Hewlett Packard Enterprise

HPE 3PAR Service Processor Software 5.x Release Notes

Abstract

The information in this document is intended for use by Hewlett Packard Enterprise customers, partners, and HPE field representatives. These release notes describe the features and known issues included in HPE 3PAR Service Console for Service Processor 5.x.

Contents

HPE 3PAR Service Processor Software 5.0.2.0 (MU2) Release Notes

HPE 3PAR Service Processor Software 5.0.2.1 Release Notes.............37

Documentation feedback..45

Firewall and Proxy server configuration...46

HPE 3PAR Service Processor Software 5.0.0.0 Release Notes

Description

The HPE 3PAR Service Processor Software 5.0 Release Notes includes information about the base release of Service Processor (SP) 5.0 and the accompanying HPE 3PAR Service Console (SC).

The HPE 3PAR Service Processor is an appliance which collects data from an attached HPE 3PAR StoreServ Storage system in predefined intervals as well as an on-demand basis and sends the data to Hewlett Packard Enterprise, if configured.

SC replaces Service Processor Online Customer Care (SPOCC), the Graphical User Interface (GUI) for SP 4.4 and earlier versions. SC is accessed through a browser and provides much of the same functionality as SPOCC.

Update recommendation

Update recommendation: Required for using the HPE 3PAR Service Console and to support HPE 3PAR OS version 3.3.1.

Upgrading from SP 4.5 to 5.0 is supported through SPMAINT only, and the upgrade must be performed by HPE service personnel.

⚠ **WARNING:**

The SP running 4.5 does not support HPE 3PAR OS 3.3.1. The SP MUST be upgraded to SP 5.0.0 Immediately following the upgrade to HPE 3PAR OS 3.3.1.

Supersede information

Supersedes: SP 4.4

Supported platforms and browsers

Physical SPs (PSPs)

- HPE ProLiant DL320e (Gen8)

- HPE ProLiant DL360e (Gen8)

- HPE ProLiant DL120 (Gen9)

Virtual SPs (VSPs)

- VMware ESXi 5.5/6.0/6.5

- Microsoft Hyper-V 2012/2012 R2/2016

Browsers

- Microsoft Internet Explorer 11

- Microsoft Windows Edge 38.14393

- Mozilla Firefox 50/51

- Google Chrome 54/55

Devices supported

The supported devices are the Physical Service Processor (PSP) or Virtual Service Processor (VSP) servicing the following HPE 3PAR Storage arrays:

- HPE 3PAR StoreServ 7000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 8000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 9000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 10000 Storage series (PSP)

- HPE 3PAR StoreServ 20000 Storage series (PSP)

Operating systems

This release is supported with the HPE 3PAR Operating System version 3.3.1.

Languages

Languages supported for this release:

- English

- Japanese

- Simplified Chinese

Features

The following features are part of the HPE 3PAR Service Console for the SP 5.0 release:

- Screens for initializing, restoring, updating, and configuring a Service Processor, adding storage systems, collecting support data, and more.

- Screens for monitoring and updating attached storage systems and hardware components such as controller nodes, ports, drive enclosures, and physical drives.

Modifications to the HPE SP OS

The following issues were addressed in this release:

Issue ID: 192845

Issue summary: SP sending unsolicited emails daily at 1:05 AM.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000

Affected software versions: 4.4.0 MU2, 4.4.0 MU3

Issue description: When local notifications are enabled, SP sends email notification daily at 1:05 AM with the subject line "Cron <rdanet@SP*******> /usr/bin/rda-cas-getcert --force-log".

Symptoms: Email notification received daily with subject line "Cron <rdanet@SP*******> /usr/bin/rda-cas-getcert --force-log".

Conditions of occurrence: None

Impact: High

Customer circumvention: None

Customer recovery steps: None

Issue ID: 195715

Issue summary: No StoreServ logs or events are transferred to HPE if non-encrypted ports are disabled during StoreServ initialization.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000

Affected software versions: 4.3.0 GA - 4.3.0 MU3, 4.4.0.GA - 4.4.0 MU3

Issue description: During StoreServ initialization via OOTB if user select to disable non-encrypted ports then SP has very limited connectivity and cannot collect any events or logs from StoreServ.

Symptoms: No events or logs related to StoreServ are transferred to HPE.

Conditions of occurrence: During OOTB non-encrypted ports are disabled.

Impact: High

Customer circumvention: If StoreServ initialization is performed via OOTB then select option "no" to when prompted to disable non-encrypted ports.

Customer recovery steps: To enable non-encrypted ports later, run CLI command 'setnet disableports no'

Issue ID: 199092

Issue summary: Alert leading to automatic case creation is not transferred to HPE.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000

Affected software versions: 4.1.0 - 4.3.0, 4.4.0 GA - 4.4.0 MU3

Issue description: An alert generates a support case when it is transferred to HPE. SP unsuccessfully transfers the alert to HPE resulting in no case creation.

Symptoms: No events or logs related to StoreServ are transferred to HPE.

Conditions of occurrence: `spcollect` process is terminated abruptly or CLI timeout occurs.

Impact: High

Customer circumvention: None

Customer recovery steps: None

Issues and workarounds

Issue ID: 154020

Issue summary: Resuming a paused advanced update activity from the Actions menu on the Activity page is not allowed.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: Cannot resume a paused advanced upgrade activity from the Actions menu on the Activity page.

Symptoms: Cannot resume a paused advanced upgrade activity from the Actions menu on the Activity page.

Conditions of occurrence: Attempting to resume a paused advanced update activity from the Actions menu on the Activity page.

Impact: Low

Customer circumvention: Click the resume option on the Update view of the Systems page to resume the update.

Customer recovery steps: None. Issue is fixed in SP 5.0.1.

Issue ID: 169634

Issue summary: Setup appears to stall when network connectivity is lost during StoreServ initialization.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: When network connectivity is lost during the StoreServ initialization process, it appears that setup stalls and does not complete.

Symptoms: Setup appears to stall and not complete.

Conditions of occurrence: Loss of network connectivity during StoreServ initialization process.

Impact: Low

Customer circumvention: None

Customer recovery steps:

1. Log back in to the SP.
2. From the Add System page, rediscover and then add the StoreServ again.

Issue ID: 171088

Issue summary: Update will not resume after Admit Hardware does not complete during an update.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: When `admithw` does not complete successfully during an update, retrying the update will not resume from the "admithw failed" state.

Symptoms: Cannot resume update after an "admithw failed" state.

Conditions of occurrence: Attempting to resume an update after Admit Hardware does not complete successfully.

Impact: Low

Customer circumvention: None

Customer recovery steps: Run `admithw` manually by selecting the **Admit Hardware** action on the Systems page.

Issue ID: 179246

Issue summary: 3PAR StoreServ Management Console (SSMC) login screen appears instead of 3PAR Service Console (SC) screen after successful SP update and reboot when using Firefox 48.0.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: After successfully updating and rebooting the SP using Firefox 48.0, the SSMC login screen appears instead of the SC screen.

Symptoms: SSMC login screen appears instead of SC screen.

Conditions of occurrence: Using Firefox 48.0 to update and reboot SP.

Impact: Low

Customer circumvention: Use another supported browser or a different supported version of Firefox.

Customer recovery steps: Clear the cache/cookies from Firefox , and then re-launch the browser.

Issue ID: 182454

Issue summary: When downgrading HPE 3PAR OS to a version earlier than 3.3.1.GA, certain SP functionality does not work.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: For SP 5.0 actions such as CLI commands, admit hardware, check health, and collect support data give unexpected results or do not complete after the attached StoreServ is reverted from OS 3.3.1 to 3.2.2, 3.2.1 or downgraded from OS version 3.3.1 to 3.2.2.

Symptoms: SP 5.0 actions do not complete or give unexpected results after OS on StoreServ is reverted or downgraded.

Conditions of occurrence: Attached StoreServ is reverted from OS 3.3.1 to 3.2.2, 3.2.1 or downgraded from OS version 3.3.1 to 3.2.2.

Impact: Low

Customer circumvention: None

Customer recovery steps: Restore the SP to a supported 4.x version to perform the actions.

Issue ID: 187126

Issue summary: Browser terminates unsuccessfully when using Chrome 54 or 55.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: When using Chrome browser version 54 or later, users might experience a browser terminating unexpectedly with the message "Aw, Snap!" on various screens and dialogs of SSMC and SC.

Symptoms: Browser terminates unsuccessfully when using Chrome 54 or 55.

Conditions of occurrence: Connected to the SC using Chrome 54 or 55.

Impact: Low

Customer circumvention: Use another supported browser or the latest version Chrome.

Customer recovery steps:

- Use another supported browser or the latest version of Chrome.

- If multiple sessions are open of same user with the same browser, then close all other open sessions, and start the Service Console again.

Issue ID: 188892

Issue summary: SP Setup page disappears after clicking the "Connect Service Processor" button.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: While attempting to launch SP Setup after completing network configuration on the console, the SP Setup page disappears after clicking the "Connect Service Processor" button.

Symptoms: SP Setup page disappears after clicking the "Connect Service Processor" button.

Conditions of occurrence: After completing network configuration on the console, the SP Setup page disappears after clicking the "Connect Service Processor" button.

Table Continued

Impact: Low

Customer circumvention: None

Customer recovery steps: Close the browser and open it again.

Issue ID: 189793

Issue summary: Time-out popup appears instead of SC login screen after updating and rebooting the SP using Firefox 48.0.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: After successfully updating and rebooting the SP using Firefox 48.0, the SSMC login screen/connection timeout pop-up appears instead of the SC login screen.

Symptoms: SSMC login screen/connection timeout pop-up appears instead of the SC login screen after updating and rebooting the SP when using Firefox 48.0.

Conditions of occurrence: Using Firefox 48.0 to update and reboot the SP.

Impact: Low

Customer circumvention: Use another supported browser or a different supported version of Firefox.

Customer recovery steps: Clear the cache/cookies from Firefox and re-launch the browser.

Issue ID: 197194

Issue summary: Critical dumps are not transferred in a timely manner.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: Critical dumps are not transferred in a timely manner. Dumps need to be prioritized to speed up transfer.

Symptoms: Critical dumps are not transferred in a timely manner.

Conditions of occurrence: Transferring dumps to HPE Support.

Impact: Low

Customer circumvention: None

Customer recovery steps: None

Issue ID: 197459

Issue summary: Pop-up appears indicating communication with StoreServ cannot be established.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: After a patch update, an attempt to apply another patch may display a pop-up indicating that communication with the StoreServ cannot be established.

Symptoms: After a patch update, an attempt to apply another patch may display a pop-up indicating that communication with the StoreServ cannot be established.

Conditions of occurrence: The message may appear in one of the following situations:

- After a patch is applied, the SP Socket Communication Layer needs to rebuild the socket pool to account for new version software on the StoreServ. This can take up to two minutes.
- The patch causes `netc`, `sysmgr`, and a number of other services to restart. This is documented by the StoreServ and takes a few minutes to stabilize. During this period, the SP may encounter loss of connectivity to the storage system.

Impact: Medium

Customer circumvention: None

Customer recovery steps: None

Issue ID: 200145

Issue summary: Current validation rules for email addresses are too restrictive.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913

Issue description: Adding an email address in a format other than <name@domain.com>, (for example, an address that contains multiple periods or more than 4 characters after the single period that is allowed).

Symptoms: Unable to add an email address in a format other than <name@domain.com>.

Table Continued

Conditions of occurrence: When attempting to add an email address in a format other than <name@domain.com.

Impact: High

Customer circumvention: None

Customer recovery steps: None. Issue is fixed in 5.0.0.1 Patch.

Prerequisites for updating to SP 5.0

- You must first upgrade to SP 4.5 before upgrading to SP 5.0. Refer to the *HPE 3PAR Service Processor Software 4.5 Release Notes* and *HPE 3PAR Service Processor Software 4.3 and 4.4 to 5.0 Upgrade Instructions* for upgrade information and instructions.

- Before performing the upgrade to the Service Processor, ensure that there are no customer firewall restrictions to the existing HP servers and new HPE servers on port 443. For a list of HP and HPE server host names and IP addresses, refer to **Firewall and Proxy server configuration** on page 46.

✔	**Verify that you have**
	SP running version 4.5.
	SP must be running in Secure Network Mode.
	If a storage system is attached, it must be running at least HPE 3PAR OS 3.3.1.GA.
	Physical SPs must be running on ProLiant servers.
	ESXi version 5.5/6.0 or Hyper-V 2012 /2012 R2 (for Virtual Service Processors)
	Virtual SPs must have at least 4096 MB memory. ⓘ **IMPORTANT:** For Hyper-V, do not reconfigure virtual memory until after the upgrade to SP 4.5 is complete.
	Virtual SPs must have 4 CPU cores. ⓘ **IMPORTANT:** For Hyper-V, do not reconfigure CPU cores until after the upgrade to SP 4.5 is complete.

⚠ **WARNING:**

Upgrade checks cannot determine the Windows Server version for Hyper-V VSPs. Do not continue upgrade on Windows Server 2008 R2. SP 4.5 is supported only on Windows Server 2012 and Windows Server 2012 R2.

Updating to SP 5.0

> ⚠️ **WARNING:**
>
> You must first verify that the HPE 3PAR OS is running version 3.3.1 before proceeding with this SP update.

Use SPMAINT with the command line option `=1.16.6==>` Upgrade SP to version 5.0 to update the SP to SP-5.0.

Service Console installation instructions

To set up a Service Processor for SP 5.0 and manage an attached 3PAR StoreServ Storage system, follow the instructions in *HPE 3PAR Service Console and StoreServ Management Console 3.1 Quick Setup Guide*.

> ⓘ **IMPORTANT:**
>
> If setting up a PSP or VSP, you must install SSMC 3.1 on a separate system, not on the SP.

Related information

The latest documentation for HPE 3PAR Service Processor 5.0 is available at the following websites:

Hewlett Packard Enterprise Support Center

HPE Information Library

Available documents include:

- *HPE 3PAR Service Processor Software 4.5 Release Notes*
- *HPE 3PAR Service Console and StoreServ Management Console 3.1 Quick Setup Guide*
- *HPE 3PAR Service Processor Software 5.0 User Guide*
- *HPE 3PAR Service Processor Software 5.0 Rebuild Instructions*

HPE 3PAR Service Processor Software 5.0.0.1 Patch Release Notes

Description

Patch SP 5.0.0.1 provides several quality improvements.

Patch summary

Security

Added Subject Alternative Name (SAN) field for Certificate Signing Request (CSR) generation.

SP setup and updates

- A confirmation dialog has been added when rebooting the SP or restarting SP services is required at the end of an SP update.

- Lessened restrictions on use of multiple periods (.) in email addresses.

Host names

The NTP host name now validates correctly when restoring an SP.

Service Console

- Event and alert files are now displayed on the Files page.

- Event messages for local notification alerts now display correctly.

For additional details see:

Update recommendation

Update recommendation: This is a required patch.

Supersede information

Supersedes: None. SP 5.0.0.1-23119 is the SP 5.0.0.0 Patch 1 and can only be applied on an SP that is running SP 5.0.0.0.

Devices supported

The supported devices are the Physical Service Processor (PSP) or Virtual Service Processor (VSP) servicing the following HPE 3PAR Storage arrays:

- HPE 3PAR StoreServ 7000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 8000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 9000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 10000 Storage series (PSP)

- HPE 3PAR StoreServ 20000 Storage series (PSP)

Languages

Languages supported for this release:

- English

- Japanese

- Simplified Chinese

SP software versioning

SP 5.x software versions use the format `SP M.m.U.P-B`

Where:

- M—Major

- m—Minor

- U—Maintenance update

- P—Patch number

- B—Build number

For example:

SP 5.0.0.0-33 refers to 5.0 GA (build 33)

SP 5.0.0.1-23119 refers to 5.0 GA Patch 1 (build 23119)

SP 5.0.1.0-23227 refers to 5.0 MU1 (build 23227)

Features

This patch contains no new features.

Issues and workarounds

Issue ID: 197754

Issue summary: Patch update stalls when network IP address is lost on StoreServ.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913, SP 5.0.0.1-23119

Issue description: While installing the HPE 3PAR OS update, the StoreServ's IP address is lost, and the update stalls.

Symptoms: Patch update stalls.

Conditions of occurrence: Network IP address is lost on StoreServ during patch update.

Impact: High

Customer circumvention: None

Customer recovery steps: Remove the StoreServ from the SP and add it again.

If the StoreServ does not appear on the Systems page, you can remove it from the SP page by hovering over the name of the storage system, and then clicking the X that appears next to the name.

This issue is fixed in SP 5.0.1.

Prerequisites for applying the SP 5.0.0.1 patch

✔	Verify that you have
	SP running version 5.0.0.0-22913.
	Firewall configured to allow access to ports specified in **Firewall and Proxy server configuration** on page 46.

Applying the SP 5.0.0.1 patch

Procedure

To apply the SP 5.0.0.1 patch, follow the instructions under **Updating the Service Processor** in *HPE 3PAR Service Console Software 5.0 User Guide*.

HPE 3PAR Service Processor Software 5.0.0.2 Patch Release Notes

Description

Patch SP 5.0.0.2 provides Linux kernel updates.

> **NOTE:**
>
> The SP reboots once the patch is applied.

For additional details, see:

Supported platforms and browsers on page 5

Operating systems on page 6

Languages on page 6

Related information on page 15

SP software versioning on page 17

Update recommendation

Update recommendation: This is a required patch.

Supersede information

Supersedes: SP 5.0.0.2-23479 is the SP 5.0.0.0 Patch 2. It can be applied on an SP that is running SP 5.0.0.0 or on an SP with patch SP 5.0.0.1 already applied.

Devices supported

The supported devices are the Physical Service Processor (PSP) or Virtual Service Processor (VSP) servicing the following HPE 3PAR Storage arrays:

- HPE 3PAR StoreServ 7000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 8000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 9000 Storage series (PSP and VSP)

- HPE 3PAR StoreServ 10000 Storage series (PSP)

- HPE 3PAR StoreServ 20000 Storage series (PSP)

Features

This patch contains no new features.

Modifications to the HPE SP OS

The following issues were addressed in this release:

Issue ID: 209179

Issue summary: Behavior altering file remains after HPE 3PAR OS upgrade.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000, StoreServ 9000

Affected software versions: SP 5.0.0.0-22913, SP 5.0.0.1-23119

Issue description: An upgrade creates a system behavior altering file to facilitate the upgrade. At the conclusion of the upgrade, the file is removed; however, it remains present.

Symptoms: A file that is removed through the upgrade process is still present.

Conditions of occurrence: Upgrading HPE 3PAR OS from 331GA, 331 EGA to 3.3.1.215-MU999.

Impact: High

Customer circumvention: None

Customer recovery steps: None

Issues and workarounds

Issue ID: 208967

Issue summary: Cannot apply 5.0 patches or updates to SP 5.0 that has been upgraded from SP 4.5 and is operating in a Secure Site mode.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913, SP 5.0.0.1-23119, SP 5.0.0.2-23479

Issue description: Cannot apply 5.0 patches or updates to SP 5.0 that has been upgraded from SP 4.5 and is operating in a Secure Site mode.

Symptoms: Cannot apply SP 5.0 patches or updates.

Conditions of occurrence: Applying patches or updates to SP 5.0 that has been upgraded from SP 4.5 and is operating in Secure Site mode.

Impact: High

Table Continued

Customer circumvention:

The work-around is to take the system out of the secure site configuration temporarily (while still not allowing any traffic in or out of system) and then restoring the secure site settings. Outbound communication will be disabled by providing an invalid "Remote support proxy" IP address and inbound communication is disabled by disabling "HPE remote support access".

From Service Console

1. Stage the patch (like 5.0.0.1.23119) and do not upgrade the system at this time.

2. Go to Edit Service Processor Configuration page.

3. Enable "Send support data to HPE".

4. Disable "HPE remote support access".

5. Configure an invalid "Remote support proxy".

6. Click OK to proceed with the configuration.

   The configuration will eventually time out and show a warning "Failed to configure remote support".

7. Go back to the Edit SP Configuration page.

8. Disable "Send support data to HPE" to turn the SP back into a secure site.

9. Go back and apply the patch or upgrade the SP.

Only perform this procedure once. After this procedure has been performed, it will be possible to apply patches or updates to the Service Processor.

Customer recovery steps: None. This issue is fixed in SP 5.0.1.

Issue ID: 208637

Issue summary: Storeserv Attach with IP address causing SP to disconnect from the network.

Affected platforms: SP only

Affected software versions: SP 5.0.0.0-22913, SP 5.0.0.1-23119, SP 5.0.0.2-23479

Table Continued

Issue description:

During the connect step of the "Add an initialized StoreServ", the process adds an access rule to the firewall to the IP address of the StoreServ. It then connects to the StoreServ to retrieve basic information on the server, and then removes the access rule from the firewall.

If the IP address of the StoreServ is a subset of the IP address of the SP, then in the removal step, the SP firewall access rules are also deleted. For example, 10.102.5.11 (StoreServ) to 10.102.5.112 (SP).

Symptoms:

When adding a system using the "Add an initialized StoreServ" option, the user will first enter a Hostname or IP address of the StoreServ, the admin user account name, and the admin password. After the options are entered, the user will press the "Connect" button.

At this point, the display shows a spinning logo and a panel pop-up stating "Request Timeout". Further refresh will show that the SP is still ping-able, but is not responding to http or ssh requests.

Conditions of occurrence: The IP address of the StoreServ array is a subset of the IP address of the SP. For example, 10.102.5.11 (StoreServ) to 10.102.5.112 (SP).

Impact: The SP stops communication on the network and must be rebooted.

Customer circumvention:

To get around this issue, do one of the following:

1. Change the IP address of the SP or StoreServ.

2. Turn off the firewall, attach the StoreServ, and then turn the firewall back on.

Customer recovery steps: To recover the SP, the SP must be rebooted. Reboot by either connecting in from the console connection and using the TUI, or rebooting by other means.

This issue is fixed in SP 5.0.1.

Prerequisites for applying the SP 5.0.0.2 patch

✔	Verify that you have:
	SP running version 5.0.0.0-22913 0r 5.0.0.1-23119.
	Firewall configured to allow access to ports specified in **Firewall and Proxy server configuration** on page 46.

Applying the SP 5.0.0.2 patch

Procedure

NOTE:

The SP reboots once the patch is applied.

To apply the SP 5.0.0.2 patch, follow the instructions under **Updating the Service Processor** in *HPE 3PAR Service Processor Software 5.0 User Guide*.

HPE 3PAR Service Processor Software 5.0.1.0 (MU1) Release Notes

Description

SP 5.0.1.0 (MU1) provides several quality improvements.

For additional details see:

Update recommendation

Update recommendation: This is a required update.

Supersede information

Supersedes: None.

Operating systems

This release is supported with the HPE 3PAR Operating System version 3.3.1 MU1 only.

Enhancements

The following features are part of the HPE 3PAR Service Console for the SP 5.0.1.0 release:

- Stop/Resume actions for Advanced OS update available from the Activity page.

- SP integration with StoreFront Remote for registration tokens and recommended SP version.

- Ability to enable/disable scrubbing of customer-sensitive data from all telemetry uploaded to HPE Support from the SP.

- Ability to enable/disable `hpepartner` account.

- Disabled ability to reboot/shutdown of SP or controller nodes from the Actions menu while an update is in progress.

- Added link to creating a Maintenance Window to the CLI session dialog.

- System readiness checks for an OS update are displayed only after the Run Checks button is clicked.

- RAP forwarding and Real Time Scrubber settings are now displayed in the Support section on the Service Processor page.

- Node names and Node <number> are now displayed on the controller node reboot and shutdown dialogs.

- Date and time and recommended SP versions are displayed on the Service Processor page.

- User confirmation is now required when changing the SP IP address.

- The "X" icon to the right of the storage system name on the Service processor page is now always visible.

- Date and time settings for an uninitialized 3PAR StoreServ Storage system default to the SP date and time settings.

Modifications to the HPE SP OS

The following issues were addressed in this release:

Issue ID: 208318

Issue summary: Events associated with remote copy snapshot creation are being treated as if they are major events, resulting in STaTS RAP and case creation.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000, StoreServ 9000

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479

Issue description: Events associated with remote copy snapshot creation are being treated as if they are major events. These (non-alert) events result in STaTS RAP and case creation, causing unnecessary alarm.

Symptoms: Technical Support and the customer may become involved in case resolution for an innocuous (non-alert) event.

Conditions of occurrence: The events occur at the snap frequency for remote copy groups.

Impact: Low

Customer circumvention: None

Customer recovery steps: N/A

Issue ID: 205371

Issue summary: Enhancement request to add statcmp -compr to the collected StoreServ performance statistics. The collected statistics are sent as call home data.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000, StoreServ 9000

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479

Table Continued

Issue description: It was determined that live monitoring of the PM CMP usage was necessary in the PERFORM collection that the SP generated.

Symptoms: N/A

Conditions of occurrence: N/A

Impact: N/A

Customer circumvention: N/A

Customer recovery steps: N/A

Issue ID: 208180

Issue summary: After an OS upgrade, the StoreServ collections are not arriving at STaTS.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 10000, StoreServ 20000, StoreServ 9000

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479

Issue description: A connection issue between SP and StoreServ during OS upgrade causes a NullPointerException to occur in the SP Post Process Monitor resulting in the StoreServ collections not restarting.

Symptoms: StoreServ collection files not arriving at STaTS

Conditions of occurrence: The array is not connectable during an OS upgrade for a sufficient length of time.

Impact: Medium

Customer circumvention: None

Customer recovery steps: Perform one of the following:

- Reboot the SP.
- Stop/Start SP Services from the TUI.
- Detach and reattach the StoreServ to the SP.

Issues and workarounds

Issue ID: 212587

Issue summary: Immediately after an OS upgrade, when selecting "Update HPE 3PAR OS" on the Actions menu, "OS package failed to load" is displayed.

Affected platforms: SP only

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: For some patch upgrades, particularly for a patch upgrade or a patch revert, the upgrade process completes fairly fast. The array connection needs time to become aware of the array OS version change, to reconnect, and to refresh cached connection parameters. If the user tries to bring up the OS upgrade dialog immediately after the completion of an OS upgrade, the connection to array reset may not have finished. If the connection to array reset has not finished, the "OS package failed to load" message may be displayed.

Symptoms: "OS package failed to load" is displayed.

Conditions of occurrence: Immediately after an OS upgrade, when selecting "Update HPE 3PAR OS" on the Actions menu.

Impact: Low

Customer circumvention: Immediately after an OS upgrade, allow several minutes before selecting the update option on the Actions menu.

Customer recovery steps: Close the dialog, wait for several minutes, and then select "Update HPE 3PAR OS" on the Actions menu.

Issue ID: 212275

Issue summary: SP restoration does not complete successfully when using a rescue file whose date and time was originally set manually and then on the restoration the date and time is set using the NTP server. If an invalid NTP server is entered, a link in the Service Console takes the user to a login page.

Affected platforms: SP only

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: SP restoration does not complete successfully when using a rescue file whose date and time was originally set manually and then on the restoration the date and time is set using the NTP server. If an invalid NTP server is entered, the Service Console displays a link for the date and time configuration, and this link takes the user to a login page in Service Console.

Symptoms: Service Console link takes the user back to a login page before SP is initialized.

Conditions of occurrence: When attempting to restore an SP from a rescue file with a manual date and time setting, and an invalid NTP server is entered.

Impact: Low

Customer circumvention: None

Customer recovery steps: Redo the restoration process with a correct NTP server, or restore the SP first and then come back and edit the date and time setting.

Issue ID: 207226

Issue summary: Recommended SP and OS versions are not available when SOCKS4 proxy is configured.

Affected platforms: SP only

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: SOCKS4 proxy is supported for SP remote support. However, SOCKS4 proxy is not used to connect to StoreFront Remote to query recommended versions.

Symptoms: Recommended versions for SP and OS are displayed as "-".

Conditions of occurrence: When SOCKS4 proxy is configured for remote support on the SP.

Impact: Low

Customer circumvention: None

Customer recovery steps: Avoid using SOCKS4 proxy or register with StoreFront Remote to receive recommended version information.

Issue ID: 210793

Issue summary: Service Console displays a warning when disabling DNS and switching the mail server from a host name to an IP address.

Affected platforms: SP only

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: When disabling DNS and changing the mail server configuration of an SP from using a host name to using an IP address, the warning "Failed to delete firewall rules for mail host" is displayed.

Symptoms: A "Failed to delete firewall rules for mail host" warning is displayed on Service Console, but no functionality is impacted.

Conditions of occurrence: Disable DNS on the SP and switch the mail server configuration from a host name to an IP address.

Impact: Low

Customer circumvention: None

Customer recovery steps: SP functionality is not affected and there is no need to recover.

Issue ID: 212497

Issue summary: Request Timeout pop-ups may be seen on the Service Processor Page.

Affected platforms: SP only

Affected software versions: 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: Periodic attempts to clean up files occur every hour. If there is a large number of files under the /sp/data directory on the SP system, then periodic attempts to clean up files, can cause certain REST calls to take longer than 30 seconds. REST calls that take longer than 30 seconds cause Request Timeouts to occur.

The following are the REST calls that are timing out:

- GET /servicesupport/REST/spservice/sp/properties

- GET /servicesupport/REST/spservice/sp/config

Symptoms: Request Timeout pop-ups may be seen on the Service Processor Page and the Service Processor Page may not show data.

Table Continued

Conditions of occurrence: Only occurs while the SP is searching for files to clean up and there are a large number of files (> ~100,000) on the SP to search through. The search happens every hour.

Impact: Low

Customer circumvention: The problem can be circumvented by reducing the number of files on the SP. Generally the large number of files are representing large number of events coming from a StoreServ. Take the following steps:

1. To collect all the files into a collection, run a Weekly Data collection and send it to HPE.

   a. From the Service Processor page, select the 'Collect Support Data' Action.

   b. From the Collection Support Data dialog, check the 'Weekly data' box and click "Collect".

   c. Wait for the Weekly Data Collection to complete. The wait could take a while depending on the number of files.

2. Manually run file clean-up deleting all non-critical files older that 1 day.

   a. From the Service Processor page, select the 'Cleanup SP Files' Action.

   b. From the Cleanup SP Files dialog, check the 'Files based on age' box, and specify Non-critical files older than **1** day.

   c. Click the "Delete" button.

Customer recovery steps: If a Request Timeout is seen, simply close the dialog. The REST calls are done periodically to refresh the Service Processor page. When the SP finishes searching for files to clean up, which may take several minutes depending on the number of files on the SP, then the operation will succeed.

Issue ID: 206776

Issue summary: SP StoreServ Upgrade process monitor is in a running state even after online upgrade does not complete successfully due to customer detaching and reattaching the StoreServ.

Affected platforms: SP only

Affected software versions: 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Table Continued

Issue description: While performing an online upgrade, the customer detaches and then reattaches the StoreServ. The Upgrade process will exit early and unsuccessfully. However the Upgrade tasks in the Activity panel still show the Upgrade process as running.

Symptoms: Upgrade tasks in the Activity panel still shows the Upgrade process as running when it is not.

Conditions of occurrence: While performing an online upgrade, the customer detaches and then reattaches the StoreServ.

Impact: Medium

Customer circumvention: Do not detach and reattach the StoreServ during a StoreServ Upgrade, unless instructed to do so by HPE Support.

Customer recovery steps: Go to the Upgrade StoreServ panel and recover the upgrade.

Issue ID: 214164

Issue summary: After an unsuccessful online OS upgrade, the SP StoreServ Upgrade Recovery process cannot start because the SP StoreServ Upgrade process monitor is still in a running state.

Affected platforms: SP only

Affected software versions: 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: After an unsuccessful online OS upgrade, the SP StoreServ Upgrade process monitor remains in a running state. The pop-up dialog: "Update in Progress - Another update cannot be started until the current update is completed" blocks the SP StoreServ Upgrade Recovery process and prevents it from starting.

Symptoms: The Upgrade tasks in the Activity panel show the Upgrade process as running even though the Update View page shows that the Upgrade process is unsuccessful. The pop-up dialog: "Update in Progress - Another update cannot be started until the current update is completed" blocks the SP StoreServ Upgrade Recovery process and prevents it from starting.

Conditions of occurrence: When online upgrade is unsuccessful due to an unexpected rare condition.

Impact: High

Table Continued

Customer circumvention: None

Customer recovery steps:

1. To ensure the Upgrade StoreServ was unsuccessful, refresh the Service Console.

2. Log in to the TUI, shut down SP services, and start SP services.

3. Go to the Upgrade StoreServ panel and recover the upgrade.

Issue ID: 213995

Issue summary: System readiness checklist is displayed incompletely.

Affected platforms: All StoreServ

Affected software versions: 3.3.1.GA, 3.3.1.EGA, 3.3.1.MU1

Issue description: The list of System Readiness checks is reported before the checks are run. The latest set of checks is then automatically installed, which may result in a mismatch in the list of checks.

Symptoms: A warning dialog box is displayed indicating the mismatch.

Conditions of occurrence: This issue occurs on the first upgrade to a new version after staging a U-type kit on systems running 3.3.1.GA, 3.3.1.EGA or 3.3.1.MU1. Subsequent upgrades are not impacted.

Impact: Low

Customer circumvention: The customer can re-run the checks a second time and will not see the dialog.

Customer recovery steps:

1. Re-run the System Readiness checks.

2. Verify that all checks have passed.

   The bottom of the page will display "You can now initiate an update on the StoreServ system". All checks have passed when this warning message is displayed.

3. Click Update to proceed.

Issue is fixed in SP 5.0.2.1.

Issue ID: 214197

Issue summary: After upgrading the SP from SP 5.0.0.0 to SP 5.0.1.0, the StoreServ system is not visible on the Systems page.

Affected platforms: SP only

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479, 5.0.1.0-23799

Issue description: After upgrading the SP from SP 5.0.0.0 to SP 5.0.1.0, the SP is rebooted. If during the reboot, the SP has trouble establishing a connection to the StoreServ, the StoreServ system will not be listed on the Systems page.

The communication with the StoreServ goes into a retry process. Once it is successfully reconnected, the StoreServ system will become visible after re-logging in.

Symptoms: The StoreServ system is not visible on the System page after an SP upgrade.

Conditions of occurrence: Upgrading the SP from SP 5.0.0.0 to SP 5.0.1.0

Impact: Low. This issue only happens if there are network issues during an SP reboot.

Customer circumvention: None

Customer recovery steps: Log in after the connection with the StoreServ is re-established, or detach and reattach the StoreServ.

Prerequisites for updating to SP 5.0.1.0

✔	**Verify that you have**
	SP running version 4.5 MU1, 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479.
	Firewall configured to allow access to ports specified in **Firewall and Proxy server configuration** on page 46.

Updating to SP 5.0.1.0

Procedure

To update to SP 5.0.1, follow the instructions under **Updating the Service Processor** in *HPE 3PAR Service Processor Software 5.x User Guide*.

HPE 3PAR Service Processor Software 5.0.2.0 (MU2) Release Notes

Description

With SP 5.0.2.0 (MU2), controller nodes now reboot and shutdown correctly when these actions are performed from the SP Systems Actions menu.

For additional details, see:

Supported platforms and browsers on page 5

Languages on page 6

SP software versioning on page 17

Related information on page 15

Update recommendation

Update recommendation: This is a required update.

Supersede information

Supersedes: SP 5.0.1.0

Operating systems

This release is supported with the HPE 3PAR Operating System version 3.3.1 MU1 only.

Modifications to the HPE SP OS

The following issue was addressed in this release:

Issue ID: 216307

Issue summary: The StoreServ system unexpectedly reboots or shuts down when you attempt to reboot or shut down a single controller node.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.1.0-23799

Issue description: The StoreServ system unexpectedly reboots when rebooting a single controller node from the SP Systems Actions menu. Likewise, the StoreServ system unexpectedly shuts down when you shut down a single controller node from the SP Systems Actions menu.

Symptoms: The StoreServ system unexpectedly reboots or shuts down.

Table Continued

Conditions of occurrence: Rebooting or shutting down a single controller node from SP Systems Actions menu

Impact: High

Customer circumvention: Using the Text-based User Interface (TUI), select the Interactive CLI / Maintenance Mode option and issue the CLI command to reboot or shut down a node.

Log on to the Service Processor using the admin or hpepartner user.

1. Select "7 == Interactive CLI / Maintenance Mode".

2. Choose the StoreServ where the CLI will be opened.

   For example, a selection for a StoreServ would display as follows: "1 == ssname HPE_3PAR model", where "ssname" is the StoreServ name and "model" is the StoreServ model.

3. At the cli% prompt, type one of the following commands to reboot or shut down the node:

   • To reboot the node, type "shutdownnode reboot x" where x is the node number.

   • To shut down the node, type "shutdownnode halt x" where x is the node number.

Customer recovery steps: N/A

Issues and workarounds

Issue ID: 216840

Issue summary: If the SP hostname contains an invalid character, the SP 4.5 upgrade to SP 5.0 process does not complete successfully.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479

Issue description: Upgrading SP 4.5 to SP 5.0 may not complete successfully with the following message:

rm: cannot remove /sp: Device or resource busy

ERROR: Contact support - the SP 5.0 upgrade failed.

Unable to migrate the 4.4.0.GA-58 settings.

You must install and configure the SP 5.0 update.

Table Continued

Symptoms: The following message is displayed:

rm: cannot remove /sp: Device or resource busy

ERROR: Contact support - the SP 5.0 upgrade failed.

Unable to migrate the 4.4.0.GA-58 settings.

You must install and configure the SP 5.0 update.

Conditions of occurrence: The SP hostname contains an underscore (_) character.

Impact: Low

Customer circumvention: Log on to the Service Processor using the admin or hpepartner user.

1. Select "1 == Configure Network".

2. To acknowledge the warning, press Enter.

3. Following the guidelines, enter the new hostname.

   The hostname can contain only alphanumeric or dash "-" characters and cannot begin with a dash.

Customer recovery steps: None

Prerequisites for updating to SP 5.0.2.0

✔	**Verify that you have**
	SP running version 4.5 MU2, 5.0.0.0-22913, 5.0.0.1-23119, 5.0.0.2-23479 or 5.0.1.0-23799.
	Firewall configured to allow access to ports specified in **Firewall and Proxy server configuration** on page 46.

Updating to SP 5.0.2.0

Procedure

To update to SP 5.0.2.0, follow the instructions under **Updating the Service Processor** in *HPE 3PAR Service Processor Software 5.x User Guide*.

HPE 3PAR Service Processor Software 5.0.2.1 Release Notes

Description

Patch SP 5.0.2.1 provides quality improvements to the Service Processor (SP).

For additional details, see:

Supported platforms and browsers on page 37

Operating systems on page 37

Languages on page 6

SP software versioning on page 17

Related information on page 15

Update recommendation

This is a required patch.

Patch details

SP patches are cumulative. Requires SP 5.0.2.0.

Operating systems

This release is supported with the HPE 3PAR Operating System version 3.3.1 EMU1.

Supported platforms and browsers

Physical SPs (PSPs)

- HPE ProLiant DL320e (Gen8)
- HPE ProLiant DL360e (Gen8)
- HPE ProLiant DL120 (Gen9)

Virtual SPs (VSPs)

- ESXi 5.5/6.0/6.5
- Hyper-V 2012/2012 R2/2016

Browsers

- Internet Explorer 11
- Firefox 53/54

- Chrome 58/59
- Edge 39/40

Devices supported

The supported devices are the Physical Service Processor (PSP) or Virtual Service Processor (VSP) servicing the following HPE 3PAR Storage arrays:

- HPE 3PAR StoreServ 7000 Storage series (PSP and VSP)
- HPE 3PAR StoreServ 8000 Storage series (PSP and VSP)
- HPE 3PAR StoreServ 9000 Storage series (PSP and VSP)
- HPE 3PAR StoreServ 10000 Storage series (PSP)
- HPE 3PAR StoreServ 20000 Storage series (PSP)

Features

This patch contains no new features.

Modifications to the HPE 3PAR SP Software

The following issues were addressed in this release:

Issue ID: 213170

Issue summary: Installing an HPE 3PAR OS patch may not complete.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.1.0-23799, 5.0.2.0-23974

Issue description: Installing an HPE 3PAR OS patch may not complete.

Symptoms: Patch upgrade may not complete while installing the patch.

Conditions of occurrence: Installing an HPE 3PAR OS patch.

Impact: High

Customer circumvention: None

Customer recovery steps: Reboot the SP and retry the upgrade.

Issue ID: 218762

Issue summary: With the Scrub private information feature enabled, HPE telemetry files may not be sent to HPE.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.1.0-23799, 5.0.2.0-23974

Issue description: With Remote Copy enabled on the array, the Scrub private information feature may not complete scrubbing and therefore does not transfer the telemetry data.

Symptoms: The Scrub private information feature does not transfer the telemetry data.

Conditions of occurrence: Customers with more than one Remote Copy Group configured and the Scrub private information feature enabled will likely encounter this problem.

Impact: High

Customer circumvention: Disable the Scrub private information feature.

Customer recovery steps: None.

Issue ID: 218726

Issue summary: HPE telemetry files may not be sent to HPE.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.2.0-23974

Issue description: HPE telemetry files may not be sent to HPE.

Symptoms: SP services are running and all SP transfer status are normal, but files are not transferred to HPE.

Conditions of occurrence: Normal operations of HPE telemetry files.

Impact: Medium

Table Continued

Customer circumvention: None.

Customer recovery steps: From the Text-Based User Interface (TUI):

1. Shut down SP Services.

2. Start SP Services.

From the Service Console:

Reboot the SP from the SP Actions Menu

Issue ID: 216976

Issue summary: Pre-update checks for an HPE 3PAR OS upgrade may not complete successfully.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 9000, StoreServ 10000, StoreServ 20000

Affected software versions: 5.0.2.0-23974

Issue description: When the Upgrade Tool package is staged with the HPE 3PAR OS package, the pre-update checks that step of the upgrade will not complete successfully.

Symptoms: The pre-update checks that step of the online upgrade does not complete successfully.

Conditions of occurrence: Performing an online upgrade to HPE 3PAR OS when the Upgrade Tool is staged with the HPE 3PAR OS package.

Impact: High

Customer circumvention: Stage and install the Upgrade Tools kit before staging the HPE 3PAR OS package.

Customer recovery steps: Stage and install the Upgrade Tools, then stage and upgrade the HPE 3PAR OS.

Issue ID: 217934

Issue summary: Files are not uploaded to HPE when an HPE 3PAR Policy Server is configured with a Secure Service Architecture (SSA) transport agent.

Affected platforms: StoreServ 7000, StoreServ 8000, StoreServ 9000, StoreServ 10000, StoreServ 20000

Affected software versions: 5.0.2.0-23974

Table Continued

Issue description: The SSA agent may not restart when an HPE 3PAR Policy Server is configured with an SSA transport agent. Files are not uploaded to HPE and there is no remote access to the SP.

Symptoms: Files are not uploaded to HPE and there is no remote access from HPE to the SP.

Conditions of occurrence: An HPE 3PAR Policy Server is configured for remote support.

Impact: High

Customer circumvention: Remove the policy server configuration.

Customer recovery steps: Install this SP patch.

Issue ID: 217306, 214533

Issue summary: Selecting some options from the Actions menu on the Systems page may result in no response. Additionally, clicking the Update button at the bottom of the Update HPE 3PAR OS page may result in no response.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.1.0-23799, 5.0.2.0-23974

Issue description: Using SP 5.0.2.0 to perform an HPE 3PAR OS update from the 3.3.1 family may result in no response selecting one of the following options.

- From the Actions menu on the Systems page:

  ◦ Update HPE 3PAR OS

  ◦ Admit hardware

  ◦ Post update checks

- From the Update HPE 3PAR OS page:

  Update button at the bottom of the page

Symptoms: The selected option does not start.

Conditions of occurrence: When selecting options from the Actions menu on the Systems page and when clicking the Update button on the Update HPE 3PAR OS page.

Impact: High

Table Continued

Customer circumvention: Perform these steps before upgrading the HPE 3PAR OS.

1. Check if the Available update package(s) drop-down list displays an Upgrade Tool (U-kit) on the Update HPE 3PAR OS page.

2. Install the U-kit before updating to any HPE 3PAR OS version.

Customer recovery steps: None

Issue ID: 220834

Issue summary: The collection of weekly support data does not complete successfully when the Scrub private information feature is enabled.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.2.0-23974

Issue description: The collection of weekly support data does not complete successfully when the Scrub private information feature is enabled and there are multiple large files in the collection.

Symptoms: HPE telemetry files will not be transferred.

Conditions of occurrence: When the Scrub private information feature is enabled, and the weekly collection is large.

Impact: High

Customer circumvention: Disable the Scrub private information feature from the Service Console (SC) using the Edit SP Configuration option.

Customer recovery steps: None.

Issue ID: 218619

Issue summary: System readiness checks do not complete when preparing to update the HPE 3PAR OS.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.2.0-23974

Issue description: If the Upgrade Tool is not installed prior to beginning the HPE 3PAR OS upgrade, the upgrade pre-checks will not complete.

Symptoms: The pre-check step will not complete when performing an online upgrade to HPE 3PAR OS.

Table Continued

Conditions of occurrence: When the Upgrade Tool is not installed prior to the start of the HPE 3PAR OS upgrade.

Impact: High

Customer circumvention: None.

Customer recovery steps: Install the Upgrade Tool.

Procedure:

1. From the Service Console (SC) main menu, click Systems.

2. Select the storage system you want to upgrade. An overview of the storage system selected will be displayed.

3. On the SP Actions menu, select Update HPE 3PAR OS.

4. To load the Upgrade Tool package, select the package from the Available update package(s) and click Update.

5. The Customer Self-Update Agreement page is displayed. Read the agreement, and click Agree to proceed with the update.

Issue ID: 220488

Issue summary: Email notifications are not sent after an SP restart.

Affected platforms: All Physical and Virtual SPs

Affected software versions: 5.0.2.0-23974

Issue description: If the SP is configured with a mail host name that contains hyphens, email notification will not be sent after an SP restart.

Symptoms: Email notifications are not sent from the SP.

Conditions of occurrence: Mail host name contains hyphens.

Impact: High

Customer circumvention: Do not use mail host names containing a hyphen.

Customer recovery steps: Reconfigure the mail server with an IP address.

Prerequisites for applying the SP 5.0.2.1 patch

✔	**Verify that you have**
	SP running version 5.0.2.0-23974
	Firewall configured to allow access to ports specified in **Firewall and Proxy server configuration** on page 46.

Applying the SP 5.0.2.1 patch

Procedure

To apply the SP 5.0.2.1 patch, follow the instructions under **Updating the Service Processor** in the *HPE 3PAR Service Processor Software 5.0 User Guide* at the Hewlett Packard Enterprise Information Library website: **http://www.hpe.com/info/storage/docs**.

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Firewall and Proxy server configuration

Firewall and proxy server configuration must be updated on the customer network to allow outbound connections from the Service Processor to the existing HP servers and new HPE servers.

HP and HPE server host names and IP addresses:

- HPE Remote Support Connectivity Collector Servers:

    ◦ **https://storage-support.glb.itcs.hpe.com** (16.248.72.63)

    ◦ **https://storage-support2.itcs.hpe.com** (16.250.72.82)

- HPE Remote Support Connectivity Global Access Servers:

    ◦ **https://c4t18808.itcs.hpe.com** (16.249.3.18)

    ◦ **https://c4t18809.itcs.hpe.com** (16.249.3.14)

    ◦ **https://c9t18806.itcs.hpe.com** (16.251.3.82)

    ◦ **https://c9t18807.itcs.hpe.com** (16.251.4.224)

- HP Remote Support Connectivity Global Access Servers:

    ◦ **https://g4t2481g.houston.hp.com** (15.201.200.205)

    ◦ **https://g4t2482g.houston.hp.com** (15.201.200.206)

    ◦ **https://g9t1615g.houston.hp.com** (15.240.0.73)

    ◦ **https://g9t1616g.houston.hp.com** (15.240.0.74)

- HPE RDA Midway Servers:

    ◦ **https://midway5v6.houston.hpe.com** (2620:0:a13:100::105)

    ◦ **https://midway6v6.houston.hpe.com** (2620:0:a12:100::106)

    ◦ **https://s54t0109g.sdc.ext.hpe.com** (15.203.174.94)

    ◦ **https://s54t0108g.sdc.ext.hpe.com** (15.203.174.95)

    ◦ **https://s54t0107g.sdc.ext.hpe.com** (15.203.174.96)

    ◦ **https://g4t8660g.houston.hpe.com** (15.241.136.80)

    ◦ **https://s79t0166g.sgp.ext.hpe.com** (15.211.158.65)

    ◦ **https://s79t0165g.sgp.ext.hpe.com** (15.211.158.66)

    ◦ **https://g9t6659g.houston.hpe.com** (15.241.48.100)

- HPE StoreFront Remote Servers:

- **https://sfrm-production-llb-austin1.itcs.hpe.com** (16.252.64.51)

- **https://sfrm-production-llb-houston9.itcs.hpe.com** (16.250.64.99)

- For communication between the Service Processor and the HPE 3PAR StoreServ Storage system, the customer network must allow access to the following ports on the storage system.

  - Port 22 (SSH)

  - Port 5781 (Event Monitor)

  - Port 5783 (CLI)

- For communication between the browser and the Service Processor, the customer network must allow access to port 8443 on the SP.