Maintain Prime Infrastructure Server Health

Overview Dashboard

The following table describes the information displayed on the **Administration > Dashboards > System Monitoring Dashboard > Overview** dashboard.

Table 1: Administration Dashboards System Monitoring Dashboard Overview Information

To view this information...	See this dashlet
PI server's hardware and software server details.	System Information
The trend over time in CPU/Memory/Disk utilization	Live Trend Information
Status of the data cleanup jobs over the selected period.	Data Cleanup
Status of backup jobs, local and remote server backups and alarms on server backup over the selected period.	Backup Information
Physical memory and swap memory utilization displaying the set threshold limit. Also provides information on threads utilizing the memory when the threshold is breached.	Memory Utilization
CPU utilization and the set threshold limit. Also provides information on the processes and the jobs running in Prime Infrastructure that consumes more CPU when the threshold is breached.	CPU Utilization

To view this information...	See this dashlet
Disk utilization and the set threshold limit. Also provides information on the files and the tablespaces using the disk when the threshold is breached.	Disk Utilization
Virtual Domain Summary - Click on the summary icon to view the association between virtuals domains and the users. Also the members without virtual domain association. It allows you export the list of respective associations.	Virtual Domain Summary
Available disk space.	Disk Statistics
The successful restore information over the selected period, the backup name and the restoration time.	Restore Information
Top 10 tables with highest number of rows inserted.	Database Monitoring

Choose **Administration > System Settings > System Event Configuration** to set the threshold limit for CPU/Disk/Memory utilization and to configure the alarm generation and clearance monitor settings.

The Memory Utilization, Disk Utilization and CPU Utilization dashlets have threshold markers indicated in red color, and a time slider provided at the bottom to zoom-in to a particular time period. You can click the pin icon in the tool-tip to extend the tool-tip display duration.

Related Topics

Performance Dashboard

The following table describes the information displayed on the **Administration** > **Dashboards** > **System Monitoring Dashboard** > **Performance Performance** dashboard.

Table 2: Administration Dashboards System Monitoring Dashboard Performance Information

To view this information...	See this dashlet
Incoming syslogs over the set collection time frame.	Syslog
Incoming traps over the set collection time frame.	Trap
Disk read and write over the set collection time frame.	System Disk Throughput
Number of read/write requests that were issued to the server per second.	System Disk IOPS
Number of requests waiting in the server queue.	System Disk Outstanding I/O
The speed at which data is currently being transferred based on the traffic flowing through available network interfaces such as eth0, eth1, and I/O interfaces.	Network Interface Traffic
Collective information on the CPU usage, disk usage, and memory usage.	Composite View

Admin Dashboard

The following table describes the information displayed on the **Administration** > **Dashboards** > **System Monitoring Dashboard** > **Admin** dashboard.

Table 3: Administration Dashboards System Monitoring Dashboard Admin Information

To view this information...	Choose this tab...	And see this dashlet
Alarms and events issued against the Prime Infrastructure server itself, including a list of events, times events occurred, and their severities.	Health	System Alarms
General health statistics for the Prime Infrastructure server, such as the number of jobs scheduled and running, the number of supported MIB variables, how much polling the server is doing, and the number of users logged in.		System Information
The relative proportion of the Prime Infrastructure server database taken up by data on discovered device inventory ("Lifecycle Clients"), their current status and performance data ("Lifecycle Statistics"), and the server's own system data ("Infrastructure" and "DB-Index")		DB Usage Distribution
How quickly the Prime Infrastructure server is responding to user service requests for information, such device reachability, alarms and events, and so on. Shows the maximum, minimum, and average response times for each API underlying a client service.	API Health	API Response Time Summary
The trend over time in how quickly the Prime Infrastructure server is responding to user service requests.	Service Details	API Response Time Trend
The activity level for each of the logged-in Prime Infrastructure users, measured by the number of service requests each is generating.		API Calls Per Client Chart
The trend over time in the total number of service requests logged-in clients are generating,		API Request Count Trend

How to Evaluate OVA Size and System Resources

Your Prime Infrastructure system implementation should match the recommendations on appropriate OVA sizes given in the "System Requirements" section of the Cisco Prime Infrastructure Quick Start Guide (see Related Topics).

Note that the limits on devices, interfaces, and flow records given in the *Quick Start Guide* are all maximums; an OVA of a given size has been tuned to handle *no more than* this number of devices, interfaces, and flows per second. Also note that the system requirements for RAM, disk space, and processors are all minimums; you can increase any of these resources and either store more data for a longer period, or process incoming flows more quickly.

As your network grows, you will approach the maximum device/interface/flow rating for your OVA. You will want to check on this from time to time. You can do so using the information available to you on the Admin dashboards, as explained in "Monitoring Prime Infrastructure Health".

If you find Prime Infrastructure is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, we recommend that you address this using one or more of the following approaches, as appropriate for your needs:

- Recover as much existing disk space as you can, following the instructions in "Compacting the Prime Infrastructure Database".
- Add more disk space—VMware OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Prime Infrastructure server and then follow the instructions provided by VMware to expand the physical disk space (see "VMware vSphere Documentation" in Related Topics). Once you restart the virtual appliance, Prime Infrastructure automatically makes use of the additional disk space.
- Limit collection—Not all data that Prime Infrastructure is capable of collecting will be of interest to you. For example, if you are not using the system to report on wireless radio performance statistics, you need not collect or retain that data, and can disable the Radio Performance collection task. Alternatively, you may decide that you need only the aggregated Radio Performance data, and can disable retention of raw performance data. For details on how to do this, see "Specifying Data Retention by Category".
- Shorten retention—Prime Infrastructure defaults set generous retention periods for all of the data it persists and for the reports it generates. You may find that some of these periods exceed your needs, and that you can reduce them without negative effects. For details on this approach, see "Controlling Report Storage and Retention", "Specifying Data Retention by Category", and "Specifying Data Retention By Database Table."
- Off load backups and reports—You can save space on the Prime Infrastructure server by saving reports and backups to a remote server. For details, see "Using Remote Backup Repositories".
- Migrate to a new server—Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of physical or virtual appliance. Back up your existing system, then restore it to a virtual machine on the higher-rated server. For details, see "Migrating to Another OVA Using Backup and Restore".

For more details, see "System Requirements", "Cisco Prime Infrastructure Quick Start Guide" and, "VMware vSphere Documentation".

Related Topics

View the Number of Devices Prime Infrastructure Is Managing

To check the total number of devices and interfaces that Prime Infrastructure is managing, choose **Administration** > **Licenses and Software Updates** > **Licenses**.

To check the total system disk space usage, choose **Administration** > **Settings** > **Appliance**, then click the **Appliance Status** tab. Then under **Inventory**, expand **Disk Usage**.

Related Topics

How to Improve the Performance of Prime Infrastructure

You can improve Prime Infrastructure's speed and scalability using several techniques.

Related Topics

Tune the Server

You can improve Prime Infrastructure's performance and scalability by increasing the amount of RAM, CPU, and disk space allocated to the Prime Infrastructure server and its virtual machine (or VM).

Successful server tuning requires you to complete the following workflow:

1. Changes to the VM include a risk of failure. Take an application backup before making any changes to the VM (for details, see "Perform an Immediate Application Backup Using the Web GUI" in Related Topics).
2. Perform the resource modifications in the VM, then restart the VM and the server (see "Modify VM Resource Allocation Using VMware vSphere Client").

Related Topics

Modify VM Resource Allocation Using VMware vSphere Client

Use the following steps to make changes to the virtual appliance RAM, CPU or disk space resource allocations.

Be sure to back up the Prime Infrastructure server before attempting these types of changes (see "Backing Up and Restoring Prime Infrastructure" in Related Topics).

Please note that Compliance Services features will not work if you expand the RAM, CPU or disk space resource allocations after installation.

Tip For better performance: If you are changing RAM and CPU resource allocations for the virtual machine on which you run Prime Infrastructure, and you have more than one virtual machine running on the same hardware, you may also want to change your RAM and CPU resource *reservations* using the vSphere Client's **Resource Allocation** tab. For details, see "VMware vSphere documentation" in Related Topics.

Step 1 Open a CLI session with the Prime Infrastructure server (see "Connecting Via CLI").

Step 2 Stop Prime Infrastructure using the **ncs stop** command (see "Stopping Prime Infrastructure").

Step 3 Halt the VMware virtual appliance:

PIServer/admin# **halt**

Step 4 Launch the vSphere Client, right-click the virtual appliance, then click **Edit Settings**.

Step 5 To change the RAM allocation, select **Memory** and change the **Memory Size** as needed. Then click **OK**.

Step 6 To change the CPU allocation, select **CPUs** and select the **Number of Virtual Processors** from the drop-down list. Then click **OK**.

Step 7 To add a new disk (you cannot expand the space of the existing disk):

a) Click **Add**.
b) Select **Hard Disk**, then click **Next**.
c) Check **Create a new virtual disk**, then click **Next**.
d) Enter the desired **Disk Size** and specify a **Location** for the new virtual disk, then click **Next**.
e) With the Advanced Options displayed, click **Next**, then click **Finish**.

Step 8 Power on the virtual appliance (see "Restarting Prime Infrastructure")

For more details, see "Backing Up and Restoring Prime Infrastructure" and VMware vSphere Documentation.

Note Cisco Prime Infrastructure is installed only using the 1 Gbps ports. To disable the 10 Gbps ports and use the 1 Gbps ports to install Prime Infrastructure, perform the following steps.

    a. Login to **CIMC Console**.

    b. Navigate to **Compute > BIOS > Configure BIOS > Advanced > LOM and PCIe Slots Configuration**.

    c. Choose the **Disabled** option from the **PCIe Slot:MLOM OptionROM** and **PCIe Slot:MLOM Link Speed** drop-down lists.

    d. Click the **Save** button.

    e. Navigate to **Host Power**, Power Cycle the machine and then Power ON.

Related Topics

Compact the Prime Infrastructure Database

You can reclaim disk space by compacting the Prime Infrastructure database.

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI" in related topics).

Step 2 Enter the following command to compact the application database:

PIServer/admin# **ncs cleanup**

Step 3 When prompted, answer **Yes** to the deep cleanup option.

Related Topics

Configure Client Performance Settings

You can configure many client processes to improve Prime Infrastructure performance and scalability (see Related Topics).

Related Topics

Enable Automatic Client Troubleshooting

The **Administration > Settings > System Settings > Client and User > Client** page allows you to enable automatic client troubleshooting on a diagnostic channel for your third-party wireless clients running Cisco Compatible Extensions (CCX).

With this feature enabled, Prime Infrastructure will process the client ccx test-association trap that invokes a series of tests on each CCX client. Clients are updated on all completed tasks, and an automated troubleshooting report is produced (it is located in dist/acs/win/webnms/logs). When each test is complete, the location of the test log is updated in the client details pages, in the V5 or V6 tab, in the Automated Troubleshooting Report area. Click **Export** to export the logs.

When this feature is not enabled, Prime Infrastructure still raises the trap, but automated troubleshooting is not initiated.

Automatic client troubleshooting is only available for clients running CCX Version 5 or 6. For a list of CCX-certified partner manufacturers and their CCX client devices, see the Cisco Compatible Extensions Client Devices page, linked under Related Topics, below.

Step 1 Choose **Administration > Settings > System Settings** > **Client and User > Client**. The Client page appears.

Step 2 In the **Process Diagnostic Trap** area**,** select the Automatically troubleshoot client on diagnostic channel check box, then click **Save**. For more details, see Cisco Compatible Extensions Client Devices page.

Related Topics

Enable DNS Hostname Lookup

DNS lookup can take a considerable amount of time, so Prime Infrastructure has it disabled by default.

You can enable or disable the DNS lookup for client hostnames, and change how long Prime Infrastructure retains the results of previous DNS lookups in its cache.

Step 1 Choose **Administration > Settings > System Settings** > **Client and User > Client**.

Step 2 Select the Lookup client host names from DNS server check box.

Step 3 Enter the number of days that you want the hostname to remain in the cache, then click Save.

Related Topics

Configure Client Performance Settings, on page 7

How to Improve the Performance of Prime Infrastructure, on page 5

Specify How Long to Retain Client Association History Data

Client association history can take a lot of database and disk space. This can be an issue for database backup and restore functions. The retention duration of client association history can be configured to help manage this potential issue.

Step 1 Choose **Administration > Settings > System Settings** > **Client and User > Client**.

Step 2 Under Data Retention, change the following parameters as needed:

- **Dissociated Clients** —Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 1 to 30 days.

- **Client session history**—Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 7 to 365 days.

- **Number of Rows To Keep**—Enter the maximum number of client session records to maintain. The default is 8,000,000.

Step 3 Click **Save**.

Related Topics

Configure Client Performance Settings, on page 7

How to Improve the Performance of Prime Infrastructure, on page 5

Poll Clients When Receiving Client Traps/Syslogs

Under normal circumstances, Prime Infrastructure polls clients on a regular schedule, every few minutes, identifying session information during the poll. You can also choose to have Prime Infrastructure poll clients immediately whenever traps and syslogs are received from them. This helps you discover new clients and their sessions quickly.

This option is disabled by default, as it can affect Prime Infrastructure performance. Busy networks with many clients can generate large amounts of traps and syslogs, especially during peak periods when clients are

roaming and associating/disassociating often. In this case, polling clients every time you receive a trap or syslog may be an unnecessary processing burden.

If you enable the Wireless Polling Clients when Receiving Client Traps/Syslogs option, Prime Infrastructure enables Client Authentication, Client Deauthentication, and Client Disassociate Traps on the WLC even if you previously disabled the traps on the WLC. Prime Infrastructure triggers the WLC Sync operation, which enables the client traps on WLC.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **Client**.

Step 2 Select the Poll clients when client traps/syslogs received check box. Prime Infrastructure will poll clients as soon as a trap or syslog is received, to identify client sessions.

Step 3 Click **Save**.

Related Topics

Configure Client Performance Settings, on page 7

How to Improve the Performance of Prime Infrastructure, on page 5

Save Client Traps as Events

In some deployments, Prime Infrastructure might receive large amounts of client association and disassociation traps. Saving these traps as events can cause slow server performance. In addition, other events that might be useful could be aged out sooner than expected because of the amount of traps being saved.

Follow the steps below to ensure that Prime Infrastructure does not save client association and disassociation traps as events.

Step 1 Choose **Administration > Settings > System Settings > Client**.

Step 2 Unselect the **Save client association and disassociation traps as events check box**.

Step 3 Click **Save** to confirm this configuration change. This option is disabled by default.

Related Topics

Configure Client Performance Settings, on page 7

How to Improve the Performance of Prime Infrastructure, on page 5

Save 802.1x and 802.11 Client Traps as Events

You must enable **Save 802.1x and 802.11 client authentication failed traps as events** for debugging purposes.

Step 1 Choose **Administration > Settings > System Settings > Client**.

Step 2 Select the **Save 802.1x and 802.11 client authentication fail traps as events** check box.

Step 3 Click **Save** to confirm this configuration change.

Related Topics

Configure Client Performance Settings, on page 7

How to Improve the Performance of Prime Infrastructure, on page 5

Enable Enhanced Client Traps

To enable enhanced client traps:

Step 1   Choose **Administration** > **Settings** > **System Settings** > **Client and User** > **Client**.

Step 2   Select the Discover Clients from enhanced client traps check box.

Step 3   Make sure that the Prime Infrastructure server is registered as a Trap receiver on Cisco WLC for receiving Client traps. The following trap flags need to be enabled on the devices for enhanced client trap to work:

- config trapflags client enhanced-802.11-associate enable

- config trapflags client enhanced-802.11-deauthenticate enable

- config trapflags client enhanced-authentication enable

- config trapflags client enhanced-802.11-stats enable

Step 4   To log the incoming enhanced client traps on the Prime Infrastructure side, you can enable client trap logging via ssh to root shell. This generates clientTraps.log file under the /opt/CSCOlumos/logs file.

- /opt/CSCOlumos/bin/setLogLevel.sh com.cisco.client.traps TRACE

Note   Enhanced clients traps from Prime Infrastructure is supported from WLC version 8.0 onwards.

Optimize Memory for Assurance Processing

Prime Infrastructure's Assurance features depend heavily on high-volume NetFlow data forwarded to the Prime Infrastructure server by devices, including NAMs. Because Prime Infrastructure always aggregates NetFlow data before storing it, supporting Assurance features with appropriate data is a memory-intensive process.

With more working memory to hold NetFlow data during aggregation, Prime Infrastructure can get this job done faster and more efficiently. This can lead to important performance improvements if your organization licenses Assurance features and makes heavy use of them.

Prime Infrastructure offers features to help you:

- Determine how much memory is currently allocated to Assurance-related data processing, and how completely individual Assurance features are using that memory pool.
- Increase the default pool of memory used to process Assurance-related data.
- Balance the memory allocated to individual Assurance features, so those with the greatest demand for memory get what they need.

The amount of performance improvement you can get from using these features depends on the memory available and how you use Assurance features, but can be substantial. For example: Given a Prime Infrastructure Professional implementation with the recommended minimum hardware Prime Infrastructure can process up to 414,000 NetFlow host records in a single five-minute aggregation cycle. With Assurance memory optimization, maximum processing for the same type of data is closer to 800,000 records per cycle.

You can increase the Assurance memory pool without balancing Assurance memory allocations, and vice versa. But using these two optimization options together is the best way to improve Prime Infrastructure performance when Assurance features are used.

Related Topics

Monitor Assurance Memory Allocation and Demand

You can quickly see Prime Infrastructure's current Assurance-related memory allocation and usage.

Step 1   Select **Services > Application Visibility & Control > Data Sources**.

Step 2   Select the text link **Assurance Memory Statistics** (in the upper right corner of the page). Prime Infrastructure displays:

- The current memory allocation in megabytes for each of the main Assurance feature categories, including Traffic, Performance Routing, Applications, Voice-Video data, Device Health, Lync and other data.

- The usage of each area's memory allocation over the last 24 hours. The percentage represents the peak memory usage over that period (that is, if 100 percent of the memory allocation is used at any point in the past 24 hours, the usage percentage shown will be 100 percent).

Related Topics

Increase the Assurance Memory Pool Via CLI

You can use the Prime Infrastructure command line to allocate more memory to all types of Assurance-related data processing. Note that using the **ncs tune-resources assurance** command requires a server restart. Once restarted, the server will increase the total pool of memory allocated to all Assurance-related data processing.

Step 1   Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI").

Step 2   Enter the following command:

PIServer/admin# **ncs tune-resources assurance**

Step 3   Restart the Prime Infrastructure server (see "Restart Prime Infrastructure").

Related Topics

How to Balance the Assurance Memory Allocation

You can use the Prime Infrastructure interface to automatically balance the allocation of the total Assurance memory pool to individual categories of Assurance-related data processing, ensuring that those Assurance features that need memory the most are getting it.

Step 1 Select **Services > Application Visibility & Control > Data Sources**.

Step 2 Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).

Step 3 Click **Rebalance**.

Prime Infrastructure will change Assurance memory allocations to individual features as needed, reducing allocations for less-used features and increasing allocations for features where usage over the past 24 hours was at or near 100 percent.

Related Topics

Reset Assurance Memory Allocation

You can use the Prime Infrastructure interface to cancel Assurance memory balancing, returning the allocation for each Assurance-related feature to its default value.

Step 1 Select **Services > Application Visibility & Control > Data Sources**.

Step 2 Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).

Step 3 Click **Reset**.

Related Topics

Reset the Assurance Memory Pool

You can use the Prime Infrastructure command line to return the Assurance memory pool to the default allocation, disabling all changes created using the **ncs tune-resources assurance** command explained in "Increase the Assurance Memory Pool Via CLI".

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI").

Step 2 Enter the following command:

PIServer/admin# **ncs tune-resources default**

Step 3 Restart the Prime Infrastructure server (see "Restart Prime Infrastructure").

Related Topics

Manage Data Sources

Prime Infrastructure depends on a variety of sources for accurate gathering and reporting of device, performance and assurance data. These sources include specialized monitoring devices such as NAMs, and protocols running on normal devices, such as Cisco Medianet, NetFlow, Flexible NetFlow, Network Based Application Recognition (NBAR), Performance Monitoring (PerfMon), and Performance Agent.

You will want to manage these sources to ensure that only the correct data is gathered from active sources. The Data Sources page allows you to review your current data sources, and delete those that are no longer active.

For details on the data sources used in dashlets, see "Advanced Monitoring" in Related Topics. For details on setting up individual data sources, see the data-source configuration sections of "Administrator Setup Tasks", also listed in Related Topics.

Related Topics

View Current Data Sources

Use the Data Sources page to review Prime Infrastructure's current data sources. Access to this page requires administrator privileges

Select **Services > Application Visibility & Control > Data Sources**. Prime Infrastructure displays a summary page that lists each device data source's:

- **Device Name**–The host name of the data source

- **Data Source**–The IP address of the data source.

- **Type**–The type of data the source is sending to Prime Infrastructure (e.g., "Netflow").

- **Exporting Device**–The IP address of the device exporting the data to Prime Infrastructure.

- **Last 5 min Flow Read Rate**–The amount of data Prime Infrastructure has received from this source during the last five minutes.

• **Last Active Time**–The latest date and time that Prime Infrastructure received data from this source.

For each Cisco NAM data collector sources, the page lists:

• **Name**–The host name of the NAM.

• **Type**–The type of data the NAM is collecting and sending to Prime Infrastructure (e.g., "Cisco Branch Routers Series Network Analysis Module").

• **Host IP Address**–The IP address of the NAM.

• **Data Usage in System**–Whether the data forwarded by this NAM is enabled for use in Prime Infrastructure.

• **Last Active Time**–The latest date and time that Prime Infrastructure received data from this NAM.

Related Topics

Delete Data Sources

Use the Data Sources page to delete inactive Prime Infrastructure data sources. Access to this page requires administrator privileges.

Note that you cannot delete a NetFlow data source until seven full days have elapsed without receipt of any data from that data source. This delay helps protect the integrity of NetFlow data (which Prime Infrastructure identifies and aggregates according to the source) by giving network operators a full week to ensure that the data source has been retired. If the source remains active during that period and sends data to Prime Infrastructure, data from that source will still be identified and aggregated properly with other data from the same source (instead of being identified as a new source).

Step 1   Select **Services > Application Visibility & Control > Data Sources**.

Step 2   Select the checkbox next to the inactive data source you want to delete.

Step 3   Click **Delete**.

Step 4   Click **OK** to confirm the deletion.

Related Topics

Special Administrative Tasks

Prime Infrastructure provides administrators with special access in order to perform a variety of infrequent tasks, including

• Connecting to the server via an SSH command-line interface (CLI) session.
• Changing server hardware setup and resource allocations.
• Starting, stopping, and checking on the status of Prime Infrastructure services.

- Running Prime Infrastructure processes accessible only via the CLI.
- Managing access rights, including changing passwords for user IDs with special tasks.
- Removing or resetting Prime Infrastructure.

Related Topics

How to Connect Via CLI

Administrators can connect to the Prime Infrastructure server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Prime Infrastructure CLI. These include commands to start the server, stop it, check on its status, and so on.

Note Disabling the SSH legacy ciphers may impact associating with the Prime Infrastructure that utilizes the legacy SSH client.

Before you begin

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Prime Infrastructure server.

Step 1 Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Prime Infrastructure physical or virtual appliance.

Step 2 Log in as appropriate: If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Prime Infrastructure server. Then initiate the connection. If you are using a command-line client or session: Log in with a command like the following:[localhost]# ssh username@IPHost -Whereusername is the user ID of a Prime Infrastructure administrator with CLI access to the server.IPHost is the IP address or host name of the

Prime Infrastructure server or appliance. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.

Prime Infrastructure will then prompt you for the password for the administrator ID you entered.

Step 3   Enter the administrative ID password. Prime Infrastructure will present a command prompt like the following: PIServer/admin#.

Step 4   If the command you need to enter requires that you enter "configure terminal" mode, enter the following command at the prompt:

PIServer/admin# configure terminal

The prompt will change from PIServer/admin# to PIServer/admin/conf#.

Related Topics

Special Administrative Tasks, on page 14

Start Prime Infrastructure

To start Prime Infrastructure:

Step 1   Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI").

Step 2   Enter the following command to start the Prime Infrastructure server or appliance:

PIServer/admin# **ncs start**

Related Topics

Check Prime Infrastructure Server Status

You can check on the status of all Prime Infrastructure server or appliance processes at any time, without stopping the server. Technical Assistance personnel may ask you to perform this task when troubleshooting a problem with Prime Infrastructure.

You can also check on the current health of the server using the dashlets on the Admin Dashboard (see "Monitoring Prime Infrastructure Health").

You can check on the status of High Availability options enabled on the server using the command **ncs ha status** (see "Checking High Availability Status").

Step 1   Open a CLI session with the Prime Infrastructure server (see "Connecting Via CLI").

Step 2   Enter the following command to display the current status of Prime Infrastructure processes and services:

PIServer/admin# **ncs status**

For more details, see "Checking High Availability Status".

Related Topics

Check Prime Infrastructure Version and Patch Status

You can check on the version of a Prime Infrastructure server and the patches applied to it at any time, without stopping the server. You will usually need to do this when upgrading or patching the server software.

Step 1   Open a CLI session with the Prime Infrastructure server (see "How to Connect via CLI").

Step 2   Enter the following command to display the current status of Prime Infrastructure processes and services:

PIServer/admin# **show version**

Related Topics

Stop Prime Infrastructure

You can stop a Prime Infrastructure server or appliance at any time using the command line interface. Any users logged in at the time you stop Prime Infrastructure will have their sessions stop functioning.

Step 1   Open a CLI session with the Prime Infrastructure server (see "How to connect via CLI").

Step 2   Enter the following command to stop the Prime Infrastructure server or appliance:

PIServer/admin# **ncs stop**

Related Topics

Restart Prime Infrastructure Using CLI

Step 1   Open a CLI session with the Prime Infrastructure server (see "How to Connect via CLI").

Step 2   Enter the following command to stop the Prime Infrastructure server or appliance:

PIServer/admin# **ncs stop**

Step 3   Wait for the previous command to complete.

Step 4   Enter the following command to restart the Prime Infrastructure server or appliance:

PIServer/admin# **ncs start**

Related Topics

Restart Prime Infrastructure Using GUI

To restart the Prime Infrastructureserver from the server GUI, do the following.

Before you begin

You must have Root or Super User privilege to restart the Prime Infrastructure server using GUI.

Step 1   Choose **Administration > System Settings > Server**.

Step 2   Click **Restart Prime Infrastructure**.

Step 3   Check the Restart acknowledgment check box in the pop-up window and click **Restart**.

Related Topics

How to Remove Prime Infrastructure

You may need to remove Prime Infrastructure in preparation for a clean "from scratch" re-installation. You can do so by following the steps below

Note that this procedure will delete all your existing data on the server, including all server settings and local backups. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

Step 1   Stop the server (see "Stop Prime Infrastructure").

Step 2   In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.

Step 3   Power off the virtual appliance.

Step 4   Right click on the powered-off virtual appliance and select **Delete from Disk option**.

Related Topics

Reset Prime Infrastructure to Defaults

You may need to reset the installed Prime Infrastructure server to factory defaults, removing all user data and customizations, but preserving the installation itself. You can do so by following the steps below.

Note that this procedure will delete all your existing data on the server host except for the default settings supplied with Prime Infrastructure. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

Step 1 Stop the server (see "Stop Prime Infrastructure").

Step 2 Download the installation ISO image appropriate for your installed version of the Prime Infrastructure virtual or physical appliance server software and burn it to DVD (see "How to Get the Installation ISO Image").

Step 3 Power off the virtual appliance.

Step 4 Reinstall the appliance or OVA by booting the host from the DVD.

Related Topics

Change the Prime Infrastructure Host Name

Prime Infrastructure prompts you for a host name when you install the server. For a variety of reasons, you may find there is a mismatch between the host name on the Prime Infrastructure server and the host name elsewhere. If so, you can recover without reinstalling by changing the host name on the server.

Note Setting the hostname using **hostnamectl** changes the uppercase letters to lowercase. Although Redhat 7 and CentOS 7 provide **hostnamectl** to set the hostname permanently, the real hostname will only be lowercase even if the users specify any uppercase letters.

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI"). Be sure to enter "configure terminal" mode.

Step 2 Enter the following command:

PIServer/admin(config)# **hostname** *newHostName*

Where *newHostName* is the new host name you want to assign to the Prime Infrastructure server.

Step 3 Restart the Prime Infrastructure server using the **ncs stop** and **ncs start** commands, as explained in "Restart Prime Infrastructure" .

Related Topics

Enable the FTP User

To use Prime Infrastructure as an FTP server for file transfers and software image management, an administrator must configure an FTP account. Use the steps below to enable the account and set a password for it.

After you enable the ftp-user, you can FTP files to and from the /localdisk/ftp folder on standalone or, if configured, High Availability primary servers only. You cannot use change directory (cd) or list directory (ls) functionality with ftp-user.

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI").

Step 2 Enter the following command:

PIServer/admin#**ncs password ftpuser ftp-user password password**

Where:

- **ftp-user** is the username for FTP operation.

- **password** is the login password for **ftp-user**.

    Note   The username for FTP must be **ftp-user**.

For example:

pi-system-999/admin# ncs password ftpuser root password MyPassword

Updating FTP password.

Saving FTP account password in credential store

Syncing FTP account password to database store - location-ftp-user

Syncing FTP account password to system store

Completed FTP password update

pi-system-999/admin#

Related Topics

Change the Root User Password

Administrators can change the password associated with this special administrative ID.

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI") in Related Topics.

Step 2 Enter the following command:

PIServer/admin# **ncs password root password** *password*

Where *password* is the root user login password. You can enter a password not exceeding 80 characters.

For example:

PIServer/admin# ncs password root password #password#

pi-system-198/admin# ncs password root password #password#

Password updated for web root user

pi-system-198/admin#

Related Topics

Change the Admin Password using CLI

A new Cli command "change-password" is introduced. Using this user can change their own passwords. This command is available for all roles.

The following CLI users roles are applicable:

- Super-user (admin): Only one super-user is allowed which is created during the initial setup.

- Security-admin: Has highest privilege after super user.

- Network-admin: Has privilages to do network related configuration

- User: Has privilages for read only permissions.

Step 1   Open a CLI session with the Prime Infrastructure.

Step 2   Enter the following command:

pi-cluster-54/admin# change-password

Changing password for user admin

Changing password for admin.

(current) UNIX password

Note   When upgrading from previous 3.7 releases:

- User with name "admin" is converted to Super-user (admin).

- Users name which does not contain "admin" account from which upgrade is performed gets coverted to super-user(admin).

- All the other admin users are converted to security-admin.

How to Recover Administrator Passwords on Virtual Appliances

You can recover (that is, reset) administrator passwords on Prime Infrastructure virtual machines (also known as OVAs) installed on your own hardware.

Before you begin

Ensure that you have:

- Physical access to the Prime Infrastructure server.

- A copy of the installation ISO image appropriate for your version of the software. See "How to Get the Installation ISO Image" in Related Topics.

- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. You should avoid accessing ESX directly from the vSphere client.

Step 1   Launch your VMware vSphere Client and connect to the ESXi host or vCenter server.

Step 2   Upload the installation ISO image to the data store on the OVA virtual machine, as follows:

a) In the vSphere Server, click **Inventory > Summary > Datastores**.
b) On the **Objects** tab, select the datastore to which you will upload the file.
c) Click the **Navigate to the datastore file browser** icon.
d) If needed, click the **Create a new folder** icon and create a new folder.
e) Select the folder that you created or select an existing folder, and click the **Upload a File** icon.

    If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.

f) On the local computer, find the ISO file and upload it.
g) Refresh the datastore file browser to see the uploaded file in the list.

Step 3   With the ISO image uploaded to a datastore, make it the default boot image, as follows:

a) Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Power Off**.
b) Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
c) Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
d) Under **Device Status,** select **Connect at power on**.
e) Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
f) Click **OK**.
g) In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
h) In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.

Step 4   Follow the steps below to reset a server administrator password:

a) Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
b) Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
c) Enter the number shown next to the administrator username for which you want to reset the password.
d) Enter the new password and verify it with a second entry.
e) Make sure to disconnect ISO image before confirming the changes using the vSphere client.
f) Click the CD icon and select Disconnect ISO image.
g) Enter **Y** to save your changes and reboot.

Step 5   Log in with the new administrator password.

Related Topics

How to Recover Administrator Passwords on Physical Appliances

You can recover (reset) administrator passwords on Prime Infrastructure physical appliances.

Before You Begin

Ensure that you have:

- Physical access to the Prime Infrastructure appliance.
- A copy of the appliance recovery CD that was supplied with the shipped appliance.

If you have lost the appliance recovery CD, download and burn a DVD copy of the ISO image, as explained in "How to Get the Installation ISO Image". You can then use the DVD to reset administrator passwords on the appliance (see "How to Recover Administrator Passwords on Virtual Appliances" for detailed steps).

You can reset the password using,

- **Console:** KVM Console (Other console options are VGA Console and Serial Console/Serial Over Lan-SOL)
- **DVD mount option:** KVM mapped DVD (Other mount options are CIMC mapped DVD and Physical External DVD)

See Cisco Prime Infrastructure Hardware Installation Guide for additional information.

To recover the password using KVM Console, follow these steps:

Step 1   Launch Cisco Integrated Management Controller .

Step 2   Choose **Server > Summary** from the left navigation pane.

Step 3   Under **Actions**, click **Launch KVM Console**.

Step 4   In the console, choose **Virtual Media > Activate Virtual Devices**.

Step 5   Select **Accept the session** radio button and click **Apply**.

Step 6   In the console, choose **Virtual Media > Map CD/DVD**.

Step 7   Browse to the location of the Prime Infrastructure ISO image and click **Map Device**.

Step 8   In the console, choose **Power > Reset System(warm boot)**.

Step 9   A confirmation message appears. Click **Yes**.

Step 10   The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.

You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.

Step 11   Select the desired DVD mount option and in this case, you must select **Cisco vKVM-Mapped vDVD1.22**.

Step 12   The vSphere client displays a list of boot options. Enter **3** to select the **Recover administrator password (Keyboard/Monitor)** boot option.

> **Note**   If you are using Serial Console to recover password, then you must enter **4** to select the **Recover administrator password (Serial Console)** boot option.

Step 13   The vSphere client displays a list of administrator user names. Enter the number shown next to the administrator user name for which you want to recover (reset) the password and press **Enter**.

Step 14   Enter the new password and verify it with a second entry.

Step 15   Enter **Y** to save your changes and reboot the system.

Step 16   Login to the admin CLI with the new administrator password.

> **Note**   You can follow the same steps to recover password using VGA console and Serial console.

To recover the password using Serial Console/Serial Over Lan-SOL, follow these steps:

Step 1   Launch Cisco Integrated Management Controller server using SSH .

```
# ssh admin@(server IP)
Enter the admin password
```

Step 2   Map the ISO image.

```
C220-FCH1840V0BL# scope vmedia
C220-FCH1840V0BL /vmedia # map-www <VOLUME_NAME> <LOCATION> <ISO_FILE>
Server username: anonymous
Server password:
Confirm password:
C220-FCH1840V0BL /vmedia # show mappings
Volume          Map-Status                Drive-Type Remote-Share            Remote-File
     Mount-Type
--------------- ----------------------- ---------- ----------------------- -----------------------
 -------- -----------------------
<VOLUME_NAME>   OK                        CD         <LOCATION> <IMAGE_NAME> www
C220-FCH1840V0BL /vmedia #
```

Step 3   Reboot the server:

```
# scope chasis
# power off
 This operation will change the server's power state.
 Do you want to continue?[y|N]y
#
#
# power on
  This operation will change the server's power state.
  Do you want to continue?[y|N]y
# exit
```

Step 4   Connect to Serial Over Lan Console.

```
# scope sol
# show detail
Serial Over LAN:
 Enabled: yes
 Baud Rate(bps): 9600
```

```
 Com Port: com0
# set enabled yes
# set baud-rate 9600
# commit

# connect host // to connect sol cosole
```

Step 5   The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.

You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.

Step 6   Select the desired DVD mount option and in this case, you must select **Cisco CIMC-Mapped vDVD1.22**.

Step 7   The vSphere client displays a list of boot options. Enter **4** to select the **Recover administrator password (Serial Console)** boot option.

> **Note**   To recover administrator password for Gen 3 appliances, it is recommended to use Serial Over Lan (Serial console)

Step 8   The vSphere client displays a list of administrator user names. Enter the number shown next to the administrator user name for which you want to recover (reset) the password and press **Enter**.

Step 9   Enter the new password and verify it with a second entry.

Step 10   Enter **Y** to save your changes and reboot the system.

Step 11   Login to the admin CLI with the new administrator password.

How to Recover Administrator Passwords on Hyper-V Virtual Appliances

You can recover (reset) administrator passwords on Prime Infrastructure Hyper-V Virtual appliances.

Before You Begin

Ensure that you have:

- Physical access to the Prime Infrastructure appliance.
- A copy of the installation ISO image appropriate for your version of the software. See How to Get the Installation ISO Image, on page 26.
- Access to the Hyper-V Machine, and to the Hyper-V manager. If you do not have the access, get help from your Hyper-V administrator.

Step 1   Launch your Hyper-V Machine and make sure ISO image available in your Hyper-V Machine.

Step 2   Connect to the Hyper-V Manager.

   a) Right-click the virtual machine for which you want to reset the password and select **Connect**.
      The **Virtual Machine Connection** window opens.
   b) Choose **Media > DVD Drive > Insert Disk**.
   c) Browse and select the ISO image.
   d) Turn Off and Start the virtual machine as follows:

      - Choose **Action > Turn Off**.

      - Click **Turn Off** in the **Turn Off Machine** pop-up.

       • Choose **Action > Start**.

Step 3   The virtual machine will boot from the ISO image and will display a list of boot options.

    a) Enter 3 (The option for recovering Administrator password)

    b) Enter the number shown for the administrator username for which you want to reset the password.

    c) Enter the new password and verify it with a second entry.

    d) Enter Y to save your changes and reboot.

    e) Wait until the machine gets rebooted.

Step 4   Log in with the new administrator password.

How to Get the Installation ISO Image

Copies of the Prime Infrastructure installation ISO image are needed for some special maintenance operations, such as resetting administrator passwords.

Prime Infrastructure ISO image files have the format PI-APL-**version**-K9.iso , where **version** is the version number of the product. The version number will often contain extended numbering indicating the patch level of the product. For example: If you were using a fully-updated version of Prime Infrastructure 3.7, you would must download the PI-APL-3.7.0.0.XXX-1-K9.iso from Cisco.com.

If you do not have a copy of the ISO image, you can download it from Cisco.com using the steps below:

Step 1   On a browser with internet access, link to the Cisco Software Download Navigator (see Related Topics).

Step 2   Use the **Find** box to search for "Cisco Prime Infrastructure".

Step 3   From the results list, select the software version you are using.

Step 4   Select **Prime Infrastructure Software** to display the list of ISOs and other downloadable image files for that software version.

Step 5   Download the ISO image from the page.

Step 6   When the download is complete, check that the MD5 checksum of the downloaded file matches the checksum shown for the file on its Cisco.com download page. If the checksums do not match, the file is corrupt, and you will need to download it from Cisco.com again.

Step 7   If you need the ISO image on disk: Burn the ISO image to a Dual Layer DVD using DVD authoring software. For reliable results, we recommend that you conduct the burn at single (1X) speed and with the "Verify" option turned on.

For more details, see https://software.cisco.com/download/navigator.html and Cisco Prime Infrastructure 3.7 Appliance Hardware Installation Guide

Related Topics

Special Administrative Tasks, on page 14

How to Update Prime Infrastructure With Latest Software Updates

Cisco provides updates to Prime Infrastructure software periodically. These updates fall into the following categories:

- Critical Fixes—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- Device Support—Adds support for managing devices which Prime Infrastructure did not support at release time. These updates are published on a monthly basis.
- Add-Ons—Provide new features, which can include new GUI screens and functionality, to supplement the Prime Infrastructure version you are using.

For details on how to find these updates, and how to get notifications when they are released, see "View Installed and Available Software Updates" in Related Topics.

The update notifications that Prime Infrastructure displays are based on the Notification Settings you specify using **Administration > Settings > System Settings > Software Update**. For details, see "Configuring Software Update Notifications".

For details on installing these updates, see "Install Software Updates".

For details on streamlining your software update notifications and installations using your Cisco.com account, see "How to Use Your Cisco.com Account Credentials with Prime Infrastructure".

Related Topics

View Installed and Available Software Updates

Prime Infrastructure allows you to:

- Receive notifications when new software updates become available.
- Modify how and when you are notified that new software updates are available.
- View the details of each update.
- See which software updates have been installed.

The following topics explain how to perform each of these tasks.

Related Topics

How to Get Software Update Notifications

When properly configured, Prime Infrastructure will notify you automatically when new software updates are available.

Step 1 Choose **Administration > Settings > System settings > Account Settings**.

Step 2 Enter a valid Cisco.com user name and password.

Step 3 Click **Save**.

Step 4 Choose **Administration > Settings > System Settings > General > Software Update**.

Step 5 Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.

Step 6 Click **Save**.

To see notifications: Click on the notifications icon at the top right, next to the alarms icon.

Related Topics

Configure Software Update Notifications

You can modify the update notifications that Prime Infrastructure displays on the **Administration > Software Update** page. For example, if you do not want to install any updates to Prime Infrastructure, you can disable all notification and prevent Prime Infrastructure from displaying notifications of available updates.

Step 1 Choose **Administration > Settings > System Settings > General > Software Update**.

Step 2 Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.

Step 3 Click **Save**.

Related Topics

View Details of Installed Software Updates

Step 1 Choose **Administration Settings > Licenses and Software Updates > Software Update**.

Step 2 Click the **Updates** tab to see the Name, Type, Version, Status and Date of each installed software update.

To filter this list, click the Filter icon at the right side of the Updates tab and select the categories of installed updates you want to see.

Step 3   Click the **Files** tab to see the list of installed UBF files and downloaded UBF files which have yet to be installed.

To delete a software update file that has not yet been installed, select the file and click **Delete**.

Related Topics

View Installed Updates From the Login Page

Step 1   Launch or log out of Prime Infrastructure. The login page displays.

Step 2   Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.

Step 3   Click the **Close** button to close the popup list.

Related Topics

View Installed Updates From the About Page

Step 1   Click the settings icon at the upper right corner of any Prime Infrastructure page.

Step 2   Click **About Prime infrastructure**. The About page appears, listing the version of the product and other details.

Step 3   Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.

Step 4   Click the **Close** button to close the popup list.

Related Topics

Install Software Updates

Prime Infrastructure periodically provides critical fixes, device support, and add-on updates that you can download and install by choosing **Administration > Software Update**. Depending on your connectivity and preference, you can install software updates by:

- Downloading updates directly from cisco.com to the Prime Infrastructure server.

  To use this method, your Prime Infrastructure server must be able to connect externally to Cisco.com. For details, see "Install Software Updates from Cisco.com" in Related Topics.

- Downloading software update files to a client or server with external connectivity,

  then uploading them to and installing them on the Prime Infrastructure server. For details, see "Upload and Install Downloaded Software Updates" in Related Topics.

Related Topics

Install Software Updates from Cisco.com

The following steps explain how to install software updates directly from Cisco.com. This procedure assumes that Prime Infrastructure has external connectivity to Cisco.com and that you want to download updates directly from Cisco.com.

Step 1   Choose **Administration > Licenses and Software Updates > Software Update**.

Step 2   Click the **download** link at the top of the page to get the latest updates from Cisco.com.

Step 3   Enter your Cisco.com login credentials. Prime Infrastructure lists the available updates.

If you receive an error indicating there was a problem connecting to cisco.com, verify your proxy settings by choosing **Administration > Settings > System Settings > General > Account Settings > Proxy**. If your proxy settings are not working, deselect **Enable Proxy**, then click **Save**.

Step 4   Click **Show Details** to see the details about the updates.

Step 5   Click **Download** next to the update you want to install.

Step 6   After the update has been downloaded, click **Install**.

Step 7   Click **Yes** in the pop-up message. The server will restart automatically.

Step 8   When the restart is complete, choose **Administration > Licenses and Software Updates > Software Update**. The Updates table should show the update as "Installed".

Related Topics

Upload and Install Downloaded Software Updates

The following steps explain how to upload and install software updates. This procedure is useful when your Prime Infrastructure server does not have external connectivity, or you prefer to download files on a different server.

Step 1   Choose **Administration > Licenses and Software Updates > Software Update**.

Step 2   Click the **upload** link at the top of the page.

Step 3   On the Upload Update window, click **Cisco Download**, which displays Cisco.com's "Download Software" page.

Step 4   Select **Products > Cloud and Systems Management > Routing and Switch Management > Network Management Solutions > Prime Infrastructure**.

Step 5   Select the correct version of Prime Infrastructure.

Step 6   Select an update software type (such as "Prime Infrastructure Device Packs").

Step 7   From the page that appears, click **Download** next to the file containing the updates you want. The file will have a UBF filename extension.

If you have not already stored your Cisco.com credentials (see "Saving Cisco.com Account Credentials in Prime Infrastructure" in Related Topics), you will be prompted to log in to Cisco.com, and to accept your organization's active license agreement with Cisco, before you can download the update file.

Be sure to download software updates that match your Prime Infrastructure version. For example, if you were running Prime Infrastructure 3.7, be sure to download software updates for version 3.7 only.

Step 8   With the update file downloaded to your client machine, return to the Prime Infrastructure tab and choose **Administration > Licenses and Software Updates > Software Update**.

Step 9   Click **Upload** and browse to locate and select the update file you downloaded.

Step 10   Click **Install**.

Step 11   Click **Yes** in the pop-up message. The server will restart automatically.

Step 12   When the restart is complete, choose **Administration > Licenses and Software Updates > Software Update**. The Updates table should show the update as "Installed".

Related Topics

How to Use Your Cisco.com Account Credentials with Prime Infrastructure

You can store your Cisco.com account user name and password in Prime Infrastructure. Doing so will allow you to streamline download and installation of software updates, and speed automatic checking and notification of updates.

Note that Prime Infrastructure stores only one set of Cisco.com credentials at a time. The password is stored in secure, encrypted form. It will use this stored user name and password to do all software update notification checks until such time as another user either deletes the stored credentials (as explained in "Deleting Cisco.com Account Credentials" in Related Topics) or overwrites them by entering a new Cisco.com user name and password.

Related Topics

Save Cisco.com Account Credentials in Prime Infrastructure

Step 1   Choose **Administration > Settings > System settings > Account Settings**

Step 2   Enter a valid Cisco.com user name and password.

Step 3 Click **Save**.

Related Topics

Deleting Cisco.com Account Credentials

Step 1 Choose **Administration > Settings > System settings > Account Settings**.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion.

Related Topics

How to Configure Support Request Settings

The Support Request Settings page allows you to configure the general support and technical support information.

Step 1 Choose **Administration > Settings > System Settings > Support Request.** The Support Request Settings page appears.

Step 2 Configure the following parameters:

- General Support Settings:

  - Enable interactions directly from the server—Select this check box to allow interactions for support requests directly from the server.

  - Sender E mail Address—Enter the email address of the support request sender.

  - Interactions via client system only—Select this check box to allow interactions for support requests only through client system.

- Technical Support Provider Information:

  - Cisco—Select this check box if the technical support provider is Cisco.

  - Default Cisco.com Username—Enter a default username to log in to Cisco.com. Click **Test Connectivity** to test the connections to the mail server, Cisco support server, and forum server.

  - Third-Party Support Provider—Select this check box if the technical support provider is a third party other than Cisco. Enter the email address, email subject line format, and website URL of the support provider.

Step 3   Click **Save Settings**.

Related Topics

Opening a Support Case

Launching the Cisco Support Community

How to Manage Disk Space Issues

Whenever disk space on the physical or virtual Prime Infrastructure server reaches 90 percent, the server will trigger a Major alert indicating that the server is low on disk space.

Threshold crossings for these alarms are calculated based on the usage of the Prime Infrastructure optvol and localdiskvol partitions only. The optvol partition contains the Oracle database used to store all of Prime Infrastructure's inventory and network data, while localdiskvol stores local application backups, WLC and MSE backups, and reports. The settings that trigger the alarms are defined in the file PackagingResources.properties, which you can find in the Prime Infrastructure server in the folder /opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging.

We recommend that administrators take action to increase disk space immediately upon receiving the Major alert. You can do this using any combination of the following methods:

- Free up existing database space as explained in "Compacting the Prime Infrastructure Database".
- Reduce the storage load on the localdiskvol partition by setting up and using remote backup repositories, as explained in "Using Remote Backup Repositories".
- Reduce the storage load on the optvol partition by reducing the amount and storage period for which you retain inventory and network data:
    - Reduce the length of time you store client association data and related events, as explained in "Specifying How Long to Retain Client Association History Data" and "Saving Client Traps as Events".
    - Reduce the length of time you store reports, as explained in "Controlling Report Storage and Retention".
    - Reduce the retention period for network inventory, performance, and other classes of data, as explained in "Specifying Data Retention by Category" and "Enabling DNS Hostname Lookup".
- Increase the amount of existing virtual disk space allocated to Prime Infrastructure, as explained in "Modifying VM Resource Allocation Using VMware vSphere Client". If you are using VMware ESXi 5.5 or later, use the vSphere Web Client to adjust disk space allocation (for details, see the "VMware vSphere documentation" in Related Topics). You can also install additional physical disk storage and then use VMware Edit Settings or the vSphere Web Client to allocate the additional storage to Prime Infrastructure.
- Move the Prime Infrastructure server installation to a server with adequate disk space, as explained in "Migrating to Another OVA Using Backup and Restore" and "Migrating to Another Appliance Using Backup and Restore". For more details, see "VMware vSphere Documentation".

Related Topics

Compact the Prime Infrastructure Database, on page 6

Using Remote Backup Repositories

Specify How Long to Retain Client Association History Data, on page 8

Save Client Traps as Events, on page 9