### Contents

Executive summary .................................................................................................................. 3

Features of HPE 3PAR SSA .................................................................................................. 3

HPE 3PAR Secure Storage Architecture ................................................................................ 3

Separation of storage .............................................................................................................. 3

Service Processor .................................................................................................................. 4

Diagnostic services ............................................................................................................... 4

Types of data collected ........................................................................................................ 5

Product support data content .............................................................................................. 5

Periodic data collection ....................................................................................................... 6

Event data collection and analysis ...................................................................................... 7

STaTS ................................................................................................................................... 8

HPE 3PAR Central Secure Service Collector Server ................................................................ 9

No single point of failure ..................................................................................................... 9

Secure service transmission ............................................................................................... 10

HTTPS .................................................................................................................................. 10

HPE 3PAR Certificate of Authority (CA) ........................................................................... 10

Network Address Translation (NAT) .................................................................................... 11

3PAR StoreServ Network Port Assignments—Node ........................................................... 11

3PAR StoreServ Network Port Assignments—Service Processor ....................................... 12

Data transfer service selection ........................................................................................... 12

Moment of Birth ................................................................................................................... 12

Secure Site ............................................................................................................................ 12

Customer Controlled Access setting .................................................................................. 13

Manual data collection transfer ......................................................................................... 13

Data Collection via Automated Services ............................................................................ 14

Pre-Stage HPE 3PAR Software components on HPE 3PAR Service Processor ................. 14

HPE 3PAR Policy Server ..................................................................................................... 15

HPE 3PAR Service Processor status indications ................................................................. 16

SPOCC website ................................................................................................................... 16

HPE 3PAR Service Processor Menu the Port 22 SSH ........................................................ 17

HPE’s Privacy Statement ..................................................................................................... 17

Frequently asked questions ............................................................................................... 17

Terminology ........................................................................................................................ 18
Executive summary

HPE 3PAR StoreServ Storage arrays are rapidly being adopted into many secure IT data centers. With this adoption comes the need for customers to rely on HPE's ability to securely provide a best in class secure communication service and architecture between the HPE 3PAR Systems and the HPE 3PAR Central remote monitoring facility.

The HPE 3PAR Secure Service Architecture (SSA) provides this secure service communication architecture by providing a path to communicate secure diagnostic data transmissions and remote service connections where enabled.

Secure communication between the customer site and HPE 3PAR Central is paramount in ensuring timely and accurate data collection of diagnostic data. Data which is captured is stored and constantly reviewed using advanced tools within HPE 3PAR’s diagnostic center. These tools can provide advanced warnings on any issues which may arise with a customer’s HPE 3PAR array and allow HPE 3PAR Central to notify customers of a pending issue. Customer data stored on the array in the form of a Virtual Volume is never collected or accessible by HPE 3PAR SSA.

Remote monitoring is an important feature of the HPE 3PAR StoreServ Storage System solution\(^1\) it enables HPE to detect, analyze, and proactively resolve any issues and to provide the best customer experience.

Features of HPE 3PAR SSA

- Provides timely and proactive response to monitored issues within the HPE 3PAR array
- Capture critical performance data for advanced analysis at HPE 3PAR Central
- Notification and stage HPE 3PAR OS Upgrades on HPE 3PAR 7000 and 10000 arrays
- Remote service connection for advanced troubleshooting with HPE 3PAR support engineers
- Historical collection of statistics on each HPE 3PAR Storage array
- All assigned ports used on HPE 3PAR StoreServ systems follow the universal standards in securing data as outlined by the “Internet Assigned Numbers Authority” iana.org

HPE 3PAR Secure Service Architecture uses industry standard mechanisms to support the transfer of data in a secure method. All data which is transferred between the user’s site and HPE 3PAR Central is done via secure authentication and negotiated ciphers.

Users who deploy the HPE 3PAR StoreServ array are given options by which the array can be monitored. These options include a secure site where all ports to and from the array are encrypted and no transmissions of array status are allowed to the most common deployment of a closely monitored array. This paper is designed to address these options.

HPE 3PAR Secure Storage Architecture

Separation of storage

Separation of storage simply means the HPE 3PAR Storage array does not internally connect to HPE 3PAR Central. Communication to HPE 3PAR Central is done via the HPE 3PAR Service Processor or a Virtual Service Processor (VSP), which type of Service Processor deployed is dependent upon the customer and the array type purchased.

HPE 3PAR 7000 customers have the option to choose between deploying a Virtual Service Processor or a physical Service Processor. A VSP can be deployed on either an ESX VMware® system using a vmdk distribution file or on a Microsoft® Server using Hyper-V.

In all other configurations, the HPE 3PAR Service Processor will be a dedicated hardware system purchased with the HPE 3PAR Storage array. In either of the two deployment models, the VSP will communicate with the HPE 3PAR StoreServ array in the same manner as a physical HPE 3PAR Service Processor\(^2\). In both cases the Service Processor is dedicated to HPE 3PAR array management and cannot be used to run any other application software or services. Figure 1 Secure Storage Connections, displays an overview of the HPE 3PAR Array connections.

\(^1\) h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-3528ENW&cc=us&lc=en
The HPE 3PAR Service Processor is an important component of the HPE 3PAR StoreServ array. The HPE 3PAR Service Processor serves as a communications interface within the customer's IP network environment for all service related communications to and from the HPE 3PAR StoreServ array.

The HPE 3PAR Service Processor deploys the SPOCC (Service Processor Onsite Customer Care) software which is a suite of service tool applications which provide a web-based user interface for support of the HPE 3PAR Service Processor and the HPE 3PAR StoreServ array.

Remote login is a form of SSH and HTTPS (SPOCC), this capability can be controlled or disabled. In the case where it is disabled, access is available via a serial cable. Additional SP hardening is available through an iptables like packet filtering feature. Like all enterprise class shared storage products, SP must be operated in an environment where the network security is commensurate with the value of the stored assets.

Diagnostic services
Diagnostic services is the process whereby the HPE 3PAR Service Processor accumulates diagnostic data from the HPE 3PAR StoreServ array and periodically transmits the data over a secure network communication to HPE 3PAR Central. Diagnostic data which is received is scanned to ensure proper health of the array during the collection period. Any abnormalities found would be followed up by further troubleshooting and possible dispatch of field personnel to remedy any diagnosed inconsistencies.

All customer-authorized remote service connections, as shown in figure 2 Remote Service Connection, to a customer HPE 3PAR StoreServ array will leverage the HPE 3PAR Service Processor as the connection point. All array service actions are directed through the HPE 3PAR Service Processor. It should be noted that in the below example the connection is enabled by the customer to allow remote access to HPE Technical Services.
All diagnostic data that is captured on the HPE 3PAR Service Processor is sent to 3PAR Central for further processing, data includes:

- System health information
- System configuration data
- System performance data
- System events

### Types of data collected

#### Product support data content

HPE 3PAR StoreServ product support data primarily consists of system logs generated by the array as illustrated in figure 3 Support Related Data Files. These logs can be collected manually or through an automated process. The collected log files are forwarded to HPE 3PAR Central for analysis. The log data files collected do not contain user data. User data can only accessed via the host or application which are attached to the storage array.

Other support data which may be requested during a support call is as follows.

- Customer contact detail
- Site-specific information—site location if not detailed in contract data
- Network connectivity as to gather additional data
- Other product related diagnostic information

---

**Note**

It is important to restate HPE 3PAR StoreServ data logs do not contain customer data. Customer data can only be accessed by the host attached to the storage array or the customer application. HPE does not have access to this data at any time.

---

**Customer asks:** How long is collected data retained by HPE 3PAR?

**Reply:** Data is typically maintained on the internal STaTS database for a period of 30 days or as long as an active support case may require. Once data is no longer needed the data is archived for future reference. Reference data is characterized as data which contains diagnostic data, performance data or event data. This data is used as reference points as to architectural enhancements, performance recommendations or array health trends.
There are two categories of data collection which are captured on the HPE 3PAR Service Processor. First type of data collection is a periodic data collection. Data on an hourly basis is captured and stored temporarily on the HPE 3PAR Service Processor. Once every four hours data which was captured during the preceding 4 hour timeframe is sent via an HTTPS connection to HPE 3PAR Central for review and analysis. This process which is illustrated in figure 4 Periodic Data Collection is periodically collected and transferred to HPE 3PAR Central for analysis. A good example of this type of data transfer is installation of additional disks in the HPE 3PAR StoreServ Array. The admittance of the new physical disks would be viewed as a non-critical event and would not need any further analysis or remedial action. The transfer of this data type would be considered informational.

HPE 3PAR Central keeps track of the 4 hour call home status received from the customers SP. If the SP fails to call home, the monitoring mechanisms within HPE 3PAR Central will record the status of File Transfer Overdue. The file transfer mechanism is the heartbeat of the HPE 3PAR StoreServ subsystem. If the heartbeat is not received within the four hour window, Technical Services will be notified of the failure of transmitted data.

### Table of Support Related Data Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Modified</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4K</td>
<td>Oct 30, 2014 12:54:47</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4K</td>
<td>Oct 30, 2014 12:54:49</td>
<td></td>
</tr>
<tr>
<td>adv</td>
<td>4K</td>
<td>Mar 05, 2015 08:45:05</td>
<td></td>
</tr>
<tr>
<td>alert</td>
<td>20K</td>
<td>Mar 05, 2015 08:01:02</td>
<td></td>
</tr>
<tr>
<td>appcore</td>
<td>4K</td>
<td>Jan 07, 2015 02:01:02</td>
<td></td>
</tr>
<tr>
<td>bloomg</td>
<td>4K</td>
<td>Mar 04, 2015 17:44:30</td>
<td></td>
</tr>
<tr>
<td>config</td>
<td>4K</td>
<td>Mar 05, 2015 04:01:01</td>
<td></td>
</tr>
<tr>
<td>eeprom</td>
<td>4K</td>
<td>Mar 04, 2015 17:44:30</td>
<td></td>
</tr>
<tr>
<td>environ</td>
<td>4K</td>
<td>Mar 04, 2015 17:44:29</td>
<td></td>
</tr>
<tr>
<td>event</td>
<td>55K</td>
<td>Mar 05, 2015 08:28:01</td>
<td></td>
</tr>
<tr>
<td>evlog</td>
<td>20K</td>
<td>Mar 05, 2015 08:01:02</td>
<td></td>
</tr>
<tr>
<td>hostconf</td>
<td>4K</td>
<td>Mar 04, 2015 17:45:25</td>
<td></td>
</tr>
<tr>
<td>initvmt</td>
<td>4K</td>
<td>Mar 05, 2015 08:01:01</td>
<td></td>
</tr>
<tr>
<td>insflore</td>
<td>4K</td>
<td>Mar 04, 2015 18:07:14</td>
<td></td>
</tr>
<tr>
<td>memdata</td>
<td>4K</td>
<td>Mar 04, 2015 17:44:31</td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>5</td>
<td>Mar 04, 2015 17:45:12</td>
<td></td>
</tr>
<tr>
<td>past_events</td>
<td>2.44M</td>
<td>Mar 04, 2015 17:45:48</td>
<td></td>
</tr>
<tr>
<td>perfdb</td>
<td>4K</td>
<td>Feb 19, 2015 18:08:00</td>
<td></td>
</tr>
<tr>
<td>perform</td>
<td>4K</td>
<td>Mar 05, 2015 07:54:10</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3. Support Related Data Files

### Periodic data collection

Periodic data collection is regularly collected and transferred to HPE 3PAR Central for analysis. A good example of this type of data transfer is installation of additional disks in the HPE 3PAR StoreServ Array. The admittance of the new physical disks would be viewed as a non-critical event and would not need any further analysis or remedial action. The transfer of this data type would be considered informational.
Event data collection and analysis
The second type of data collection is immediate event data collection. An immediate data event can be categorized in the following two categories.

• Major—an event which can disrupt processing of data on the HPE 3PAR StoreServ Array, an immediate response is needed to remedy the event

• Minor—an event which is monitored and may result in an actionable remedy

Event analysis for events which occur on the HPE 3PAR StoreServ Array is aided by an internal process which runs on the HPE 3PAR Service Processor and at HPE 3PAR Central. The tool identified as FAST or Fault Analysis Support Tool as shown in figure 5 FAST Analytics uses a complex set of rules to determine the severity of the event which occurred on the HPE 3PAR StoreServ Array.

Analytics run on the HPE 3PAR Service Processor contains a set of rules which can help determine the severity of the event. As an example, a physical disk within the array reports a read error on a particular block of data. Through the normal operations on the HPE 3PAR StoreServ array, the user would not be notified of this event since these events can be a common day event. The FAST rules set would note this event on the HPE Service Processor would and send it forward to HPE 3PAR Central. HPE 3PAR Central using FAST Analytics would also note this event but also look for event history within the HPE 3PAR STaTS database (covered in next section). FAST at 3PAR Central would see over the past 3 days the HPE 3PAR StoreServ array has recorded 10 of these events.

Identifying that there have been 10 of these events in 3 days and comparing this against the rules database at HPE 3PAR Central would result in an actionable event in which the physical disk should be replaced as a precautionary measure.
The FAST Analytics Tool features include the following:

- Analysis of event files
- Analysis of node and application dumps
- Report generator
- Historical event timeline maintained for each reporting HPE 3PAR StoreServ Array
- External notifications

**STaTS**

Data collected via the HPE 3PAR SSA is stored at HPE in a central repository known as STaTS (Service Tools and Technical Service). STaTS allows authorized HPE Technical Service personnel access to historical performance, event and configuration data from customers of HPE 3PAR StoreServ arrays. STaTS data is guarded data and always treated as HPE Confidential data. Included at the end of this paper is HPE's policy of safeguarding customer data.

In some cases, customer site specific data (see limitations mentioned previously above, under Support Data Content) may be retained in HPE service records as a service to customers. The data retention can sometime allow for quick analysis of customers storage without the need for timely involvement of the customer. Data retention also allows support engineers quick access to event data from previous data captures.

Further analysis of customer retained data can help Storage Solutions Architects forecast future storage needs based on storage allocation trends over a specific timeframe allowing the customer continued growth with no disruption due to lack of storage space.

Figure 6 STaTS Database, illustrates the data flow for the HPE 3PAR Service Processor and HPE 3PAR Central.
The HPE 3PAR Central Secure Service Collector Server (discussed in next section) is the main interface between the users HPE 3PAR Service Processor and HPE 3PAR Central. Files received via a secure HTTPS connection are forwarded on to a number of file watch servers. These servers identify information which has been passed onto them and marks them for processing. In the example above we have event data, performance data and administrative data.

Different data collections will result in different actions, a failed physical disk drive will raise a service alert, while heartbeat information from a remote HPE 3PAR Service Processor will just be logged to keep track that the remote site is correctly connecting and sending data. Data which is stored within the STaTS database can only be accessed by securely authenticated and authorized HPE employees associated with the users account.

**HPE 3PAR Central Secure Service Collector Server**

The HPE 3PAR Secure Service Collector server is a central collection server within HPE 3PAR Central for the collection of all service data sent by the Service Processor. Once data is received by the collector, HPE support personnel can review collection data and follow up any items noted in the data received. Data received at the HPE 3PAR Secure Service Collector Server includes the following.

- System health information
- Configuration data
- Performance data
- System events

The HPE 3PAR Secure Service Collector Server communicates with the customers HPE 3PAR StoreServ Service Processor through an HTTPS connection. All communications are initiated, controlled and driven by the SP in the field. As a strict security practice the collector server never initiates the communication. Figure 5 illustrates the connection point between the SP and internal servers within HPE 3PAR Central. All data transmissions are done through secure communication and no Clear Text Data is ever sent. All data transferred is dependent upon using a Certificate of Authority and a secure cipher. For security, HPE 3PAR use ciphers in data transmission, ciphers to include, aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc and aes128-cbc.

**No single point of failure**

The HPE 3PAR StoreServ subsystem is designed so that there is no single point of failure. Diagnostic data collection is stored in various locations within the diagnostic system.

Upon initialization of the HPE 3PAR array and admin volume is created on the array. This admin volume is integral part of the HPE 3PAR OS. Event information is stored on part of the admin volume.

On the HPE 3PAR Service Processor there is a folder where diagnostic data is collected and stored. In the event the SP cannot communicate with HPE 3PAR Central, the data will be stored until such time the connection becomes available. For customers who operate a secure site where no outside connections are allowed, the customer can retrieve collected data from the SP and then transfer the collected data to an anonymous FTP site for processing.
Data collected and then transmitted to HPE 3PAR Central is kept active for approximately 30 days. Once data exceeds the 30 days the data is archived and kept active for 1 year. Past the one year timeframe data is backed up and securely stored. The database in which the data is collected and stored on consists of multiple HPE 3PAR clustered arrays for optimal storage configuration.

### Secure service transmission

**HTTPS**

Hypertext Transfer Protocol Service (HTTPS) is a communications protocol for secure communication transfer of data over a computer network. HTTPS utilizes the SSL/TLS protocol security standards to securely transfer data within a computer network. The security therefore in HTTPS is that of the TLS standard which uses secret keys to encrypt the data flow between the client and the server.

The secure data transfer between the user site and HPE 3PAR Central is illustrated in figure 7 secure service transmission.

![Figure 7. Secure service transmission](image)

The data transfer between the HPE 3PAR Service Processor and HPE 3PAR Central is accomplished in a secure fashion and employs the following standards.

- Data transmission between customer site and HPE 3PAR Central use HTTPS and are secure (SSL)
- HPE 3PAR Service Processor initiates all communications in an outbound manner
- Data authentication at HPE 3PAR Central uses a Certificate of Authority authenticated by VeriSign
- Data is NOT transferred in Clear Text

This paper is intended to brief the user on methods used by HPE 3PAR to secure data transfer, any secure protocols used in the secure transfer are beyond the scope of this paper.

**HPE 3PAR Certificate of Authority (CA)**

A Trusted Certificate is used to make secure connections from the HPE 3PAR Service Processor to HPE 3PAR Central. This CA is used to avoid malicious attempts to gain access to confidential customer data. HPE 3PAR deploys a CA which authenticated for use by VeriSign. This CA cannot be substituted when communicating between the HPE 3PAR Service Processor and HPE 3PAR Central.

**Certificate used in communication with CLI/MMC/SSMC**

The user however can change the CA to administer their own CA within their datacenter when using communication to the HPE 3PAR StoreServ array. An example of a customer using their own CA would be the communication link between the Management Console and the HPE 3PAR StoreServ array. Figure 8 HPE 3PAR Service Process to HPE 3PAR Communication, is an example of a secure data transmission using SSH Port 22.
To manage these CA's HPE 3PAR includes within the HPE 3PAR StoreServ OS four tools by which the user may manage their own CA's.

- **Createcert**—allows the creation of a self-signed cert or a certificate signing request
- **Importcert**—once the user has a signed CSR (Certificate Signing Request), it and CA are imported with the Importcert command
- **Showcert**—displays a table of certificate metadata and their uses
- **Removecert**—clears out unused certificates

**Customer asks:** Can I use my own signed Certificate of Authority within the datacenter for communication to the array?

**Reply:** Yes, any internal communication within the customer’s network can use a customer provided CA. The CA can be a signed CA by an independently verified authority or can be self-generated by the customer's own security office.

**Network Address Translation (NAT)**

NAT is the methodology of modifying network address information in the Internet Protocol datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.

As outlined earlier the SP uses SSH to validate authentication between the SP and the HPE 3PAR StoreServ array. The ipaddress of the SP is part of the SSH key as a validation to the array, if we were to support NAT, the remapping of the IP address which is known by the array would invalidate the SSH key and thereby would not allow authentication between the SP and the HPE 3PAR StoreServ array.

**3PAR StoreServ Network Port Assignments—Node**

The following is a collection of the ports assigned on the HPE 3PAR StoreServ array. Reference to each of the ports shown can be verified through the Internet Assigned Numbers Authority iana.org

<table>
<thead>
<tr>
<th>PORT</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>SSH daemon (required) communication between SP and HPE 3PAR StoreServ array as well as optional use for end-user CLI (listener)</td>
</tr>
<tr>
<td>123</td>
<td>(UDP) NTP (required) peer communication for network time protocol</td>
</tr>
<tr>
<td>161</td>
<td>SNMP agent (optional) communications between 3rd party SNMP manager and 3PAR SNMP agent (listener)</td>
</tr>
<tr>
<td>162</td>
<td>SNMP trap origination (optional) source port for unsolicited SNMP traps to 3rd party SNMP manager (source)</td>
</tr>
<tr>
<td>427</td>
<td>SLP (optional) Service Location Protocol (CIM) required in CIM/SLP are to be used (listener)</td>
</tr>
<tr>
<td>5781</td>
<td>Event consumer interface (required) communication between Service Processor and HPE 3PAR StoreServ array as well as some RM/VM/VASA event logic is used (listener)</td>
</tr>
<tr>
<td>5782</td>
<td>CLI unsecured (optional) provides plain text access to the CLI if end user chooses to use it</td>
</tr>
<tr>
<td>5783</td>
<td>CLI secured with TLS (required) encrypted access to CLI Service Processor to HPE 3PAR StoreServ nodes communication as well as end user CLI usage</td>
</tr>
</tbody>
</table>
CIM (optional) unsecured web services access for CIM clients if customer wishes to use plain text access

Web Services Application Program Interface (unsecure)
Web Services Application Program Interface (encrypted)

Secure port used by Management Console in the transmission of data to and from HPE 3PAR StoreServ array if check box checked at bottom of login screen. (Note with the release of StoreServ Management Console (SSMC) in late 2014, this is the default communication protocol)

3PAR StoreServ Network Port Assignments—Service Processor

The following is a collection of the ports assigned on the HPE 3PAR StoreServ Service Processor.

<table>
<thead>
<tr>
<th>PORT</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>SSH daemon (optional) if customer wants to connect to Service Processor using SSH</td>
</tr>
<tr>
<td>443</td>
<td>Webserver (required) secure access to the Service Processor GUI</td>
</tr>
<tr>
<td>123</td>
<td>(UDP) NTP (required) peer communications for network time protocol</td>
</tr>
</tbody>
</table>

Data transfer service selection

To this point in the paper we have identified the HPE 3PAR Service Processor as the tool used in helping customers and HPE 3PAR support personnel maintain the high level of uptime on the HPE 3PAR StoreServ array. We have also identified we use the data acquired by the HPE 3PAR Service Processor to monitor performance of the array, do predictive analysis of event data generated by the HPE 3PAR StoreServ array and monitor system health.

Getting all this important data to HPE 3PAR Central is another key element of the overall support strategy. Prior to installation of the HPE 3PAR StoreServ array, a questionnaire will be sent to the user or in the case where the array is self-installed the HPE 3PAR Smart Start Tool will be deployed. The information used to deploy the HPE 3PAR StoreServ array will guide the user or installation team in properly installing the HPE 3PAR StoreServ array.

Moment of Birth

Moment of Birth (MOB) is the initialization of the Service Processor or Virtual Service Processor. Independent of which you use, the MOB initializes and sets up the Service Processor for communication between the 3PAR StoreServ array and HPE 3PAR Central. During the MOB process the user will be required to supply some parameters which will be used for communication.

Secure Site

A Secure Site is a site in which the Service Processor is not allowed to access the internet as illustrated in figure 9 Secure Site Installation. The Service Processor will only have access to the HPE 3PAR StoreServ array. All other functions as to connections to HPE 3PAR Central will not be connected.
Customers who choose this option still should register their HPE 3PAR StoreServ array with HPE 3PAR. Once the array is registered customers can still utilize monitoring functions by manually uploading collected data from the Service Processor to an anonymous FTP site.

Customer sites which have security policies restricting outbound connectivity between the 3PAR Service Processor and HPE 3PAR Central are able to maintain some limited remote monitoring by utilizing a manual transfer method. HPE strongly recommends wherever possible that customers do have their 3PAR Service Processor connected to HPE 3PAR Central. The specifics for this procedure are covered in a SAW article. Please refer to this article for complete instructions “HPE 3PAR Storage—HPE 3PAR Service Processor weekly file retrieval process.”

Customer Controlled Access setting
Customer Control Access (CCA) allows the user to limit the network communication of external sources inbound and outbound to the HPE 3PAR Service Processor. There are three settings mode settings which enable communication of the HPE 3PAR Service Processor to HPE 3PAR Central:

- **Turn off HPE 3PAR Central communication**—this setting blocks all communication between the HPE 3PAR Service Processor and HPE 3PAR Central as well as any other inbound/outbound communication
- **Set outbound only communication**—this setting allows the HPE 3PAR Service Processor to send data outbound to HPE 3PAR Central but all inbound communications are blocked
- **Set bi-directional communication**—this setting allows for communication both in and out of the HPE 3PAR Service Processor including remote access by qualified HPE 3PAR Support Personnel and allowing HPE 3PAR Central to stage on the HPE 3PAR Service Processor new software updates.

Manual data collection transfer
Manual collection is initiated by a user if the HPE 3PAR StoreServ array and Service Processor are to be excluded from communicating with HPE 3PAR Central. In these cases where outside connectivity to 3PAR Central are strictly prohibited, the user may still send data to HPE 3PAR Central via HPRC File Transfer Service. ftp.usa.hp.com/hprc. HPRC file transfer service is used to deposit log files and collected data by which the customer has been directed by HPE Services to provide.

When using the HPRC website, HPE support will provide the customer the needed credentials to login and transfer requested data. Customers should transmit manually collected support data only after a support case has been opened. The HPRC file transfer service supports HTTPS, SFTP, and FTPS for secure data transfers. It is the customer responsibility to ensure that their corporate and regulatory data privacy requirements are met. Industry best practice is encrypting the file and securely sharing the key with the recipient as well as choosing a secure transport method (SFTP, HTTPS or FTPS).

---

3 h20564.www2.hp.com/hpsc/doc/public/display?docId=mrr_kc-0123444
HPRC is not backed up, and the information on the site is deleted after 1 year. HPE support, or the customer can manually delete the information prior to the 1 year expiration.

In order to resolve support incidents, the HPE support organization may share the manually collected data with HPE’s product support teams.

**Data Collection via Automated Services**

Automated data collection and transmission (when enabled) offers customers a means by which their HPE 3PAR StoreServ array is continually monitored. The collection of support data is uploaded to HPE 3PAR Central and then analyzed. This process is part of the Secure Service Architecture (SSA).

The use of SSA enables the following capabilities:

- Fault and event monitoring—diagnostic events are monitored and reported to HPE
- Automatic case logging—in the event a monitored alert meets a pre-defined rules criteria through FAST analytics, HPE Support Automation can create support calls
- Configuration and log data collection—systems configured to periodically collect configuration and log data which is reported to HPE 3PAR Central via secure channels
- Over Subscribed System Alert (OSSA)—The HPE 3PAR OSSA tool performs proactive utilization checks on key system elements. By monitoring your system and comparing current health, performance, and utilization statistics with historical data, this tool can identify when your system appears to be over-subscribed in any of these key areas and proactively notify you so that you can avert issues that have the potential to impact your operations

**Customer asks: What is done with the data once it is collected?**

**Reply:** This is dependent on the collected data. Some data is used to forecast trending models such as rate of consumption and needs assessment prior to the customer running out of space. Other data is used to monitor event data which has transpired over the last collection period, this model helps to maintain a healthy environment for the array and based on events may trigger HPE to proactively replace components which show a trend towards failure in the near future. Other collected data may be used in support cases or as reference points, e.g. over the past month, parity errors within a controller memory region have been increasing, this would warrant a proactive service call to maintain a high level of uptime.

**Pre-Stage HPE 3PAR Software components on HPE 3PAR Service Processor**

A software change was implemented in the HPE 3PAR Service Processor beginning with version 4.2 on the HPE 3PAR Service Processor. In support of Customer Self Upgrades on the HPE 3PAR StoreServ 7200, 7400 and 7450, HPE started pre-staging upgrades to the HPE 3PAR Service Processor when permitted. HPE 3PAR Central will periodically push software updates and patches to a folder location on the HPE 3PAR Service Processor.

Pre-staging the software does not institute the upgrade process, the customer is still required to initiate the upgrade process using the upgrade tool contained within the HPE 3PAR Service Processor Onsite Customer Care located on the HPE 3PAR Service Processor. For information regarding upgrading software please refer to hp.com/support/manuals on all documentation pertaining to upgrade HPE 3PAR OS.

Figure 10 HPE 3PAR OS Updates, illustrates the process in which HPE 3PAR OS updates is transferred.
• Data transmissions between HPE 3PAR Central on users site uses HTTPS and Secure SSL
• HPE 3PAR Central initiates request to transfer HPE 3PAR OS updates
• If update authorized, HPE 3PAR Central initiates handshake and Certificate of Authority Verification
• Secure cipher is negotiated and software updates of the HPE 3PAR Storage components are staged on HPE 3PAR Service Processor
• All data is staged on HPE 3PAR Service Processor, no data is communicated to HPE 3PAR StoreServ array
• Customer is notified of upgraded software is pending on the HPE 3PAR Service Processor

HPE 3PAR Policy Server

The HPE 3PAR Policy Server software is a server-based software application that allows customers to define and implement remote service access policies. This software application resides on a customer's network and sets and controls all Secure Service permissions. With the HPE 3PAR Policy Server, customers can allow or deny outbound communications or remote service connections to and from HPE 3PAR StoreServ arrays. The HPE 3PAR Policy Server also serves as a centralized collection point for collecting and storing audit log files of all diagnostic transfers and authorized remote service connections to and from a HPE 3PAR StoreServ arrays managed by the policy server.

![Diagram](Image)

**Figure 11.** HPE 3PAR Policy Server

Figure 11 HPE 3PAR Policy Server illustrates the implementation of the HPE 3PAR Policy Server within inside a customer environment. The HPE 3PAR Policy Server is used in the authentication of access to the HPE 3PAR StoreServ environment. The HPE 3PAR Policy Server is a licensed feature.

The HPE 3PAR Policy Server supports SSL/TLS protocols and uses either port 443 or 8443 with the application. During the installation of the policy server it will be configured with an SSL protocol. The connection of HPE 3PAR Service Processor to the policy server is defined at the MOB on the SP. If a user were to add the policy server after the SP MOB, the SP can be changed to reflect the addition of the policy server.

The HPE 3PAR Policy Server offers the following features:

• Provides flexible and granular control in defining and implementing remote services access policies
• Allows centralized audit for all devices being managed
• Provides a secure audit log for the purpose of reporting and compliance
HPE 3PAR Service Processor status indications

A key element in monitoring for optimal operation of a user’s HPE 3PAR StoreServ array is the indication that data being monitored is transmitting status information from the HPE 3PAR Service Processor. The user can inquire about these operations by either using a secure port login on port 443 for the webserver or an SSH login from port 22 using a serial connection program such as PuTTY.

SPOCC website

The SPOCC website login page displays status of the HPE 3PAR Service Processor. The Home page displays the following information regarding both the HPE 3PAR Service Processor and the HPE 3PAR StoreServ array.

- **SP Version**—current code version of the HPE 3PAR Service Processor
- **StoreServ HPE 3PAR OS Version**—current version of HPE 3PAR OS and notification of new version of HPE 3PAR OS which has been staged on the Service Processor
- **Customer Controlled Access**—customer controls network access to Service Processor, selections are
  - Turn off HQ communications
  - Set outbound only HQ communications—no remote access
  - Set Bi-directional HQ communications—remote access allowed
  - Enable automatic software download from HQ
- **Data Transfer**—data transfer medium
- **Remote Operations**—transfer medium i.e. Ethernet
- **SP Firewall Status**—displays the SP Firewall Control
- **Transfer Status**—status of the ability to transfer data from the Service Processor figure 12 HPE 3PAR Service Processor data transfer status
- **SP Process Status**—displays all currently collecting processes on the Service Processor
- **SP Storage Space Status**—displays the status of space available on Service Processor disk

**SP File Transfer Monitor**

Transfer Media: ethernet

**Last transfer status**

- **Transfer time:** Thu Jul 24 18:38:56 2014
- **Target server:** SP0001414091
- **Local filename:** /tmp/ftpGRP_1406244121.5943
- **Server filename:** is a group of 1 files
  - **Size in bytes:** 932
  - **Status:** OK

**Current transfer status**

No file transfer is in progress

**Number of file(s) on**

- **transfer queue:** 0
- **retry queue:** 0

**Service Processor upload queue:** 0 file(s)
**SSAgent upload queue:** 0 file(s)
**Last file to start upload via the SSAgent:**
  - 07-24-2014,18:23:34 SP0001414091.1414091.event.140724.162126.0-89103.CMR

**Figure 12.** HPE 3PAR Service Processor Data Transfer Status
**HPE 3PAR Service Processor Menu the Port 22 SSH**

The user has the ability to log through the SSH port 22 into the HPE 3PAR Service Processor. Data displayed via this login media is done through a menu driven system. Status and control of above controls can be gained by selecting item 1 on the menu and then appropriate menu selections from there.

**HPE's Privacy Statement**

While most of the data being collected for product support is not personally identifiable information, some of the contact information collected may contain personally identifiable information (e.g. customer contact information). To the extent that HPE collects personally identifiable information, it will be treated in accordance with the HPE Privacy Standard viewable at hp.com/us/en/privacy/privacy.html. Any data in which HPE collects during the process of routine maintenance or in the process of a support call is sensitive data. This data cannot be shared with third-parties without the approval of the customer.

**Frequently asked questions**

**Q.** I am company XY Widget and I currently hold a CA, can I use my CA to communicate with HPE 3PAR Central?

**A.** No, you cannot use your CA to communicate with HPE 3PAR Central, the communication must use the signed HPE Certificate of Authority.

**Q.** Can I turn the unneeded ports on the HPE 3PAR StoreServ array off at the array?

**A.** At this point the user can only either enable all ports to be encrypted or unencrypted. User cannot identify individual ports to be turned off or on.

**Q.** What kind of log information is required?

**A.** Required log information is any support information which is deemed warranted by support personnel to maintain the high level of customer up time. See figure 3 Support Related Data Files which illustrates an example of files which are collected and sent.

**Q.** How are data log files transmitted?

**A.** The data log files which are captured are transmitted via a manual process or automatic process. Each of these two processes are discussed in sections titled "Secure Service Transmission."

**Q.** Is the data repository at HPE Central secure, who has access to this data?

**A.** HPRC referenced in section titled “Manual Data Collection Transfer” uses secure protocols to transfer data. Data which is deposited on this site was requested via a customer support case. Data which has been sent may be viewed by authorized internal HPE engineers to help resolve the customer issue. Data is not shared to non-authorized HPE support personnel or shared with outside resources. Refer to section in this document titled “Manual Data Collection Transfer.”

**Q.** Can I use my own signed Certificate of Authority within the datacenter for communication to the array?

**A.** Yes, any internal communication within the data center can use a User’s CA. The CA can be a signed CA by a verified authority or can be self-generated. Refer to section in document titled “HPE 3PAR Certificate of Authority (CA).”

**Q.** Can I change my Secure Service options once I have completed the Moment of Birth or do I need to rerun the Moment of Birth again?

**A.** Yes, the user through the HPE 3PAR Service Processor and the Service Processor Onsite Customer Care webpage can make policy changes any time after Moment of Birth.

**Q.** How long is my data kept at HPE 3PAR Central?

**A.** Data is constantly being refreshed on the STaTS database. Current retention period is approximately 30 days or as long a support case remains open. Data is then moved off to long term storage to use as reference data. Refer to section “No single point of failure.”

**Q.** Does HPE still deploy modems on their storage arrays?

**A.** No, Modem support was discontinued with the release of HPE 3PAR Service Processor 4.1.0. Modem use is considered an unsecure transmission medium and can be compromised very easily. HPE decided to use the secure features of CA and SSH in the transmission of the data to HPE 3PAR Central.
**Terminology**

MC—Management Console

SP—Service Processor

VSP—Virtual Service Processor

RAP—Remote Access Protocol

STaTS—Service Tools and Technical Service

HPE 3PAR OS—Operating System for HPE 3PAR StoreServ array

MOB—Moment of Birth

HTTPS—Hypertext Transfer Protocol Service

SSA—Secure Service Architecture

SPOCC—Service Processor Onsite Customer Care

SSH—Secure Shell

FTP—File Transfer Protocol

CA—Certificate of Authority

CSR—Certificate Signing Request

NAT—Network Address Translation

SLP—Service Location Protocol

SSMC—StoreServ Management Console

NTP—Network Time Protocol

CCE—Common Computing Evaluation

CCA—Customer Control Access

TLS—Transport Layer Security

SSL—Secure Sockets Layer

Learn more at hp.com/go/StoreServ