MICRO FOCUS

PlateSpin® Transformation Manager

Appliance Guide

June 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.

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 1.1 SP1 Documentation website (https://www.netiq.com/documentation/platespin-transformation-manager-1-1/).

In addition to English, some documentation is available shortly after general availability in the Japanese national language.

Contact Information

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 page of the online documentation, or send an email to Documentation-Feedback@netiq.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1 Overview of the 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 VM also includes an installed instance of the PlateSpin Migrate Connector that is configured to work with the Transformation Manager server. For information about setting up additional instances of Migrate Connector, see "Installing, Upgrading, or Uninstalling PlateSpin Migrate Connector" in the *PlateSpin Migrate Connector Quick Start*.

1.1 Benefits of the Appliance

Delivery of PlateSpin Transformation Manager as an appliance 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 configure only what is required to deploy or 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 the Appliance Terminal Console as the `root` user. Your support representative will provide guidance on any required actions. Otherwise, there are no administrative tasks that involve `root` access or the `bash` interface.
- **Easy update.** The Appliance provides an Online Update capability to download and apply patches to the appliance.

1.2 Appliance Requirements

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

- Section 1.2.5, “Network Connectivity and Access Requirements,” on page 12
- Section 1.2.6, “Security Guidelines,” on page 15

1.2.1 Appliance Host Server

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

- “Virtualization Host Server” on page 8
- “Virtual Machine” on page 8
- “Virtual Storage” on page 9

Virtualization Host Server

PlateSpin transformation supports the following virtualization software:

- **VMware ESXi version 5.5 or higher.** The ESXi host must have a VMware enterprise license.
- **VMware vSphere Client 5.x or higher.** Use this tool to set up the hypervisor environment for the appliance VM.

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

Virtual Machine

The OVF creates a virtual machine. This section describes the VM minimum requirements.

- **Memory:** The host server must provide a minimum of 4 GB of memory for the virtual machine. This memory configuration is the appliance default.
- **Processor:** The host server must provide a minimum of 2 vCPUs for the virtual machine. This processor configuration is the appliance default.
- **IP Address Information:** During the deployment, you must provide the following IP address information for the appliance, including:
  - Static IP address
  - Network mask
  - Gateway IP address
  - DNS host name associated with the IP address
  - IP address of a DNS server
  - IP address or DNS name of the NTP server

    Micro Focus recommends setting up NTP for the VM in accordance with the *VMware Time Keeping Best Practices for Linux Guests (KB 1006427)* (https://kb.vmware.com/kb/1006427).

Virtual Storage

You must provide a boot disk and a data disk when you deploy the appliance:

- **Disk 1 Boot:** The boot partition for the appliance stores the system files, including the guest operating system, all appliance-specific software, and the appliance system event logs that are stored in the `/var` directory. The default size is 20 GB.
- **Disk 2 `/vastorage`:** The `/vastorage` partition stores the PlateSpin Transformation Manager software and PostgreSQL database, the appliance configuration information, and the Ganglia health metrics. You must create and add this virtual disk during the appliance installation. The required size is 20 GB or larger.

1.2.2 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.

- "Supported Web Browsers" on page 9
- "Supported Languages" on page 9
- "Ports and Firewalls" on page 9

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

Supported Languages

The Appliance Management Console supports English (En) and Japanese (Ja) languages in your web browser. Modify the Language setting in your web browser with your preferred language as the first in the list. For translated Online Help, also set your Language preference on www.netiq.com and allow cookies.

Ports and Firewalls

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

Table 1-1 Communications Ports for Appliance Management

Component	Port	Description
Appliance Management Console	9443 (HTTPS, secure SSL)	Use this port to securely manage the appliance.
Transformation Manager Database (PostgreSQL)	5432	If you configure a remote PostgreSQL database for the 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 appliance.
SSH	22	You can use SSH to remotely access the appliance to start, stop, or restart it without using a VMware client. SSH is disabled by default. See Section 3.4.1, “Starting, Stopping, or Restarting System Services,” on page 31.
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 3.7.3, “View Ganglia Metrics Directly Using Port 9080 (Not Secure),” on page 37.

1.2.3 Transformation Manager Web Interface

PlateSpin Transformation Manager server software is automatically installed on the Appliance. User interaction with the PlateSpin Transformation Manager Server takes place through the browser-based PlateSpin Transformation Manager Web Interface.

- “Supported Web Browsers” on page 10
- “Supported Languages” on page 11
- “Internet Access” on page 11
- “Ports and Firewalls” on page 11

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.

Supported Languages

The Web Interface supports English (En) and Japanese (Ja) languages in your web browser. Modify the Language setting in your web browser with your preferred language as the first in the list.

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 *PlateSpin Transformation Manager User Guide*.

To provide Internet access through a proxy server, you must configure the Appliance as a proxy client for that server. See "Configuring Proxy Client Settings" on page 39.

Ports and Firewalls

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

Table 1-2 *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.

Table 1-3 shows the protocol and port required for event messaging in a PlateSpin Migration Factory environment. These messages reflect events and state changes and do not contain sensitive information.

Table 1-3 *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 PlateSpin Transformation Manager Appliance, which includes a pre-installed instance of PlateSpin Migrate Connector. Open this port on all other Connector host servers, the PlateSpin Migrate servers configured for the project, and the firewalls between them.

1.2.4 PlateSpin Migrate Connector

An instance of the PlateSpin Migrate Connector is automatically installed and configured to work with all projects on the PlateSpin Transformation Manager server on 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. See the *PlateSpin Migrate Connector Quick Start*.

You can install additional instances of Migrate Connector on your SUSE Linux Enterprise Server servers in the same network as source workloads. See "Installing, Upgrading, or Uninstalling PlateSpin Migrate Connector" in the *PlateSpin Migrate Connector Quick Start*.

1.2.5 Network Connectivity and Access Requirements

Ensure that the network connections are working:

- Between the PlateSpin Migrate Connector and the source workloads
- Between the PlateSpin Migrate Connector and the PlateSpin Migrate servers
- Between the source network and target network

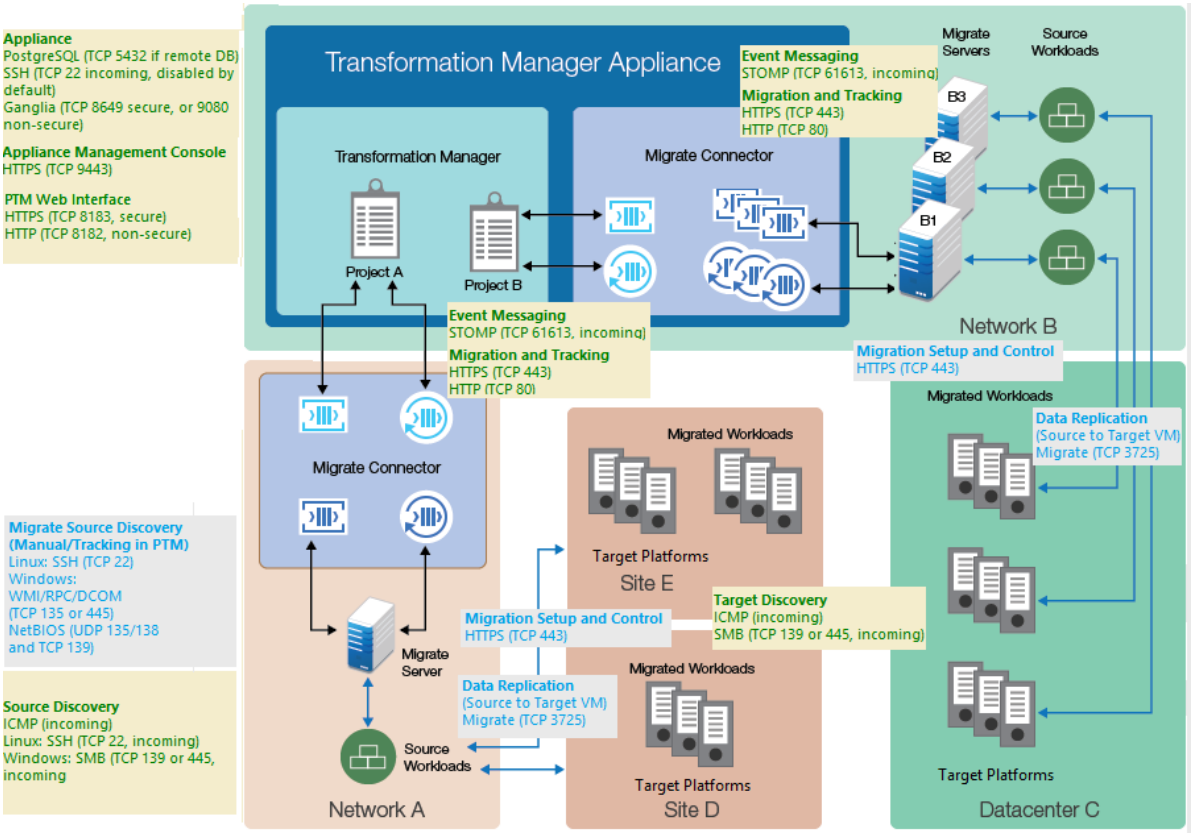
PlateSpin Migrate Connector requires network connectivity to the following resources, based on its assignment to the PlateSpin Transformation Manager server or to a specific project:

- Its assigned PTM server
- Source workloads
- Target VMware cluster hosts
- PlateSpin Migrate servers

In addition, review the security guidelines in Section 1.2.6, "Security Guidelines," on page 15.

Your environment must meet the requirements described in this section for network connectivity and access. Refer to the ports map in Figure 1-1.

Figure 1-1 *Ports Map for PlateSpin Migration Factory*



- “Event Messaging” on page 13
- “Workload Discovery” on page 14
- “Target Host Discovery” on page 14
- “Workload Migration” on page 15

Event Messaging

PlateSpin Migrate provides an event messaging service based on RabbitMQ for use in the PlateSpin Migration Factory environment. Each PlateSpin Migrate server can publish workload migration state change messages to PlateSpin Migrate Connector instances that subscribe to the service on behalf of PlateSpin Transformation Manager projects.

Table 1-3 shows the protocol and port required for event messaging in a PlateSpin Migration Factory environment. These messages reflect events and state changes and do not contain sensitive information.

Table 1-4 *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 PlateSpin Transformation Manager Appliance, which includes a pre-installed instance of PlateSpin Migrate Connector. Open this port on all other Connector host servers, the PlateSpin Migrate servers configured for the project, and the firewalls between them.

Workload Discovery

Workload discovery in PlateSpin Transformation Manager requires that you enable incoming ping (ICMP echo reply and ICMPv4-In echo request) traffic for source workloads and firewalls. PlateSpin supports only IPv4. For information about required software, network, and port settings for workload discovery, see Table 1-5.

Table 1-5 *Workload Discovery Requirements for Network Access and Communications*

Discovery Target	Network Protocols and Ports	Other Requirements
Windows workloads	◆ ICMP, incoming ◆ SMB (TCP 445 or 139)	◆ Microsoft .NET Framework 2.0 SP2, 3.5 SP1 or 4.0 ◆ Credentials with Domain Admin or built-in Administrator privileges
Linux workloads	◆ ICMP, incoming ◆ SSH (TCP 22, incoming)	Root-level access. For information on using an account other than `root`, see KB Article 7920711 (https://www.netiq.com/support/kb/doc.php?id=7920711).

Target Host Discovery

Host discovery requires that you enable incoming ping (ICMP echo reply and ICMPv4-In echo request) traffic for target VMware hosts and firewalls. PlateSpin supports only IPv4. For information about required software, network, and port settings for host discovery, see Table 1-6.

Table 1-6 *Host Discovery Requirements for Network Access and Communications*

Discovery Target	Network Protocols and Ports	Other Requirements
VMware Cluster hosts	◆ ICMP, incoming ◆ SMB (TCP 445 or 139, incoming)	VMware account with an Administrator role

Workload Migration

Table 1-7 provides the ports to open in the firewall and on each of the Migrate servers in order for PlateSpin Transformation Manager to use the Migrate REST APIs for automated migration. In addition, the Migration Server resource for Migrate server must provide a valid Credentials resource for the Migrate Administrator user.

Table 1-7 *REST API Requirements for Network Access and Communications*

REST API Traffic	Network Protocol and Port	Access
HTTPS (secure)	Port 443, TCP, incoming and outgoing	Administrator login credentials for the Migrate server
HTTP (non-secure)	Port 80, TCP, incoming and outgoing	Administrator login credentials for the Migrate server

In addition, Transformation Manager requires that your migration environment meets the PlateSpin Migrate requirements for network communications. See "Requirements for Migration" in the *PlateSpin Migrate 12.2.1 User Guide*.

1.2.6 Security Guidelines

PlateSpin Transformation Manager provides several key security options.

SSL (HTTPS) for Secure Communications

For secure connections between PlateSpin Migrate Connector and PlateSpin Transformation Manager, the Jetty SSL settings on the PlateSpin Transformation Manager Appliance VM are configured with the latest recommended security settings.

Ensure that you configure the Appliance to use port 8183 for secure communications.

SSL Certificate for Secure Communications

The installation of the PlateSpin Transformation Manager Appliance generates and installs a self-signed certificate for SSL (Secure Sockets Layer) communications. It uses the DNS name that you specify for the PlateSpin Transformation Manager Appliance. The certificate applies to the appliance and the software.

For higher security, Micro Focus recommends that you use a 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.

NOTE: The DNS name of the server must match the subject of the security certificate.

To import your signed certificate, you must provide the certificate and key, as described in "Digital Certificates" in the *PlateSpin Transformation Manager Appliance Guide*.

Antivirus Setup for Discovery

To run discovery on Windows workloads, you might need to exclude certain services, files, and folders from antivirus protection.

- **Service:** Exclude the PTM Discovery Service (`PTMDiscoverySvc.exe`) from antivirus protection.

  This service uses the `PsExec` utility to run remote commands on the target `MachineDiscoveryReader.dll`.
- **Files and Folders:** Exclude the `PlateSpinDiscovery` directory, including any subdirectories and files, from antivirus protection.

  During each discovery attempt, all binaries and services files the PTM Discovery Service creates and uses are located under the `PlateSpinDiscovery` directory in the first Windows share it discovers, such as `Admin$`.
- **Ports:** The antivirus software must not restrict any of the ports needed for discovery. For port information, see "Workload Discovery" on page 14.

Proxy Services

PTM Server is proxy aware. It can use the Proxy Client settings on the host Appliance for communications with the Micro Focus License Server. Persistent Internet access is required to license the individual workloads during the planning process. You might need to configure proxy services in a highly restrictive networking environment.

See "Configuring Proxy Client Settings" in the *Appliance Guide.*

Unique Login Credentials for Each Connector Instance

To distinguish actions initiated by the project's Connector instance, we strongly recommend that you create a unique User object to use for the Connector login credentials instead of using a real User object. Create this special user as a System user, then assign it a Project Architect role at the Project level. Create a different User object for each Connector instance with permissions appropriate for its assigned project.

Password Security for Credentials Resources

PlateSpin Transformation Manager uses industry-standard strong encryption to secure passwords in the PTM database for the Credentials resources used to access source machines and target hosts. The 16-digit key is randomly generated during the Appliance installation. The key is unique to each PTM server. As new Credentials resources are created, their passwords will be encrypted with this key.

The encryption key is stored as the `tm.encrypt.key` property in the `system.properties` file:

`/opt/microfocus/ps_transform_mgr/config/system.properties`

PTM writes the `system.properties` file to a ZIP file and saves it in the `/vastorage/conf/` folder when the appliance shuts down.

The `system.properties` file is protected by the strength of the password you set for root and other system users on the Appliance as well as other security best practices in your data center.

2 Installing and Configuring the 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 "Appliance Requirements" on page 7.

2.1 Downloading the Appliance Software

Installation files for PlateSpin Transformation Manager 1.1 and PlateSpin Migrate Connector 1.1 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 1.1 (https://download.microfocus.com/Download?buildid=vcuzrdZizRU~) in the results. Use your Micro Focus Customer Center account credentials to log in to this site.

PlateSpin Transformation Manager 1.1 and PlateSpin Migrate Connector 1.1 installation files include the following. An instance of the Migrate Connector is automatically installed on the Appliance when you install and configure the Appliance.

Download File Name	Description
`PlatespinTM.x86_64-1.1.0.`*`xxx`*`.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-1.1.0-`*`xxx`*`.noarch.rpm` Where *xxx.x* is the build number	Contains the files to install a new instance of PlateSpin Migrate Connector 1.1 on your intended Migrate Connector hosts.
`ptm_public-key.key`	Contains a PlateSpin Transformation Manager Public Key for new installs 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 Pubic 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_64-1.1.0.xxx.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. Configure the virtualization host server where you will run the appliance. Continue with Section 2.3, “Deploying the Appliance and Configuring the Virtual Environment,” on page 20.

2.2 Downloading Appliance Software Updates

PlateSpin Transformation Manager 1.1.1 updates for the version 1.1 Appliance are available through the Online Updates channel and Micro Focus Patch Finder. See Section 6, “Upgrading PlateSpin Transformation Manager from 1.1 to 1.1.1,” on page 53.

2.3 Deploying the Appliance and Configuring the Virtual Environment

Use the instructions in this section to prepare your VMware host server for the appliance. Before you begin, ensure that you understand the Section 1.2, “Appliance Requirements,” on page 7.

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 appliance.

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

   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**.

Page	Action
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 2.6.2, "Change the SCSI Controller to VMware Paravirtual SCSI for Hard Disk 2," on page 25. 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 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 2.4, "Configuring the Appliance," on page 21.

2.4 Configuring the Appliance

After you have downloaded the appliance and successfully deployed the virtual machine in the virtual environment, you are ready to configure 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 appliance, then type it again to confirm it.
Vaadmin password	Type the `vaadmin` user password that you want to set for the appliance, then type it again to confirm it. The `vaadmin` user is the preferred identity to use when you log in to the appliance. 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 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 2.5, “Configuring the PlateSpin Transformation Manager Server for the First Time,” on page 23.

2.5 Configuring the PlateSpin Transformation Manager Server for the First Time

After you install the PlateSpin Transformation Manager Appliance and configure its network settings, you are ready to configure the PlateSpin Transformation Manager Server for the first time. This configuration process uses a quick wizard that gets your system up and running. You can then make further configuration decisions, as described in Section 2.6, “Post-Installation Tasks,” on page 24.

To configure the PlateSpin Transformation Manager Server:

1. After you have installed the appliance, as described in Section 2.4, “Configuring the Appliance,” on page 21, navigate to the following URL from a web browser:

   `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 it has not been configured yet or if it detects that an update is needed. In these cases, skip Step 3.

3. Click the **Server Configuration** icon.

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

   4a 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 2-1 shows the default settings.

     Table 2-1 *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 username and password for the database user who will be created as the administrator user (default: `tmadmin`) for the PlateSpin Transformation Manager database instance.

4b Initial User Configuration

The initial user for the PlateSpin Transformation Manager Server is the System Administrator user who has all rights for configuration and management 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 this user from the Appliance Management Console. You can add another System Administrator user for the PlateSpin Transformation Manager Server if it becomes necessary to replace or augment the initial user account. See Administrative Users.

NOTE: You add and manage other users on the Users page in the PlateSpin Transformation Manager Web Interface. See "Managing Users" in the *PlateSpin Transformation Manager User Guide*.

4c 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.

5 On successful configuration, select one of the following options to continue with Section 2.6, "Post-Installation Tasks," on page 24:

- **Appliance Home:** View or set the configuration settings for the appliance. See Section 2.6.3, "View or Modify Appliance Settings," on page 25.
- **Add Certificate:** Add your signed SSL certificate for the appliance. See Section 2.6.1, "Add a Self-Signed Digital Certificate to the Appliance," on page 25.
- **Launch PlateSpin Transformation Manager Web Console:** Open the Web Interface to configure the PTM software or to set up your transformation projects. See the following:
  - Section 2.6.5, "Configure the Web Interface," on page 25
  - Section 2.6.6, "Configure Transformation Projects," on page 26

2.6 Post-Installation Tasks

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

- Section 2.6.1, "Add a Self-Signed Digital Certificate to the Appliance," on page 25
- Section 2.6.2, "Change the SCSI Controller to VMware Paravirtual SCSI for Hard Disk 2," on page 25
- Section 2.6.3, "View or Modify Appliance Settings," on page 25
- Section 2.6.4, "Configure the Appliance to Use Your Proxy Server," on page 25

- Section 2.6.5, “Configure the Web Interface,” on page 25
- Section 2.6.6, “Configure Transformation Projects,” on page 26

2.6.1 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 3.5, “Digital Certificates,” on page 32.

2.6.2 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.

2.6.3 View or Modify Appliance Settings

After you configure the appliance for the first time, you can view or modify the settings by using the Appliance System Configuration page. See Chapter 3, “Managing the Appliance,” on page 27.

2.6.4 Configure the Appliance to Use Your Proxy Server

If you have a proxy server in your network, you can optionally configure the PlateSpin Transformation Manager Appliance as a proxy client. See Section 3.15, “Configuring Proxy Client Settings,” on page 35.

2.6.5 Configure the Web Interface

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

- “Accessing the Web Interface”

- “Managing Licenses”
- “Configuring Operating Systems”

2.6.6 Configure Transformation Projects

Use the PlateSpin Transformation Manager Web Interface to plan, manage, and execute your transformation projects. See the following in the *PlateSpin Transformation Manager User Guide:*

- “Users”
- “Planning Transformation Projects”
- “Workloads”
- “Resources”

3 Managing the 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 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 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`.
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 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 the guest operating system have been upgraded. You must complete the upgrade before you can manage the appliance or the PlateSpin Transformation Manager Server.
4. Continue using the Appliance Configuration tools.

The Appliance System Configuration page displays the following options:

- Administrative Passwords
- Network
- Time
- System Services
- Digital Certificates
- Firewall
- Ganglia Configuration and Monitoring
- Storage
- /var Mount Configuration
- Reboot or Shutdown
- Logout
- Configuring Proxy Client Settings

3.1 Administrative Passwords

Use the Administrative Passwords tool to modify the passwords and SSH access permissions for the 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 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 3.4, “System Services,” on page 30.

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:

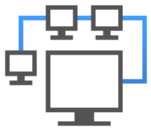
1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Administrative Passwords**  .
3. Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.
4. Click **OK**.

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**.

3.2 Network

Use the Network tool to configure settings for the DNS servers, search domains, gateway, and NICs for the 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 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**.

3.3 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 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**.

3.4 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 3.4.1, “Starting, Stopping, or Restarting System Services,” on page 31
- Section 3.4.2, “Making System Services Automatic or Manual,” on page 31

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.5 Digital Certificates

Use the Digital Certificates tool to add and activate certificates for the 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 3.5.1, “Using the Digital Certificate Tool,” on page 33
- Section 3.5.2, “Using an Existing Certificate and Key Pair,” on page 34
- Section 3.5.3, “Activating the Certificate,” on page 34

3.5.1 Using the Digital Certificate Tool

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 33.

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 3.5.3, “Activating the Certificate,” on page 34.

3.5.2 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 3.5.3, “Activating the Certificate,” on page 34.

3.5.3 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.

3.6 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 “Ports and Firewalls” on page 9.

To view firewall settings for the 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

3.7 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.

3.7.1 Configure Ganglia

Use the Ganglia Configuration tool to configure monitoring for the 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 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.

3.7.2 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 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.

3.7.3 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.

3.8 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 in Section 2.3, “Deploying the Appliance and Configuring the Virtual Environment,” on page 20. 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.

3.9 /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**.

3.10 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**.

3.11 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.

3.12 Configuring Proxy Client Settings

If you have a Proxy Server in your environment, you can enable PlateSpin Transformation Manager to use that server for Internet communications by configuring the Proxy client settings on the PlateSpin Transformation Manager Appliance and host servers of PlateSpin Migrate Connector instances. 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 3.12.1, “Configuring Proxy Client Settings for the PTM Appliance,” on page 39
- Section 3.12.2, “Configuring Proxy Client Settings for Migrate Connector Hosts,” on page 41

3.12.1 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. Log in to the Appliance via SSH, then use YaST to configure the Internet proxy client settings that the Appliance, Web Interface, and PlateSpin Migrate Connector instance will use for HTTP and HTTPS communications.

To configure Proxy client settings on the Appliance:

1 Enable the SSH protocol 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.

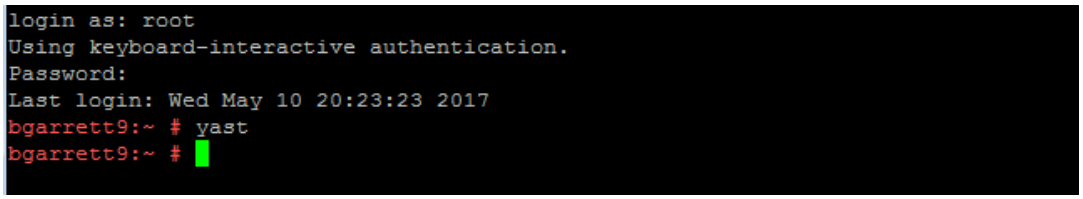
2 Configure the Proxy client settings needed to access your Proxy Server:

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.

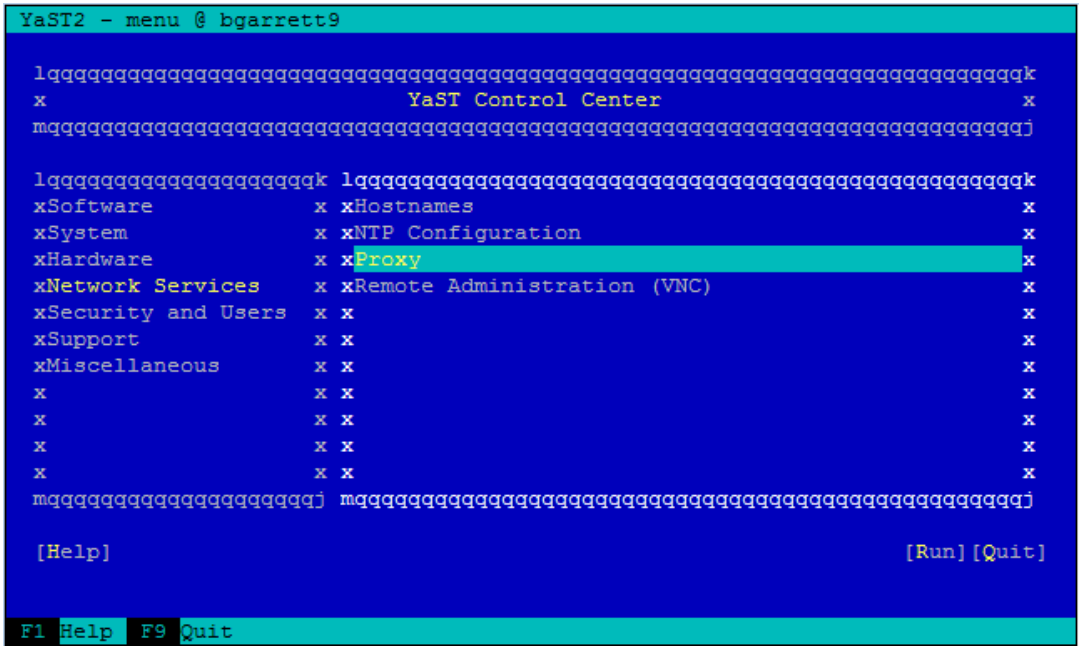
You can use any SSH tool, such as Putty (http://www.putty.org/).

2b At the terminal prompt, enter

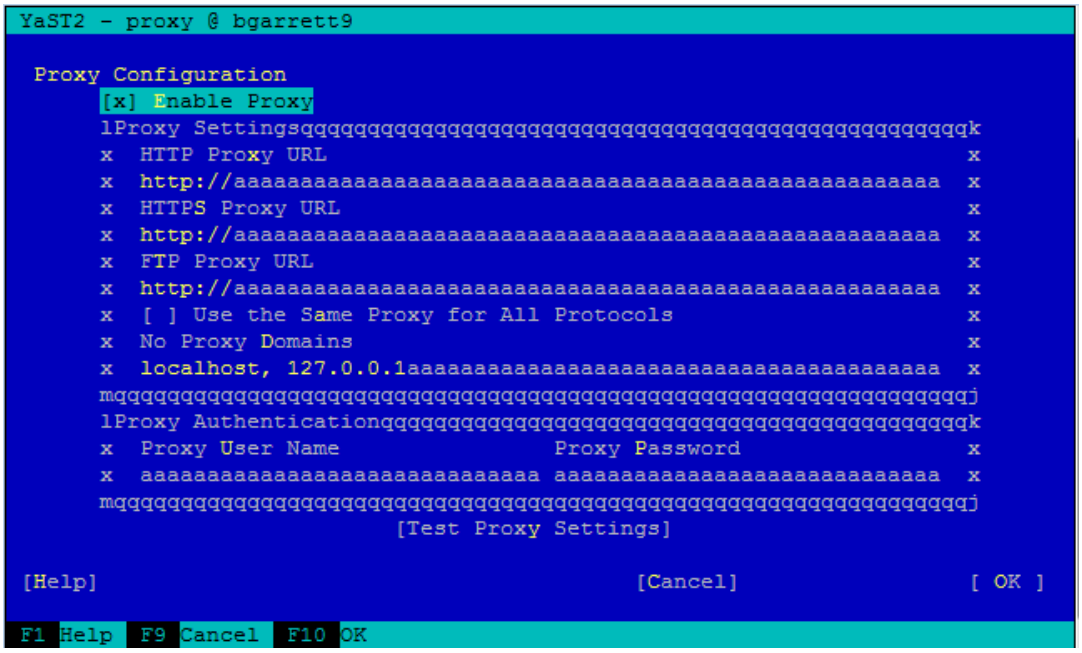
```
yast
```



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



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



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 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.

3.12.2 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. 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 that the Connector instance will use for HTTP and HTTPS communications.

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.

4 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

4.1 Support

Use the Support tool to send configuration information to Technical Support (https://www.netiq.com/support/) 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://www.netiq.com/support/):

- 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://www.netiq.com/support/) using a method of your choice.

4 Click **OK** to complete the process.

4.2 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.

4.3 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 release version only. It does not display version upgrades (*x.x.x.x*) for major, minor, support pack, and hotfix releases for the product that might be made available in the channel. For release version upgrades, follow the instructions in Section 6, “Upgrading PlateSpin Transformation Manager from 1.1 to 1.1.1,” on page 53.

Use the Online Update option to register for the online patch update service from the Customer Center (https://www.netiq.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.netiq.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.

5 Configuring the PlateSpin Transformation Manager 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 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 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 the guest operating system have been upgraded. You must complete the upgrade before you can manage the appliance or the PlateSpin Transformation Manager Server.
5. Continue using the PlateSpin Transformation Manager Server Tools.

The PlateSpin Transformation Manager Tools page displays the following options:

5.1 Initial Configuration

You can configure or reconfigure the PlateSpin Transformation Manager Server settings. You should use the Administrative Users tool and the Web Server Configuration tool 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 one of the following:

- **Server Configuration:** This option is available if the PlateSpin Transformation Manager application is not configured.
- **Overwrite Configuration:** This option is available if the PlateSpin Transformation Manager application is already configured.

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

5 Complete the configuration information.

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 5-1 shows the default settings.

  Table 5-1 *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 username and password for the database user who will be created as the administrator user (default: `tmadmin`) for the PlateSpin Transformation Manager database instance.

5b Initial User Configuration

The initial user for the PlateSpin Transformation Manager Server is the System Administrator user who has all rights for configuration and management 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 this user from the Appliance Management Console. You can add another System Administrator user for the PlateSpin Transformation Manager Server if it becomes necessary to replace or augment the initial user account. See Administrative Users.

NOTE: You add and manage other users on the Users page in the PlateSpin Transformation Manager Web Interface. See "Managing Users" in the *PlateSpin Transformation Manager User Guide*.

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**.

5.2 Administrative Users

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

NOTE: In the Web Interface, the default System Administrator can set up additional users and assign them to the Administrators group. Members of the Administrators group will also have global permissions in 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 **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**.

5.3 Web Server Configuration

The administrative users of the PlateSpin Transformation Manager Appliance can reconfigure the Jetty WebServer 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**.

5.4 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 3.4.4, “Enabling or Disabling the SSH Service,” on page 32.

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 3.4.4, “Enabling or Disabling the SSH Service,” on page 32.

5.5 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 3.4, “System Services,” on page 30.

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 Upgrading PlateSpin Transformation Manager from 1.1 to 1.1.1

PlateSpin Transformation Manager 1.1.1 is a service pack upgrade for PlateSpin Transformation Manager 1.1. To upgrade, you must have an existing installation of the PTM 1.1 Appliance, with or without interim field patches applied. Other direct upgrades are not supported. You cannot deploy version 1.1.1 directly.

PlateSpin Migrate Connector 1.1.1 is a service pack upgrade to PlateSpin Migrate Connector 1.1. You can use the download file to upgrade existing Connector instances or to install new instances.

NOTE: In the PTM 1.1.1 release, you must deploy a separate Connector instance for each project in PTM.

After you upgrade the software, you must log in as the `vaadmin` user to the Appliance Management Console (on port 9443). The PlateSpin Transformation Manager Upgrade page is presented instead of the Appliance Management Console because the Appliance detects that the RPM files for PlateSpin Transformation Manager have been modified. You must complete the upgrade before you can manage the appliance or log in to the PlateSpin Transformation Manager Web Interface.

6.1 Upgrade Requirements

PlateSpin Transformation Manager 1.1.1 supports the following components of PlateSpin Migration Factory:

- PlateSpin Transformation Manager 1.1.1
- PlateSpin Migrate Connector 1.1.1

  IMPORTANT: You cannot use PlateSpin Migrate Connector 1.1.1 with earlier versions of PlateSpin Transformation Manager and PlateSpin Migrate.

- PlateSpin Migrate 12.2.1

  PlateSpin Transformation Manager and PlateSpin Migrate Connector requires PlateSpin Migrate servers for automated migration and external migration tracking. Other discovery and planning features do not require PlateSpin Migrate servers.

Upgrade PlateSpin Transformation Manager software before you upgrade the instances of PlateSpin Migrate Connector.

NOTE: For PlateSpin Transformation Manager 1.1.1, you must deploy a separate Connector instance for each project in PTM.

6.2 Before You Upgrade

We recommend that you make a copy of the `vastorage` disk before you upgrade software on the appliance.

To copy the `vastorage` disk:

1. (Optional) Note the settings you made for your custom Theme.

   Your custom Theme files are not stored on the `vastorage` disk. If you configured a custom Theme, you should note the settings you made to your custom files. The files will not be overwritten during an upgrade, but you will need to apply the settings to the new or upgraded master Theme files after the upgrade, or if you need to roll back to a redeployed appliance. See Chapter 7, “Configuring a Custom UI Theme for the Web Interface,” on page 59.

2. Log in to the Appliance Console, then shut down the PTM service and the Migrate Connector service.

   See Section 3.4.1, “Starting, Stopping, or Restarting System Services,” on page 31.

3. Wait for the services to shut down gracefully, then log out of the Appliance Console.

4. Log in to VMware vSphere for the Appliance host, then power down the Appliance VM.

   At shutdown, PTM copies essential configuration files to the `/vastorage/conf/` folder, including the configuration for the Migrate Connector instance installed on the Appliance:

```
Archive:  vaconfig.zip
 etc/sysconfig/novell/NvlVAinit
 etc/Novell-VA-release
 usr/lib64/jvm/java/jre/lib/security/cacerts
 etc/opt/novell/ganglia/monitor/gmond.conf
 etc/opt/novell/ganglia/monitor/gmetad.conf
 etc/opt/novell/ganglia/monitor/net.d/recv.conf
 etc/opt/novell/ganglia/monitor/net.d/send.conf
 etc/sysconfig/SuSEfirewall2
 etc/sysconfig/scripts/SuSEfirewall2-custom
 etc/opt/microfocus/ps_transform_mgr/config/com.netiq.tm.backend.connpool.cfg
 etc/opt/microfocus/ps_transform_mgr/config/com.netiq.tm.backend.auth.cfg
 etc/opt/microfocus/ps_transform_mgr/config/connector.properties.save
 etc/opt/microfocus/ps_transform_mgr/config/connector.properties
 etc/opt/microfocus/ps_transform_mgr/config/version.properties
 etc/opt/microfocus/ps_transform_mgr/config/system.properties
 etc/opt/microfocus/ps_transform_mgr/config/transformationmanager-themes.cfg
 etc/opt/microfocus/ps_transform_mgr/config/pgusr.in
 etc/opt/microfocus/ps_transform_mgr/config/quartz-scheduler.cfg
 etc/opt/microfocus/ps_transform_mgr/config/system.properties.rpmnew
 etc/opt/microfocus/ps_transform_mgr/config/system.properties.save
 etc/opt/microfocus/ps_transform_mgr/config/war-tm-config.xml
 etc/opt/microfocus/ps_transform_mgr/config/security/tmKeystore.jks
 etc/opt/microfocus/ps_transform_mgr/config/security/tm_cert.der
 etc/sysconfig/postgresql
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/servlet.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/https.ini.bak
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/ssl.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/https.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/ssl.ini.bak
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/logging.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/http.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/annotations.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/jaas.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/gzip.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/servlets.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/webapp.ini
 opt/microfocus/ps_transform_mgr/tm-jetty-base/resources/logback.xml
 opt/microfocus/ps_transform_mgr/tm-jetty-base/resources/logging.properties
 opt/microfocus/ps_transform_mgr/tm-jetty-base/resources/jetty-logging.properties
 opt/microfocus/migrate_connector/config/settings.cfg
 opt/microfocus/migrate_connector/custom_callouts/post_cutover_testing_callout.py
 opt/microfocus/migrate_connector/custom_callouts/submit_validation_callout.py.rpmnew
 opt/microfocus/migrate_connector/custom_callouts/submit_validation_callout.py
 opt/microfocus/migrate_connector/custom_callouts/pre_cutover_testing_callout.py.rpmnew
 opt/microfocus/migrate_connector/custom_callouts/__init__.py
 opt/microfocus/migrate_connector/custom_callouts/pre_cutover_testing_callout.py
 opt/microfocus/migrate_connector/custom_callouts/custom_import_callout.py
```

5 In vSphere, navigate to the datastore that contains the `vastorage` disk and make a copy of it.

6 When the copy is complete, restart the Appliance, then continue with the upgrade.

See “Upgrading PlateSpin Transformation Manager” on page 56.

If the upgrade fails, you can roll back to a previous state.

1 Reinstall the previous Appliance OVF and attach the copied disk as its `vastorage` disk.

The installation uses the stored configuration files to configure the Appliance, and requires minimal configuration information, such as the `vaadmin` password. When the system comes up, it functions as it did previously.

2 (Optional) If you previously imported custom certificates, re-import them.

6.3 Downloading Software

PlateSpin Transformation Manager 1.1.1 and PlateSpin Migrate Connector 1.1.1 service pack files are available on the Micro Focus Patch Finder website under the PlateSpin Transformation Manager 1.1.1 name.

6.3.1 File Description

PlateSpin Transformation Manager 1.1.1 and PlateSpin Migrate Connector 1.1.1 service pack files include the following:

Download File Name	Description
`platespin-transformationmanager-1.1.1-`*`xxx.x`*`.x86_64.rpm` Where *xxx.x* is the build number	Contains the files to upgrade your existing installation of PlateSpin Transformation Manager 1.1. You cannot deploy version 1.1.1 directly.
`platespin-migrate-connector-1.1.1-`*`xxx.x`*`.x86_64.rpm` Where *xxx.x* is the build number	Contains the files to install a new instance of PlateSpin Migrate Connector 1.1 on your intended Migrate Connector hosts.
`ptm_public-key_1-1-1.key`	Contains a PlateSpin Transformation Manager Public Key for new installs 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 Pubic Key file to your keyring on the intended Migrate Connector host before you install the Connector RPM.

6.3.2 Download Instructions for Micro Focus Patch Finder

The upgrade RPM files for PlateSpin Transformation Manager 1.1.1 and PlateSpin Migrate Connector 1.1.1 are available on the Micro Focus Patch Finder website (https://download.microfocus.com/patch/finder/). Search for **PlateSpin Transformation Manager 1.1.1**. No license is required. A public Internet connection is required for download. Use your Micro Focus Customer Center account credentials to log in to this site.

To download the RPM files from Micro Focus Patch Finder:

1. In a web browser, connect to the Micro Focus Patch Finder website (https://download.microfocus.com/patch/finder/), and log in with your Customer Center credentials.
2. Search for PlateSpin Transformation Manager, and follow the download link for version 1.1.1.
3. Download the files to your computer:

   `platespin-transformationmanager-1.1.1-`*`xxx.x`*`.x86_64.rpm`
   `platespin-migrate-connector-1.1.1-`*`xxx.x`*`.x86_64.rpm`
   `ptm_public-key_1-1-1.key`

4. Continue with Section 6.4, “Upgrading PlateSpin Transformation Manager,” on page 56.

6.4 Upgrading PlateSpin Transformation Manager

Before you begin, download the files for PlateSpin Transformation Manager 1.1.1 and PlateSpin Migrate Connector 1.1.1 from the Micro Focus Patch Finder website (https://download.microfocus.com/patch/finder/). See Section 6.3, “Downloading Software,” on page 55.

To upgrade the PTM and Migrate Connector software on the Appliance:

1. Enable SSH on the PTM Appliance.

   See Section 3.4.4, “Enabling or Disabling the SSH Service,” on page 32

2. 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/).

3. Copy the files that you downloaded to a location on the Appliance.
4. Launch a terminal console, then navigate to the location where you copied the files.
5. Save a copy of the `/opt/microfocus/ps_transform_mgr/tm-jetty-base/start.d/ssl.ini` file, or make a note of the Jetty keystore settings for the following parameters. The default values for PTM 1.1 are shown here. Your settings might be different if you have ever made changes to the Jetty keystore using the appropriate keytool software. You will need to reset these keystore settings after the upgrade.

   ```
   # Setup a keystore and truststore
   jetty.keystore=certs/keystore
   jetty.truststore=certs/keystore

   # Set the passwords.
   jetty.keystore.password=changeit
   jetty.keymanager.password=changeit
   jetty.truststore.password=changeit
   ```

6. Import the PTM Public Key to your keyring.

   Launch a terminal, then enter one of the following commands as the root user:

```
gpg --import <ptm-public-key-filename>
```

or

```
rpm --import <ptm-public-key-filename>
```

7 Apply the PlateSpin Transformation Manager upgrade files. In the console, enter

```
rpm -Uvh platespin-transformationmanager-1.1.1-xxx.x.x86_64.rpm
```

Replace *xxx.x* with the actual build numbers.

8 Upgrade the Migrate Connector instance on the Appliance:

8a Apply the PlateSpin Migrate Connector upgrade files. In a console, enter

```
rpm -Uvh platespin-migrate-connector-1.1.1-xxx.x.x86_64.rpm
```

Replace *xxx.x* with the actual build numbers.

9 Exit the SSH session.

10 In the Appliance Management Console, complete the upgrade by running the Transformation Manager upgrade script:

10a In a web browser, connect to the PlateSpin Transformation Manager Appliance Management Console and log in as the `vaadmin` user:

https://<*ptm-server-ipaddr-or-fqdn*>:9443

10b When you are redirected to the Upgrade page, click **Complete Upgrade**, then wait for the upgrade to complete.

The upgrade automatically stops and restarts the PlateSpin Transformation Manager service and the PlateSpin Migrate Connector for PTM service.

The upgrade script performs the following tasks:

- Stops the PlateSpin Transformation Manager service.
- Applies the Transformation Manager service pack upgrade.
- Stops the PlateSpin Migrate Connector service.
- Applies the Migrate Connector service pack upgrade.
- Expands the PTM database schema and applies the changes to your PTM database.

NOTE: If necessary, the upgrade process expands the database schema and applies the schema changes to your database. The existing database values are not affected.

- Restarts the Migrate Connector service.
- Restarts the Transformation Manager service.

The process takes about 5 minutes.

11 Use a keytool to reset the Jetty keystore settings to what they were before the upgrade. Use the values you saved in Step 5.

12 (Optional) Re-configure your custom Theme.

If you configured a custom Theme, you must copy the upgraded master Theme files to your Themes folder, and then apply your preferred theme settings. See Chapter 7, “Configuring a Custom UI Theme for the Web Interface,” on page 59.

13 If you have installed instances of PlateSpin Migrate Connector on your standalone SUSE Linux Enterprise Server 11 SP4 servers, you must also upgrade Connector on those servers. See "Before You Install or Upgrade to PlateSpin Migrate Connector 1.1.1" and "Upgrading PlateSpin Migrate Connector from 1.1 to 1.1.1" in the *PlateSpin Migrate Connector Quick Start*.

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.

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.

A Documentation Updates

This section contains information on documentation content changes that were made in the English translation of this *Appliance Guide* after the initial release of PlateSpin Transformation Manager 1.1 SP1 (1.1.1).

A.1 June 2018

Location	Update
Section 1.2.5, “Network Connectivity and Access Requirements,” on page 12	This section contains information about port requirements for the PlateSpin Migration Factory environment. Duplicate information is included in the *PlateSpin Transformation Manager User Guide*.
Section 1.2.6, “Security Guidelines,” on page 15	This section contains information about security considerations for your deployment of PTM. Duplicate information is included in the *PlateSpin Transformation Manager User Guide*.
Chapter 4, “Patching the Appliance,” on page 43	The content in this section was relocated from “Managing the Appliance” to make it easier to find.
Chapter 6, “Upgrading PlateSpin Transformation Manager from 1.1 to 1.1.1,” on page 53	The content in this section was relocated from “Configuring the PlateSpin Transformation Manager Server” to make it easier to find.

A.2 May 2018

Location	Update
“Online Update” on page 45	The Online Update page is reserved for patch updates for the currently installed release version of PTM Server, Migrate Connector, or the Appliance operating system. It does not display version upgrades (*x.x.x.x*) for major, minor, support pack, and hotfix releases. For release upgrades, use the instructions in Section 6, “Upgrading PlateSpin Transformation Manager from 1.1 to 1.1.1,” on page 53.