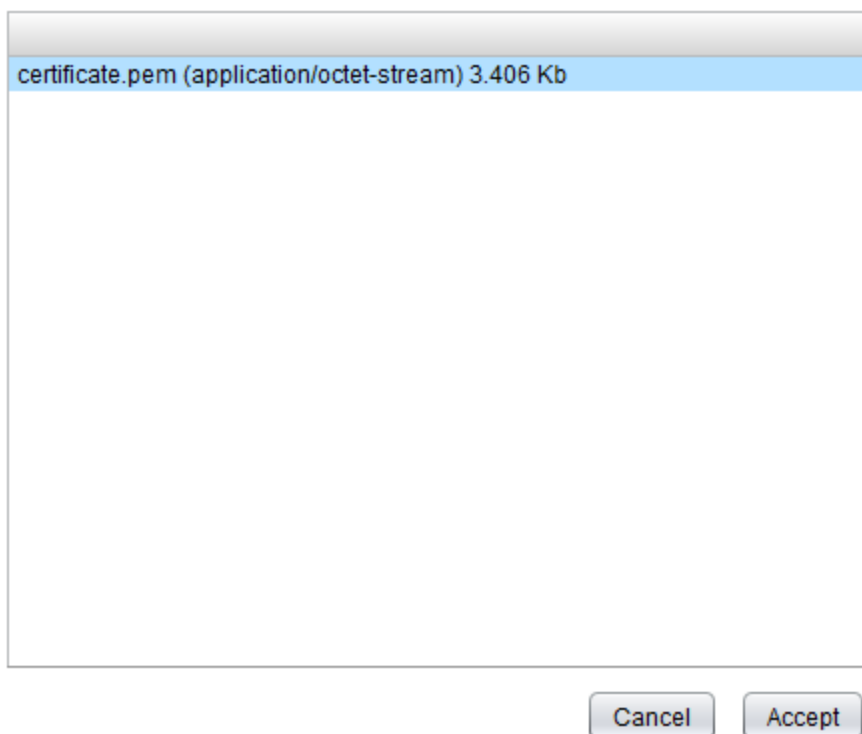
2. Click **Not set**.
3. Browse to and select the relevant file to be uploaded.

Array of MimeAttachment

New value : certificate.pem (application/octet-stream)

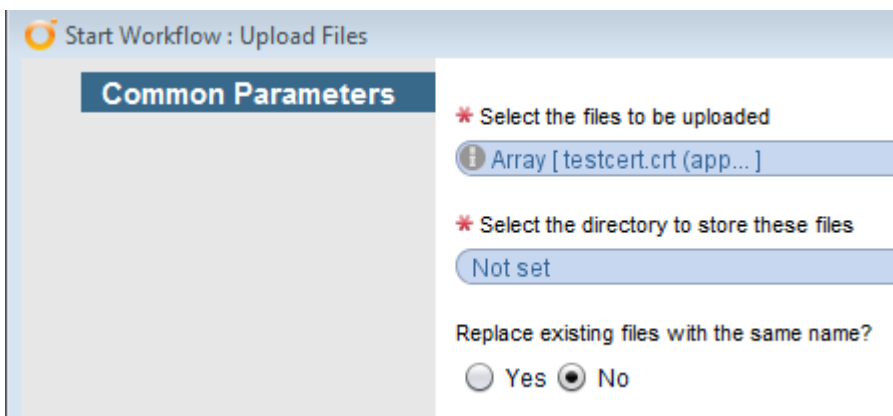
Insert value

4. Click **Insert value**.

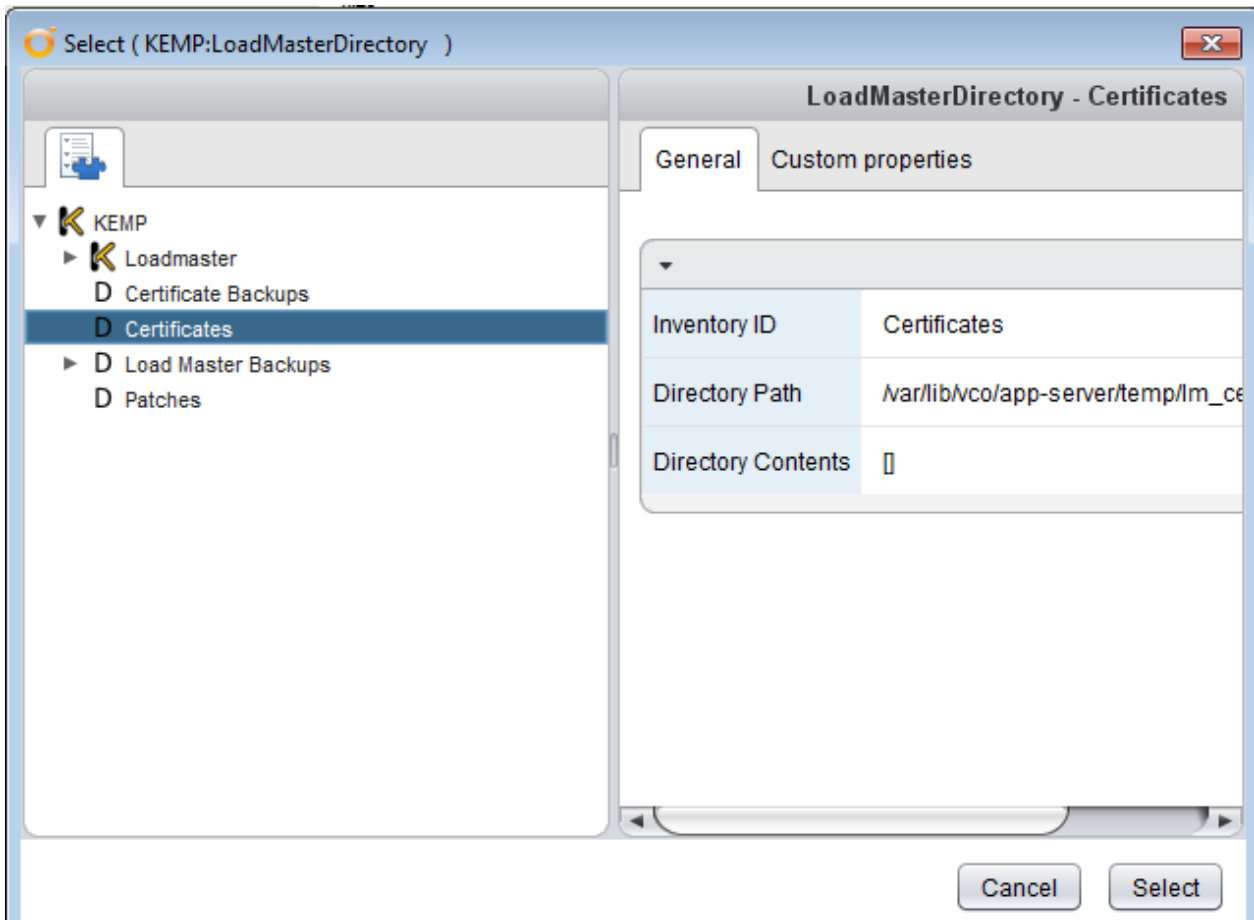


Note: Multiple files can be uploaded at the same time, if needed. Simply browse to and select another file and click **Insert value** to add it to the list of files to be uploaded.

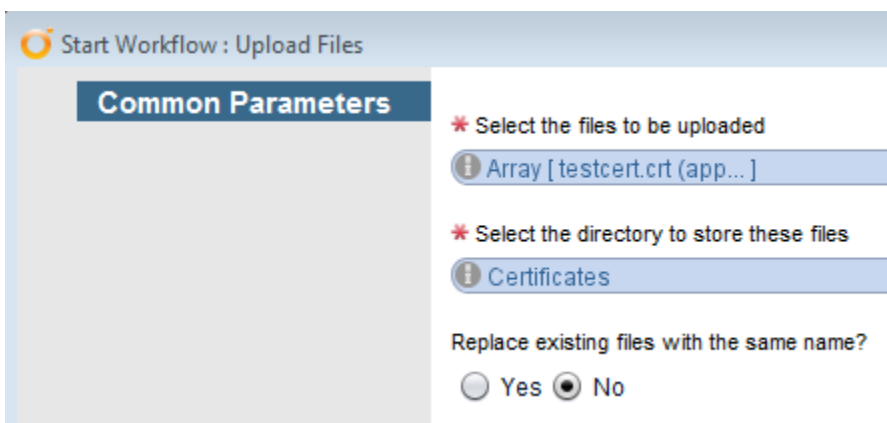
5. Click **Accept**.



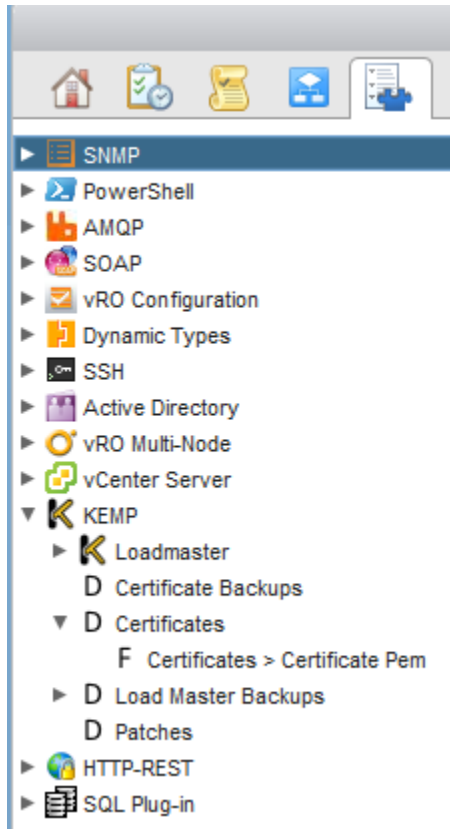
6. Click **Not set** in the **Select the directory to store these files** field.



7. Expand the **Kemp** directory.
8. Select the relevant directory to store the file in.
9. Click **Select**.



10. If you want to replace an existing file of the same name, select **Yes**.
11. Click **Submit** to upload.



The file will then be visible in the **Inventory** tab in the relevant directory.

Uploading Files which are Bigger than 2MB

There is a limit of 2MB on the file sizes that can be uploaded via the Progress Kemp Orchestrator plugin. This means that firmware upgrade patch files are not able to be uploaded using the method listed in the section above. This section outlines a workaround that can be used to upload files greater than 2MB in size.

The following are valid LoadMaster directories on the Orchestrator server:

- lm_config_backups
- lm_certs
- lm_certs_backups
- lm_patches

You can use a number of options to copy/download the file to the Orchestrator Server. Two of the options - using SCP or using cURL, are outlined below.

Using SCP to Copy a File to the Orchestrator Server

This process requires SSH access to be enabled when deploying the Orchestrator appliance. Follow the steps below:

1. Navigate to the directory containing the file to transfer on the source machine.

2. Run the following command:

```
scp <File_To_Transfer> root@<Orchestrator_Server_IP_Address>:/var/lib/vco/app-server/temp/  
<LoadMaster_Directory>/<Filename>
```

Note: In order for the files to be visible in the Orchestrator client, one of the four directories listed in the Uploading Files which are Bigger than 2MB section must be used in place of **<LoadMaster_Directory>**.

3. After authenticating with the server, the file transfer should proceed.

Use cURL to Download the File

The file must then be downloaded using a cURL command:

1. Connect to the Orchestrator server via SSH.

Note: Unless additional users have been configured on the server, you must log in as **root**.

2. Navigate to /var/lib/vco/app-server/temp/<LoadMasterDirectory>

Note: Replace **<LoadMasterDirectory>** with one of the directories listed in the Uploading Files which are Bigger than 2MB section.

3. Invoke cURL with the **-o <Filename>** parameter to transfer the output of the command to a file, for example:

```
curl -u user:password -o <NewFilename> <URL>/<File_To_Download>
```

Configuring Permissions

After the file has been successfully transferred, the permissions of the file must be modified in order for it to be accessible to the Orchestrator client. To modify the permissions, run the following command:

```
chown vco <FileName>
```

Note: If this step is not performed, the files in question will not be visible in the Orchestrator client.

LoadMasters

LoadMasters

In the **LoadMasters** directory, there are a number of workflows that can be executed which relate to managing LoadMasters, such as adding and removing LoadMasters from Orchestrator. For details on each of the LoadMaster workflows, refer to the sections below.

Before any of the other LoadMaster workflows can be run on a LoadMaster, the relevant LoadMaster needs to be added to Orchestrator. The first section below provides details on the **Add LoadMaster** workflow.

Related Links

- [Add LoadMaster](#)
- [Add Certificate](#)
- [Backup Certificates](#)
- [Backup LoadMaster](#)
- [Delete Certificate](#)
- [Disable API](#)
- [Enable API](#)
- [Get Parameter](#)
- [Install Patch](#)
- [Reboot LoadMaster](#)
- [Remove LoadMaster](#)
- [Restore Certificates](#)
- [Restore LoadMaster](#)
- [Set Credentials](#)
- [Set Parameter](#)

Add LoadMaster

Add LoadMaster

A LoadMaster can be added to Orchestrator using the **Add LoadMaster** workflow. A LoadMaster must be added to Orchestrator before any workflows can be run on that LoadMaster.

Start Workflow : Add LoadMaster

1 Authentication

2 LoadMaster Configuration

* Enter the username for the LoadMaster

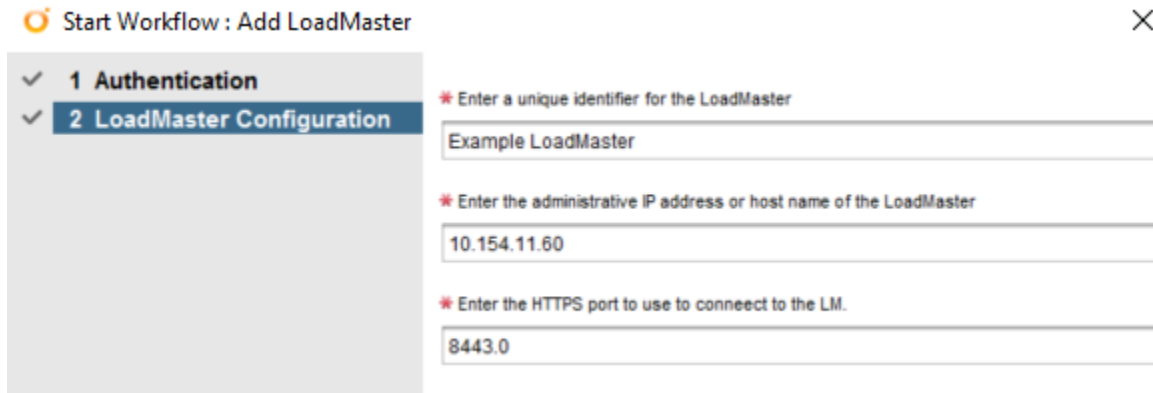
bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **LoadMaster Configuration**.



Start Workflow : Add LoadMaster

✓ 1 Authentication

✓ 2 LoadMaster Configuration

* Enter a unique identifier for the LoadMaster

Example LoadMaster

* Enter the administrative IP address or host name of the LoadMaster

10.154.11.60

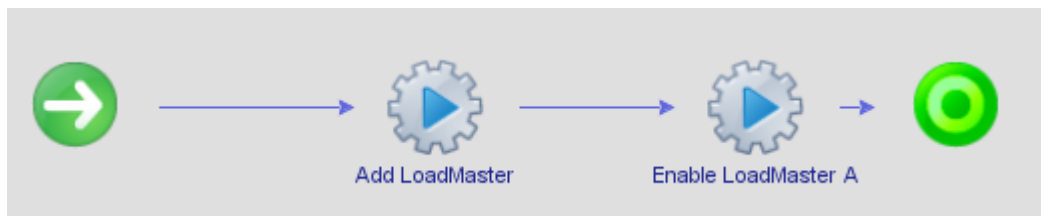
* Enter the HTTPS port to use to connect to the LM.

8443.0

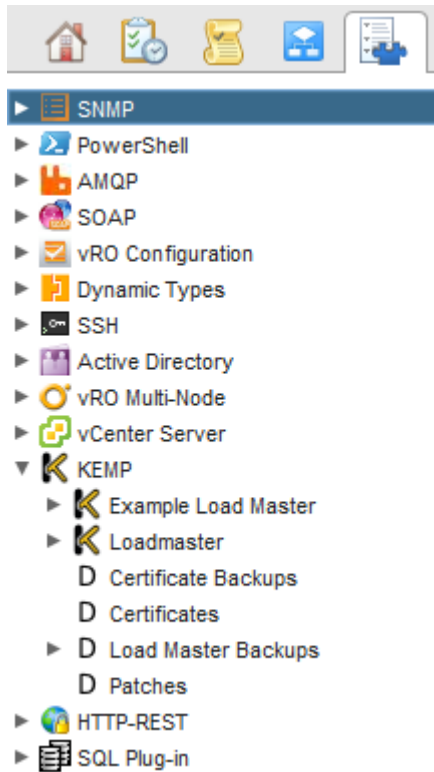
4. Enter a recognizable name in the **Enter a unique identifier for the LoadMaster** text box. This is a friendly name for the LoadMaster, which appears in Orchestrator.
5. Enter the IP address of the LoadMaster to be added.
6. Enter the HTTPS port to use to connect to the LoadMaster.

Note: If you cannot see the port field, you may need to install the latest Progress Kemp package. To do this, select the **Administer** option from the drop-down at the top, go to the **Packages** tab on the left, select the **com.kemptechnologies** package, click the **Import package** icon and import the latest Progress Kemp package. Both the .dar and the .package files must be updated. The latest Progress Kemp package is available on the Progress Kemp website.

7. Click **Submit**.



8. Wait for the LoadMaster to be added.



The LoadMaster will then be listed in the **Kemp** directory in the **Inventory** tab.

Add Certificate

Add Certificate

Before uploading a certificate to the LoadMaster, the certificate file must first be uploaded to Orchestrator. For step-by-step instructions on how to upload a file, refer to the [Upload Files](#) section.

```

testcert.crt
1 -----BEGIN CERTIFICATE-----
2 MIICyzCCAjQCCQD9Zrq+3HKfJDANBgkqhkiG9w0BAQsFADCBqTELMakGA1UEBhMC
3 SUUxEDAObgNVBAGMB011bnN0ZXIxEtAPBgNVBACMCExpWVyaWNrMR0wGAYDVQQK
4 DBFLRU1QIFRlY2hub2xvZ2llcyEcmBoGA1UECwwTUHVJvZHVjdCBZLWZlbnB9bWVu
5 dDEOMAwGA1UEAwwFamFtZXMxKzApBgkqhkiG9w0BCQEWHPvYnJpZW5Aa2VtcHRl
6 Y2hub2xvZ2llcy5jb20wHhcNMTUwNzI4MTU1MTQ4WhcNMTYwNzI3MTU1MTQ4WjCB
7 qTELMakGA1UEBhMCSUUxEDAObgNVBAGMB011bnN0ZXIxEtAPBgNVBACMCExpWVya
8 aWNrMR0wGAYDVQQKDBFLRU1QIFRlY2hub2xvZ2llcyEcmBoGA1UECwwTUHVJvZHVj
9 dCBZLWZlbnB9bWVuDEOMAwGA1UEAwwFamFtZXMxKzApBgkqhkiG9w0BCQEWHPv
10 YnJpZW5Aa2VtcHRlY2hub2xvZ2llcy5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0A
11 MIGJAoGBAPZyfvEy+JeX4JT336h3IZqd022E8jsSMShZazcuI/GICrBbAGowhBtf
12 kVoESNpq7PysaQR0PYfqJii41HUwqJo/Wr/8ulBoewYzoLAGzYfpAe6Rax+lKtc7
13 7mlKoQ3zheBk9Hj3fw1RToSgU9F5oiQJT3jT6zprt0sFuBp+UC8JAgMBAAEwDQYJ
14 KoZIhvcNAQELBQADgYEAeoGA22dXIVAIZ0G8uYOne/KOg7QhV+RX1B6a9j51QW6E
15 H72GzQaI3K11TgkP/UKUTCTjQgVw+4tHx3eU+7Dq9BXA4fx30bvqfONCxBHG8eXy
16 N6gw8BAapDftliwRCKlZjBjRtdpP+G8kk7OmPh2ZZOvCY4ylSeWZPDgLCy0tYsw=
17 -----END CERTIFICATE-----
18 -----BEGIN RSA PRIVATE KEY-----
19 Proc-Type: 4, ENCRYPTED
20 DEK-Info: DES-EDE3-CBC, 59951F4DADCDF43D
21
22 /8x45hW4xrUpX6eDalZfNDFVN8AUx+saxRYnRYvPSuic463o5UhxRUXi+TUE6eeF
23 CqOB5k5ZeFn2n7x45AHRXlauVGvt4g6oaFZH+GXPvdWCSQWES2TrcQp7KCXY7zth
24 +rn5qsFVqCIXsfdw22EV4intoysSj89Fxbqqs8BME9WETCu2w7NN21BS6ji3fv/f
25 uMSS/cOOuv2jPCpMavaDGmqCKtOy8dKfJlySKhWFacOCjdGyU7uw+SrP/IpzljBV
26 YWyyxmSXzmRdsN2d0L1Az8L3h921amHIRCmXs8Hc2vNGDnN9zdJ+SF3vKs256FN
27 Ovmscty9zs362nl+nUWTPSqFhDsb6bWY7hMJMARGVTfi/Qjw75XoEQpj0jdDy4oq
28 hCvsliaWU+FC9I1j+bKUU4z3J7CSEkFdtJk4iRsfzk9oGC8gdj6zOfsV0905yIQs
29 2RxKXo1U0RrsAwmYdpQPK5TRLWDnyyIajsHjI2fH3wHOPcwTilWkv+VzOC1ohKzK
30 dExxW6GAoUgDbbsLuqT4y93x9E+IWA1OBpJ4Z5s4LKkyaiD0jzSvP5OG+Mo17+jg
31 dcKvyJcWuXqs6wI7m/hIeS4Ghhq1JjDiuARX60Ws3NcyX4ntWXq8edx1PXvR2+cW
32 oesvuxzqFBncwgnBw01jryWt+7u8TIuOQVUjJlMtaeSYifjofKPP3c/Xud0FE8ck
33 1SEKK+wDTQp8/j7iDxkfyZlh0Ti+NneY2TLsIF+YhLqSvbu2rHkITEBn6PLiTH5k
34 V789ENrdQJU50b+riVKyzZhh2YsWuD3xWK/5RAT83FSi5+N37PQIMA==
35 -----END RSA PRIVATE KEY-----
36

```

When uploading a certificate file via Orchestrator (or via the Progress Kemp API), both the certificate and key must be concatenated into the one file. The certificate file must be listed on top, followed by the private key at the bottom - this is the format which is required by the API which is what the Progress Kemp Orchestrator plugin is based upon. An example file is shown in the screenshot above.

After a certificate file has been uploaded to Orchestrator, it can then be uploaded to the LoadMaster using the **Add Certificate** workflow.

Start Workflow : Add Certificate

1 Authentication

2 Certificate Configuration

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

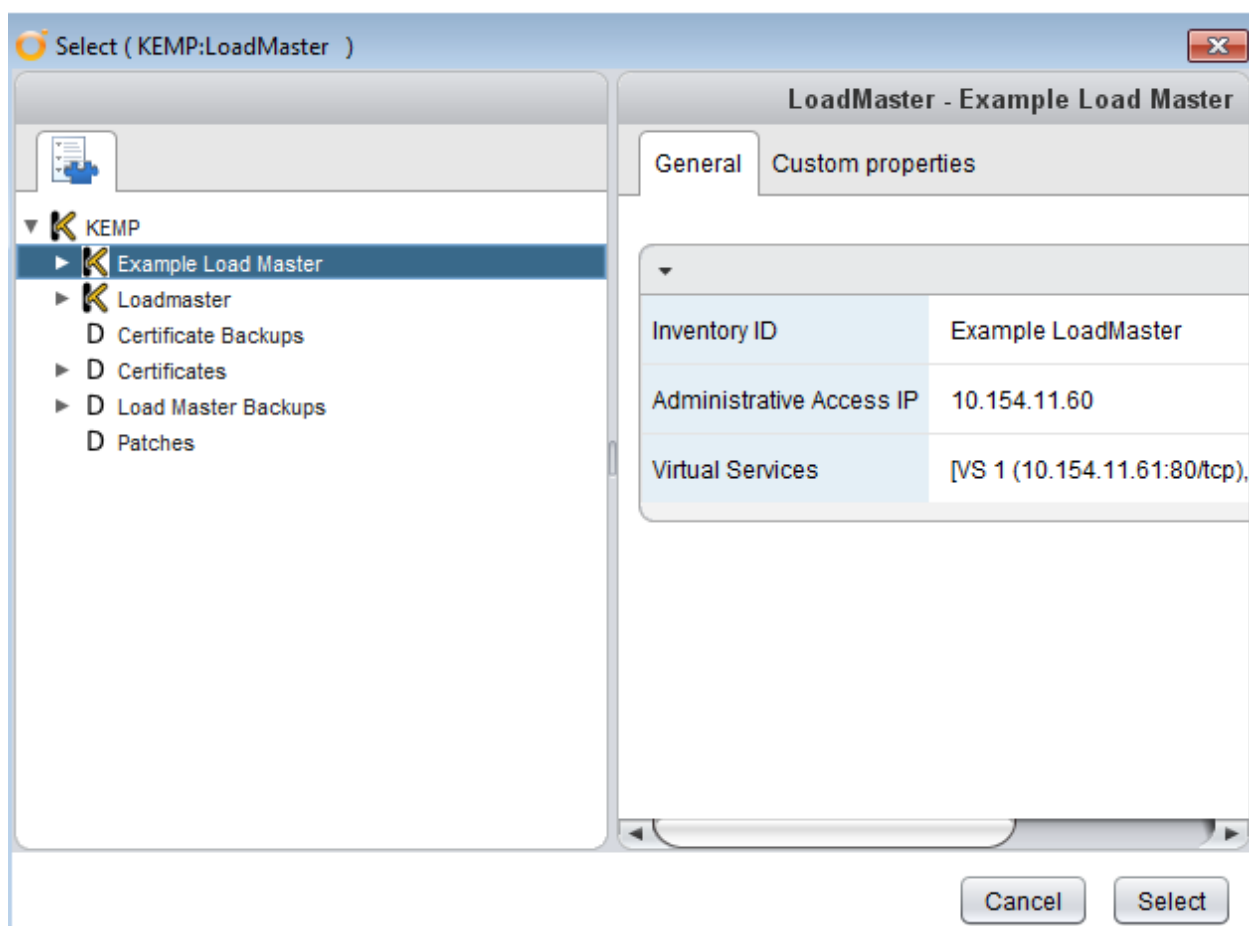
* Select the LoadMaster to add the certificate to

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

Note: This is the certificate file used to authenticate to the LoadMaster - this is not the field used to upload a new certificate.

3. Click **Not set** in the **Select the LoadMaster to add the certificate to** field.



4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.

Start Workflow : Add Certificate

1 Authentication

2 Certificate Configuration

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to add the certificate to

i Example Load Master

7. Click **Certificate Configuration**.

Start Workflow : Add Certificate

✓ 1 Authentication

2 Certificate Configuration

* Select the certificate file to be added

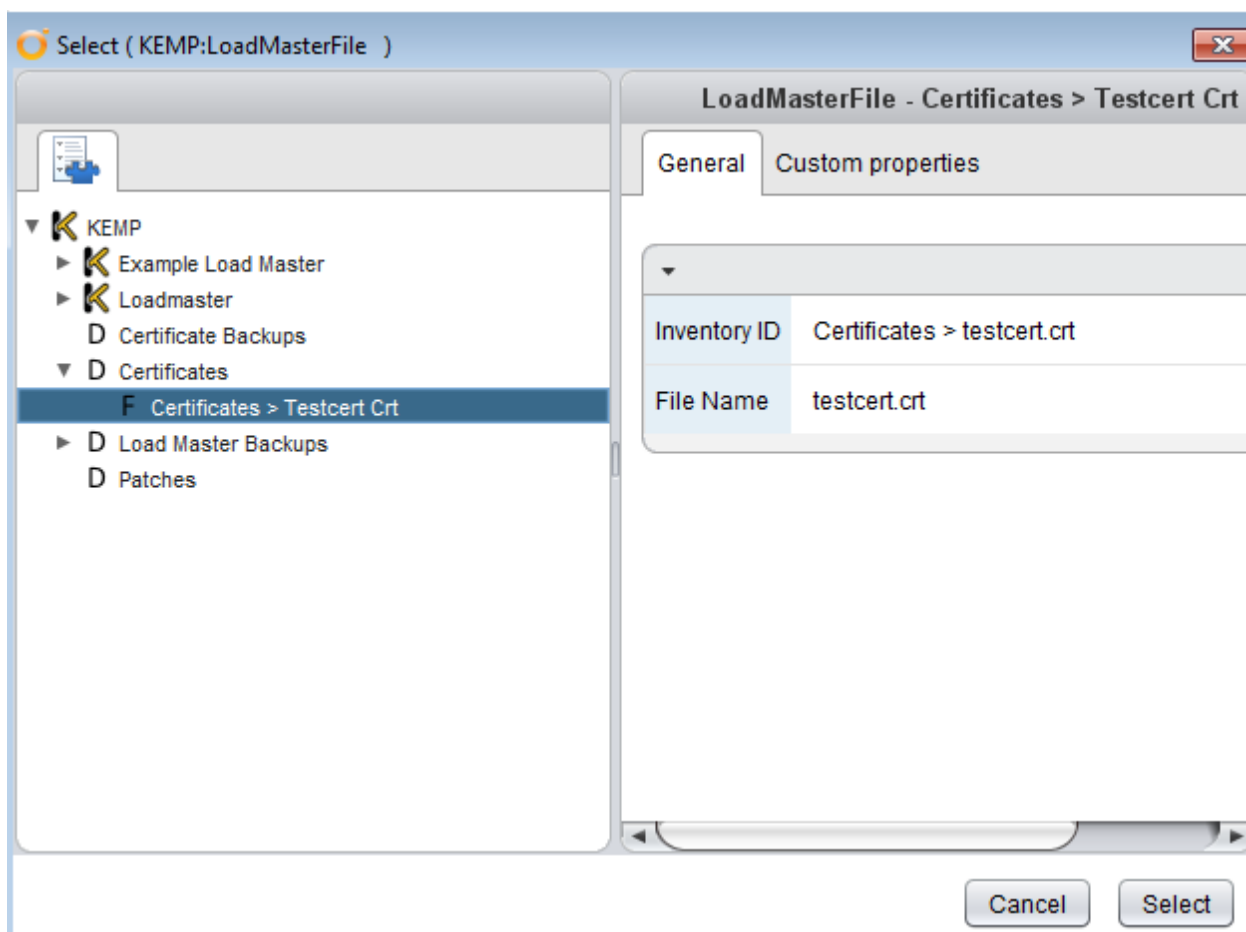
Not set

* Enter the passphrase for this certificate

* Enter a LoadMaster identifier for this certificate

Replace any existing certificate that uses this identifier?

☐ Yes ☒ No

8. Click **Not set**.

9. Expand the **Kemp** directory.
10. Expand the **Certificates** directory.
11. Select the relevant certificate.
12. Click **Select**.

Start Workflow : Add Certificate

✓ **1 Authentication**

2 Certificate Configuration

* Select the certificate file to be added
Certificates > Testcert.Crt

* Enter the passphrase for this certificate

* Enter a LoadMaster identifier for this certificate
Example Certificate

Replace any existing certificate that uses this identifier?
☐ Yes ☒ No

Cancel Back Next Submit

13. Enter the passphrase which was used when creating the certificate in the **Enter the passphrase for this certificate** text box.
14. Enter a recognizable name for the certificate in the **Enter a LoadMaster identifier for this certificate** text box. This is a friendly name for the certificate which will be displayed in the LoadMaster.
15. If replacing an existing certificate of the same name, select **Yes**.
16. Click **Submit**.

Backup Certificates

Backup Certificates

The certificates on a LoadMaster can be backed up via Orchestrator. To do this, run the **Backup Certificates** workflow.

Start Workflow : Backup Certificates

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

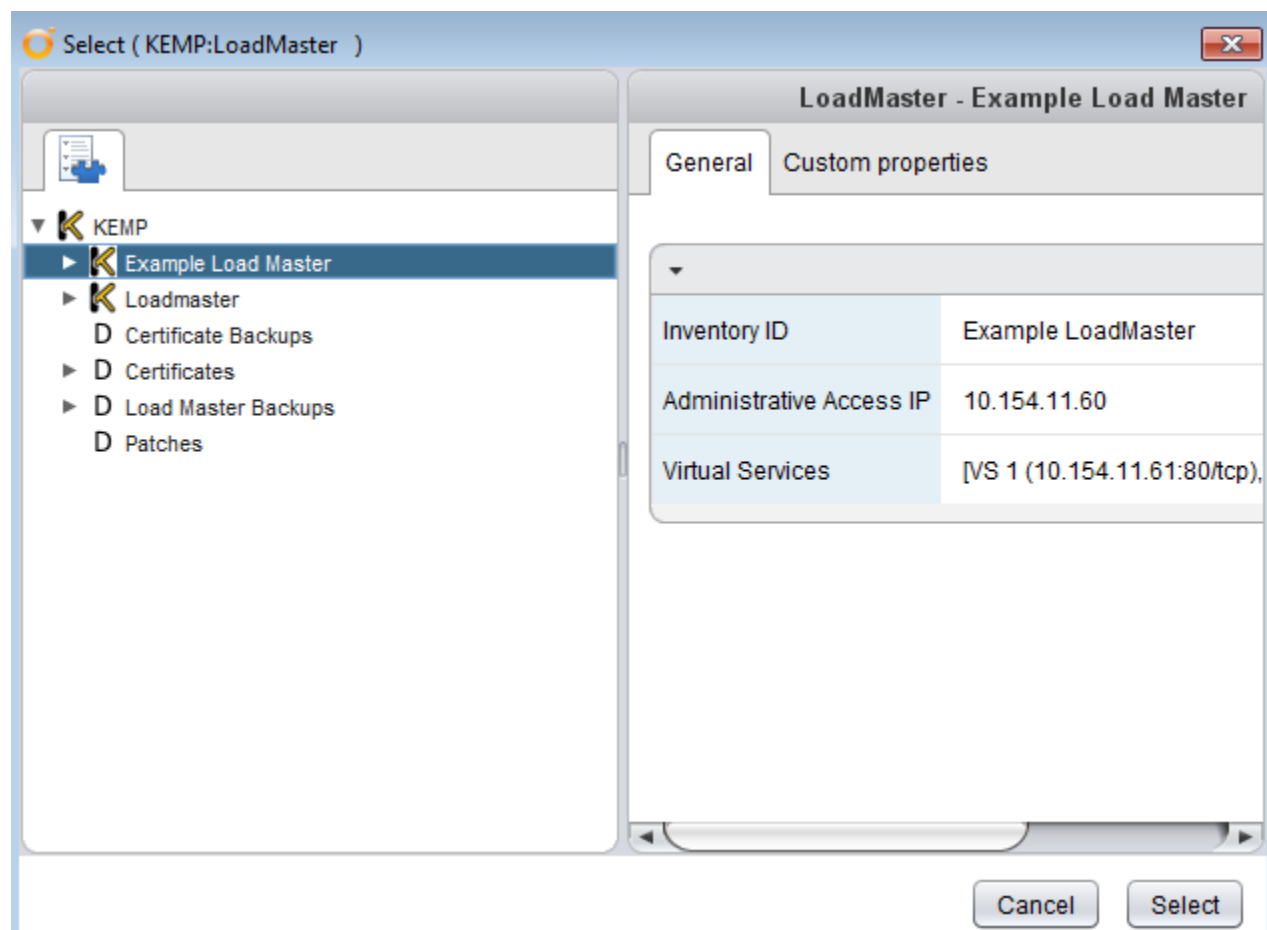
Not set

* Select the LoadMaster to perform the backup on.

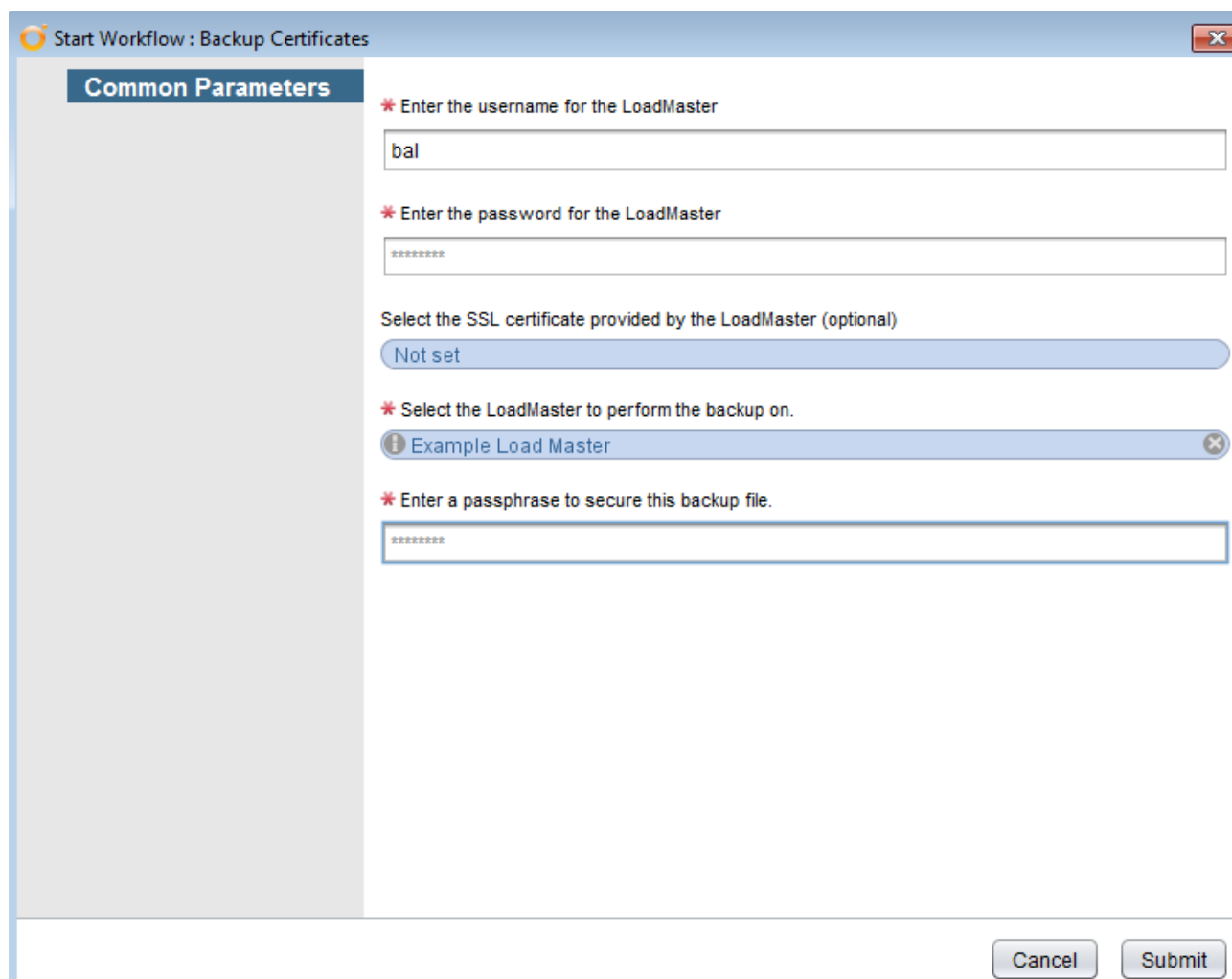
Not set

* Enter a passphrase to secure this backup file.

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to perform the backup on** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.



Start Workflow : Backup Certificates

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

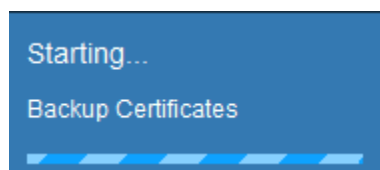
* Select the LoadMaster to perform the backup on.

i Example Load Master

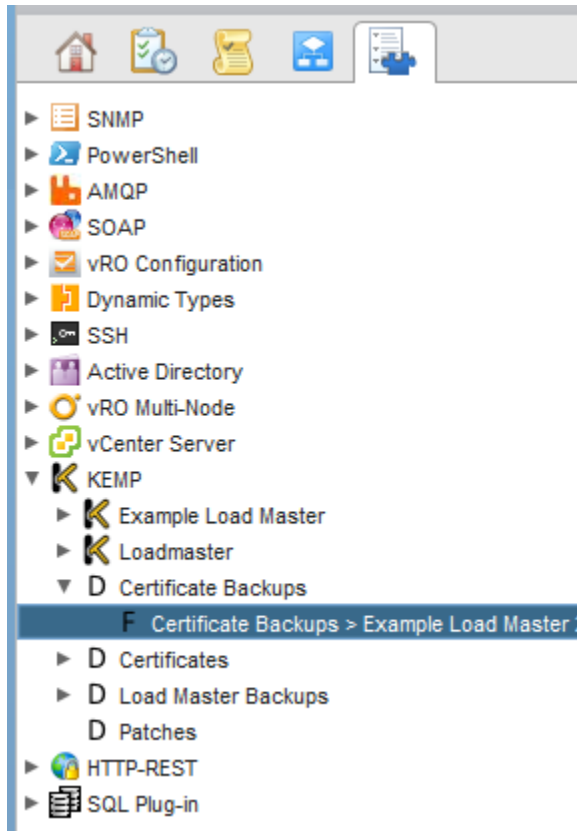
* Enter a passphrase to secure this backup file.

Cancel Submit

1. Enter a passphrase to secure this backup file.
2. Click **Submit**.



1. Wait for the backup to complete.



The backup will be saved to the **LoadMaster Backups** directory in the **Inventory** tab.

Backup LoadMaster

Backup LoadMaster

The LoadMaster configuration can be backed up via Orchestrator. To do this, run the **Backup LoadMaster** workflow.

Start Workflow : Backup LoadMaster

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to perform this backup on.

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to perform this backup on** field.

Select (KEMP:LoadMaster)

LoadMaster - Example Load Master

General Custom properties

Inventory ID	Example LoadMaster
Administrative Access IP	10.154.11.60
Virtual Services	[VS 1 (10.154.11.61:80/tcp),

Cancel Select

1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Backup LoadMaster

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

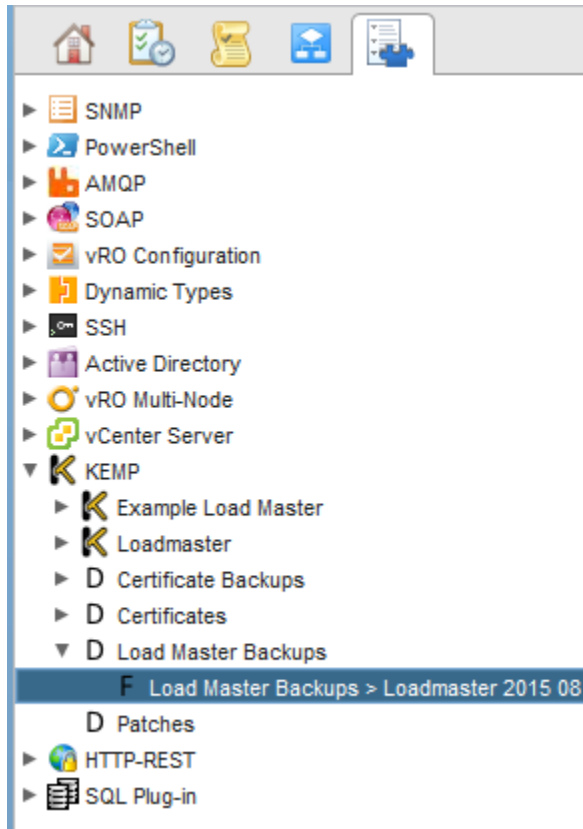
Not set

* Select the LoadMaster to perform this backup on.

Example Load Master

Cancel Submit

1. Click **Submit**.



The backup will be stored in the **LoadMaster Backups** directory in the **Inventory** tab. The backup can be restored to a LoadMaster via Orchestrator. For instructions on how to do this, refer to the [Reboot LoadMaster](#) section.

Delete Certificate

Delete Certificate

Certificates can be deleted from the LoadMaster by running the **Delete Certificates** workflow.

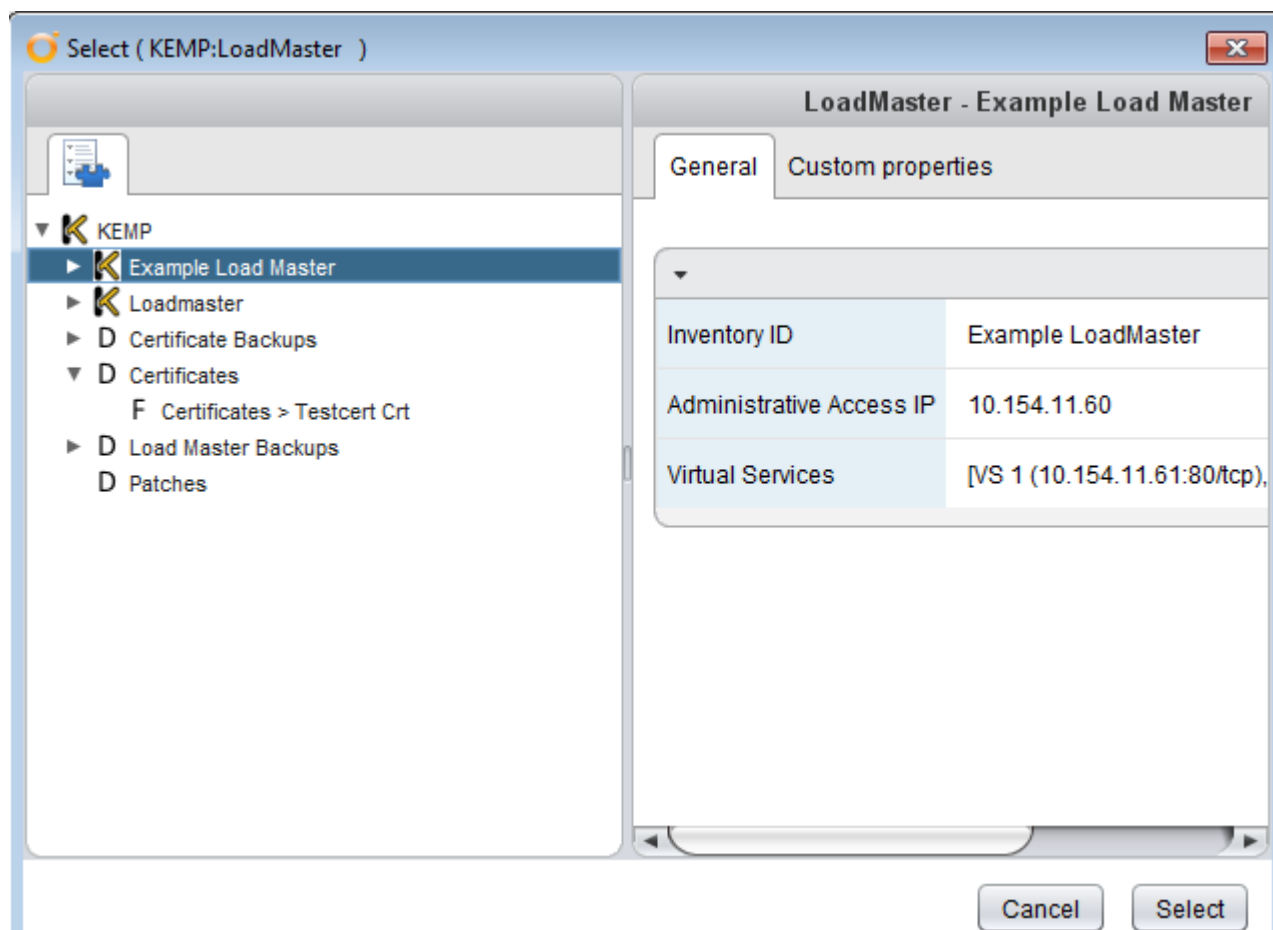
Start Workflow : Delete Certificate

Common Parameters

- * Enter the username for the LoadMaster
bal
- * Enter the password for the LoadMaster

- Select the SSL certificate provided by the LoadMaster (optional)
Not set
- * Select the LoadMaster to delete a certificate from
Not set
- * Enter the identifier of the certificate to be deleted

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to delete a certificate from** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Delete Certificate

Common Parameters

* Enter the username for the LoadMaster
bal

* Enter the password for the LoadMaster

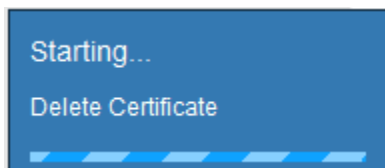
Select the SSL certificate provided by the LoadMaster (optional)
Not set

* Select the LoadMaster to delete a certificate from
Example Load Master

* Enter the identifier of the certificate to be deleted
Example Certificate

Cancel Submit

1. Enter the identifier of the certificate to be deleted.
2. Click **Submit**.



1. Wait for the deletion to finish.

Disable API

Disable API

The API interface on the LoadMaster can be disabled via Orchestrator.

Note: If the API is disabled, most of the workflows will not work. The only workflows that will work when the API is disabled are **Add LoadMaster** and **Enable API**.

Start Workflow : Disable API

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

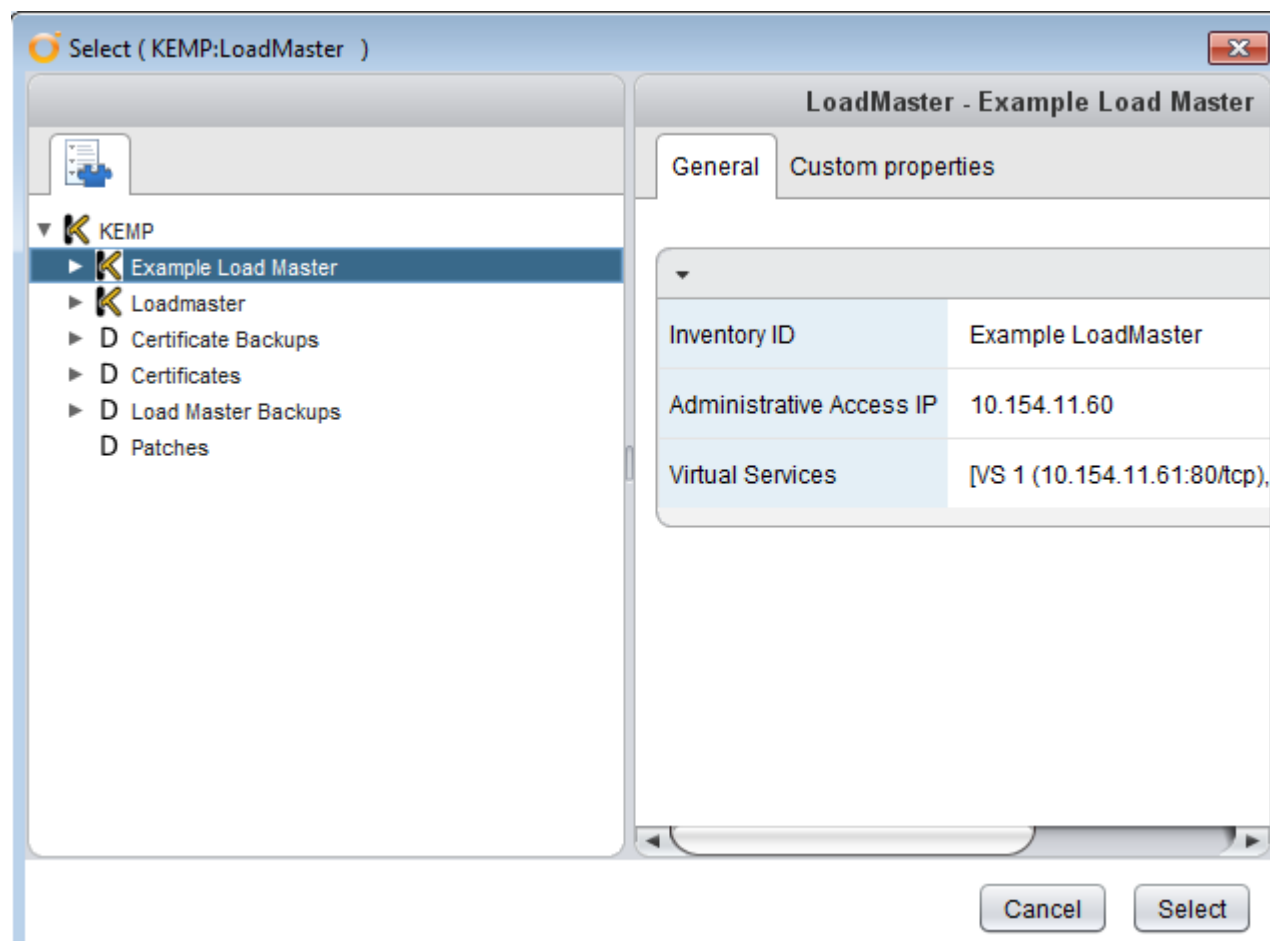
Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to disable the API of

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to disable the API of** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Disable API

Common Parameters

* Enter the username for the LoadMaster
bal

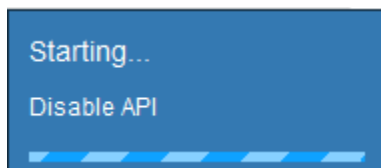
* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)
Not set

* Select the LoadMaster to disable the API of
Example Load Master

Cancel Submit

1. Click **Submit**.



1. Wait for the API to be disabled.

Enable API

Enable API

The API interface of a LoadMaster which exists in Orchestrator can be enabled via Orchestrator. The API interface needs to be enabled on a LoadMaster for most of the workflows to run. To enable the API, run the **Enable API** command.

Start Workflow : Enable API

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

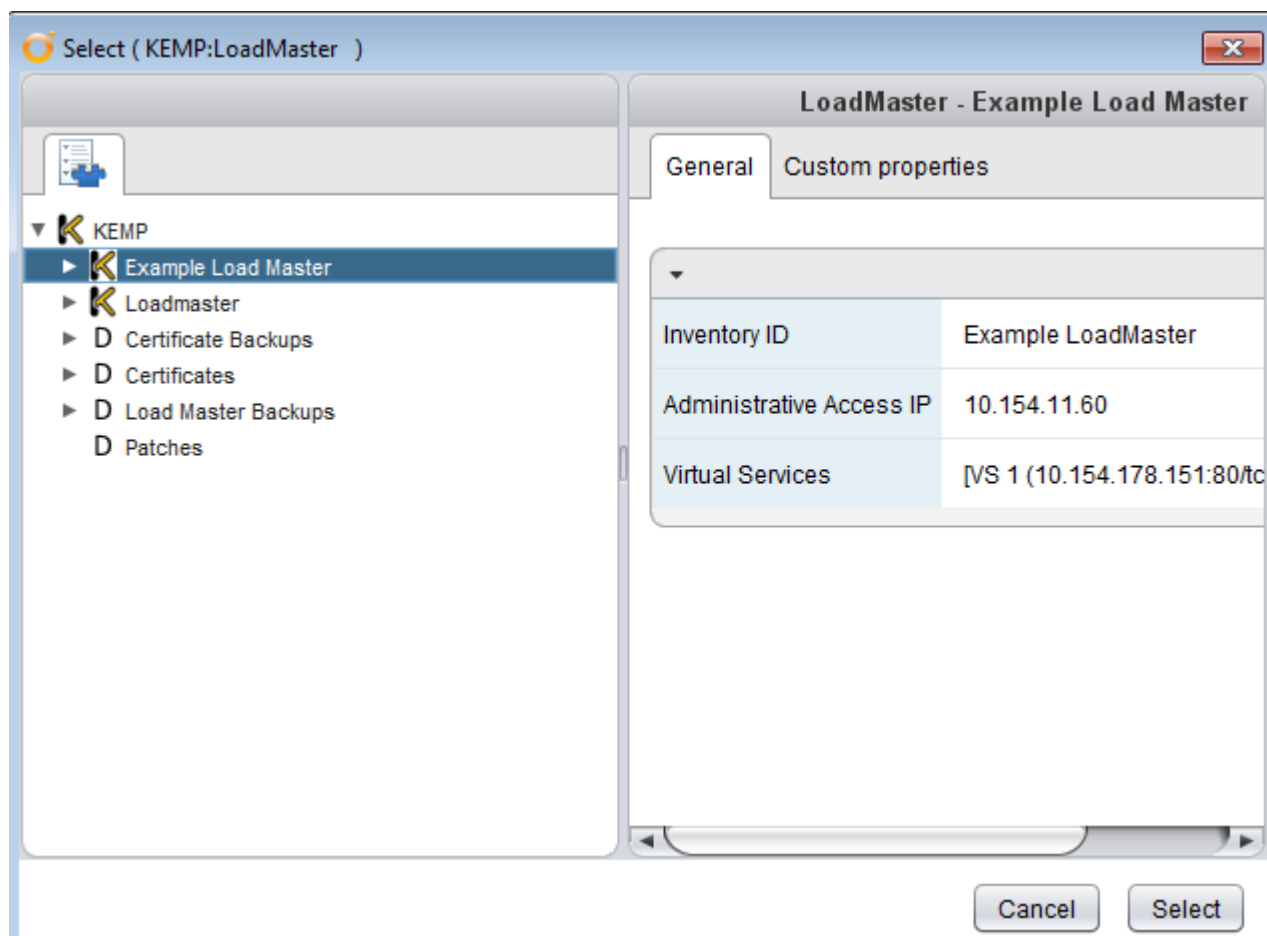
Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to enable the API of

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to enable the API of** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Enable API

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to enable the API of

Example Load Master

Cancel Submit

1. Click **Submit**.

Get Parameter

Get Parameter

The **Get Parameter** workflow can be used to retrieve a number of LoadMaster field values. For a list of parameter names that can be retrieved, refer to [Appendix A - Get and Set Parameters](#).

Start Workflow : Get Parameter

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

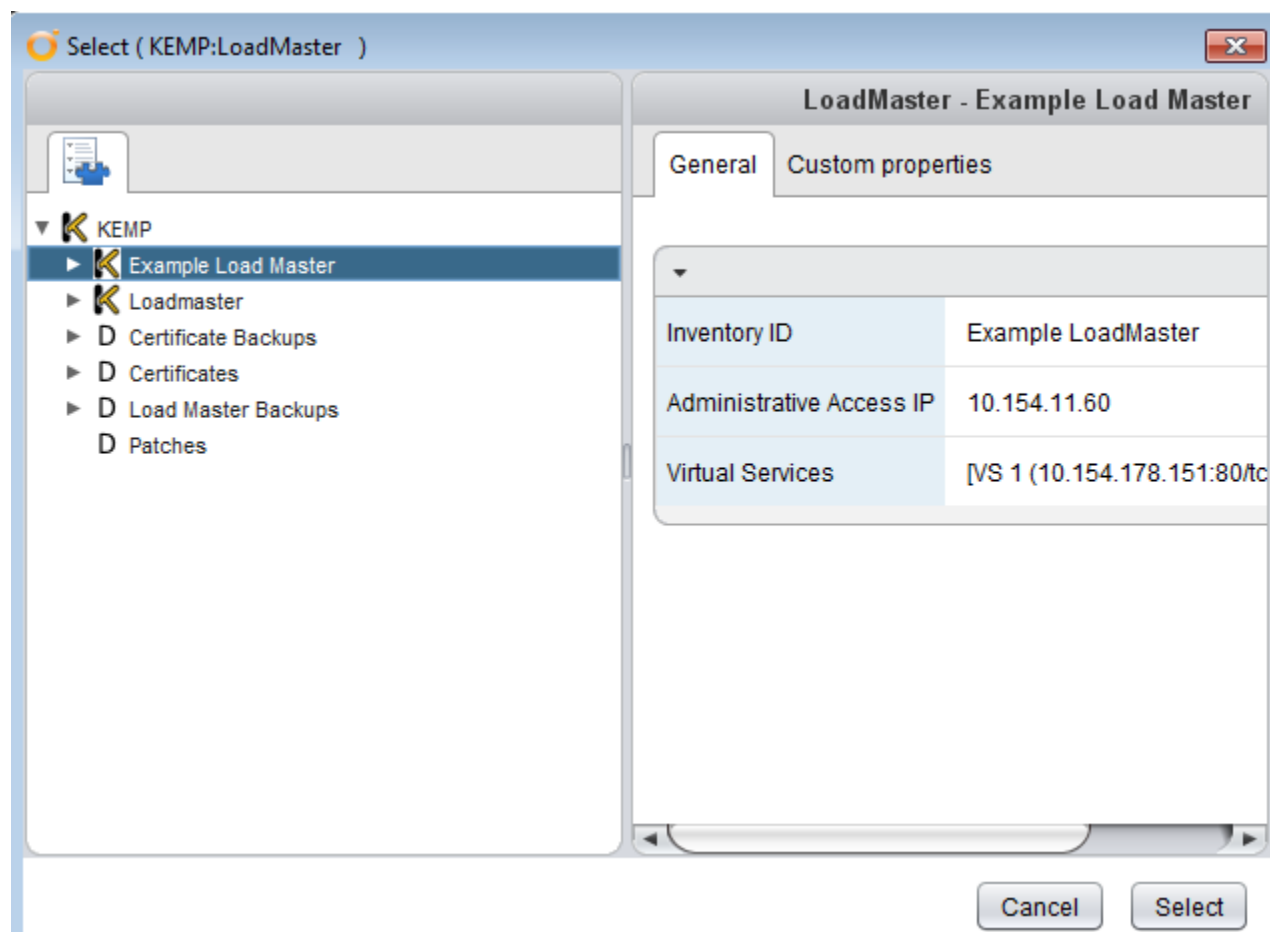
Not set

* Select the LoadMaster to be queried

Not set

* Enter the name of the parameter to be read

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to be queried** field.



1. Expand the **Kemp** directory.
2. Select the LoadMaster to retrieve the value from.
3. Click **Select**.

Start Workflow : Get Parameter

Common Parameters

* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

* Select the LoadMaster to be queried

* Enter the name of the parameter to be read

Cancel Submit

1. Enter the relevant parameter name in the **Enter the name of the parameter to be read** field.
2. Click **Submit**.

General Variables Logs		
Name	Type	Value
username	string	bal
password	SecureString	
certFile	KEMP:LoadMasterFile	Not set
loadMaster	KEMP:LoadMaster	Example Load Master
paramName	string	motd
paramValue	string	Example Message of the Day

1. To view the value, select the **Variables** tab at the bottom.
2. The parameters and their values will be displayed.

Install Patch

Install Patch

The LoadMaster firmware can be updated with a firmware patch file via Orchestrator. Before uploading the firmware patch file to the LoadMaster, first it must be uploaded to Orchestrator. For step-by-step instructions on how to upload a file, refer to the [Upload Files](#) section.

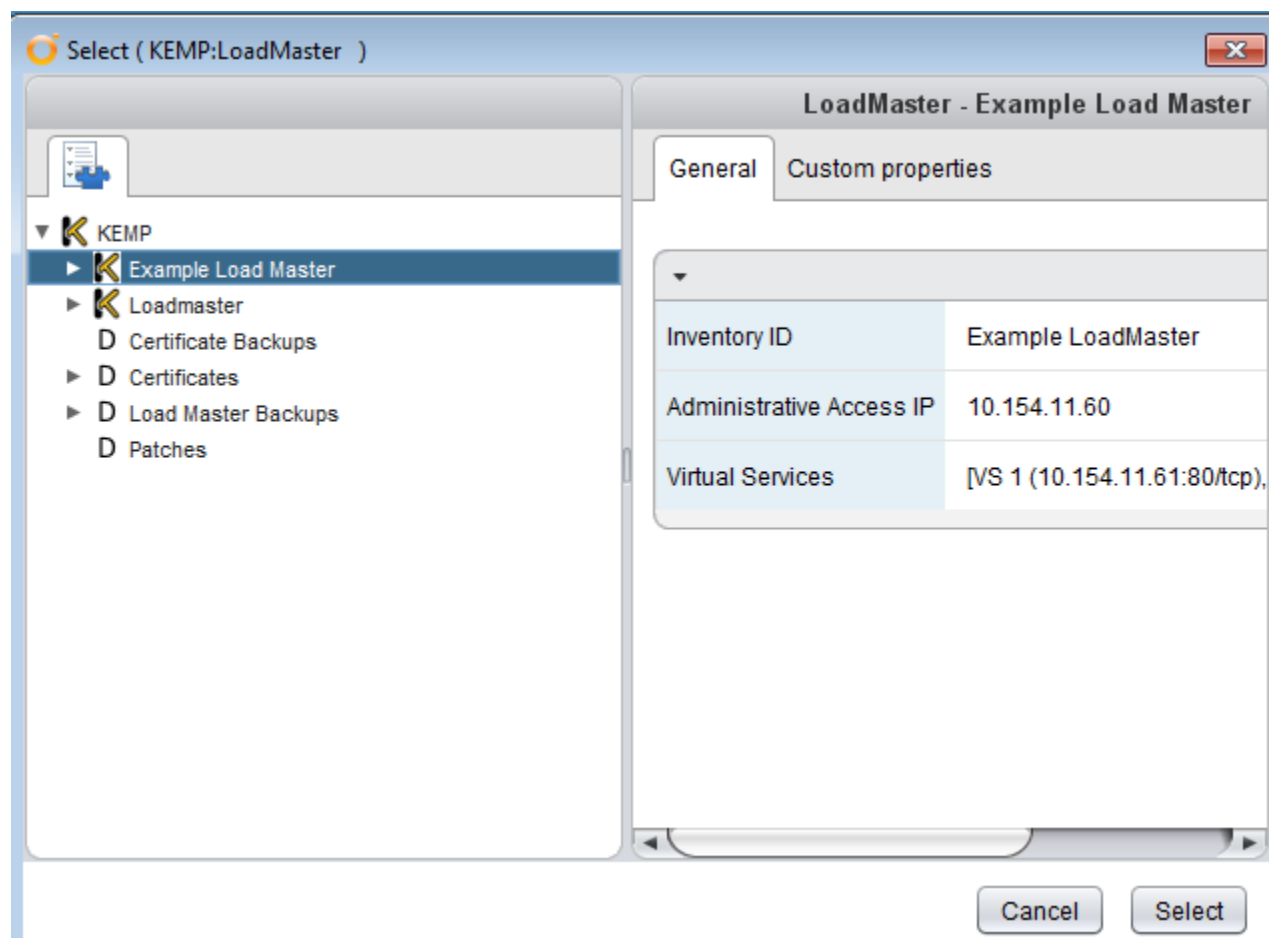
After a firmware patch file has been uploaded to Orchestrator, run the **Install Patch** workflow to update the LoadMaster.

Start Workflow : Install Patch

Common Parameters

- * Enter the username for the LoadMaster
- * Enter the password for the LoadMaster
- Specify the SSL certificate provided by the LoadMaster (optional)
- * Select the LoadMaster to be patched
- * Select the patch to apply
- Reboot the LoadMaster after the patch is applied?
☐ Yes ☒ No

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to be patched** field.



1. Expand the **Kemp** directory.
2. Select the LoadMaster to be patched.
3. Click **Select**.

Start Workflow : Install Patch

Common Parameters

* Enter the username for the LoadMaster
bal

* Enter the password for the LoadMaster

Specify the SSL certificate provided by the LoadMaster (optional)
Not set

* Select the LoadMaster to be patched
i Example Load Master

* Select the patch to apply
Not set

Reboot the LoadMaster after the patch is applied?
☐ Yes ☒ No

1. Click **Not set** in the **Select the patch to apply** field.
2. Expand the **Kemp** directory.
3. Expand the **Patches** directory.
4. Select the relevant patch file.
5. Click **Select**.
6. Select **Yes** to reboot the LoadMaster after the patch has been uploaded.

Note: The LoadMaster must be rebooted after the patch file has been installed in order for the changes to be applied correctly.

1. Click **Submit**.
2. Wait for the installation and reboot to complete.

Reboot LoadMaster

Reboot LoadMaster

A LoadMaster which exists in Orchestrator can be rebooted via Orchestrator. To reboot a LoadMaster, run the **Reboot LoadMaster** workflow.

Start Workflow : Reboot LoadMaster

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to be rebooted

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to be rebooted** field.

Select (KEMP:LoadMaster)

LoadMaster - Example Load Master

General Custom properties

Inventory ID	Example LoadMaster
Administrative Access IP	10.154.11.60
Virtual Services	[VS 1 (10.154.178.151:80/tc

Cancel Select

1. Select the relevant LoadMaster to be rebooted.
2. Click **Select**.

The screenshot shows a dialog box titled "Start Workflow : Reboot LoadMaster". It has a "Common Parameters" tab. The parameters are:

- * Enter the username for the LoadMaster: A text box containing "bal".
- * Enter the password for the LoadMaster: A password box containing "*****".
- Select the SSL certificate provided by the LoadMaster (optional): A dropdown menu showing "Not set".
- * Select the LoadMaster to be rebooted: A dropdown menu showing "Example Load Master" with a close button (X) on the right.

At the bottom right, there are "Cancel" and "Submit" buttons.

1. Click **Submit**.
2. Wait for the LoadMaster to reboot.

Remove LoadMaster

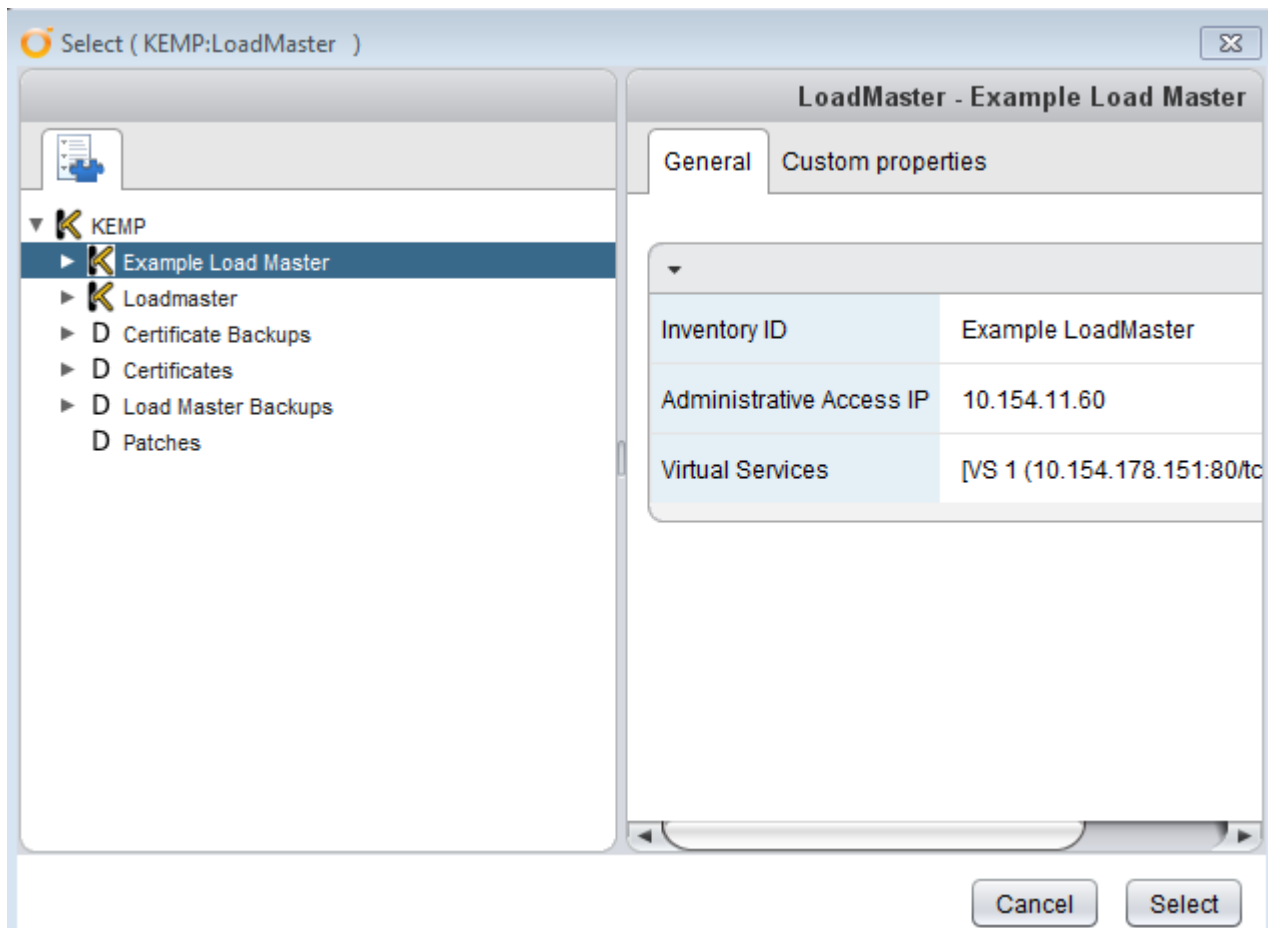
Remove LoadMaster

A LoadMaster can be removed from Orchestrator by running the **Remove LoadMaster** command.

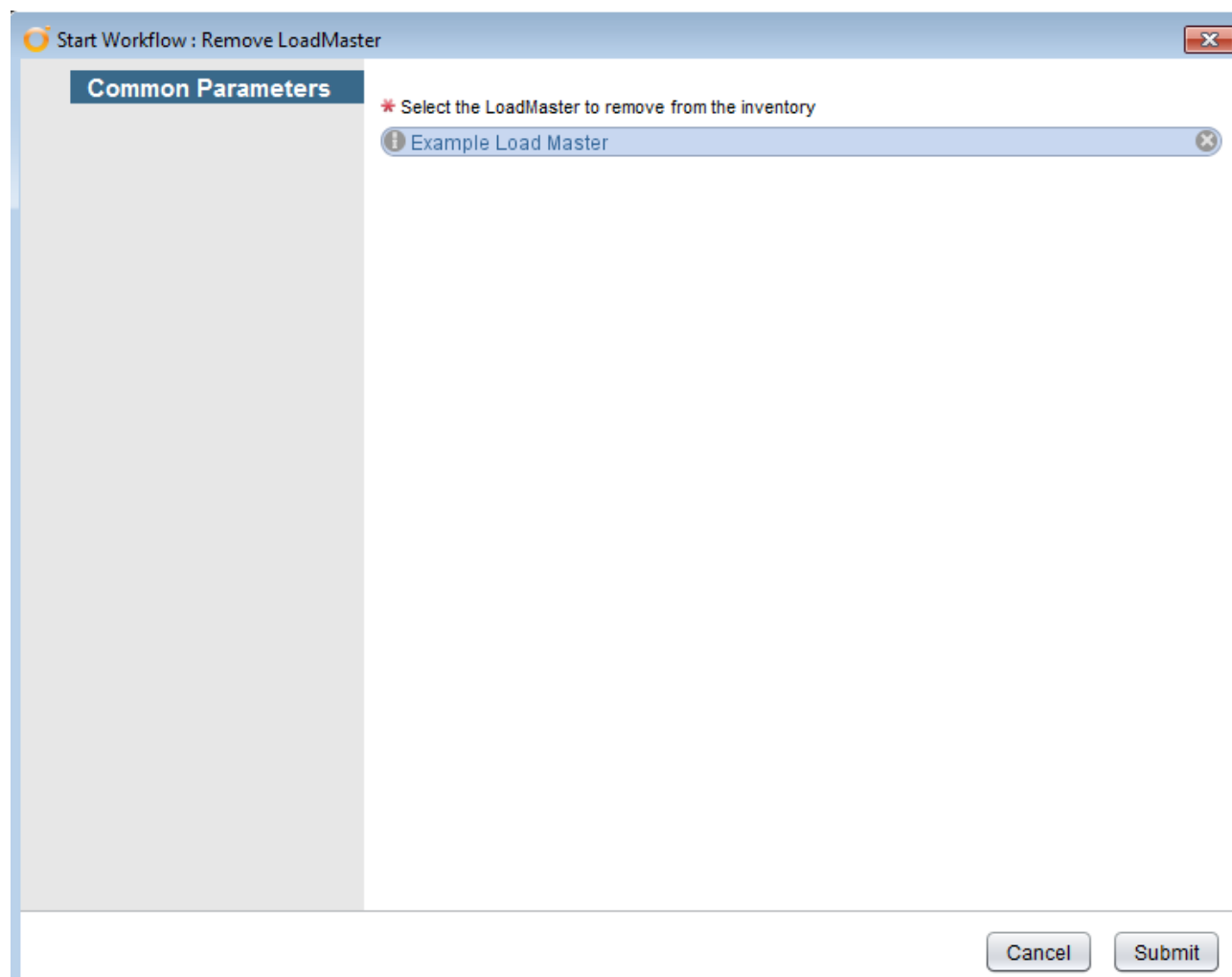
The screenshot shows a dialog box titled "Start Workflow : Remove LoadMaster". It has a "Common Parameters" tab. The parameters are:

- * Select the LoadMaster to remove from the inventory: A dropdown menu showing "Not set".

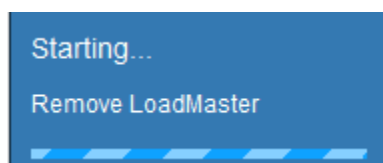
1. Click **Not set**.



1. Select the relevant LoadMaster.
2. Click **Select**.



1. Click **Submit**.



1. Wait for the LoadMaster to be removed.

Restore Certificates

Restore Certificates

If a certificate backup file exists in Orchestrator, it can be restored to a LoadMaster. To back up the certificates on a LoadMaster, refer to the [Backup Certificates](#) section. To restore the certificates, run the **Restore Certificates** command.

Start Workflow : Restore Certificates

1 Authentication

2 Backup Options

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to restore

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set**.

Select (KEMP:LoadMaster)

KEMP

- Example Load Master
- Loadmaster
- D Certificate Backups
- D Certificates
- D Load Master Backups
- D Patches

LoadMaster - Example Load Master

General Custom properties

Inventory ID	Example LoadMaster
Administrative Access IP	10.154.11.60
Virtual Services	[VS 1 (10.154.178.151:80/tc

Cancel Select

1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Restore Certificates

1 Authentication

2 Backup Options

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the LoadMaster to restore

Example Load Master

1. Click **Backup Options**.

Start Workflow : Restore Certificates

✓ **1 Authentication**

2 Backup Options

* Select the certificate backup to be restored

Not set

* Enter the passphrase used to secure the backup file

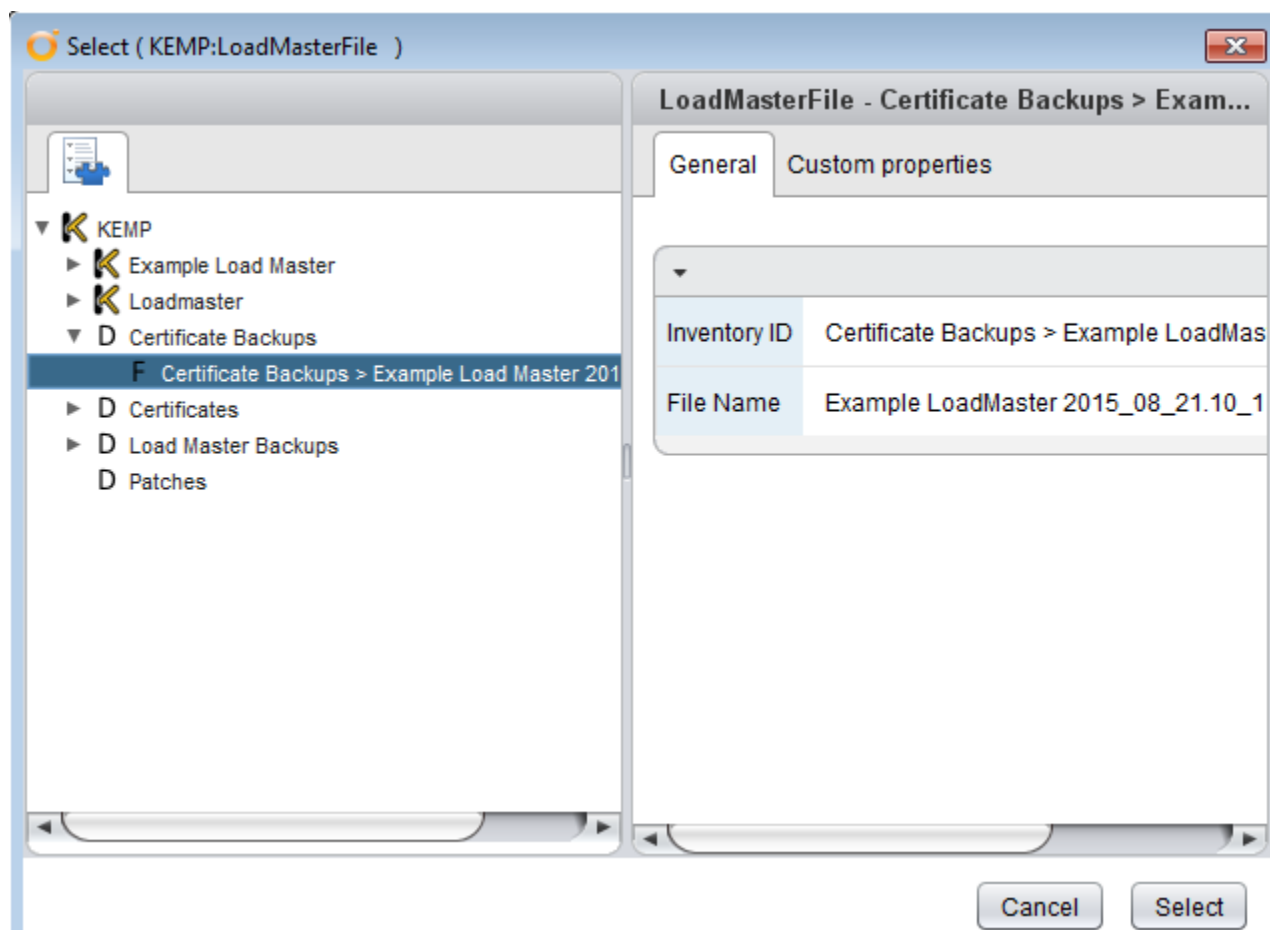
Restore Virtual Service certificates?

☐ Yes ☒ No

Restore intermediate certificates?

☐ Yes ☒ No

1. Click **Not set**.



1. Expand the **Kemp** directory.
2. Expand the **Certificate Backups** directory.
3. Select the relevant backup.
4. Click **Select**.

Start Workflow : Restore Certificates

✓ 1 Authentication

2 Backup Options

* Select the certificate backup to be restored

Certificate Backups > Example Load Master 2015 08 21 10 11

* Enter the passphrase used to secure the backup file

Restore Virtual Service certificates?

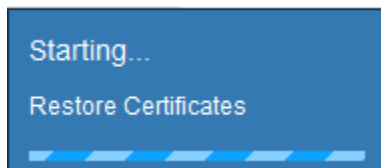
☒ Yes ☐ No

Restore intermediate certificates?

☒ Yes ☐ No

Cancel Back Next Submit

1. Enter the passphrase used to secure the backup file.
2. Specify which certificates to restore.
3. Click **Submit**.



1. Wait for the certificates to restore.

Restore LoadMaster

Restore LoadMaster

Before restoring a LoadMaster configuration, a backup configuration must be available in Orchestrator. To back up a LoadMaster configuration in Orchestrator, refer to the [Backup LoadMaster](#) section.

When a backup configuration exists in Orchestrator, run the **Restore LoadMaster** workflow to restore the configuration.

Note: A GEO LoadMaster backup configuration cannot be restored on a non-GEO LoadMaster configuration

Start Workflow : Restore LoadMaster

1 Authentication

2 Backup Options

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

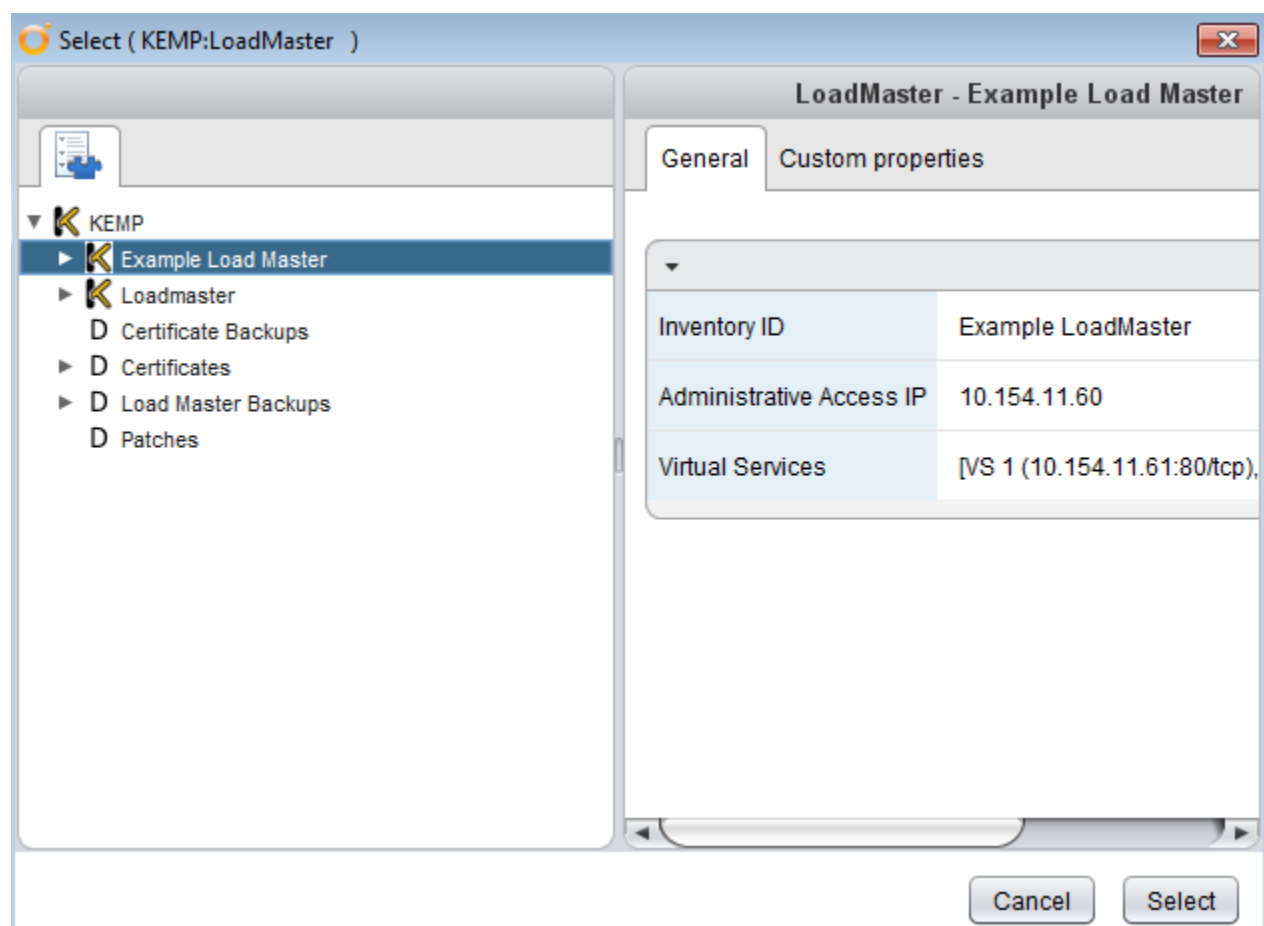
Specify the SSL certificate provided by the LoadMaster (optional)

Not set

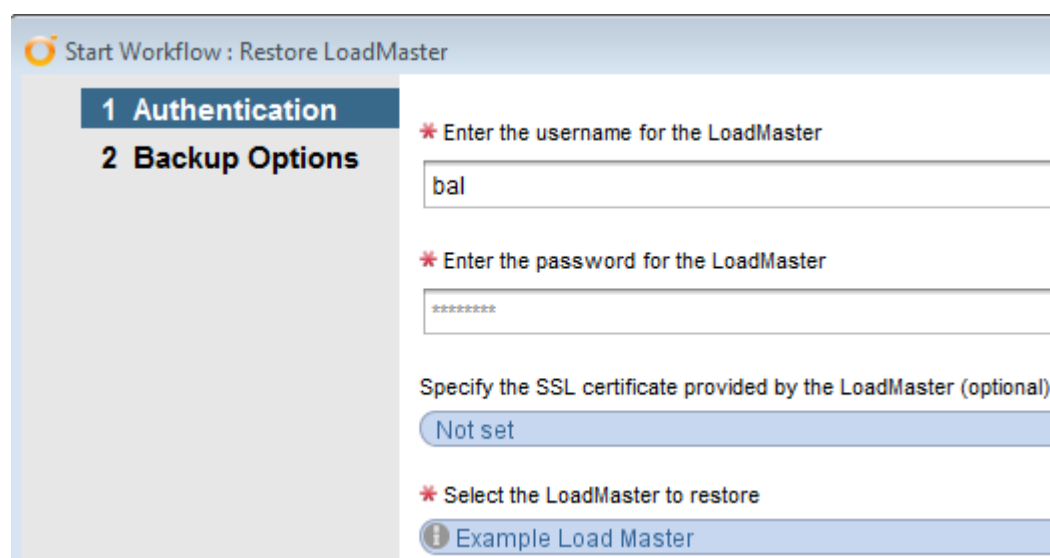
* Select the LoadMaster to restore

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to restore** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.



1. Click **Backup Options**.

Start Workflow : Restore LoadMaster

✓ 1 Authentication

2 Backup Options

* Select the backup configuration to be restored

Not set

Restore the base LoadMaster configuration?

☐ Yes ☒ No

Restore the Virtual Service configuration?

☐ Yes ☒ No

Restore the GEO configuration?

☐ Yes ☒ No

1. Click **Not set**.

Select (KEMP:LoadMasterFile)

LoadMasterFile - Load Master Backups > Loa...

General Custom properties

Inventory ID	LoadMaster Backups > Loadmaster 2015 08 20
File Name	Loadmaster 2015_08_20.15_29

Cancel Select

1. Expand the **Kemp** directory.

2. Expand the **LoadMaster Backups** directory.
3. Select the relevant backup.
4. Click **Select**.

Start Workflow : Restore LoadMaster

✓ 1 Authentication

2 Backup Options

* Select the backup configuration to be restored

Load Master Backups > Loadmaster 2015 08 20 15 29

Restore the base LoadMaster configuration?

☒ Yes ☐ No

Restore the Virtual Service configuration?

☒ Yes ☐ No

Restore the GEO configuration?

☐ Yes ☒ No

Reboot the LoadMaster after restoration?

☒ Yes ☐ No

Cancel Back Next Submit

1. Specify the configurations to be restored by selecting **Yes** for the relevant options.
2. If restoring the base LoadMaster configuration, another field will appear asking if the LoadMaster should be rebooted after restoration. If restoring the base configuration, please set this to **Yes** as the LoadMaster needs to be rebooted for the changes to be applied.
3. Click **Submit**.
4. Wait for the restoration to complete.

Set Credentials

Set Credentials

When a LoadMaster is added to Orchestrator via the **Add LoadMaster** command, the credentials are set. If, for any reason, the LoadMaster credentials which are saved in Orchestrator need to be updated (for example if the credentials have changed), the **Set Credentials** workflow can be run.

Start Workflow : Set Credentials

Common Parameters

- * Select the LoadMaster to set the credentials of
Not set
- * Enter the username for the LoadMaster
- * Enter the password for the LoadMaster
- Select the SSL certificate provided by the LoadMaster (optional)
Not set

1. Click **Not set** in the **Select the LoadMaster to set the credentials of** field.

Select (KEMP:LoadMaster)

LoadMaster - Example Load Master

General Custom properties

Inventory ID	Example LoadMaster
Administrative Access IP	10.154.11.60
Virtual Services	[VS 1 (10.154.178.151:80/tc

Cancel Select

1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.

3. Click **Select**.

Start Workflow : Set Credentials

Common Parameters

* Select the LoadMaster to set the credentials of
Example Load Master

* Enter the username for the LoadMaster
bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)
Not set

Cancel Submit

1. Enter the updated LoadMaster credentials.
2. Click **Submit**.

Set Parameter

Set Parameter

The **Set Parameter** workflow can be used to set a number of LoadMaster field values. For a list of parameter names that can be set, refer to [Appendix A - Get and Set Parameters](#).

Start Workflow : Set Parameter

1 Authentication

2 Parameter Configuration

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

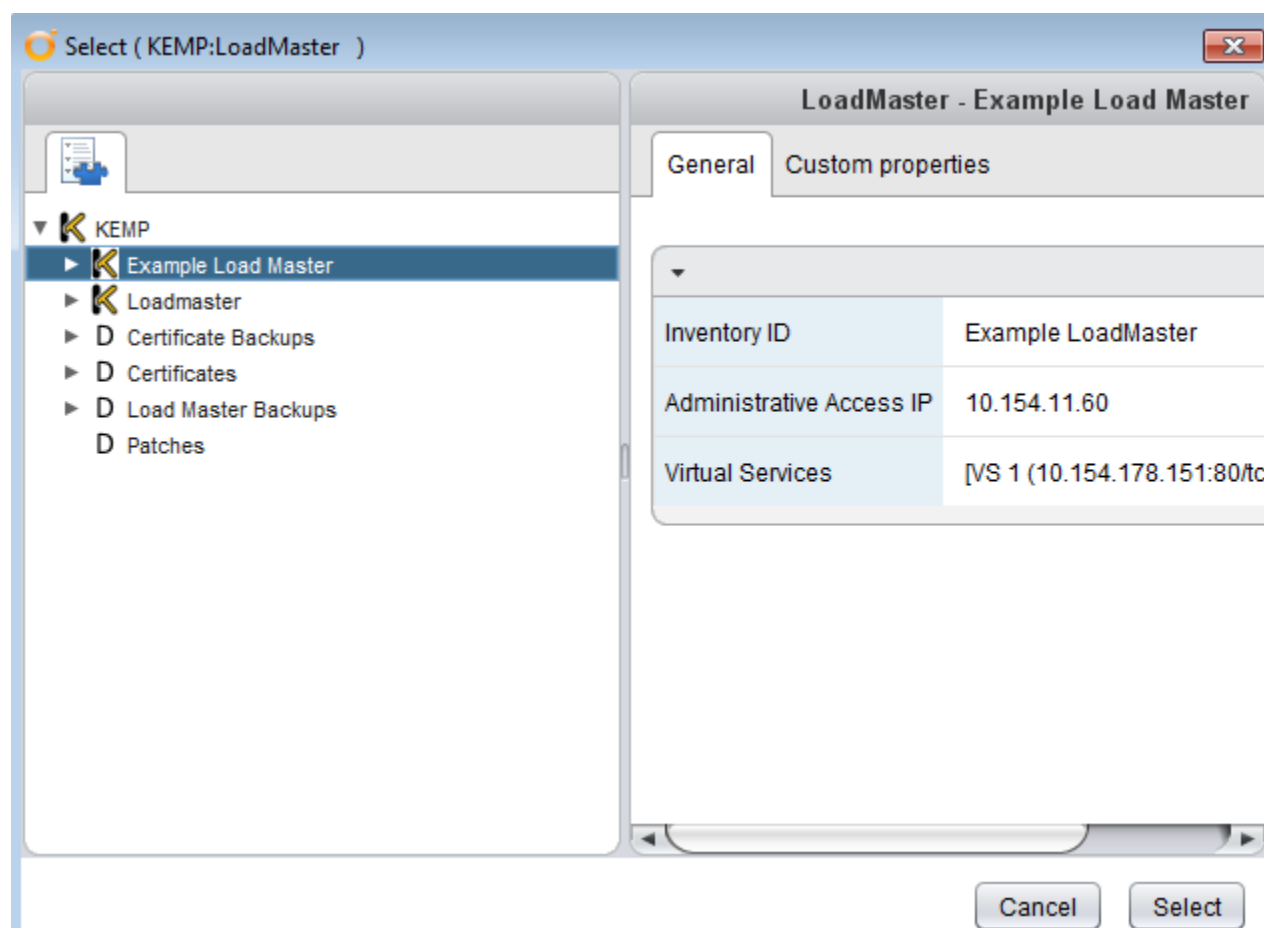
Select the SSL certificate provided by the LoadMaster (optional)

Not set

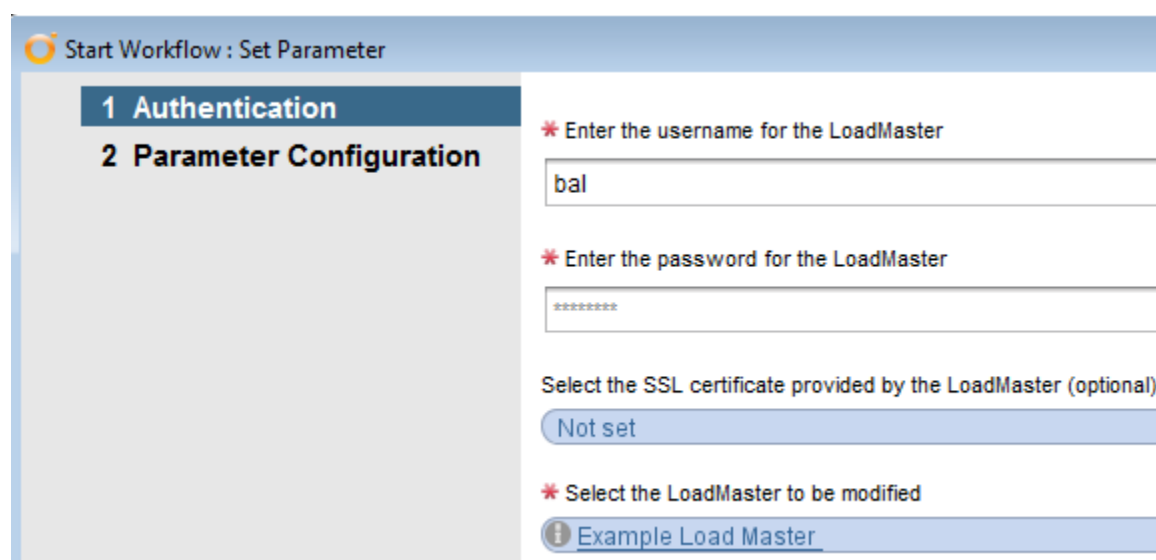
* Select the LoadMaster to be modified

Not set

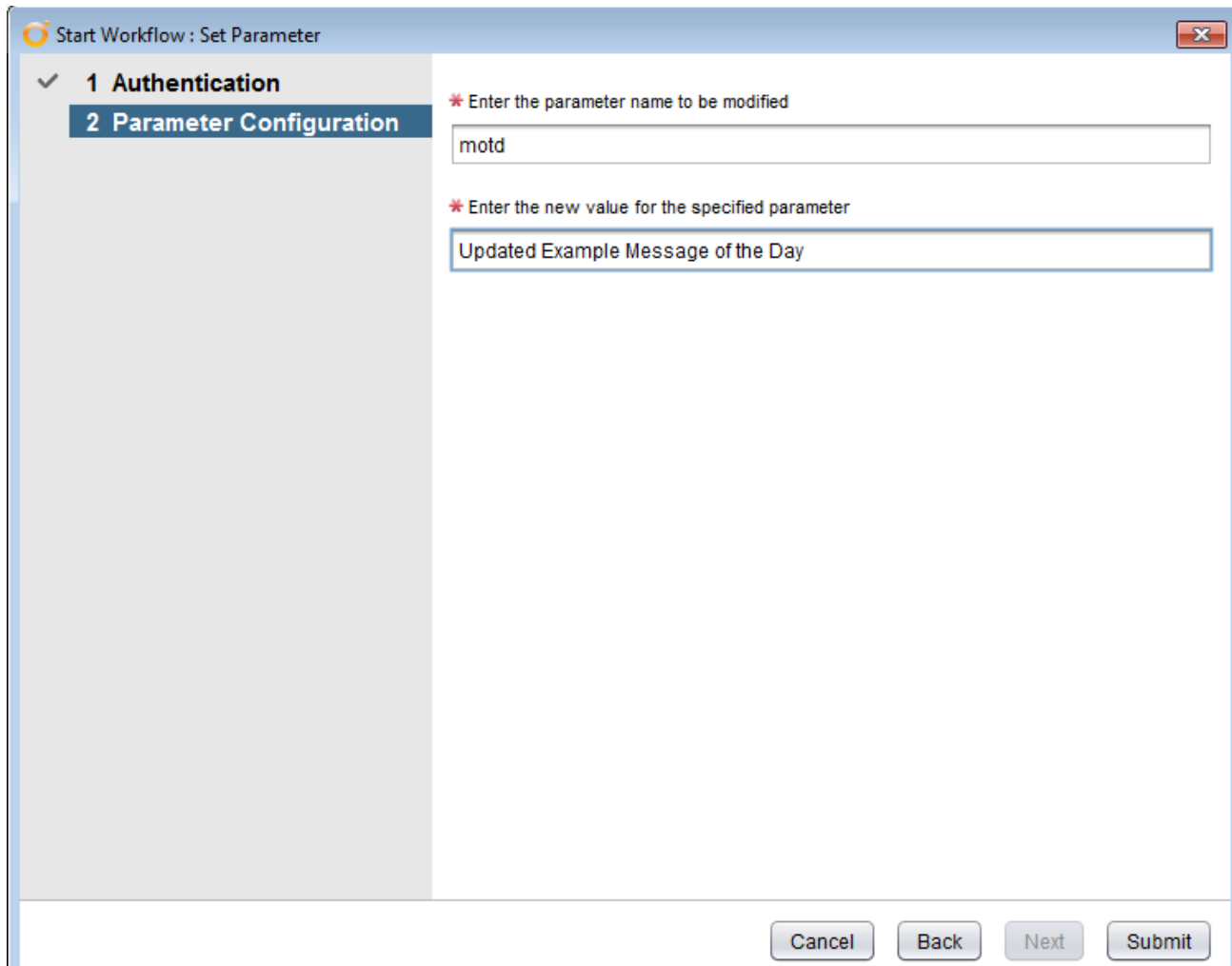
1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the LoadMaster to be modified** field.



1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.



1. Click **Parameter Configuration**.



Start Workflow : Set Parameter

✓ 1 Authentication

2 Parameter Configuration

* Enter the parameter name to be modified

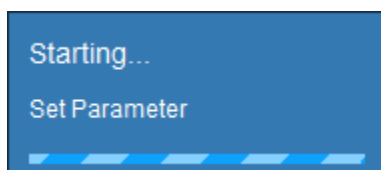
motd

* Enter the new value for the specified parameter

Updated Example Message of the Day

Cancel Back Next Submit

1. Enter the name of the parameter to be modified.
2. Enter the new value for the specified parameter.
3. Click **Submit**.



1. Wait for the parameter to be set.

Virtual Services

Virtual Services

A number of tasks can be performed in relation to Virtual Services, such as adding and removing them. Refer to the sections below for further details.

Related Links

- [Add Virtual Service](#)
- [Assign Virtual Service Certificates](#)
- [Modify Virtual Service Name](#)
- [Remove Virtual Service](#)

Add Virtual Service

Add Virtual Service

A Virtual Service can be added to a LoadMaster via Orchestrator by running the **Add Virtual Service** command.

Start Workflow : Add Virtual Service

1 Authentication

2 Virtual Service Configur...

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Virtual Service Configuration**.

Start Workflow : Add Virtual Service

✓ 1 Authentication

2 Virtual Service Configur...

* Select the LoadMaster to add the Virtual Service to
Not set

* Enter the IP address of the Virtual Service

* Enter the port of the Virtual Service

* Select the protocol of the Virtual Service
TCP

1. Click **Not set**.

Select (KEMP:LoadMaster)

LoadMaster - Example Load Master

General Custom properties

Inventory ID	Example LoadMaster
Administrative Access IP	10.154.11.60
Virtual Services	[VS 1 (10.154.178.151:80/tc

Cancel Select

1. Expand the **Kemp** directory.
2. Select the relevant LoadMaster.
3. Click **Select**.

Start Workflow : Add Virtual Service

✓ 1 Authentication

2 Virtual Service Configur...

* Select the LoadMaster to add the Virtual Service to

Example Load Master

* Enter the IP address of the Virtual Service

10.154.11.61

* Enter the port of the Virtual Service

80

* Select the protocol of the Virtual Service

TCP


Cancel Back Next Submit

1. Enter a valid IP address in the Enter the IP address of the Virtual Service text box.
2. Enter the desired port in the **Enter the port of the Virtual Service** text box.
3. Select the relevant protocol from the drop-down list.
4. Click **Submit**.

Assign Virtual Service Certificates

Assign Virtual Service Certificates

Certificates can be assigned to a Virtual Service via Orchestrator. To do this, run the **Assign Virtual Service Certificates** command.

 Start Workflow : Assign Virtual Service Certificates

Common Parameters

* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

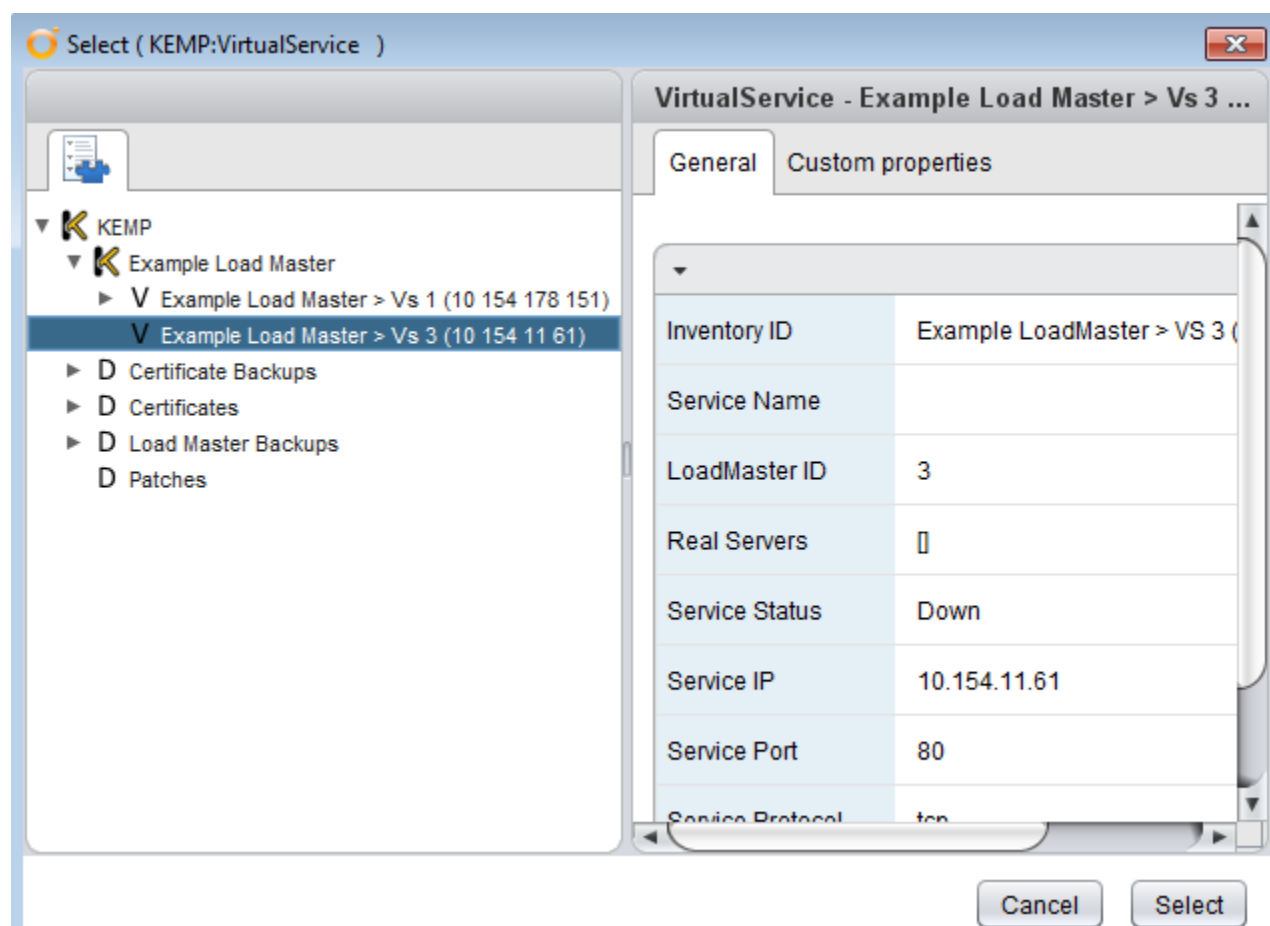
* Select the Virtual Service to assign certificates to

Not set


Enter the certificate identifiers to assign to the Virtual Service

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the Select the **Virtual Service to assign certificates to** field.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant Virtual Service.
4. Click **Select**.

 Start Workflow : Assign Virtual Service Certificates

Common Parameters

* Enter the username for the LoadMaster


* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

* Select the Virtual Service to assign certificates to

Enter the certificate identifiers to assign to the Virtual Service

1. Click **Not set** in the **Enter the certificate identifiers to assign to the Virtual Service** field.

 Array of string ✕

New value :

✕ ↑ ↓

Example Certificate

1. In the **New value** text box, enter the certificate identifier (friendly name) of the certificate to be assigned.
2. Click **Insert value**.
3. Click **Accept**.

Start Workflow : Assign Virtual Service Certificates

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the Virtual Service to assign certificates to

Example Load Master > Vs 3 (10 154 11 61)

Enter the certificate identifiers to assign to the Virtual Service

Array [Example Certificate]

Cancel Submit

1. Click **Submit**.

Modify Virtual Service Name

Modify Virtual Service Name

The name of a Virtual Service can be modified using the **Modify Virtual Service Name** workflow.

Start Workflow : Modify Virtual Service Name

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

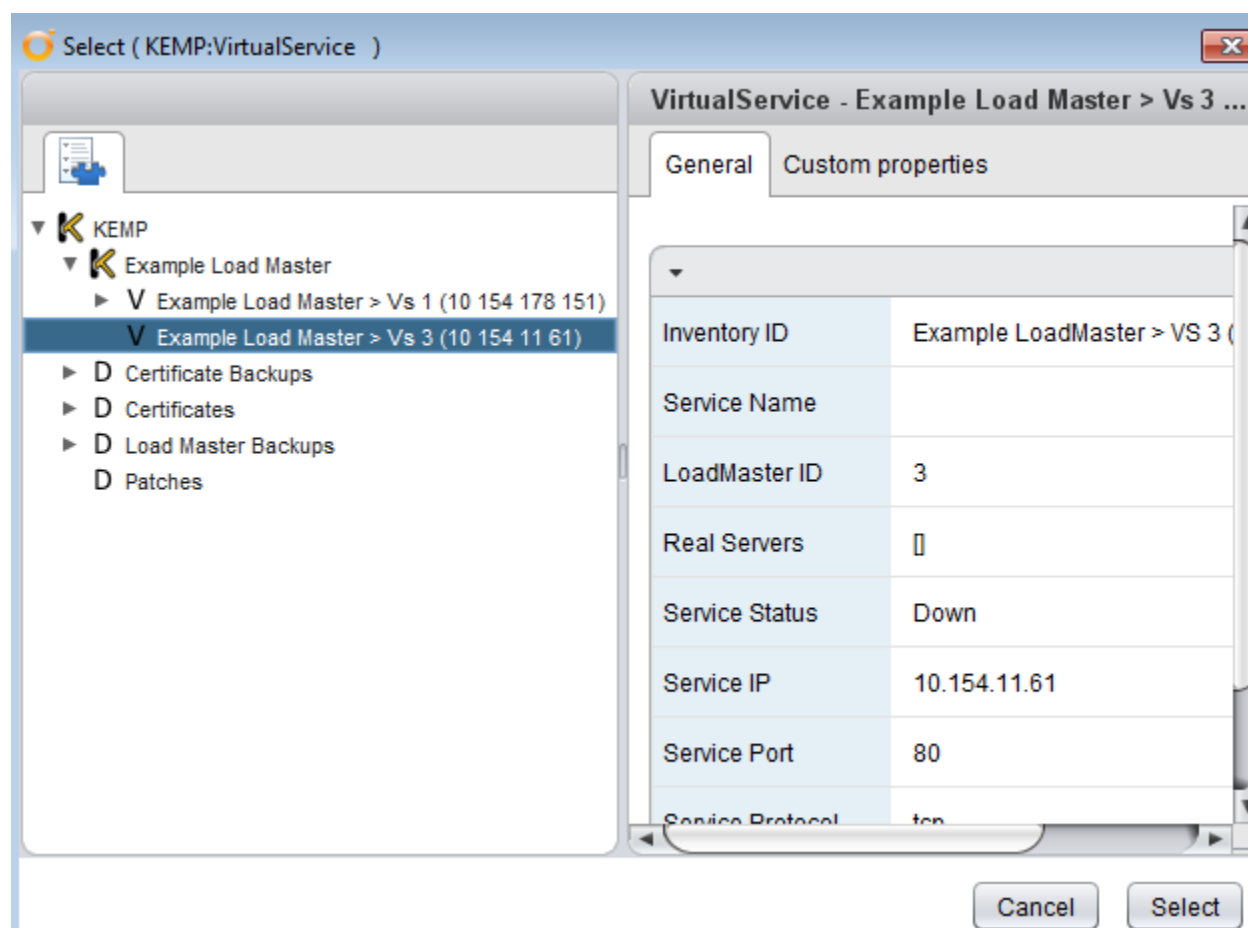
Not set

* Select the Virtual Service to be renamed

Not set

Enter the new name for the Virtual Service

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the Virtual Service to be renamed** field.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant Virtual Service.
4. Click **Select**.

Start Workflow : Modify Virtual Service Name

Common Parameters

* Enter the username for the LoadMaster
bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)
Not set

* Select the Virtual Service to be renamed
Example Load Master > Vs 3 (10 154 11 61)

Enter the new name for the Virtual Service
Example Service Name

Cancel Submit

1. Enter the new name for the Virtual Service.
2. Click **Submit**.

Remove Virtual Service

Remove Virtual Service

A Virtual Service can be deleted via Orchestrator by running the **Remove Virtual Service** workflow.

Start Workflow : Remove Virtual Service

Common Parameters

* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

* Select the Virtual Service to be removed

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the Virtual Service to be removed** field.

Select (KEMP:VirtualService)

VirtualService - Example Load Master > Vs 3 ...

General Custom properties

Inventory ID	Example LoadMaster > VS 3 (
Service Name	
LoadMaster ID	3
Real Servers	[]
Service Status	Down
Service IP	10.154.11.61
Service Port	80
Service Protocol	ten

Cancel Select

1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant Virtual Service.
4. Click **Select**.

Start Workflow : Remove Virtual Service

Common Parameters

* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

* Select the Virtual Service to be removed

1. Click **Submit**.

Sub Virtual Services

Sub Virtual Services

A number of tasks can be performed in relation to SubVSes, such as adding and removing a SubVS. Refer to the sections below for further details.

Related Links

- [Add SubVS](#)

- [Modify SubVS Name](#)
- [Remove SubVS](#)

Add SubVS

Add SubVS

A SubVS can be added by running the **Add SubVS** workflow.

Start Workflow : Add SubVS

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

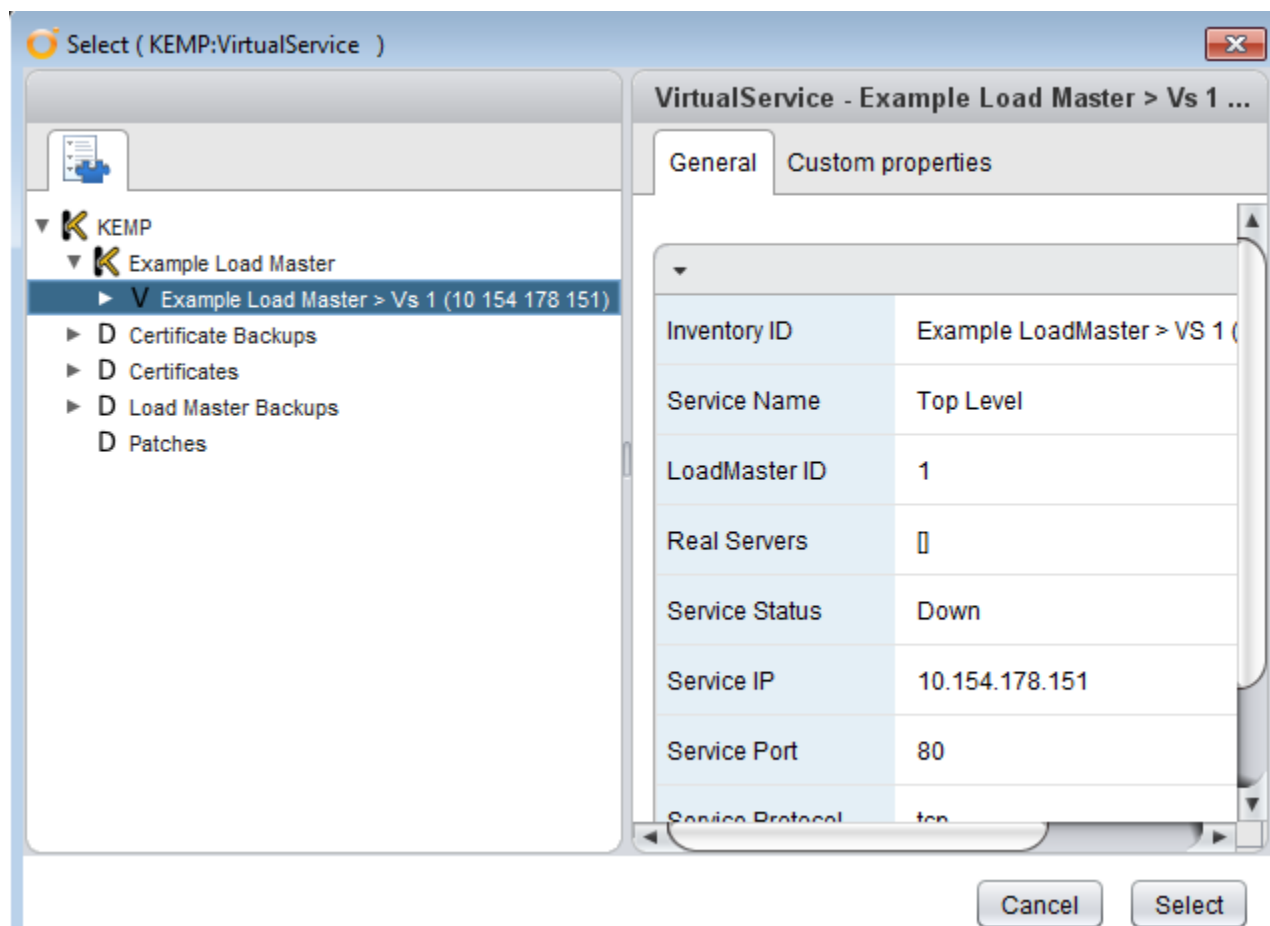
Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the Virtual Service to add a SubVS to

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the Virtual Service to add a SubVS to** field.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant Virtual Service.
4. Click **Select**.

Start Workflow : Add SubVS

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the Virtual Service to add a SubVS to

Example Load Master > Vs 1 (10 154 178 151)

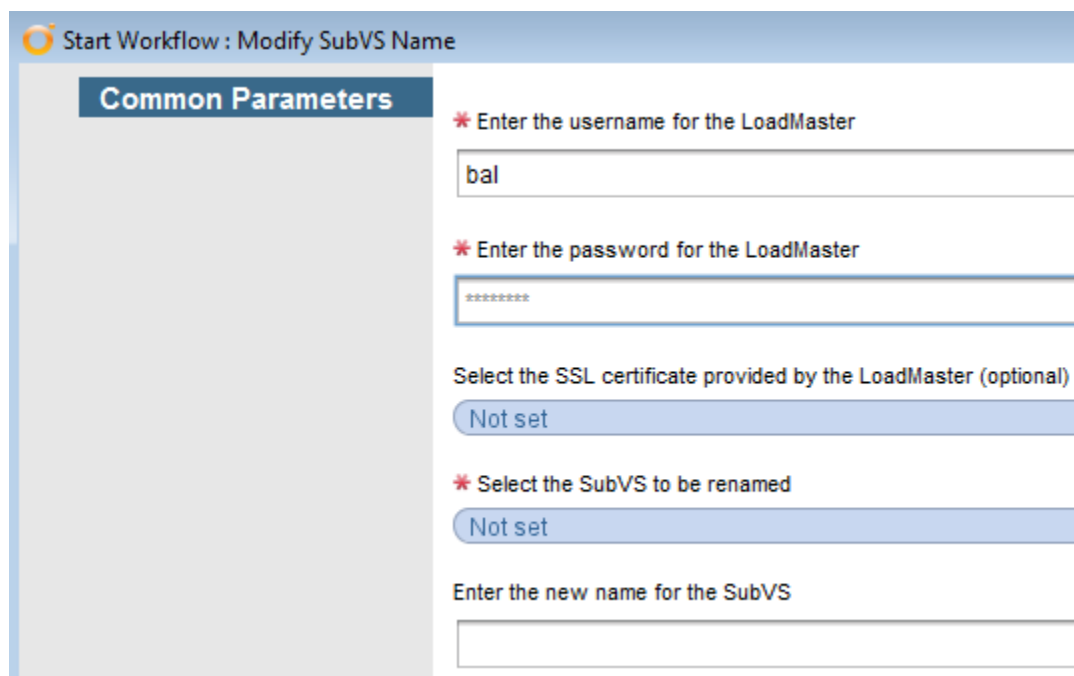
Cancel Submit

1. Click **Submit**.

Modify SubVS Name

Modify SubVS Name

The name of a SubVS can be modified using the **Modify SubVS Name** workflow.



Start Workflow : Modify SubVS Name

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

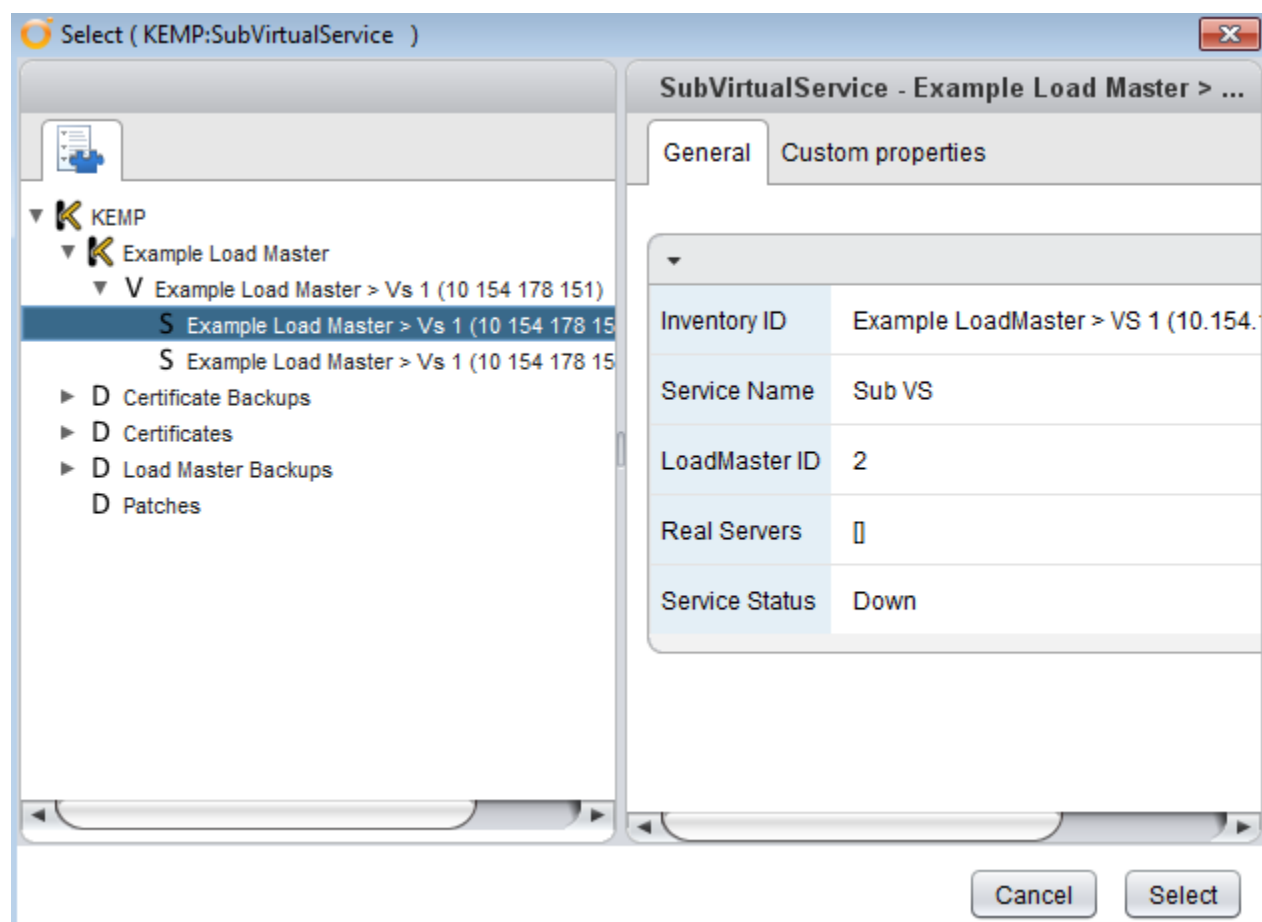
Not set

* Select the SubVS to be renamed

Not set

Enter the new name for the SubVS

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the SubVS to be renamed** field.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant SubVS.
4. Click **Select**.

Start Workflow : Modify SubVS Name

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the SubVS to be renamed

Example Load Master > Vs 1 (10 154 178 151) > Sub Vs 2

Enter the new name for the SubVS

Example SubVS Name

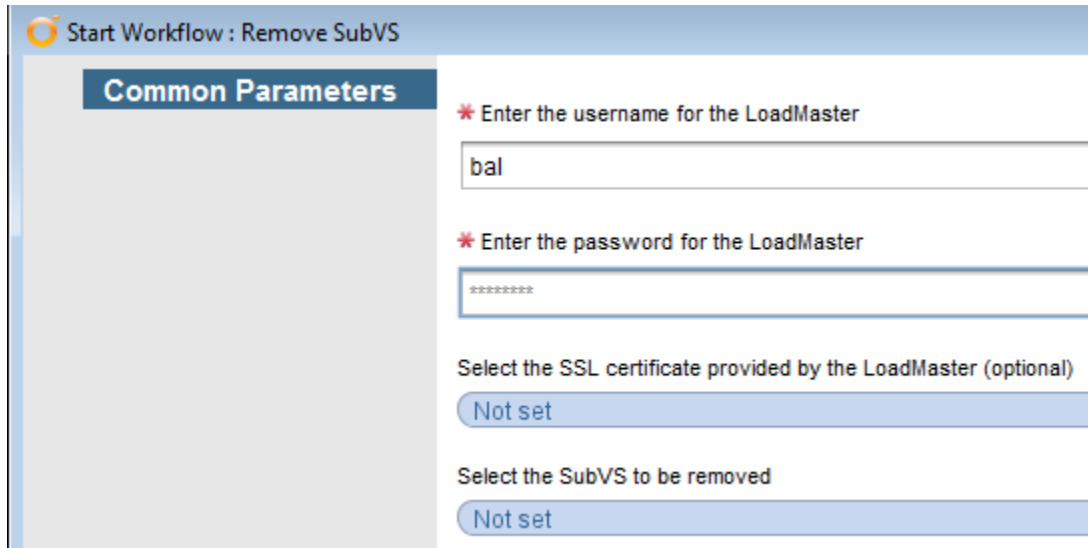
Cancel Submit

1. Enter the new name for the SubVS.
2. Click **Submit**.

Remove SubVS

Remove SubVS

A SubVS can be deleted via Orchestrator by running the **Remove SubVS** command.



Start Workflow : Remove SubVS

Common Parameters

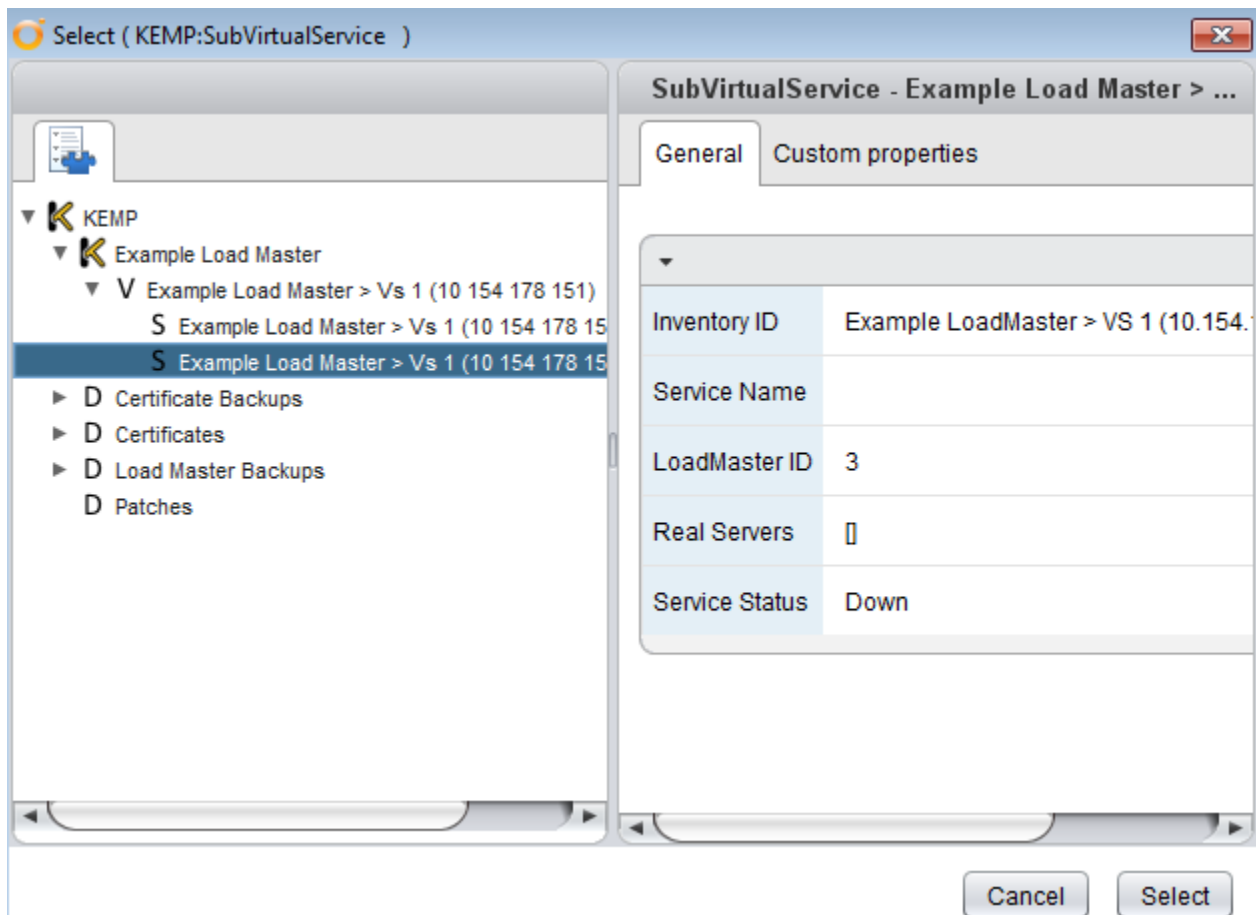
* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Select the SubVS to be removed

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the SubVS to be removed** field.



Select (KEMP:SubVirtualService)

SubVirtualService - Example Load Master > ...

General Custom properties

Inventory ID	Example LoadMaster > VS 1 (10.154.178.151)
Service Name	
LoadMaster ID	3
Real Servers	[]
Service Status	Down

Cancel Select

1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Expand the relevant Virtual Service.
4. Select the relevant SubVS.
5. Click **Select**.

Start Workflow : Remove SubVS

Common Parameters

* Enter the username for the LoadMaster

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Select the SubVS to be removed

1. Click **Submit**.

Real Servers

Real Servers

A number of tasks can be performed in relation to Real Servers, such as adding a Real Server to a Virtual Service or removing a Real Server. Refer to the sections below for further details.

Related Links

- [Add Real Server to Sub Virtual Service](#)
- [Add Real Server to Virtual Service](#)
- [Remove Real Server](#)

Add Real Server to Sub Virtual Service

Add Real Server to Sub Virtual Service

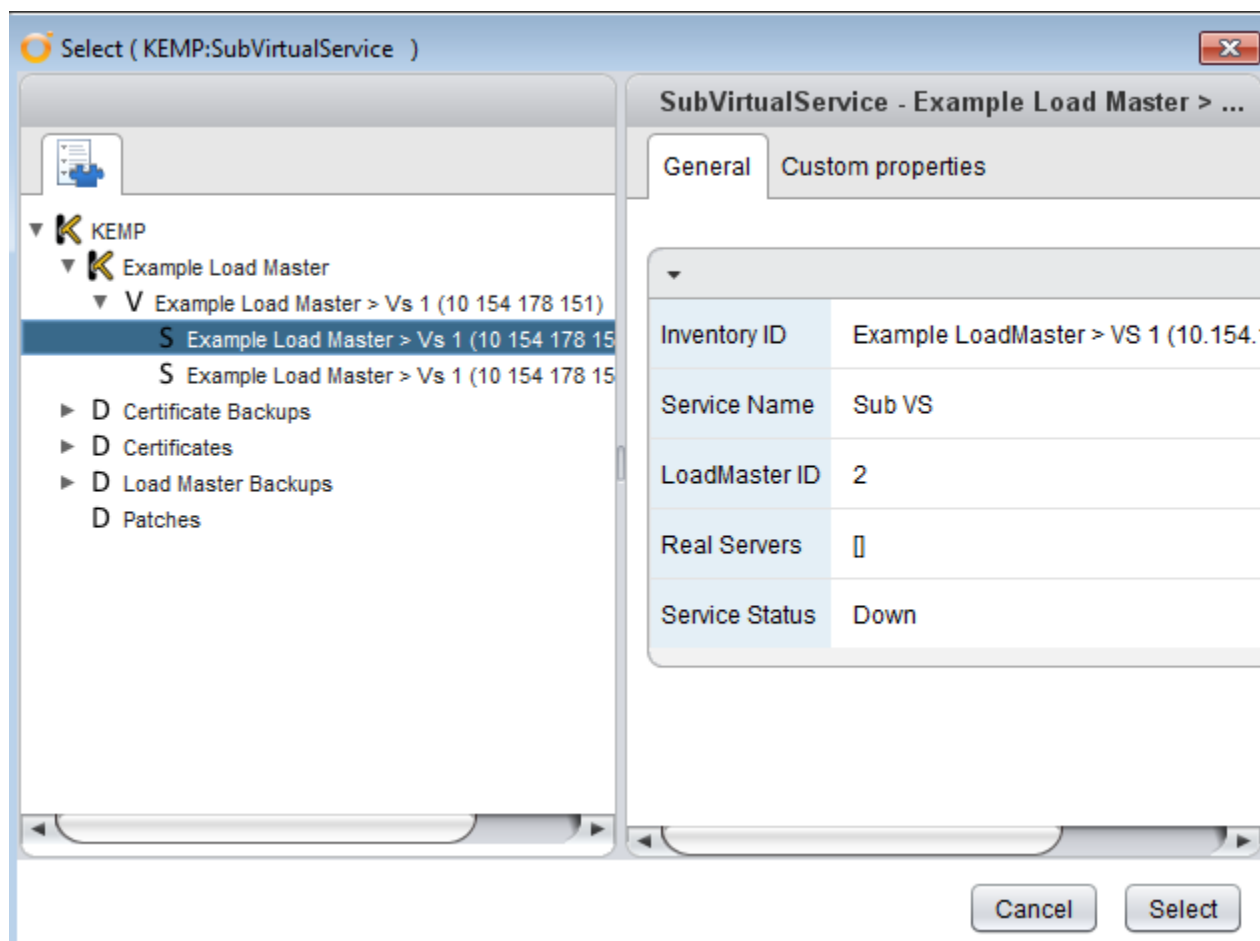
A Real Server can be added to a SubVS by running the **Add Real Server to Sub Virtual Service** workflow.

The screenshot shows the 'Start Workflow : Add Real Server To SubVS' form. On the left, a sidebar contains two steps: '1 Authentication' (highlighted in blue) and '2 Real Server Configuration'. The main area contains three fields: a username field with 'bal' entered, a password field with '*****' entered, and an optional SSL certificate field with a 'Not set' button.

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Real Server Configuration**.

The screenshot shows the 'Start Workflow : Add Real Server To SubVS' form. On the left, a sidebar contains two steps: '1 Authentication' (marked with a checkmark) and '2 Real Server Configuration' (highlighted in blue). The main area contains three fields: a SubVS selection field with a 'Not set' button, an IP address field, and a port field.

1. Click **Not set**.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Expand the relevant Virtual Service.
4. Select the relevant **SubVS**.
5. Click **Select**.

Start Workflow : Add Real Server To SubVS

✓ 1 Authentication

2 Real Server Configuration

* Select the SubVS to add this Real Server to

Example Load Master > Vs 1 (10 154 178 151) > Sub Vs 2

* Enter the IP address of the Real Server

10.154.11.62

* Enter the port of the Real Server

80

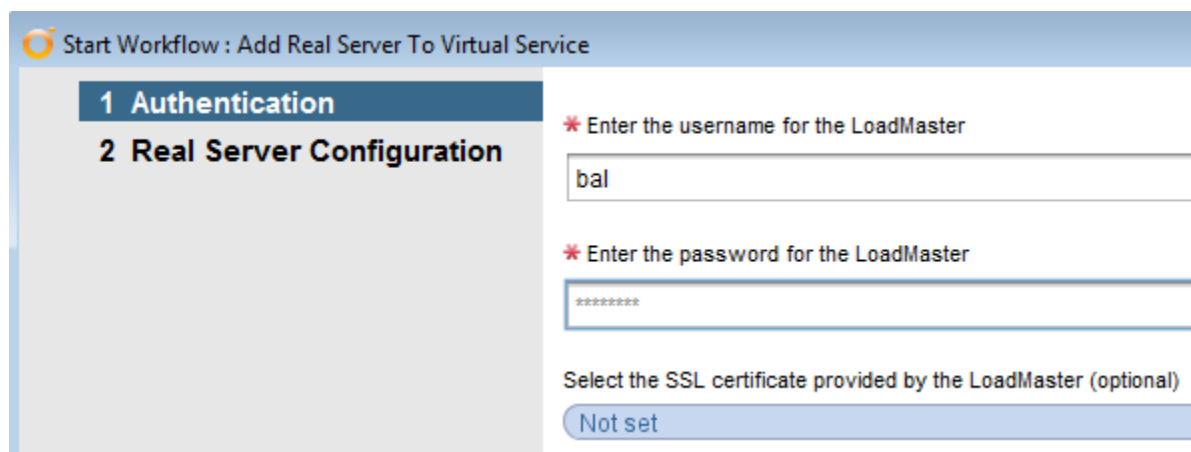
Cancel Back Next Submit

1. Enter the IP address of the Real Server to be added.
2. Enter the port of the Real Server.
3. Click **Submit**.

Add Real Server to Virtual Service

Add Real Server to Virtual Service

A Real Server can be added to a Virtual Service via Orchestrator by running the **Add Real Server to Virtual Service** workflow.



Start Workflow : Add Real Server To Virtual Service

1 Authentication

2 Real Server Configuration

* Enter the username for the LoadMaster

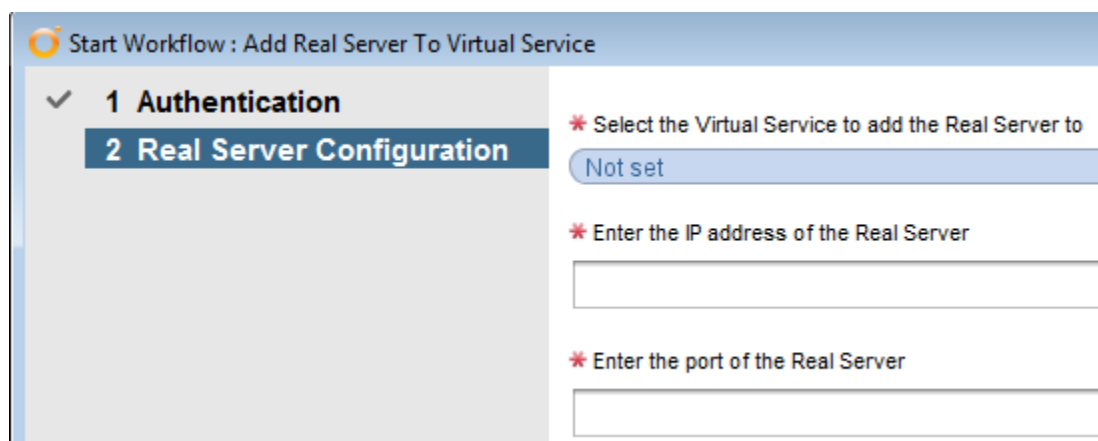
bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Real Server Configuration**.



Start Workflow : Add Real Server To Virtual Service

✓ **1 Authentication**

2 Real Server Configuration

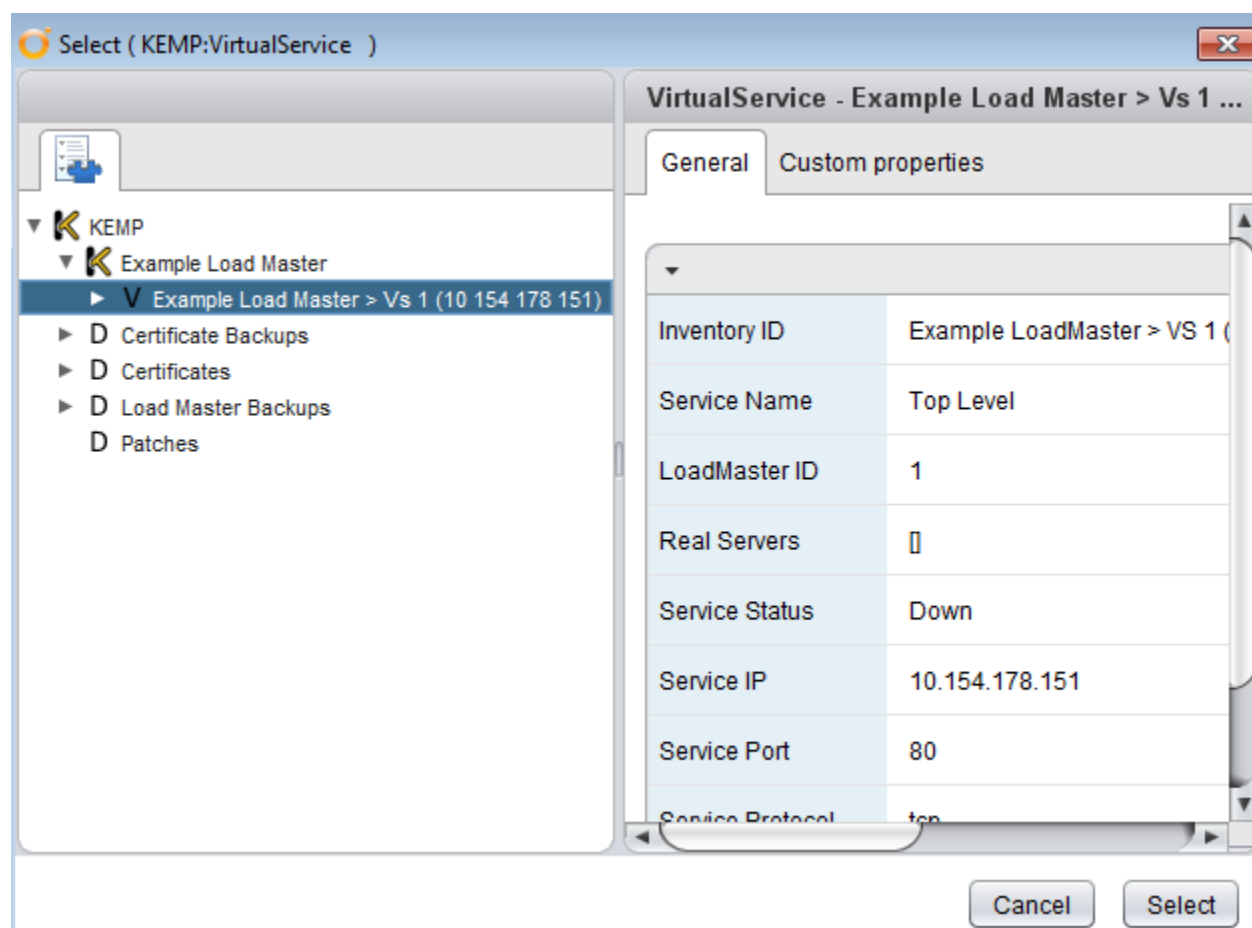
* Select the Virtual Service to add the Real Server to

Not set

* Enter the IP address of the Real Server

* Enter the port of the Real Server

1. Click **Not set**.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Select the relevant Virtual Service.
4. Click **Select**.

Start Workflow : Add Real Server To Virtual Service

✓ 1 Authentication

2 Real Server Configuration

* Select the Virtual Service to add the Real Server to

Example Load Master > Vs 1 (10 154 178 151)

* Enter the IP address of the Real Server

10.154.11.63

* Enter the port of the Real Server

80

Cancel Back Next Submit

1. Enter the IP address of the Real Server.
2. Enter the port of the Real Server.
3. Click **Submit**.

Remove Real Server

Remove Real Server

A Real Server can be removed by running the **Remove Real Server** workflow.

Start Workflow : Remove Real Server

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

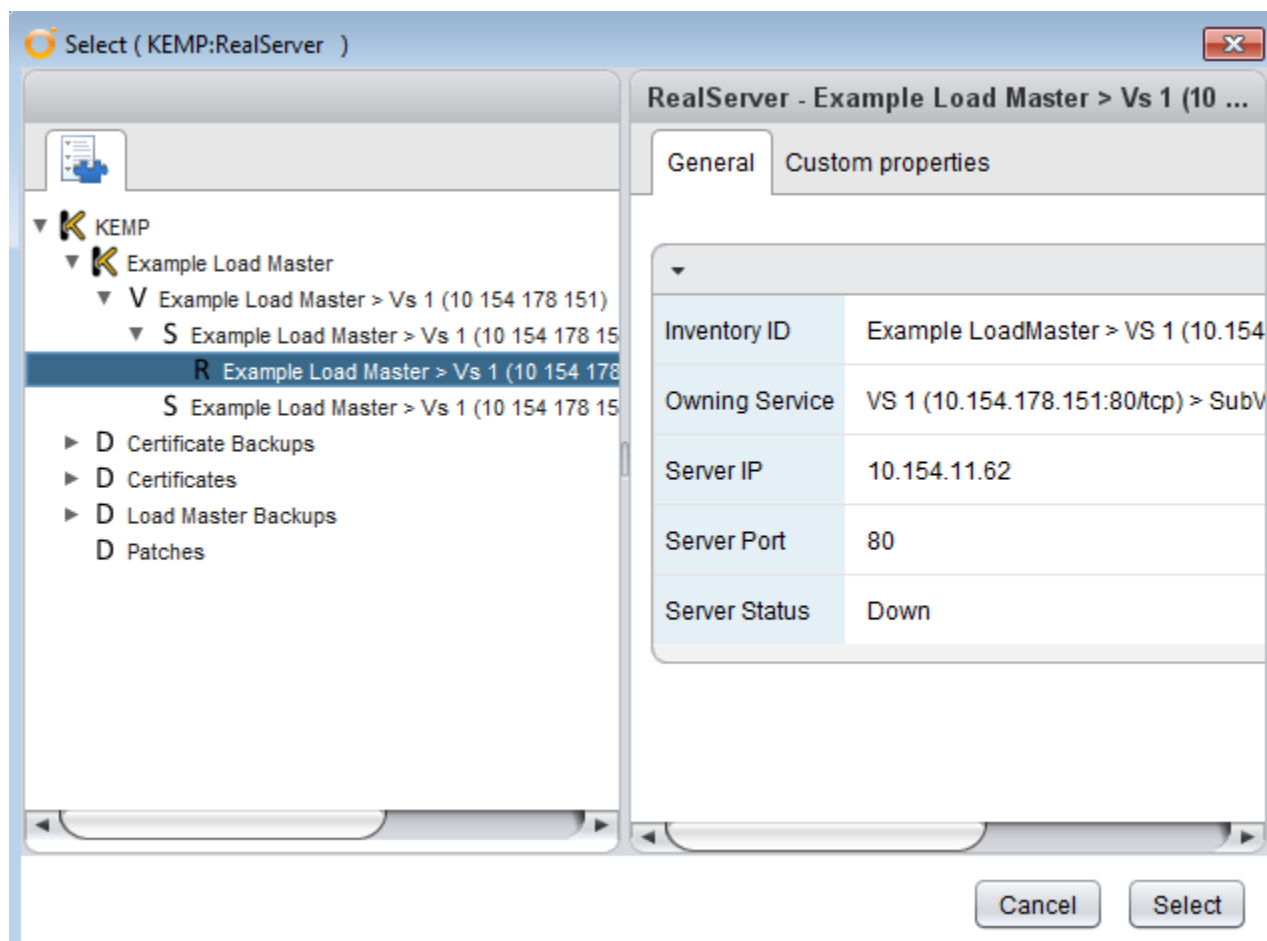
Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the Real Server to be removed

Not set

1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Not set** in the **Select the Real Server to be removed** field.



1. Expand the **Kemp** directory.
2. Expand the relevant LoadMaster.
3. Expand the Virtual Service and/or SubVS.
4. Select the relevant Real Server.
5. Click **Select**.

Start Workflow : Remove Real Server

Common Parameters

* Enter the username for the LoadMaster

bal

* Enter the password for the LoadMaster

Select the SSL certificate provided by the LoadMaster (optional)

Not set

* Select the Real Server to be removed

Example Load Master > Vs 1 (10 154 178 151) > Sub Vs 2 > 10 154 11 62 80

Cancel Submit

1. Click **Submit**.

4

Uninstall the Progress Kemp Orchestrator Plugin

Uninstall the Progress Kemp Orchestrator Plugin

There are three steps that need to be completed in order to uninstall the Progress Kemp Orchestrator plugin. Refer to the sections below for step-by-step instructions.

Related Links

- [Uninstall the Workflows](#)
- [Remove the Progress Kemp Orchestrator Plugin](#)
- [Restart the Service](#)

Uninstall the Workflows

Uninstall the Workflows

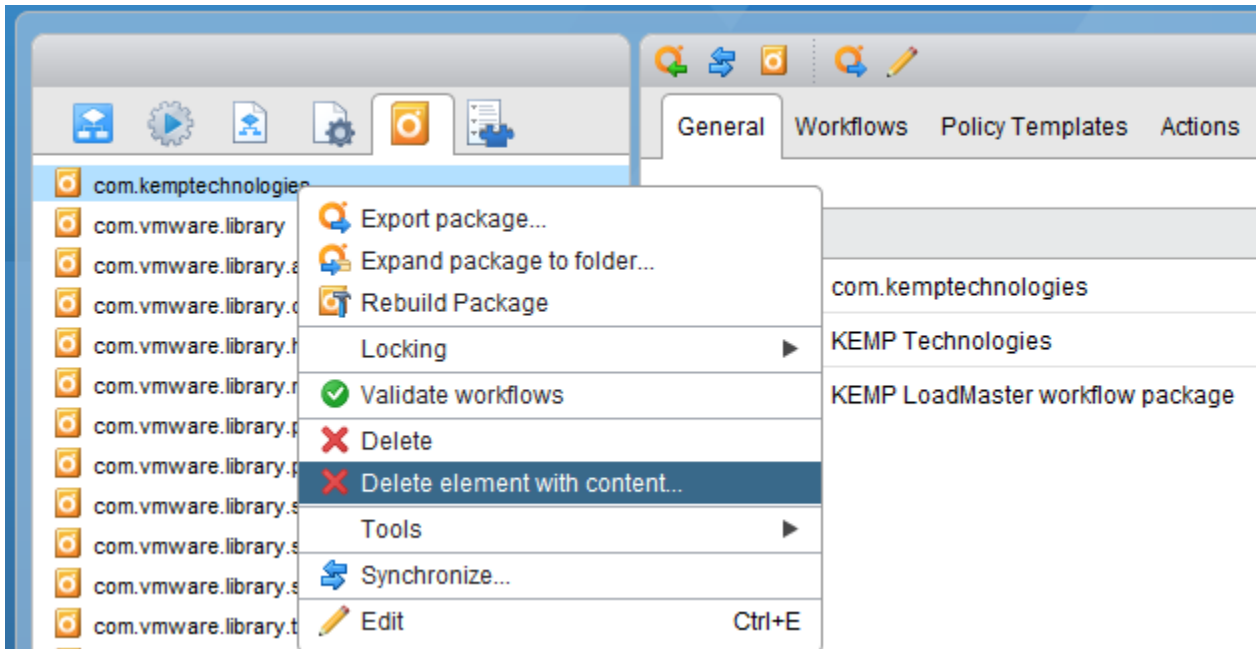
The first step is to uninstall the workflows. To do this, follow the steps below:



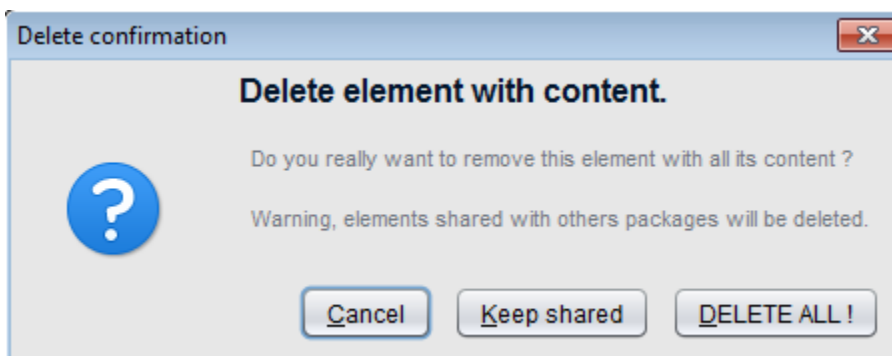
1. Select **Design** from the drop-down menu in the top-left of the screen.



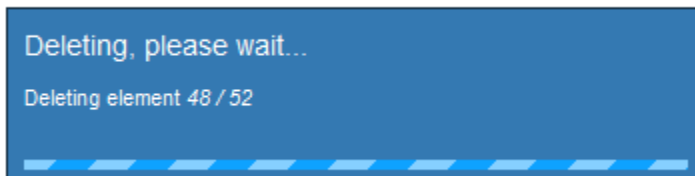
2. Select the packages tab (orange icon).



3. Right-click **com.kemptechnologies** and select **Delete element with content**.



4. Click **DELETE ALL**.



5. Wait for the deletion to complete.

Now that the workflows have been uninstalled, the Progress Kemp plugin can be uninstalled. Follow the steps in the next section to do this.

Remove the Progress Kemp Orchestrator Plugin

Remove the Progress Kemp Orchestrator Plugin

Then, after uninstalling the workflows - follow these steps:

1. Remotely connect to the Orchestrator server.
2. Navigate to the Orchestrator plugins folder:

```
cd /var/lib/vco/app-server/plugins
```

3. Remove the Progress Kemp Orchestrator plugin by running the following command:

```
rm <KempPluginFilename>.dar
```

Now that the Progress Kemp Orchestrator plugin has been removed, the service needs to be restarted for the changes to be applied.

Restart the Service

Restart the Service

After uninstalling, restart the service to complete the uninstallation. To do that, follow the steps below:

1. In a web browser, navigate to the IP address of the Orchestrator server followed by the :8281 port.

Configure the Orchestrator Server

To make additional configuration changes to the Orchestrator server, use the Orchestrator configuration interface:

- [Orchestrator Configuration](#)
- [Orchestrator Control Center \(Beta\)](#)

1. Click the **Orchestrator Configuration** link.

VMware vRealize™ Orchestrator™

Welcome

Enter your username and password to login in VMware vRealize Orchestrator Configuration

Username:

vmware

Password:

••••••••

Login

1. Enter the Orchestrator credentials and click **Login**.

 General	
 Network	
 Authentication	
 Database	
 Server Certificate	
 Licenses	
 Startup Options	
 Server Availability	

1. Click **Startup Options** on the left.

Server startup options

vRO Server

Status Running [Refresh](#)

▶ Start service

■ Stop service

▶▶ Restart service

vRO Configuration Server

▶▶ [Restart the vRO configuration server](#)

1. Click **Restart service**.



Restarting service

1. Wait for the service to restart.

Server startup options

✓ Server is restarted.

A message will appear when the service has been restarted.

Appendix A - Get and Set Parameters

Appendix A - Get and Set Parameters

A number of LoadMaster fields can be retrieved and set using the **Get Parameter** and **Set Parameter** workflows. The fields are retrieved and set using API parameters. The list of API parameters that can be used are listed below. For descriptions of what each of the parameters correspond to, please refer to the [RESTful API, Interface Description](#).

- dfltgw
- dfltgwv6
- admingw
- snat
- hatimeout
- hawait
- haprefered
- hamode
- haif
- havhid
- hastyle
- hainitial
- tcpfailover
- cookieupdate
- vmac

- sshaccess
- sshport
- sshv1prot
- wuiaccess
- mcast
- wuiiface
- wuiport
- sshiface
- hoverhelp
- routefilter
- transparent
- alwayspersist
- expect100
- localbind
- addcookieport
- subnetoriginating
- nonlocalrs
- multigw
- addforwardheader
- conntimeout
- authtimeout
- finalpersist
- tcptimestamp
- paranoia
- cachesize
- hostcache
- resetclose
- rfconform
- keepalive
- backupday
- backupenable
- backuphost
- backuphour
- backupminute
- backuppassword
- backuppath
- backupuser

- backupuser
- emailuser
- emaildomain
- emailpassword
- emailserver
- emailsslmode
- emailport
- emailcritical
- emailemergency
- emailerror
- emailinfo
- emailnotice
- emailwarn
- addvia
- allowupload
- dropatdrainend
- droponfail
- closeonerror
- limitinput
- rsarelocal
- slowstart
- subnetorigin
- syslogcritical
- syslogemergency
- syslogerror
- sysloginfo
- syslognotice
- syslogwarn
- sslrenegotiate
- emailenable
- irqbalance
- snmpenable
- snmpV3enable
- snmpv3user
- snmpv3userpasswd
- snmpcontact
- snmpcommunity

- snmplocation
- snmpHaTrap
- snmpv1sink
- snmpv2sink
- snmpclient
- snmptrapenable
- motd
- wuidisplaylines
- linearesplogs
- onlydefaultroutes
- sessionauthmode
- sessionidletime
- sessionmaxfailattempts
- sessioncontrol
- sessionlocalauth
- ntphost
- netconsole
- netconsoleinterface
- namserver
- radiusbackupport
- radiusbackupsecret
- radiusbackupserver
- radiusport
- radiussecret
- radiusserver
- radiusrevalidateinterval
- ldapserver
- ldapbackupserver
- ldapsecurity
- ldaprevalidateinterval
- geoclients
- geopartners
- geosshport
- ha1hostname
- ha2hostname
- hostname
- searchlist

- timezone
- admincert
- localcert
- time
- ntphost
- version
- Tethering
- multihomedwui
- logsplitinterval
- allowemptyposts
- OCSPPort
- OCSPUseSSL
- OCSPOnServerFail
- OCSPServer
- OCSPUrl
- SSLStapling
- SSLRefreshInterval
- L7LimitInput
- sdnstatsmode

Appendix B - Memory and CPU Usage Details

Appendix B - Memory and CPU Usage Details

The memory and CPU utilization details relating to the Progress Kemp Orchestrator plugin are summarized in the tables below.

The below table shows the specifications of the Orchestrator server that was used when running the tests.

Specification	Type
Hypervisor	VMware vSphere
Memory	3GB
CPU	Dual-core @ 2.0GHz

The below table shows the approximate range of memory usage when the plugin is and is not installed.

Plugin Installed?	Memory Usage
Without plugin installed	381MB -> 395MB
With plugin installed	394MB -> 410MB
With plugin installed (load: ~600 objects)	454MB -> 463MB

The below table shows the CPU usage percentages in various states.

State	CPU Usage
Without plugin installed	~1%
With plugin installed	~1%
Expanding tree view (load: ~100 objects)	~8%
Expanding tree view (load: ~500 objects)	~19%
Empty workflow	~13%
Configure Server Availability workflow	~17%
Add LoadMaster workflow (load: 0 objects)	~17%
Add LoadMaster workflow (load: ~500 objects)	~40%
Remove LoadMaster workflow (load: 0 objects)	~17%

State	CPU Usage
Remove LoadMaster workflow (load: ~500 objects)	~28%

References

References

Unless otherwise specified, the following documents can be found at <http://kemptechnologies.com/loadmaster-documentation>.

Java API, Interface Description

RESTful API, Interface Description