MICRO® FOCUS

PlateSpin® Transformation Manager 2

Appliance Guide

December 2018

Legal Notice

Contents

About This Book

The *Appliance Guide* provides information about the requirements, initial configuration, and maintenance for the PlateSpin Transformation Manager Appliance and the PTM Server application.

Intended Audience

This document is intended for IT administrators who will deploy and maintain the PlateSpin Transformation Manager Appliance. A basic knowledge of virtual machine deployment is assumed.

Additional Documentation

For the most recent version of this guide and other PlateSpin Transformation Manager documentation resources, visit the PlateSpin Transformation Manager 2 Documentation website (https://www.microfocus.com/documentation/platespin/platespin-transformation-manager-2/).

Feedback

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the**comment on this topic** link at the bottom of any HTML page of the online English documentation.

Contact Information

For specific product issues, contact Micro Focus Support at https://support.microfocus.com/contact/.

Additional technical information or advice is available from several sources:

- **Product information and resources:** https://www.microfocus.com/products/platespin/transformation-manager/
- **Micro Focus Customer Center:** https://www.microfocus.com/customercenter/
- **Product Knowledge Base and Videos:** https://www.microfocus.com/support-and-services/
- **Micro Focus Communities:** https://www.microfocus.com/communities/
- **PlateSpin Idea Exchange:** https://community.softwaregrp.com/t5/PlateSpin-Idea-Exchange/idb-p/PlateSpin_Ideas/

Deploy PTM Appliance

The PlateSpin Transformation Manager Appliance is a virtual machine that hosts the PlateSpin Transformation Manager Server software, PostgreSQL database software, and PTM database instance for your transformation projects. The Appliance also hosts an instance of PlateSpin Migrate Connector that is preconfigured to work with all projects on the PTM server.

PlateSpin Transformation Manager is deployed as an appliance on your VM host environment. Appliance deployment provides the following benefits:

- **Simple deployment.** The appliance is ready to configure and run on your VMware hypervisor. You do not need to install the operating system, set up prerequisite applications, or configure its databases.
- **Better performance.** The appliance is built on a specific and tuned version of the SUSE Linux Enterprise Server (SLES) operating system. The appliance includes everything that PlateSpin Transformation Manager needs, and only what it needs. It omits the unneeded applications and services that can consume system resources.
- **Web-based appliance administration.** The appliance provides a web-based Appliance Management Console that allows you to easily manage the appliance in your environment. You do not need to understand the underlying operating system, software, or databases.

  If you contact Technical Support with a PlateSpin Transformation Manager support incident, you might be asked to access a Linux terminal console on the Appliance as the `root` user. Your support representative will provide guidance on any required actions.

1 PTM Appliance Requirements

Ensure that your system meets the requirements in this section before you begin the installation of the PlateSpin Transformation Manager Appliance.

- Section 1.1, “Appliance Virtualization Host Environment,” on page 11
- Section 1.2, “PTM Server,” on page 13
- Section 1.3, “PTM Database,” on page 14
- Section 1.4, “PTM Appliance Management Console,” on page 15
- Section 1.5, “PTM Web Interface,” on page 15
- Section 1.6, “Event Messages,” on page 16
- Section 1.7, “PlateSpin Migrate Connector,” on page 16
- Section 1.8, “Network Access and Communications,” on page 17

1.1 Appliance Virtualization Host Environment

You deploy the OVF file for the PlateSpin Transformation Manager Appliance on your virtualization host server.

- Section 1.1.1, “Virtualization Host Server,” on page 11
- Section 1.1.2, “Virtual Machine,” on page 12
- Section 1.1.3, “Virtual Storage,” on page 12
- Section 1.1.4, “NTP Configuration for the VM and Host,” on page 13

1.1.1 Virtualization Host Server

PlateSpin Transformation Manager supports the virtualization software described in Table 1-1.

Table 1-1 *Virtualization Host Server Requirements*

Virtualization Host Server	Minimum Requirement	Remarks
VMware ESXi	5.5 or higher	The ESXi host must have a VMware enterprise license.
VMware vSphere Client	5.5 or higher	Use this tool to set up the hypervisor environment and resources for the PTM Appliance VM.

1.1.2 Virtual Machine

The OVF file creates a virtual machine on the virtualization host server. The minimum requirements for the PTM Appliance VM are described in Table 1-2.

Table 1-2 *Virtual Machine Requirements*

PTM Appliance VM	Minimum Requirement	Remarks
Memory	4 GB RAM	This virtual memory size setting is the appliance default.
Processor	2 vCPUs	This virtual CPU setting is the appliance default.
IP Address Information	◆ Static IP address for the VM ◆ Network mask ◆ Gateway IP address ◆ DNS host name associated with the static IP address ◆ DNS server IP address ◆ NTP Server IP address or DNS name	Gather this information before you deploy the PTM Appliance. You must provide this information during the appliance installation.

1.1.3 Virtual Storage

You must provide a boot disk and a data disk when you deploy the PTM Appliance. The minimum requirements for the PTM Appliance VM are described in Table 1-3.

Table 1-3 *Virtual Storage Requirements*

Virtual Storage	Minimum Requirements	Remarks
Disk 1 Boot	20 GB	The boot partition for the PTM Appliance stores the system files: ◆ guest operating system ◆ all appliance-specific software ◆ appliance system event logs that are stored in the `/var` directory This boot disk size is the appliance default.

Virtual Storage	Minimum Requirements	Remarks
Disk 2 `/vastorage`	20 GB or larger	The `/vastorage` disk stores the software and data: - PlateSpin Transformation Manager Server software - PlateSpin Migrate Connector software - PostgreSQL database with a PTM database instance - Appliance configuration information - Ganglia health metrics You must create and add this virtual disk during the appliance installation.

1.1.4 NTP Configuration for the VM and Host

Micro Focus recommends setting up NTP (Network Time Protocol) for the PTM Appliance VM and the virtualization host server in accordance with the *VMware Time Keeping Best Practices for Linux Guests (KB 1006427)* (https://kb.vmware.com/kb/1006427).

In a PlateSpin Migration Factory environment, consider using the same NTP server for all PlateSpin components to help avoid time drifts that might prohibit successful migration.

1.2 PTM Server

PlateSpin Transformation Manager Server software is automatically installed on the PlateSpin Transformation Manager Appliance when you deploy the appliance.

During the Appliance deployment, you will set up a System Administrator account for the PTM server and specify passwords for the local users of the Appliance. See Table 1-3 for information about these default users.

Table 1-4 *PTM Default Users*

Default Users	Description
vaadmin user password	The vaadmin user is a default local Appliance administrator user with Linux root-level trans mgr. Use the `vaadmin` credentials to log in to the Appliance Management Console.

Default Users	Description
`root` user password	The `root` user is the default Linux administrator user for the PTM virtual machine. Use the `root` user credentials if you need to log in directly to the VM through the VMware vSphere VM console or through SSH to a Linux console. Technical Support might instruct you to access the Linux console on the Appliance with the `root` credentials.
PTM System Administrator	The System Administrator user has global permissions throughout the PTM Web Interface. During the PTM configuration, specify a valid email address as the user name for this account, then specify a secure password. Use the System Administrator credentials to log in to the PTM Web Interface after the Appliance is up and running. You add other PTM users by using the Users tab in the Web Interface. See "Users" in the *PTM 2 Administrator Guide*.

1.3 PTM Database

PlateSpin Transformation Manager automatically pre-installs the PostgreSQL database on the appliance. You can alternatively set up the PlateSpin Transformation Manager database as a database instance on an existing PostgreSQL database in your network. The minimum requirements for the PTM database are described in Table 1-5.

***Table 1-5** PostgreSQL Database Requirements*

Parameter	Local (Default)	Remote
Database Host	localhost	Specify the DNS name or IP address of the host server for the remote PostgreSQL database.
Database Port	5432	5432 (or your custom port)
Database administrator credentials	Automatically creates a PostgreSQL database administrator user and password	Specify the credentials of the database administrator user who has the schema rights necessary to create a new database instance for PTM and to create a new administrator user account for the new instance.
Create a New Database	Selected	Selected

Parameter	Local (Default)	Remote
Database Name	transmgr	transmgr (or specify a custom name for the PTM database instance)
Database User Name	tmadmin	tmadmin (or specify a custom user name and password for the database administrator user account that will be created for the new PTM database instance)

1.4 PTM Appliance Management Console

Most of your management interaction with the PlateSpin Transformation Manager Appliance takes place through the browser-based PlateSpin Transformation Manager Appliance Management Console.

- Section 1.4.1, “Supported Web Browsers,” on page 15

1.4.1 Supported Web Browsers

PlateSpin Transformation Manager supports the following web browsers for the Appliance Management Console:

- Google Chrome (latest version)
- Microsoft Internet Explorer 11
- Mozilla Firefox (latest version)

NOTE: You must enable JavaScript (Active Scripting) and the TLS 1.2 protocol in your web browser.

1.5 PTM Web Interface

User interaction with the PlateSpin Transformation Manager Server takes place through the browser-based PlateSpin Transformation Manager Web Interface.

- Section 1.5.1, “Supported Web Browsers,” on page 15

1.5.1 Supported Web Browsers

PlateSpin Transformation Manager supports the following web browsers for the PlateSpin Server Web Interface:

- Google Chrome (latest version)

- Microsoft Internet Explorer 11
- Mozilla Firefox (latest version)

NOTE: JavaScript (Active Scripting) must be enabled in your web browser.

1.6 Event Messages

PlateSpin Transformation Manager publishes workload workflow state change messages for its registered listeners. Each PlateSpin Migrate Connector instance registers with its assigned Transformation Manager server or project and listens for events and performs the appropriate actions.

In a PlateSpin Migration Factory environment, each PlateSpin Migrate server publishes workload migration state change messages for its registered listeners. Each PlateSpin Migrate Connector instance registers with its assigned Migrate servers, then listens for messages and delivers them to the appropriate project and workload in Transformation Manager.

PlateSpin uses RabbitMQ for event messaging. The event message queues are pre-configured on the PTM Server and the PlateSpin Migrate Server. The messaging function starts, stops, and restarts automatically with its parent PTM service or Migrate service, respectively.

NOTE: Do not modify the PlateSpin default settings for the RabbitMQ message service.

The PlateSpin Migrate message queues are inactive unless you open the required STOMP port on the Migrate Server. When the port is open, one or more PlateSpin Migrate Connector instances can register as subscribers for the event messages.

1.7 PlateSpin Migrate Connector

An instance of the PlateSpin Migrate Connector is automatically installed on the PlateSpin Transformation Manager Appliance. This Connector instance is preconfigured to work with all projects. It supports discovery and migration for source workloads in the same network where you deploy the appliance.

User interaction with the PlateSpin Migrate Connector takes place through a configuration file on the Appliance and global settings in the PlateSpin Transformation Manager Web Interface. You can use the configuration file to configure the Connector instance to work with a specific project instead of with all projects. See “Configuring a Connector Instance for PTM” in the *PTM 2 Administrator Guide*.

You can install additional instances of Migrate Connector on Linux servers in the same network as source workloads. See “Migrate Connector Requirements” in the *PTM 2 Administrator Guide*.

1.8 Network Access and Communications

Ensure that your network environment meets the PlateSpin Transformation Manager requirements for access, discovery, and migration.

For information about the network access requirements for PlateSpin Migrate, see "Access and Communication Requirements across Your Migration Network" in the *PlateSpin Migrate 2018.11 User Guide*.

- Section 1.8.1, "Public Internet Access," on page 17
- Section 1.8.2, "Appliance Management Console: Ports and Firewalls," on page 17
- Section 1.8.3, "PTM Web Interface: Ports and Firewalls," on page 18
- Section 1.8.4, "Event Messaging: Ports and Firewalls," on page 19

1.8.1 Public Internet Access

PlateSpin Transformation Manager must be able to communicate across the public Internet with the Micro Focus License Server, using the following URL:

https://www.novell.com/center/nodeactivationservice/1_0/subscriptions/getPTMLicenseCount

Internet access is required to activate your License Key on the **Configuration** > **Licenses** page in the PlateSpin Transformation Manager Web Interface. As you begin to configure workloads, Transformation Manager communicates with the License Server to verify license availability as you edit workloads individually or with bulk actions. It also synchronizes license information daily. See "Managing Licenses" in the *PTM 2 Administrator Guide*.

To provide Internet access through a proxy server, you must configure the PTM Appliance as a proxy client for your proxy server. See "Configure Proxy Client Settings" on page 31.

1.8.2 Appliance Management Console: Ports and Firewalls

PlateSpin Transformation Manager Appliance communications use the following ports. Ports are opened by default for the PTM Appliance, as noted. Ensure that you open the following ports in all firewalls in your network between the PTM Appliance and the computers you use to access the appliance and software.

Table 1-6 *Communications Ports for Appliance Management*

Component	Port	Description
Appliance Management Console	9443 (HTTPS, secure SSL)	Use this port to securely manage the PTM Appliance.

Component	Port	Description
Transformation Manager Database (PostgreSQL)	5432	If you configure a remote PostgreSQL database for the PTM Appliance, this port is used by PTM to access to your remote database. PostgreSQL allows TCP traffic, incoming and outgoing. Secure traffic by enabling SSL in the `postgresql.conf`file on your remote PostgreSQL server. This port is closed by default if the PostgreSQL is installed on the PTM Appliance.
SSH	22	You can use SSH to remotely access the PTM Appliance to start, stop, or restart it without using a VMware client. SSH is disabled by default. See Section 8.4.1, "Starting, Stopping, or Restarting System Services," on page 55.
Ganglia	8649 (secure, default) 9080 (non-secure)	The Ganglia `gmond` daemon uses UDP port 8649 for communications. The `gmetad` daemon uses TCP port 8649 for metrics data. You can enable port 9080 to allow anonymous access to the Ganglia monitoring information. See Section 8.7.3, "View Ganglia Metrics Directly Using Port 9080 (Not Secure)," on page 61.

1.8.3 PTM Web Interface: Ports and Firewalls

PlateSpin Transformation Manager uses the following ports for PTM Server. Ensure that you open the following ports in all firewalls in your network between the PTM Appliance and the computers you use to access the appliance and the PTM-related services running on it.

Table 1-7 *Communications Ports for the Transformation Manager Web Interface*

Component	Port	Description
Web Interface	8183 (HTTPS, secure SSL; allow TCP traffic, incoming and outgoing) 8182 (HTTP, non-secure; allow TCP traffic, incoming and outgoing)	Port 8183 is enabled by default. **NOTE:** Micro Focus recommends that you use the secure port and SSL options for accessing the Web Interface. For security reasons, port 8182 is disabled by default.

1.8.4 Event Messaging: Ports and Firewalls

Table 1-8 shows the protocol and port required for event messaging between the PTM Server and the PlateSpin Migrate Connector instances registered with PTM Server. Each Migrate Connector instance also handles event messages for its assigned PlateSpin Migrate servers.

NOTE: The messages reflect events and state changes and do not contain sensitive information.

Table 1-8 *Event Messaging Requirements for Network Protocols and Ports*

Traffic	Network Protocol and Port	Other Requirements
Event Messaging	61613 (Stomp, allow TCP, incoming) (not secure)	This port is open by default on the PTM Appliance VM. Open this port on all other Connector host servers, the PlateSpin Migrate servers configured for the project, and the firewalls between them.

2 Installing PTM Appliance

PlateSpin Transformation Manager is distributed as an appliance that you deploy on your VMware virtualization host. The appliance includes the PlateSpin Transformation Manager Server software and the PostgreSQL database.

NOTE: Before you begin, ensure that you understand the "PTM Appliance Requirements" on page 11.

- Section 2.1, "Downloading the PTM Software," on page 21
- Section 2.2, "Deploying the Appliance on Your Virtualization Host," on page 22
- Section 2.3, "Configuring the Appliance," on page 24

2.1 Downloading the PTM Software

Installation files for PlateSpin Transformation Manager Appliance and PlateSpin Migrate Connector are available on the Micro Focus Downloads website (https://download.microfocus.com/). Select **PlateSpin Transformation Manager**, then follow the **Download** link for **PlateSpin Transformation Manager 2** in the results. Use your Micro Focus Customer Center account credentials to log in to this site.

Table 2-1 describes the installation files needed for PlateSpin Transformation Manager and PlateSpin Migrate Connector.

Table 2-1 *PTM Download Files*

Download File Name	Description
`PlatespinTM.x86_64-2.0.0.x.x.ovf.zip`, where *xxx*represents the build number. Where *xxx.x* is the build number	Contains the OVF file that you use to deploy the PlateSpin Transformation Manager Appliance in your virtualization environment.
`platespin--migrate-connector-2.0.0-x.x.noarch.rpm` Where *xxx.x* is the build number	Contains the files to install a new instance of PlateSpin Migrate Connector on your intended Migrate Connector hosts as needed in your migration environment. An instance of the Migrate Connector is automatically installed on the Appliance when you deploy the Appliance VM.

Download File Name	Description
`ptm_public-key.key`	Contains a PlateSpin Transformation Manager Public Key for new installations of remote instances of PlateSpin Migrate Connector on your intended Migrate Connector hosts. **NOTE:** To install the Migrate Connector RPM without warnings, you must import the PTM Public Key file to your keyring on the intended Migrate Connector host before you install the Connector RPM.

To extract the OVF file:

1. Extract the `PlatespinTM.x86_64-2.0.0.`*`x.x`*`.ovf.zip` file on your management workstation so that the `PlateSpinTM-`*`version`* file folder appears.

   Extract the file using a third-party extractor; do not use the default Windows extractor.

2. Continue with Section 2.2, “Deploying the Appliance on Your Virtualization Host,” on page 22.

2.2 Deploying the Appliance on Your Virtualization Host

Use the instructions in this section to deploy the PTM Appliance VM on your VMware host server and configure its virtual environment. Before you begin, ensure that you understand the Section 1, “PTM Appliance Requirements,” on page 11.

1. On the VMware host server, deploy the appliance:

   1a In the vSphere client, click **File** > **Deploy OVF Template**.

   If the virtualization software you are using does not support `.ovf`, you must convert the `.ovf` file to `.vmx` using the VMware OVF Tool available on the VMware Website.

   1b Browse to and select the `.ovf` file in the `PlateSpinTM-`*`version`* file folder, then click **Next**.

   1c Review the settings, then click **Next**.

   1d In the **Name** field, rename the appliance to a name of your choosing, then click **Next**.

   1e Select the datastore (Hard Disk 1, the Boot partition) where you want to store the virtual machine files, then click **Next**.

   1f Review the default disk format setting, then click **Next** to accept it.

   1g Click **Finish**.

2. In the vSphere client, create a separate VMware hard disk (Hard Disk 2) for the PTM Appliance.

   This hard disk stores your PlateSpin Transformation Manager files. It also stores configuration files that are used for appliance upgrades.

   2a In the vSphere client, select the virtualization host where you set up the virtual machine, then click the Virtual Machines tab.

   2b Right-click the virtual machine that you just created and for which you want to create secondary storage, then click **Edit Settings**.

   2c On the Virtual Machine Properties page, select the Hardware tab, then click **Add**.

2d In the Add Hardware wizard, configure the hard disk.

Page	Action
Device Type	1. Select **Hard Disk**, then click **Next**.
Select a Disk	1. Select **Create a new virtual disk**, then click **Next**.
Create a Disk	1. In the **Capacity** section, specify the amount of hard disk space that you want to allocate. See Disk 2 /vastorage for information about minimum disk capacity requirements. 2. In the **Disk Provisioning** section, select either of the following disk formats, depending on the VMware version that you are running: ◆ **Thick Provision Eager Zeroed** ◆ **Support clustering features such as Fault Tolerance** 3. In the **Location** section, select **Specify a datastore or datastore cluster**, click **Browse**, select a datastore, then click **OK**. 4. Click **Next**.
Advanced Options	1. In the **Virtual Device Node** section, select **SCSI (1:0)** from the drop-down list. **NOTE:** Do not change the controller to VMware Paravirtual at this point of the installation process. You can optionally modify this setting as a post-installation task. See Section 5.3, “Change the SCSI Controller to VMware Paravirtual SCSI for Hard Disk 2,” on page 35. 2. In the **Mode** section, select **Independent** and **Persistent**. These settings allow the appliance to be updated. 3. Click **Next**.
Summary	1. Review the specifications you set for the new hard disk, then click **Finish**.

3 Increase the amount of memory that VMware allocates for the PTM Appliance.

3a In the Virtual Machine Properties window, select **Memory**, then increase the setting to a suitable size for your environment.

3b Click **OK** to exit the Virtual Machine Properties window.

4 (Optional) Upgrade the virtual machine hardware version to the latest that your infrastructure can support. To do so, in the vSphere client, right-click the virtual machine that you just created, and for which you want to upgrade the hardware, then click **Upgrade Virtual Hardware**.

5 Power on the appliance (virtual machine).

6 (Optional) Install VMware Tools on the host server.

7 Continue with Section 2.3, “Configuring the Appliance,” on page 24.

2.3 Configuring the Appliance

After you have successfully deployed the virtual machine in the virtual environment, you are ready to configure the credentials, network, and storage settings for the appliance.

1. In the vSphere client, power on the appliance.
2. Click the **Console** tab.
3. After the appliance starts, select your preferred keyboard layout in the **Keyboard Language** drop-down, then accept the license agreement.
4. On the Passwords and Time Zone page, specify the following appliance information:

Option	Action
root password	Type the `root` user password that you want to set for the PTM Appliance, then type it again to confirm it.
vaadmin password	Type the `vaadmin` user password that you want to set for the PTM Appliance, then type it again to confirm it. The `vaadmin` user is the preferred identity to use when you log in to the Appliance Management Console. The `vaadmin` user name is case sensitive and should use all lowercase letters.
NTP Server	Type the IP address or DNS name of a reliable external Network Time Protocol (NTP) server. For example, `time.example.com`. For the best results, set up NTP in accordance with the VMware *Timekeeping Best Practices for Linux Guests* (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427).
Region	Specify your local region.
Time Zone	Specify your local time zone.

5. Click **Next**.
6. On the Network Configuration page, specify the following network information:

Option	Action
Hostname	Type the fully qualified DNS host name associated with the appliance IP address. For example, `ptm.example.com`.
IP address	Type the static IP address for the PTM Appliance. For example, `10.10.10.10`.
Network mask	Type the network mask associated with the appliance IP address. For example, `255.255.255.0`.
Gateway	Type the IP address of the gateway on the subnet where your appliance is located. For example, `10.10.10.254`.
DNS servers	Type the IP address of a primary DNS server for your network. For example, `10.10.10.1`. A secondary DNS server is optional.
Domain search	Type the domain that is associated with the **Hostname** setting.

7 Click **Next**.

8 Select the Hard Drive for Hard Disk 2.

The Hard Disk 2 that you created for `/vastorage` is automatically detected and **sdb** is displayed as the hard drive. Accept the defaults for the other options on this page, then click **Next**.

9 Click **Configure**.

The appliance displays a message indicating that the installation was successful. Do not log in at the terminal prompt. Appliance administration requires the Appliance Management Console to configure the appliance settings. Using native Linux tools can result in service disruption or failure.

10 Continue with Section 3, “Configuring PTM Server,” on page 27.

3 Configuring PTM Server

After you install and configure the PlateSpin Transformation Manager Appliance as described in Part I, “Deploy PTM Appliance,” on page 9, you are ready to configure the PlateSpin Transformation Manager Server application for the first time.

- Section 3.1, “Initial PTM Server Configuration,” on page 27

After the initial configuration of PTM Server, you can modify some settings. Reconfiguration is also possible. See Chapter 6, “Managing PTM Server,” on page 39.

3.1 Initial PTM Server Configuration

The Server Configuration process uses a quick wizard that gets your system up and running.

To configure the PlateSpin Transformation Manager Server application:

1 In a web browser, navigate to the following URL:

`https://`*`ip_address_or_DNS_name`*`:9443`

Use the IP address or DNS name of the server that you specified during the appliance installation.

2 Log in to the appliance using the `vaadmin` user and the password that you set.

The Appliance takes you directly to the PlateSpin Transformation Manager Server Initial Server Configuration page if the PTM Server application has never been configured.

3 On the Initial Server Configuration page, complete the following information, then click **Submit**.

3a **PostgreSQL Database Connection**

Use one of the following options:

- **Local database:** PlateSpin Transformation Manager automatically pre-installs the PostgreSQL database on the appliance. Select **Auto Setup Local Database**to automatically create a database instance, database administrator user, and a password for the user. Table 3-1 shows the default settings.

Table 3-1 *PostgreSQL Database Default Values*

Parameter	Default Value
Database Host	localhost
Database Port	5432
Create a New Database	Selected
Database Name	transmgr
Database User Name	tmadmin

- **Remote database:** You can alternatively set up the PlateSpin Transformation Manager database as a database instance on an existing PostgreSQL database in your network.
  1. Deselect **Auto Setup Local Database**.
  2. Replace `localhost` with the DNS name or IP address of the host server for the remote PostgreSQL database, and specify the PostgreSQL port.
  3. Specify the credentials of the database administrator user who has the schema rights necessary to create a new instance for the PlateSpin Transformation Manager database.
  4. Specify a name for the PlateSpin Transformation Manager database instance (default: `transmgr`).
  5. Specify the user name and password for the database administrator user account (default: `tmadmin`) that will be created for the newly created PlateSpin Transformation Manager database instance.

3b Initial User Configuration

The initial user for the PlateSpin Transformation Manager Server is the PTM System Administrator user. This user has global permissions for all organizations, projects, and features throughout the Web Interface.

Provide the full name, a valid email address that is unique to your PlateSpin Transformation Manager environment, and a password for this user.

You cannot delete the System Administrator user account. However, you can add another System Administrator user for the PlateSpin Transformation Manager Server if necessary. See "Administrative Users for the Web Interface".

NOTE: You create other PTM users from the Users page in the PlateSpin Transformation Manager Web Interface. You can grant Administrator privileges to trusted users by adding them to the Administrators group.

3c Web Server Configuration

Micro Focus recommends that you use the secure port 8183 and SSL options for accessing the Web Interface. You can enable or disable the HTTP port 8182 to allow non-secure traffic.

Specify the DNS name for the PlateSpin Transformation Manager Server. It is populated automatically with the DNS address used as the subject of the SSL certificate on the appliance.

4 On successful configuration, continue with Chapter 5, "Post-Installation Tasks," on page 31.

4 Configuring PlateSpin Migrate Connector

An instance of the PlateSpin Migrate Connector is automatically installed on the PlateSpin Transformation Manager Appliance. This Connector instance is preconfigured to work with all projects. It supports discovery and migration for source workloads in the same network where you deploy the appliance. Table 4-1 provides information about configuring, deploying, and managing Migrate Connectors in your migration environment.

Table 4-1 *Migrate Connector Configuration Checklist*

Connector Configuration Tasks	Description
1. Configure Migrate Connector global settings. In the Web Interface, select **Configuration** > **Migrate Connector**.	Migrate Connector settings in PTM apply to all Migrate Connectors associated with the PTM Server across all projects. See “Configuring Global Settings for PlateSpin Migrate Connector” in the *PTM 2 Administrator Guide*.
2. (Optional) Configure the Connector instance to work with a specific project instead of with all projects.	After you create a project, you can use its Project ID to configure a Connector instance to work with a specific project. See “Configuring a Dedicated Project for a Connector” in the *PTM 2 Administrator Guide*.
3. (Optional, recommended) Create a special-purpose user for Migrate Connector.	The default instance of Migrate Connector on the PTM Appliance uses the credentials of the PTM System Administrator user to perform actions. We recommend that you create a unique user identity for the Connector instance instead. Having a unique Connector user for each Migrate Connector helps you more easily distinguish actions performed by the Connector instance in logs and transformation histories. See “Creating a User for Connector Login” in the *PTM 2 Administrator Guide*.
4. (PlateSpin Migration Factory) Add one or more PlateSpin Migrate servers as Migration Server resources and associate them with the Connector instance.	In a PlateSpin Migration Factory environment, a Connector instance is required for automating migrations or tracking migrations performed on your PlateSpin Migrate servers. Users with Project Manager or Project Architect permissions can assign a Connector by creating or editing a Migration Server resource. See “Connector” in “About Migration Server Resources” in the *PTM 2 User Guide*.

Connector Configuration Tasks	Description
5. Monitor Connector status.	See “Monitoring Connectors” in the *PTM 2 Administrator Guide*.
6. (Optional) Install additional instances of Migrate Connector on your Linux servers.	Migrate Connector instances are typically deployed in each source network and in target VMware networks if they are different than your source networks. See “Planning for PlateSpin Migrate Connector” and “Deploying PlateSpin Migrate Connector” in the *PTM 2 Administrator Guide*.

5 Post-Installation Tasks

After you set up the appliance, perform the following post-installation tasks as needed:

- Section 5.1, “Configure Proxy Client Settings,” on page 31
- Section 5.2, “Add a Self-Signed Digital Certificate to the Appliance,” on page 35
- Section 5.3, “Change the SCSI Controller to VMware Paravirtual SCSI for Hard Disk 2,” on page 35
- Section 5.4, “View or Modify Appliance Settings,” on page 35
- Section 5.5, “Getting Started with PTM,” on page 35
- Section 5.6, “PlateSpin Migrate Connector Instances,” on page 36

5.1 Configure Proxy Client Settings

If you have a proxy server in your network, you can optionally configure the PlateSpin Transformation Manager Appliance VM as a proxy client. You should also configure each PlateSpin Migrate Connector host in the network as a proxy client. As proxy clients, the appliance VM and Connector hosts will use your proxy server for HTTP and HTTPS communications over the Internet.

The Proxy client informs applications of the Proxy Server URL and credentials to use (if you specify them). It does not affect how the applications communicate with the server.

- Section 5.1.1, “Configuring Proxy Client Settings for the PTM Appliance,” on page 31
- Section 5.1.2, “Configuring Proxy Client Settings for Migrate Connector Hosts,” on page 34

5.1.1 Configuring Proxy Client Settings for the PTM Appliance

You can enable the PlateSpin Transformation Manager Appliance to work with the Proxy Server in your environment. The PTM Server, PlateSpin Migrate Connector instance, PTM Web Interface, and Appliance Management Console running on the Appliance will use the proxy client settings you set for the Appliance VM.

To configure proxy client settings, log in to the Appliance VM through SSH, then use YaST to configure the Internet proxy client settings compatible with your proxy server.

To configure proxy client settings on the PTM Appliance VM:

1 Enable the SSH protocol on the Appliance VM.

SSH is disabled by default on the Appliance.

1a In a web browser, log in to the Appliance Management Console as the `vaadmin` user.

https://<*ptm-ipaddr-or-dns-name*>:9443

1b Click **System Services** ⚙.

1c Select the SSH service.

1d Select **Action > Start**.

1e Click **Close** to exit System Services.

1f Log out of the Appliance Management Console, then close your web browser.

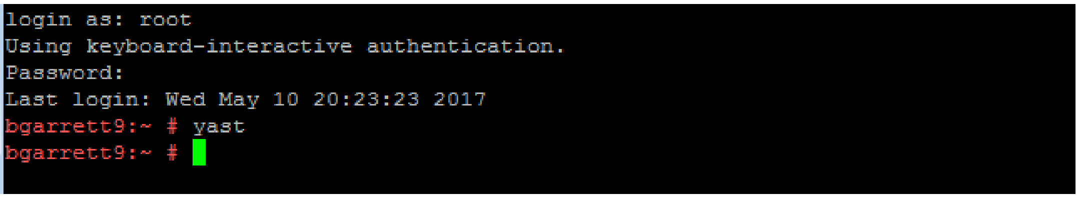
2 Configure the Proxy client settings needed to access your Proxy Server:

2a From your computer, start an SSH session for *ptm-ipaddr-or-dns-name* on port 22, then log in as the `root` user to the Appliance.

You can use any SSH tool, such as Putty (http://www.putty.org/).

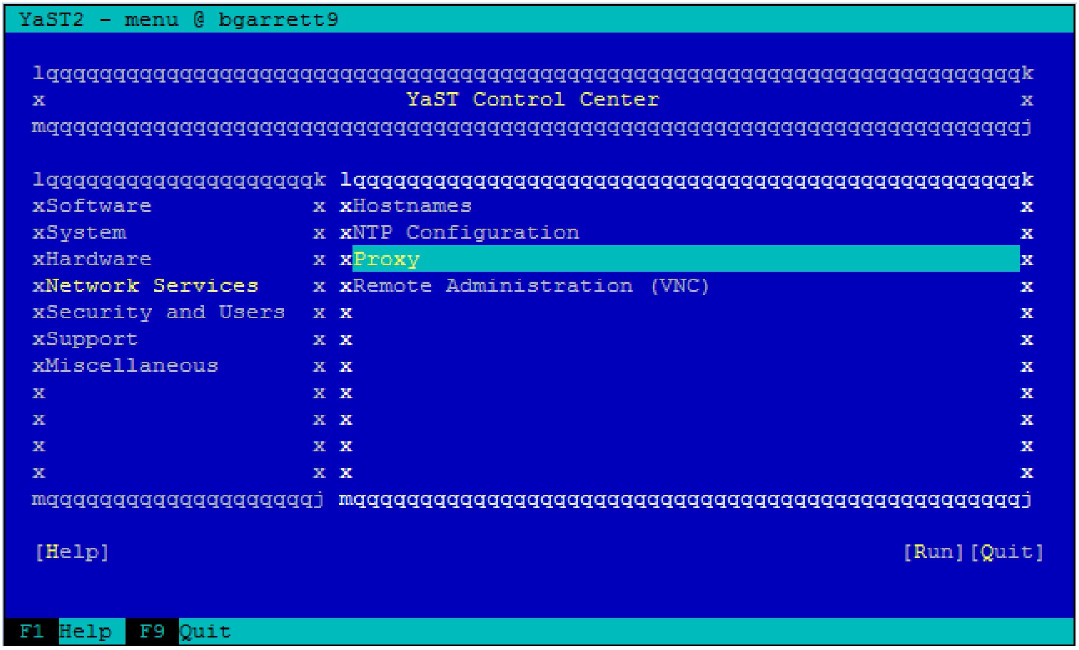
2b At the terminal prompt, enter

```
yast
```



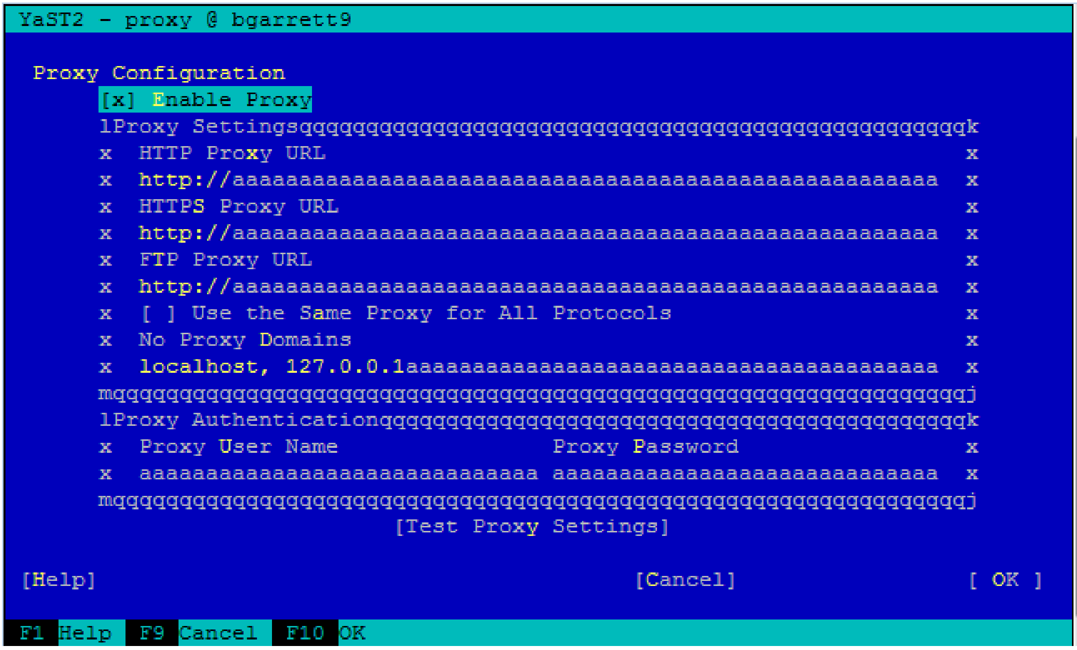
```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Wed May 10 20:23:23 2017
bgarrett9:~ # yast
bgarrett9:~ #
```

2c In YaST, navigate to **Network Services,** select **Proxy**, then press Enter.



```
 YaST2 - menu @ bgarrett9

  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
  x                            YaST Control Center                         x
  mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

  lqqqqqqqqqqqqqqqqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
  xSoftware             x xHostnames                                         x
  xSystem               x xNTP Configuration                                 x
  xHardware             x xProxy                                             x
  xNetwork Services     x xRemote Administration (VNC)                       x
  xSecurity and Users   x x                                                  x
  xSupport              x x                                                  x
  xMiscellaneous        x x                                                  x
  x                     x x                                                  x
  x                     x x                                                  x
  x                     x x                                                  x
  x                     x x                                                  x
  mqqqqqqqqqqqqqqqqqqqqqj mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

  [Help]                                                           [Run][Quit]


 F1 Help  F9 Quit
```

2d On the Proxy Configuration page, on **Enable Proxy**, press the Space bar to select the check box.



```
YaST2 - proxy @ bgarrett9

  Proxy Configuration
       [x] Enable Proxy
       lProxy Settingsqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
       x  HTTP Proxy URL                                                x
       x  http://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa   x
       x  HTTPS Proxy URL                                               x
       x  http://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa   x
       x  FTP Proxy URL                                                 x
       x  http://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa   x
       x  [ ] Use the Same Proxy for All Protocols                      x
       x  No Proxy Domains                                              x
       x  localhost, 127.0.0.1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa   x
       mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
       lProxy Authenticationqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
       x  Proxy User Name               Proxy Password                  x
       x  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaa   x
       mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
                             [Test Proxy Settings]

 [Help]                                          [Cancel]                  [ OK ]

 F1 Help  F9 Cancel  F10 OK
```

2e Tab to navigate to the fields and configure the Proxy settings by using the information for your Proxy Server. Provide the URL for the Proxy Server for HTTP or HTTPS (or both) communications, depending on what protocols you enabled for the Appliance.

HTTP Proxy URL: The URL (with host name and port number) of the Proxy Server used for non-secure access to the Internet. For example: http://proxy1.example.com:3126/

HTTPS Proxy URL: The URL (with host name and port number) of the Proxy Server used for secure access to the Internet. For example: https://proxy2.example.com:3128/

FTP Proxy URL: The URL (with host name and port number) of the Proxy Server used for access to the file transfer services (FTP). For example: https://ftp.proxy.example.com:2121/

Use the Same Proxy for All Protocols: Enable this option and provide a single URL in **HTTP Proxy URL** that will be used as the Proxy Server for HTTP, HTTPS, and FTP communications.

No Proxy Domains: Specify a comma-separated list of domains for which requests should be made directly without caching. The default is `localhost`.

Proxy User Name and Proxy Password: Provide the credentials for your Proxy Server if it requires authorization.

2f (Optional) Tab to **Test Proxy Settings**, then press Enter.

2g Tab to **OK**, then press Enter to save and apply the settings.

2h Tab to **Quit**, then press Enter to exit YaST.

2i At the terminal prompt, enter `exit` to close the SSH session.

3 (Optional) Disable the SSH protocol on the Appliance.

3a In a web browser, log in to the Appliance Management Console as the `vaadmin` user.

https://<*ptm-ipaddr-or-dns-name*>:9443

3b Click **System Services** ⚙.

3c Select the SSH service.

3d Select **Action > Stop**.

3e Click **Close** to exit System Services.

3f Log out of the Appliance Management Console, then close your web browser.

5.1.2 Configuring Proxy Client Settings for Migrate Connector Hosts

You can enable the PlateSpin Migrate Connector host servers to work with the Proxy Server in your environment. The Connector instance will use the proxy client settings you set for the Connector host.

On SUSE Linux Enterprise Server (SLES) servers that host an instance of Migrate Connector, log in to the desktop and use YaST2 to configure the Internet proxy client settings compatible with your proxy server.

NOTE: YaST2 is a management tool for SUSE Linux Enterprise operating system. If your Connector host runs a different Linux operating system, use the OS management tool from your Linux vendor to apply the settings described in this procedure.

To configure proxy client settings on SLES servers that host a Migrate Connector instance:

1. Log in as the `root` user to the desktop on the SLES server.
2. Start the YaST Control Center from the main menu. Provide the `root` user password if you are prompted for it.

   To start the YaST Control Center from the command line, open a terminal, then enter `yast2`.
3. Select **Network Services,** then select **Proxy**.
4. Configure the Proxy settings by using the information for your Proxy Server. Provide the URL for the Proxy Server for HTTP and HTTPS communications.

   HTTP Proxy URL: The URL (with host name and port number) of the Proxy Server used for non-secure access to the Internet. For example: http://proxy1.example.com:3126/

   HTTPS Proxy URL: The URL (with host name and port number) of the Proxy Server used for secure access to the Internet. For example: https://proxy2.example.com:3128/

   FTP Proxy URL: The URL (with host name and port number) of the Proxy Server used for access to the file transfer services (FTP). For example: https://ftp.proxy3.example.com:2121/

   Use the Same Proxy for All Protocols: Enable this option and provide a single URL in **HTTP Proxy URL** that will be used as the Proxy Server for HTTP, HTTPS, and FTP communications.

   No Proxy Domains: Specify a comma-separated list of domains for which requests should be made directly without caching. The default is `localhost`.

   Proxy User Name and Proxy Password: Provide the credentials for your Proxy Server if it requires authorization.
5. Click **Test Proxy Settings**.
6. Click **Finish** to save and apply the settings.
7. Exit YaST.
8. Log out of the server.

5.2 Add a Self-Signed Digital Certificate to the Appliance

The appliance ships with a self-signed digital certificate. The certificate works for both the appliance (port 9443) and the PlateSpin Transformation Manager software (ports 8182 and 8183).

NOTE: This configuration task is optional. For higher security, Micro Focus recommends that you use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

You can use your own existing signed certificate, or you can use the Digital Certificate tool on the appliance to create a certificate, have it signed by a trusted certificate authority, and then add it to the appliance. See Section 8.5, “Digital Certificates,” on page 57.

5.3 Change the SCSI Controller to VMware Paravirtual SCSI for Hard Disk 2

For Hard Disk 2, you can optionally change the SCSI controller to **VMware Paravirtual** (PVSCSI) for Hard Disk 2.

NOTE: This configuration task is optional.

1. After the installation is complete, power on the appliance.
2. Ensure that the system is running. Log in as the appliance vaadmin user and verify the health of the appliance and services.
3. Shut down the appliance.
4. In VMware, change the SCSI controller for Hard Disk 2 to **VMware Paravirtual**.
5. Power on the appliance.

5.4 View or Modify Appliance Settings

After you configure the PTM Server for the first time, you can view or modify the PTM Appliance settings by using the Appliance Management Console to access the Appliance System Configuration page. See Chapter 8, “Managing PTM Appliance,” on page 51.

5.5 Getting Started with PTM

The PTM System Administrator user performs administrative tasks through the PTM Web Interface to prepare PTM for project users. See the following topics in the *PTM 2 Administrator Guide*.

- Section 5.5.1, “Configure Global PTM Settings,” on page 36
- Section 5.5.2, “Configure Users,” on page 36
- Section 5.5.3, “Configure Transformation Projects,” on page 36

5.5.1 Configure Global PTM Settings

Use the PlateSpin Transformation Manager Web Interface to configure and manage the software. See the following in the *PTM 2 Administrator Guide:*

- "Accessing the Web Interface"
- "Managing Licenses"
- "Configuring Operating Systems"
- "Configuring Global Settings for PlateSpin Migrate Connector"

5.5.2 Configure Users

Use the PlateSpin Transformation Manager Web Interface to add users and assign PTM user roles to them. See "Users" in the *PTM 2 Administrator Guide*.

5.5.3 Configure Transformation Projects

After an Administrator user configures global settings and assigns project roles, the PlateSpin Transformation Manager Web Interface is ready for users to plan, manage, and execute transformation projects. See the following topics in the *PTM 2 User Guide:*

- "Projects"
- "Target Platforms"
- "Workloads"
- "Resources"

5.6 PlateSpin Migrate Connector Instances

If a source network or target VMware network is in a different network than the PTM Appliance, you must deploy an instance of PlateSpin Migrate Connector on a Linux server in that network. See "Deploying PlateSpin Migrate Connector" in the *PTM 2 Administrator Guide*.

II Manage PTM Server Application

PlateSpin Transformation Manager Appliance automatically installs the PlateSpin Transformation Manager Server application. It includes a tool to manage basic settings for the PTM server. You can also modify files on the Appliance that control the look and feel of the PTM Web Interface.

- Chapter 6, “Managing PTM Server,” on page 39
- Chapter 7, “Configuring a Custom UI Theme for the Web Interface,” on page 45

6 Managing PTM Server

The PlateSpin Transformation Manager Appliance provides additional tools to manage the PlateSpin Transformation Manager Server that it hosts.

To access the PlateSpin Transformation Manager Tools:

1. In a web browser, specify the DNS name or the IP address for the PTM Appliance with the port number 9443. For example:

   `https://10.10.10.1:9443`

   or

   `https://ptm.example.com:9443`
2. Specify the administrative username and password for the PTM Appliance, then click **Sign in**. The default users are `vaadmin` or `root`.
3. Under **PlateSpin Transformation Manager Tools**, click **Configuration** .
4. (Conditional) The Appliance Management Console automatically opens the following PlateSpin Transformation Manager Tools if it detects the stated condition:
   - **Initial Configuration:** The Initial Configuration tool opens if the PlateSpin Transformation Manager Server has not been configured. You must complete the initial setup before you can manage the appliance or the PlateSpin Transformation Manager Server.
   - **Upgrade:** The Upgrade tool opens if the RPM files for PlateSpin Transformation Manager or for the guest operating system have been updated by applying patches, support packs, or new versions to your existing appliance. You must complete the upgrade before you can manage the appliance or the PTM Server.
5. Continue using the PlateSpin Transformation Manager Server Tools.
   - Administrative Users for the Web Interface
   - Web Server Configuration

Refer to the following sections to manage the PlateSpin Transformation Manager service:

- Section 6.1, "Administrative Users for the Web Interface," on page 40
- Section 6.2, "Web Server Configuration," on page 40
- Section 6.3, "Web Interface Session Timeout," on page 41
- Section 6.4, "Stopping, Starting, or Restarting PTM Service," on page 41
- Section 6.5, "Reconfigure PTM Server," on page 41

6.1 Administrative Users for the Web Interface

During the initial configuration of PlateSpin Transformation Manager Server, you create a default System Administrator user account for the PTM Server Web Interface. The login credentials are the email address and password you assigned for this user. PTM assigns the user to the System Administrator role and adds it as a default member of the Administrators group. The user has global permissions for all organizations, projects, and features throughout the Web Interface. The user cannot be deleted.

Log in to the Web Interface as the System Administrator user to set up other user accounts, as well as organizations and groups. To grant Administrator privileges to a trusted user, add the user account to the Administrators group.

NOTE: Members of the Administrators group inherit the System Administrator role and will also have global permissions in the Web Interface. Members can manage membership in the Administrators group, but they cannot remove the System Administrator user as a member and cannot delete the group.

You might need to add a new System Administrator user to the PlateSpin Transformation Manager Server if you forget the username and password for the initial System Administrator, or if that initial user is no longer available to manage the PTM Server application. The new user has the same global privileges as the default System Administrator user.

To add a System Administrator user for the PTM Web Interface:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Under **PlateSpin Transformation Manager Tools**, click **Configuration** .
3. On the PlateSpin Transformation Manager Configuration page, select **Administrative Users**.
4. Provide the full name, a valid email address that is unique to your PlateSpin Transformation Manager environment, and a password for this user.
5. Click **Submit**.

6.2 Web Server Configuration

The administrative users of the PlateSpin Transformation Manager Appliance can reconfigure the Jetty Web Server HTTPS and HTTP ports for the Web Interface.

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Under **PlateSpin Transformation Manager Tools**, click **Configuration** .
3. On the PlateSpin Transformation Manager Configuration page, select **Web Server Configuration**.
4. For the Web Console HTTPS Port, specify the port to use for secure SSL connections with the PlateSpin Transformation Manager Web Interface. The default port is 8183
5. (Optional, not recommended) Select Enable HTTP to allow users to access the PlateSpin Transformation Manager Web Interface over port 8182 for non-secure connections.
6. Click **Submit**.

6.3 Web Interface Session Timeout

A user session in the PlateSpin Transformation Manager Web Interface times out by default after 30 minutes of browser inactivity. The Web Interface Session Timeout interval is configurable with the `tm.session.timeout.minutes` property in the `/opt/microfocus/ps_transform_mgr/config/system.properties` file. If the property is not specified in this file, the session timeout defaults to 30 minutes.

1. Enable the SSH service on the Appliance VM.

   See Section 8.4.4, "Enabling or Disabling the SSH Service," on page 56.
2. Start an SSH session with the Appliance VM, then log in as the `vaadmin` user or `root` user.
3. Navigate to the `/opt/microfocus/ps_transform_mgr/config/` directory.
4. Open the `system.properties` file in a text editor.
5. Add the `tm.session.timeout.minutes` property and specify the value in minutes to set the interval of browser inactivity to allow before a Web Interface session times out.
6. Save the file and close the text editor.
7. Restart the PlateSpin Transformation Manager service to allow the Web Interface Session Timeout value to take effect.

   In your SSH session, enter the following at a terminal console:

   ```
   rcps_transform_mgr restart
   ```
8. Exit your SSH session.
9. (Optional) Disable the SSH service on the Appliance VM.

   See Section 8.4.4, "Enabling or Disabling the SSH Service," on page 56.

6.4 Stopping, Starting, or Restarting PTM Service

System Services

You can stop, start, or restart the PlateSpin Transformation Manager service on the Appliance by using System Services in the Appliance Management Console. See Section 8.4, "System Services," on page 54.

Command Line

You can stop, start, or restart the PlateSpin Transformation Manager service on the Appliance by using the `/etc/init.d/ps_transform_mgr` or `rcps_transform_mgr` commands, with the options `stop`, `start`, or `restart`. Log in as `root` in an SSH session, the launch a terminal console.

6.5 Reconfigure PTM Server

After the initial configuration, you can reconfigure the PlateSpin Transformation Manager Server settings. You should use the Administrative Users tool and the Web Server Configuration tool instead to modify the application settings without losing any data.

WARNING: A reconfiguration restores the PlateSpin Transformation Manager application and its PostgreSQL database to their initial state. All data is lost.

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 Under **PlateSpin Transformation Manager Tools**, click **Configuration** .

3 On the PlateSpin Transformation Manager Configuration page, select **Initial Configuration**.

4 Select **Overwrite Configuration**.

This option is available if the PlateSpin Transformation Manager application is already configured.

NOTE: Select this option only if you want to overwrite the existing configuration settings and delete all project data.

5 Complete the information for the reconfiguration of the PTM Server.

5a PostgreSQL Database Connection

Use one of the following options:

- **Local database:** PlateSpin Transformation Manager automatically pre-installs the PostgreSQL database on the appliance. Select **Auto Setup Local Database**to automatically create a database instance, database administrator user, and a password for the user. Table 6-1 shows the default settings.

Table 6-1 *PostgreSQL Database Default Values*

Parameter	Default Value
Database Host	localhost
Database Port	5432
Create a New Database	Selected
Database Name	transmgr
Database User Name	tmadmin

- **Remote database:** You can alternatively set up the PlateSpin Transformation Manager database as a database instance on an existing PostgreSQL database in your network.
  1. Deselect **Auto Setup Local Database**.
  2. Replace `localhost` with the DNS name or IP address of the host server for the remote PostgreSQL database, and specify the PostgreSQL port.
  3. Specify the credentials of the database administrator user who has the schema rights necessary to create a new instance for the PlateSpin Transformation Manager database.

4. Specify a name for the PlateSpin Transformation Manager database instance (default: `transmgr`).
5. Specify the user name and password for the database administrator user account (default: `tmadmin`) that will be created for the newly created PlateSpin Transformation Manager database instance.

5b Initial User Configuration

The initial user for the PlateSpin Transformation Manager Server is the PTM System Administrator user. This user has global permissions for all organizations, projects, and features throughout the Web Interface.

Provide the full name, a valid email address that is unique to your PlateSpin Transformation Manager environment, and a password for this user.

You cannot delete the System Administrator user account. However, you can add another System Administrator user for the PlateSpin Transformation Manager Server if necessary. See "Administrative Users for the Web Interface".

NOTE: You create other PTM users from the Users page in the PlateSpin Transformation Manager Web Interface. You can grant Administrator privileges to trusted users by adding them to the Administrators group.

5c Web Server Configuration

Micro Focus recommends that you use the secure port 8183 and SSL options for accessing the Web Interface. You can enable or disable the HTTP port 8182 to allow non-secure traffic.

Specify the DNS name for the PlateSpin Transformation Manager Server. It is populated automatically with the DNS address used as the subject of the SSL certificate on the appliance.

6 Click **Submit**.

7 Configuring a Custom UI Theme for the Web Interface

PlateSpin Transformation Manager enables you to create a custom look-and-feel for the Web Interface to suit your business needs. You can specify preferences for the following aspects of the UI theme:

- Product name
- Icons for various objects in the Configuration, Dashboard, Resources, Projects, Users, and Workloads pages
- Color settings that affect text, titles, underscores, buttons, shadings, and so on throughout the interface

The configurable components reside on the PlateSpin Transformation Manager Appliance.

Use the information in this section to understand how to set up and implement your custom UI theme.

- Section 7.1, "Configurable Theme Components," on page 45
- Section 7.2, "Setting Up Your Custom Theme," on page 46
- Section 7.3, "Resetting Your Custom Theme after an Upgrade," on page 47

7.1 Configurable Theme Components

PlateSpin Transformation Manager allows you to create a custom look-and-feel for the Web Interface. You copy the default theme files to a new directory, customize the files as appropriate, and then point to the custom theme location in the Web Interface configuration file.

PlateSpin Transformation Manager provides two key configurable components for the Web Interface theme. The configurable components reside on the PlateSpin Transformation Manager Appliance.

- **Theme folder:** `/vastorage/ptm/themes/<your_theme_directory>/`
  - **Color variables:** A custom CSS file defines about 20 colors that, along with their derivative colors, affect about 80 percent of text, titles, underscores, buttons, shadings, and so on throughout the Web Interface. You can modify the color definitions to suit the color scheme for your business.
  - **Images:** You can replace any of the various images related to icons displayed for configuration, dashboard, resources, projects, users, and workloads.
- **Theme configuration file:** `/etc/opt/microfocus/ps_transform_mgr/config/transformationmanager-themes.cfg`
  - **Product Name:** You can specify the full and short product name that displays in the Web Interface.
  - **Theme:** You can specify the default `TransformationManager` theme directory, or specify your custom theme directory.

7.2 Setting Up Your Custom Theme

To create a custom theme for the PTM Web Interface:

1 Enable the SSH service on the appliance:

1a Log in to the Appliance Management Console as the `vaadmin` user.

1b Click **System Services**.

1c Select the SSH service.

1d Select **Action > Start**.

1e Click **Close** to exit System Services.

2 Start an SSH session and log in as the `vaadmin` user to the user appliance.

3 Set up your custom theme files:

3a Navigate to the `/vastorage/ptm/themes/` directory.

3b Create a subdirectory under `themes` for your custom theme, such as `MyCompanyTheme`.

3c Copy the contents of the `/vastorage/ptm/themes/TransformationManager` directory to your new theme directory (`/vastorage/ptm/themes/MyCompanyTheme`).

3d In your custom theme directory, update the custom CSS file for color variables;

`/vastorage/ptm/themes/<your_theme_directory>/en/web/theme_variables.tmcss`

3e In your custom theme directory, change the image files as appropriate to define your custom theme for the PTM Web Interface.

4 Modify the `transformationmanager-themes.cfg` file with your custom settings:

4a Open the `/etc/opt/microfocus/ps_transform_mgr/config/transformationmanager-themes.cfg` file in a text editor.

4b Modify the `server.theme` directive to replace the `TransformationManager` theme with your custom theme `MyCompanyTheme`.

For example, change this line:

```
server.theme=TransformationManager
```

to this:

```
server.theme=MyCompanyTheme
```

4c (Optional) Modify the lines that specify the product name.

```
server.productname=<span>PlateSpin</span> Transformation Manager
server.shortproductname=Transformation Manager
```

4d Save your changes.

5 Restart the PlateSpin Transformation Manager service to allow the theme changes to take effect.

Do one of the following:

- In your SSH session, enter the following at a terminal console:

  ```
  rcps_transform_mgr restart
  ```

- Log in to the Appliance Management Console, click **System Services**, select PlateSpin Transformation Manager (`ps_transform_mgr`), then select **Action** > **Restart**.

6 Log in to the PTM Web Interface to verify your UI changes.

To make additional changes, return to the appliance to update your custom theme files as appropriate, then restart the service to apply the changes.

7 After your theme changes are complete, end your SSH session.

8 Disable the SSH service:

8a Log in to the Appliance Management Console as the `vaadmin` user, then click **System Services**.

8b Select the SSH service.

8c Select **Action > Stop**.

8d Click **Close** to exit System Services.

8e Log out of the Appliance Management Console, then close your web browser.

7.3 Resetting Your Custom Theme after an Upgrade

An appliance update ignores your custom theme directory, but updates files in the default theme location. After an upgrade or update, you must verify that your themes are still valid and manually update your theme files as necessary.

After a patch or online update, manually update your theme:

1 Enable the SSH service on the appliance:

1a Log in to the Appliance Management Console as the `vaadmin` user, then click **System Services**.

1b Select the SSH service.

1c Select **Action > Start**.

1d Click **Close** to exit System Services.

2 Start an SSH session and log in as the `vaadmin` user to the appliance.

3 Navigate to the `/vastorage/ptm/themes/TransformationManager` directory.

4 Copy the latest version of the CSS and image files that you modified from the `TransformationManager` location to a working location.

5 Merge your custom settings to these new files.

6 Copy the updated files to your theme directory (`/vastorage/ptm/themes/MyCompanyTheme`).

7 Restart the PlateSpin Transformation Manager service to allow the theme changes to take effect.

Do one of the following:

- In your SSH session, enter the following at a terminal console:

  ```
  rcps_transform_mgr restart
  ```

- Log in to the Appliance Management Console, click **System Services**, select PlateSpin Transformation Manager (`ps_transform_mgr`), then select **Action > Restart**.

8 Log in to the PTM Web Interface to verify your UI changes.

To make additional changes, return to the appliance to update your custom theme files as appropriate, then restart the service to apply the changes.

9 After the theme changes are complete, end your SSH session.

10 Disable the SSH service:

10a Log in to the Appliance Management Console as the `vaadmin` user, then click **System Services**.

10b Select the SSH service.

10c Select **Action > Stop**.

10d Click **Close** to exit System Services.

10e Log out of the Appliance Management Console, then close your web browser.

III Manage PTM Appliance

PlateSpin Transformation Manager provides an Appliance Management Console with various options for managing and updating the Appliance. It enables you to configure services for the server without working directly in the Linux interface.

8 Managing PTM Appliance

The PlateSpin Transformation Manager Appliance is the virtual machine that hosts the PlateSpin Transformation Manager Server and its database. You can use the Appliance Management Console to change certain configuration settings for the PTM Appliance, such as administrative passwords for the `vaadmin` user and `root` user, network settings, and certificate settings. You should perform these tasks only from the Console, because native Linux tools are not aware of the configuration requirements and dependencies of the PlateSpin Transformation Manager services.

To access the Appliance Management Console:

1. In a web browser, specify the DNS name or the IP address for the PTM Appliance with the port number 9443.

   https://<*ptm-ipaddr-or-dns-name*>:9443

   For example:

   `https://10.10.10.1:9443`

   or

   `https://ptm.example.com:9443`

2. Specify the administrative username and password for the PTM Appliance, then click **Sign in**. The default users are `vaadmin` or `root`.

3. (Conditional) The Appliance Management Console automatically displays one the following PlateSpin Transformation Manager options if it detects the stated condition:

   - **Initial Configuration:** The Initial Configuration tool opens if the PlateSpin Transformation Manager Server has not yet been configured. You must complete the initial setup before you can manage the appliance or the PlateSpin Transformation Manager Server.
   - **Upgrade:** The Upgrade tool opens if the RPM files for PlateSpin Transformation Manager or for the guest operating system have been updated by applying patches, support packs, or new versions to your existing appliance. You must complete the upgrade before you can manage the appliance or the PTM Server.

4. Continue using the Appliance Configuration tools in the Appliance Management Console.

The Appliance Management Console provides web-based configuration tools for the PTM Appliance

- Administrative Passwords
- Network
- Time
- System Services
- Digital Certificates
- Firewall
- Ganglia Configuration and Monitoring
- Storage
- /var Mount Configuration

- Reboot or Shutdown
- Logout

8.1 Administrative Passwords

Use the Administrative Passwords tool to modify the passwords and SSH access permissions for the PTM Appliance administrators: the `vaadmin` user and the `root` user. You might need to modify passwords periodically in keeping with your password policy, or if you reassign responsibility for the PTM Appliance administration to another person.

The `vaadmin` user can use the Administrative Passwords page to perform the following task:

- Modify the `vaadmin` user password. To change a password, you must be able to provide the old password.
- The vaadmin user automatically has permissions necessary to remotely access the appliance with SSH instead of using a VMware client. The SSH service must be enabled and running to allow SSH access.

NOTE: The SSH service is disabled and is not running by default. For information about how to start SSH on the appliance, see Section 8.4, “System Services,” on page 54.

The `root` user can use the Administrative Passwords page to perform the following tasks:

- Modify the `root` user password. To change a password, you must be able to provide the old password.
- Enable or disable (default) `root` user SSH access to the appliance.

  When this option is selected, the root user is able to SSH to the appliance. If this option is deselected, only the `vaadmin` user can SSH to the appliance, and the root user cannot SSH even if the `sshd` service is running.

To manage the administrative access as the `vaadmin` user:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Administrative Passwords** .
3. Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.
4. Click **OK**.

To manage the administrative access as the `root` user:

1. Log in to the Appliance Management Console as the `root` user.
2. Click **Administrative Passwords** .

3 Specify a new password for the `root` administrator. You must also specify the current `root` password.

4 (Optional) Select or deselect **Allow root access to SSH**. It is deselected by default.

5 Click **OK**.

8.2 Network

Use the Network tool to configure settings for the DNS servers, search domains, gateway, and NICs for the PTM Appliance. You might need to modify these settings after the initial setup if you move the appliance VM to a new host server, or move the host server to a new domain in your network environment. You can also optionally restrict the networks that are allowed to access the appliance.

To configure network settings for the PTM Appliance:

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 Click **Network**.

3 In the **DNS Configuration** section, you can modify the DNS name servers, search domains, and gateway settings for your appliance network.

If the **Search Domains** field is left blank, it is auto-populated with the domain of the appliance host name. For example, if the host name of the appliance is `ptm.mycompany.com`, the domain is auto-populated with `mycompany.com`.

4 In the **NIC Configuration** section, you can modify the IP address, host name, and network mask of any NIC associated with the appliance.

4a Click the ID of the NIC.

4b Edit the IP address, host name, or network mask for the selected NIC.

4c Click **OK**.

4d Repeat these steps for each NIC that you want to configure.

5 (Optional) In the **Appliance Administration UI (port 9443) Access Restrictions** section, do one of the following:

- Specify the IP address of each network for which you want to allow access to the appliance. Only the listed networks are allowed.
- Leave this section blank to allow any network to access the appliance.

NOTE: After you configure the appliance, changes to your appliance network environment can impact the appliance communications.

6 Click **OK**.

8.3 Time

Use the Time tool to configure the Network Time Protocol (NTP) server, the geographic region, and the time zone where you have deployed the appliance.

To configure time parameters for the PTM Appliance:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Time** 🕓.
3. Change the following time configuration options as appropriate:

   NTP Server: Specify the NTP server that you want to use for time synchronization.

   Region: Select the geographic region where your appliance is located.

   Time Zone: Select the time zone where your appliance is located.
4. Click **OK**.

8.4 System Services

Use the System Services tool to view the status of services running on the appliance, or performs on them. System services include the following:

- SSH
- Jetty
- PostgreSQL
- PlateSpin Transformation Manager
- PlateSpin Migrate Connector for PTM

To access the System Services page:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **System Services** ⚙.

You can perform the following actions:

- Section 8.4.1, "Starting, Stopping, or Restarting System Services," on page 55
- Section 8.4.2, "Making System Services Automatic or Manual," on page 55
- Section 8.4.3, "Downloading Log Files for System Services," on page 55
- Section 8.4.4, "Enabling or Disabling the SSH Service," on page 56

8.4.1 Starting, Stopping, or Restarting System Services

You might want to start, stop, or restart the SSH, Jetty, PostgreSQL, or PlateSpin Transformation Manager services.

For example, if you create a custom theme for the PTM Web Interface, you will enable and disable SSH and restart PlateSpin Transformation Manager as part of the setup process.

To start, stop, or restart a service on the appliance:

1. Click **System Services** ⚙.
2. Select the service that you want to start, stop, or restart.
3. Click **Action**, then select **Start**, **Stop**, or **Restart**.
4. Click **Close** to exit System Services.

8.4.2 Making System Services Automatic or Manual

1. Click **System Services** ⚙.
2. Select the service that you want to make automatic or manual.
3. Click **Options**, then select either **Set as Automatic** or **Set as Manual**.
4. Click **Close** to exit System Services.

8.4.3 Downloading Log Files for System Services

If you experience an issue with the Web Interface, you might need to download the log files to send them to Technical Support.

1. Click **System Services** ⚙.
2. In the **Log Files** column, click the **download** link for the appropriate service to download the log files to your management workstation:

   SSH: The SSH service that is running on the appliance has no relevant log files for download.

   Jetty: Downloads the `jetty.stderrout.log` file.

PostgreSQL: The database for the PlateSpin Transformation Manager product has no relevant log files for download.

PlateSpin Transformation Manager: Collects, zips, and downloads the following log files:

- `tm_server.log`
- `platespin-transformmgr.out`
- `platespin_transformmgr_config.log`

PlateSpin Migrate Connector for PTM: Collects, zips, and downloads the following log files:

- `migrate_connector.log`
- `platespin-migrate-connector.out`

3 Click **Close** to exit System Services.

8.4.4 Enabling or Disabling the SSH Service

To enable the SSH service on the Appliance VM:

1. Log in to the Appliance Management Console as the `vaadmin` user, then click **System Services**.
2. Select the SSH service.
3. Select **Action > Start**.
4. Click **Options**, then select either **Set as Automatic** or **Set as Manual**.
5. Click **Close** to exit System Services.
6. Log out of the Appliance Management Console, then close your web browser.
7. From your computer, start an SSH session and log in as the `vaadmin` user or `root` user to the user appliance.

To disable the SSH service on the Appliance VM:

1. Exit any open SSH sessions.
2. Log in to the Appliance Management Console as the `vaadmin` user, then click **System Services**.
3. Select the SSH service.
4. Select **Action > Stop**.
5. Click **Close** to exit System Services.
6. Log out of the Appliance Management Console, then close your web browser.

8.5 Digital Certificates

Use the Digital Certificates tool to add and activate certificates for the PTM Appliance. You can use the digital certificate tool to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

NOTE: The appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, Micro Focus recommends that you use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

The certificate works for both the appliance (port 9443) and the PlateSpin Transformation Manager Web Interface (ports 8182 and 8183). You do not need to update your certificate when you update the software.

Complete the following sections to change the digital certificate for your appliance:

- Section 8.5.1, “Using the Digital Certificate Tool,” on page 57
- Section 8.5.2, “Using an Existing Certificate and Key Pair,” on page 58
- Section 8.5.3, “Activating the Certificate,” on page 59

8.5.1 Using the Digital Certificate Tool

- “Creating a New Self-Signed Certificate” on page 57
- “Getting Your Certificate Officially Signed” on page 58

Creating a New Self-Signed Certificate

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 Click **Digital Certificates** .

3 In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.

4 Click **File** > **New Certificate (Key Pair)**, then specify the following information:

4a General

Alias: Specify a name that you want to use to identify and manage this certificate.

Validity (days): Specify how long you want the certificate to remain valid.

4b Algorithm Details

Key Algorithm: Select either **RSA** or **DSA**.

Key Size: Select the desired key size.

Signature Algorithm: Select the desired signature algorithm.

4c Owner Information

Common Name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

Organizational Unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

Organization (O): (Optional) Large organization name. For example, Micro Focus.

City or Locality (L): (Optional) City name. For example, Provo.

State or Province (ST): (Optional) State or province name. For example, Utah.

Two-letter Country Code (C): (Optional) Two-letter country code. For example, US.

5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.

6 Make the certificate official, as described in "Getting Your Certificate Officially Signed" on page 58.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then mails the new certificate and certificate chain back to you.

3 After you have received the official certificate and certificate chain from the CA:

3a Revisit the Digital Certificates page.

3b Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.

3c Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.

3d Browse to and upload the official certificate to be used to update the certificate information.

On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in Section 8.5.3, "Activating the Certificate," on page 59.

8.5.2 Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use a `.P12` key pair format.

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 Click **Digital Certificates** .

3 In the **Key Store** drop-down menu, select **JVM Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

5 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate chain for the certificate that you selected in Step 4, then click **OK**.

6 Click **File** > **Import** > **Key Pair**. Browse to and select your `.P12` key pair file, specify your password if needed, then click **OK**.

7 Continue with Section 8.5.3, “Activating the Certificate,” on page 59.

8.5.3 Activating the Certificate

1 On the Digital Certificates page, in the **Key Store** drop-down menu, select **Web Application Certificates**.

2 Select the certificate that you want to make active, click **Set as Active**, then click **Yes**.

3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

4 When you successfully activate the certificate, click **Close** to exit Digital Certificates.

8.6 Firewall

Use the Firewall tool to view your current firewall configuration directly from the appliance. By default, all ports are blocked except those needed by the appliance. For example, the Login page for the Appliance Management Console uses port 9443, so this port is open by default.

NOTE: To have a seamless experience with the appliance, ensure that you do not block the ports with your firewall settings. See “Appliance Management Console: Ports and Firewalls” on page 17.

To view firewall settings for the PTM Appliance:

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 Click **Firewall** .

The Firewall page lists port numbers with the current status of each port number. The page is for informational purposes and is not editable.

3 Click **Close** to exit the Firewall page

8.7 Ganglia Configuration and Monitoring

Ganglia is a scalable, distributed monitoring system that allows you to gather important information about your appliance. The default metrics that you can monitor are CPU, disk, load, memory, network, and process.

- Section 8.7.1, “Configure Ganglia,” on page 60
- Section 8.7.2, “View Ganglia Metrics Using the Appliance Management Console Port 9443 (Secure),” on page 61
- Section 8.7.3, “View Ganglia Metrics Directly Using Port 9080 (Not Secure),” on page 61

8.7.1 Configure Ganglia

Use the Ganglia Configuration tool to configure monitoring for the PTM Appliance. The Ganglia `gmond` daemon uses UDP port 8649 for communications. The `gmetad` daemon uses TCP port 8649 for metrics data. You can also enable or disable non-secure HTTP viewing of the metrics on port 9080.

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Ganglia Configuration** .
3. As appropriate, change the following Ganglia configuration options:

   Monitoring Services

   - **Enable Full Monitoring Services:** Select this option to receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the appliance. This option is enabled by default.

     You might want to disable Ganglia monitoring by deselecting this option:

     - If you already have a monitoring system that you plan to use for the PTM Appliance.
     - If you plan to configure a dedicated appliance for viewing monitoring information.

       You specify a dedicated appliance by selecting **Unicast** under Monitoring Options, and then specifying the DNS name or IP address of the appliance that collects the monitoring information.

   Monitoring Options

   - **Enable monitoring on this appliance:** Select this option to enable Ganglia monitoring on this appliance.
     - **Multicast:** Select this option to send monitoring information to other appliances on the network. This option is selected by default.
     - **Unicast:** (Recommended) Select this option to send monitoring information to a single destination.

NOTE: Unicast mode is recommended for improving performance of the system.

Publish to: Specify the URL where Ganglia sends monitoring information when it is running in Unicast mode.

Monitoring Tool Options

- **Enable direct http port 9080 access:** Select this option to enable the Ganglia Monitoring dashboard to be available directly at the following URL using the non-secure http protocol and port 9080:

  http://*ptm_dns_server_name*:9080/gweb/

4. (Optional) Click **Reset Database** to remove all existing Ganglia metrics from the Ganglia database on this appliance.

   This option is not related to the PlateSpin Transformation Manager database.

5. Click **OK**.
6. Click **Close** to exit Ganglia Configuration.

8.7.2 View Ganglia Metrics Using the Appliance Management Console Port 9443 (Secure)

Use the Ganglia Monitoring tool to securely view the Ganglia Dashboard in the Appliance Management Console using port 9443. The dashboard displays the health and status metrics for the PTM Appliance.

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Ganglia Monitoring** .

   The Ganglia Dashboard opens in a new tab to the following web page:

   https://*ptm_dns_server_name*:9443/gweb/

3. When you are done viewing information, close the Ganglia tab in your web browser.

8.7.3 View Ganglia Metrics Directly Using Port 9080 (Not Secure)

1. Ensure that you have enabled **Monitoring Tool Options > Enable direct http port 9080 access.**
2. In a web browser, go to the following URL:

   http://*ptm_dns_server_name*:9080/gweb/

   No login is required.

3. When you are done viewing information, close your web browser.

8.8 Storage

Use the Storage tool to expand the storage space for the Boot partition (Hard Disk 1) and the `/vastorage` (virtual appliance storage) partition (Hard Disk 2) that you created when you deployed the appliance. You can also expand the `/var`partition if you created a separate disk for the log files.

To expand the size of an appliance disk partitions:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Storage** .
3. Use the tools provided by your virtualization platform vendor to expand the virtual disks that contain the partitions you are expanding.
4. In the virtual disks table, select the partitions to be expanded.
5. Click **Expand partitions**.

   This action stops the appliance services, expands the selected partitions to the size of their respective disks, and restarts appliance services.
6. Restart the appliance so the operating system can detect the disks that have been expanded.

8.9 /var Mount Configuration

Use the `/var` Mount Configuration tool to configure the location of the `/var` directory if you move it to a separate hard disk on the appliance or to a remote NFS directory. By default, the appliance logs its system events in the `/var` directory on the Boot partition (Hard Disk 1). Because the `/var` directory can fill up with log files and cause the Boot partition to grow, you can locate the `/var` directory on a separate dedicated hard disk on the appliance, or on a dedicated remote NFS directory.

To move the `/var` directory to a dedicated disk or to a remote NFS directory:

1. Use the VMware vSphere client to create a virtual disk and assign it to the appliance's virtual machine.
2. Log in to the Appliance Management Console as the `vaadmin` user.
3. Click **/var Mount Configuration** .

4 Specify the hard disk information for the `/var` directory:

- **Select disk:** Select the hard disk where you want to place the `/var` directory.
- **File system type:** Specify the type of file system.

5 Click **OK**.

8.10 Reboot or Shutdown

You might need to initiate a graceful shut down or to restart the appliance for maintenance. Using the Appliance Management Console options is preferred over using a Power Off/On option in the hypervisor's VM management tool.

1 Log in to the Appliance Management Console as the `vaadmin` user.

2 In the upper right corner of the Appliance Configuration pane, click **Reboot** or click **Shutdown**.

8.11 Logout

For security reasons, you should sign out to exit your management session with the appliance, then close your web browser. Your session terminates automatically when you close your web browser.

To sign out of the Appliance Management Console:

1 In the upper-right corner of the Appliance Management Console page, next to the user name, click **Logout**.

2 Close the web browser.

9 Patching the Appliance

PlateSpin Transformation Manager Appliance provides built-in tools to help you apply field patches and patches for the Appliance. You should perform these tasks only from the Appliance Management Console, because native Linux tools are not aware of the configuration requirements and dependencies of the PlateSpin Transformation Manager services.

To access the Appliance Management Console:

1. In a web browser, specify the DNS name or the IP address for the appliance with the port number 9443.

   https://<*ptm-ipaddr-or-dns-name*>:9443

   For example:

   ```
   https://10.10.10.1:9443
   ```

   or

   ```
   https://ptm.example.com:9443
   ```

2. Specify the administrative username and password for the appliance, then click **Sign in**. The default users are `vaadmin` or `root`.

The Appliance System Configuration page displays the following options to help you manage patches to the current release version:

- Support
- Field Patch
- Online Update

9.1 Support

Use the Support tool to send configuration information to Technical Support (https://support.microfocus.com/contact/) by uploading files directly with FTP, or by downloading the files to your management workstation and sending them by an alternative method.

To send configuration files to Technical Support:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Support** .

3. Use one of the following methods to send the appliance’s configuration files to Technical Support (https://support.microfocus.com/contact/):
   - Select **Automatically send the configuration to Micro Focus using FTP** to initiate the FTP transfer of configuration information.
   - Select **Download and save the configuration file locally, then send it to Micro Focus manually** to download configuration information to your management workstation. You can then send the information to Technical Support (https://support.microfocus.com/contact/) using a method of your choice.
4. Click **OK** to complete the process.

9.2 Field Patch

Use the Field Patch option to manage patches for Transformation Manager Server software, patches for the PlateSpin Migrate Connector software for the installed instance, and security patches for the software and operating system. You can install new patches, view currently installed patches, and uninstall patches. You can download patches from the Micro Focus Patch Finder website (https://download.microfocus.com/patch/finder/).

To manage patches:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Field Patch** .
3. (Conditional) Install a downloaded patch:

   3a Download the PlateSpin Transformation Manager patch file from the Micro Focus Patch Finder website (https://download.microfocus.com/patch/finder/) to your management computer.

   3b On the Field Patch page in the **Install a Downloaded Patch** section, click **Browse**.

   3c Browse to and select the patch that you downloaded in Step 3a.

   3d Click **Install**.
4. (Conditional) Uninstall a patch:

   You might not be able to uninstall some patches.

   4a In the **Patch Name** column of the Field Patch list, select the patch that you want to uninstall.

   4b Click **Uninstall Latest Patch**.
5. (Conditional) Download a log file that includes details about the patch installation.

   5a Click **Download Log File** for the appropriate patch.
6. Click Close to exit the Field Test Patch page.

9.3 Online Update

Online Update enables you to receive patch updates for the currently installed release version of the PlateSpin Transformation Manager Appliance through a channel service.

NOTE: The Online Update page in the Appliance Management Console is reserved for patch management within the current release version only.

Use the Online Update option to register for the online patch update service from the Customer Center (https://www.microfocus.com/customercenter/). You can alternatively register with a Local Subscription Management Tool (SMT) server from which you can download the patches. You can install the received patches automatically or manually.

Use the Online Update option to manage product release patches for installed release version of Transformation Manager Server software and PlateSpin Migrate Connector software, as well as security patches for the Appliance operating system.

To activate the Update Channel, you use the same Full License key that you used to activate the product. An Evaluation key will not activate the channel. Internet access is required to register for the service or to retrieve patches through the channel.

To register for the Online Update Service:

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Online Update** .
3. If the Registration dialog does not open automatically, click the **Register** tab.
4. Specify the **Service Type**:
   - Local SMT (Go to Step 5.)
   - Customer Center (Go to Step 6.)
5. (Local SMT) Specify the following information for the SMT server, then continue with Step 7.
   - Host name such as `smt.example.com`
   - (Optional) SSL certificate URL that communicates with the SMT server
   - (Optional) Name space path of the file or directory
6. (Customer Center) Specify the following information about the Customer Center (https://www.microfocus.com/customercenter/) account for this PlateSpin Transformation Manager Appliance:
   - Email address of the account in Customer Center
   - Activation key (the same Full License key that you used to activate the product)

    - Allow data send (select any of the following)
        - Hardware Profile
        - Optional information

7. Click **Register**.

   Wait while the appliance registers with the service.

8. Click **OK** to dismiss the confirmation.

After you have registered the appliance, you can view a list of any available patches, or view a list of installed patches. You can use manual or automatic options to apply the patches to the Appliance.

To perform other actions after registration:

- **Update Now:** Click **Update Now** to trigger the download of available patches in the channel.
- **Schedule:** Configure the type of patches to download and whether to automatically agree with the licenses.

  To schedule online update:

  1. Click the **Schedule** tab.
  2. Select a schedule for download updates (**Manual**, **Daily**, **Weekly**, **Monthly**).
- **View Info:** Click **View Info** to display a list of installed and downloaded software patches.
- **Refresh:** Click **Refresh** to reload the status of patches on the Appliance.