Technical white paper

HPE 3PAR Secure Service Architecture

Us against the bad guys

Contents

Executive summary

The past few years has seen an unprecedented amount of successful attacks targeting proprietary data. In today's day and age, minimizing these attacks are paramount to a company survival. Unfortunately, one of the best examples of identifying and minimizing an attack was a large department store security breach in December of 2013. The result of that attack left an estimated 70 million customer accounts vulnerable, millions of dollars lost as banks had to cover funds which had been stolen, high ranking employees lost their jobs and a tarnished reputation of a large retailer almost scuttled a reputable brand name.

The intrusion breached all three access points within the system architecture, **hardware** was the Point of Sale system where consumer credit cards were swiped. The **software** was the application which collected the stolen data, as the cards were swiped and the **network** as the stolen data was communicated via ICMP traffic from the POS systems to the corporate LAN and subsequently to drop points all over the world.

This one example exemplifies the vulnerability by which consumers face every day. Each of the above manufacturers must stay vigilant in the engineering of safeguards against such attacks as often these attacks yield to the compromise of valuable data.

Guarding against these unscrupulous attempts to gain access to valuable data often uncovers vulnerabilities within hardware, network, and software (software to include Operating systems and applications). Once these vulnerabilities are uncovered it becomes the responsibility of all parties to help mitigate the vulnerability and block any type data breach. To do this many companies have created their own internal security teams whose sole purpose is to maintain high confidence in data security while minimizing any new threats which have been uncovered in the industry. This is a difficult task as there are individuals who decisively are trying to breach your data every hour of the day.

Hewlett Packard Enterprise and HPE 3PAR is committed to working and partnering with both our respective customers and the security community to help prevent and mitigate any and all the threats which occur daily across the world. Protecting your data is a battle and not a task, someone once pointed out the bad guys far outweigh the good guys in this battle. With every new threat and every new vulnerability HPE continues to evaluate the risk and formulate the approach to block the attack while continuing to engineer better and safer products to help our customers protect their data.

This paper is targeted to inform about current strategies and offerings around the world's leading all flash storage provider, the HPE 3PAR StoreServ array, along with the new offerings included in HPE 3PAR OS 3.3.1. Topics included in this paper are as follows:

- HPE 3PAR Secure Storage Architecture
  - HPE 3PAR StoreServ
  - HPE 3PAR OS 3.3.1
  - HPE Service Processor 5.0
- HPE 3PAR Policy Server
- HPE 3PAR Secure Transfer Service
  - Axeda
  - RDA Domino
- HPE 3PAR Data at Rest Encryption
- HPE 3PAR Remote Syslog Server
- HPE 3PAR Certifications and Compliance
- HPE 3PAR StoreServ Management Console (SSMC)
- Security Protocols
- HPE 3PAR Two Factor Authentication
- Common customer questions

HPE 3PAR Secure StoreServ architecture

The HPE 3PAR Secure StoreServ architecture is a large eco system comprised of many different components as illustrated in Figure 1.

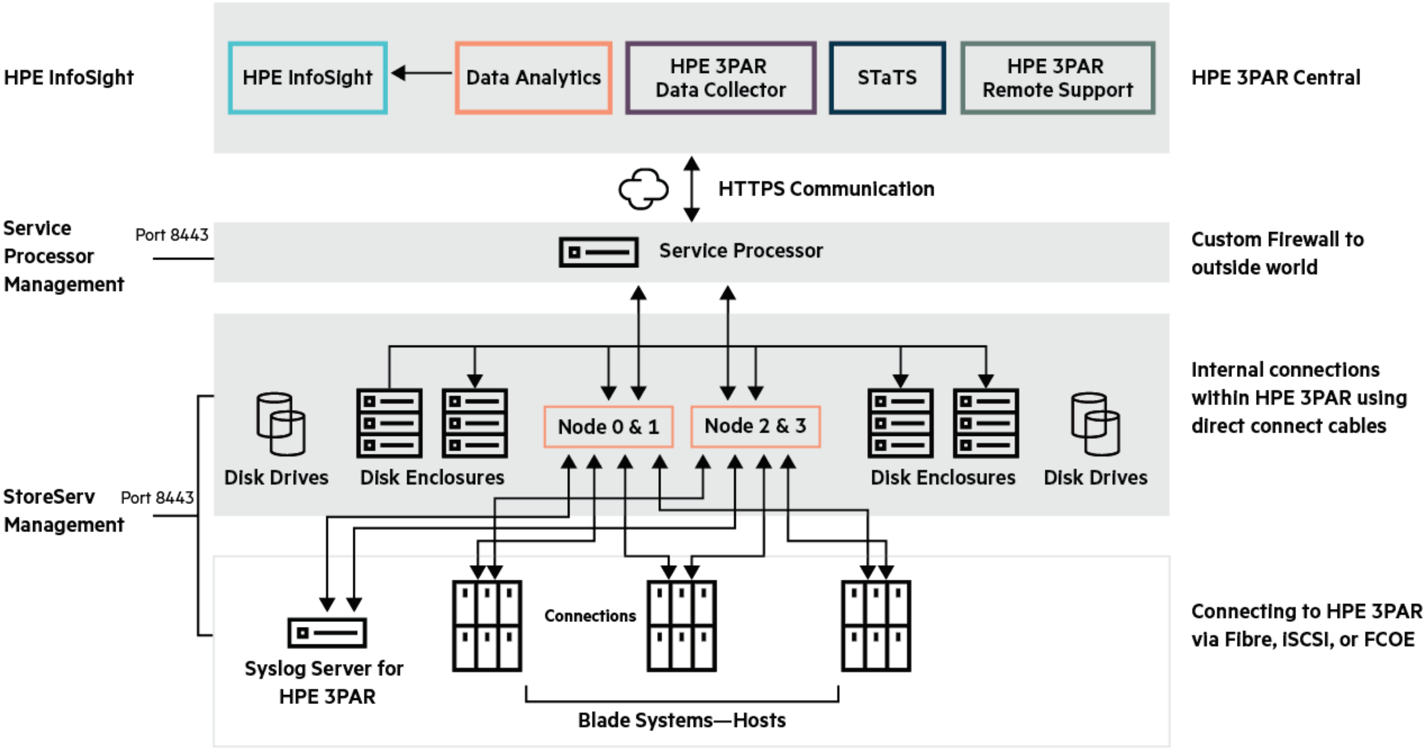


Figure 1. HPE 3PAR Secure StoreServ architecture

The HPE 3PAR consists of hardware with controllers and disks, virtualization with common provisioning groups (CPG) and virtual volumes, highly redundant in all hardware along with remote copy and federation and with management using HPE 3PAR StoreServ Management Console (SSMC). The combination of all these components provide customers with a highly available world class storage system designed to deliver optimum performance at the lowest cost possible.

HPE 3PAR ensures secure datacenter environment for customers.

HPE 3PAR OS Structure

The HPE 3PAR OS architecture is structured around Debian Linux® kernel. The kernel itself is isolated from users as the command structure uses a sophisticated structure command line (CLI) architecture to manage the HPE 3PAR StoreServ array. Each command in the cli is a captive command which maintains barrier from the internal structure of Linux. Since the OS is built on a solid operating system such as Linux, the 3PAR OS uses the up to date features of the Linux kernel.

Communication

Current 3PAR OS structure communicates through TLS 1.2 as its standard. TLS 1.0 and 1.1 have been turned off as these variations were susceptible to a compromised data structure. TLS clients which are configured for older TLS versions may no longer connect to the 3PAR array after the array is updated to 3.3.1.

Best practice
Update or reconfigure, affected TLS clients to use TLS 1.2.

Common Vulnerability and Exposure (CVE)—Ciphers

In the recent months there have been several vulnerabilities which have pointed to areas of concern in ciphers. A ciphers definition is an algorithm for performing encryption—decryption of data, it is a series of defined steps by which data is either encrypted from standard character to encrypted data. There are a number of different ciphers used in the industry to mask plaintext data. AES and DES are samples of such ciphers. More information can be gained on ciphers by exploring the web and searching for computer ciphers.

There are a number of different ciphers which can be used to secure information, HPE 3PAR StoreServ supports the following ciphers in the code, AES128-SHA, AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA. As part of an ongoing investigation into security and scanning for known vulnerabilities, HPE 3PAR StoreServ addresses any vulnerabilities that may have an impact. Many vulnerabilities that may have had an impact were addressed with the HPE 3PAR OS 3.3.1.

Best practice

Previously supported ciphers are no longer supported: DHE-RSA-AES256-GCM-SHA384, DHE-RSA-AES128-GCM-SHA256

Newly supported ciphers are now in place with OS 3.3.1: AES128-SHA, AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA

HPE 3PAR StoreServ Port Assignments—Node (Block)

Ports on any storage array can be a weak point unless they are closely monitored and aligned with the hardening of the storage array itself. On the HPE 3PAR StoreServ array the following ports are considered harden ports and allow traffic. All other ports on the array should be disabled. Table 1 contains a list of currently supported ports on the HPE 3PAR StoreServ array. Reference for port settings are contained in the "HPE 3PAR StoreServ 3.2.x Security Technical Implementation Guide Version 1, Release 1" dated 25th July 2016.

Table 1. Port Assignments HPE 3PAR OS

Port	Used by
22	SSH daemon (required) communication between SP and HPE 3PAR StoreServ array as well as optional use for end-user CLI (listener)
123	(UDP) NTP (required) peer communication for network time protocol
161	SNMP agent (optional) communications between third-party SNMP manager and 3PAR SNMP agent (listener)
162	SNMP trap origination (optional) source port for unsolicited SNMP traps to third-party SNMP manager (source)
5783	CLI secured with TLS (required) encrypted access to CLI, Service Processor to HPE 3PAR StoreServ nodes communication as well as end user CLI usage
5989	Default port for CIM-XML connections (anticipated to be supported in next STIG)

Best practice

Use the following script from a Linux host to identify unneeded ports which may be open.

cli% nmap -sT -sU -sV --version-all -vv -p1 -65535 <ip address of storage system>

If any other ports are opened other than the above ports, the user should use the following command.

cli% setnet disableports yes

Confirm the operation by entering "y" and pressing "Enter".

Note: Using the command to disable ports specifies the network configuration functionality where if the option is specified as "yes" will disable the non-encrypted ports, if option "no" is specified, it will enable the non-encrypted ports. Disabling non-encrypted ports will also prevent the service processor from monitoring events, which will prevent the generation of email notifications about system issues.

HPE 3PAR StoreServ Port Assignments—Node (File)

The HPE 3PAR File Persona Software suite provides a converged storage solution for file services and object access along with block services on HPE 3PAR StoreServ systems. The HPE 3PAR File Persona Software is a feature of the HPE 3PAR OS which enables a rich set of file protocols and core file data services on the following converged HPE 3PAR StoreServ.

In Table 2 is a list of port numbers and protocols needed for the HPE 3PAR File Persona feature to function.

Table 2. HPE 3PAR File Persona Ports

Port	Used by	Traffic flow
21	FTP for Incoming traffic used by Node IP	Incoming
53	DNS used by Node IP	Outgoing
137	NetBIOS name service used by Node IP	Incoming
138	NetBIOS datagram service required by Node IP	Incoming
139	NetBIOS session service required by Node IP	Incoming
389	Enterprise class open source LDAP server	Outgoing
443	Standard TCP port that is used for website which use SSL	Incoming
445	Server Message Blocks or (SMB) over IP	Incoming
464	Used by Kerberos V Change and Set Password	Outgoing
636	Secure port used by LDAP server	Outgoing
662	Used for datagram transmissions	Incoming
749	Kerberos administration	Outgoing
875	NFS quota	Incoming
892	NFS mountd	Incoming
1344	ICAP port used with AntiVirus software	Outgoing
2020	NFS Stat	Outgoing
2049	NFSv4	Incoming
3260	iSCSI for NDMP backups	Outgoing
10000	Network Data Management Protocol (NDMP)	Incoming
32769	NFS lock manager (lockd) handles file-lock requests from clients	Incoming
32803	NFS lock manager (TCP)	Incoming

StoreServ Management Console (SSMC) Ports

SSMC requires specific ports for communication. Hewlett Packard Enterprise also recommends configuring an LDAP server as an authentication method for connecting to a 3PAR StoreServ array.

Inbound and outbound port settings

To allow inbound communication from a browser, SSMC uses inbound port 8443 (default). You can change this port to another secured port setting without reinstalling SSMC. To communicate with an array, SSMC uses outbound port 5783. You cannot change this port. SSMC also uses port 443 to communicate with infosight.hpe.com and retrieves version information about SSMC and the HPE 3PAR operating system.

HPE 3PAR Service Processor Ports

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 Service Processor Onsite Customer Care (SPOCC) 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.

The service processor communicates with 3PAR Central via secure transmissions using either Axeda or RDA Domino (covered in separate section) as illustrated in Figure 2.

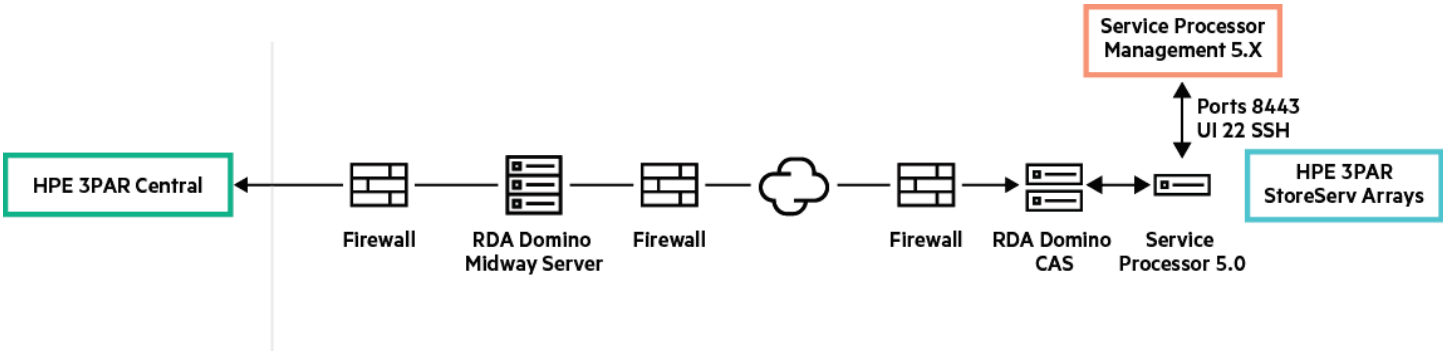


Figure 2. Service processor secure communication

All interactive communication with the service process is through either one of two ports:

Port	Used by
22	SSH used initially to designate IP address of service processor or to change IP parameters of the service processor
8443	SSL port which is used by the UI as the management interface to the service processor
443	Used by transport engine to transmit telemetry data back to HPE 3PAR Central

Transport Agents

The transport agents work to transmit data back to HPE 3PAR central. The transport agents whether it be Axeda or HPE RDA Domino use Hypertext Transfer Protocol Service (HTTPS) as the 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 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)

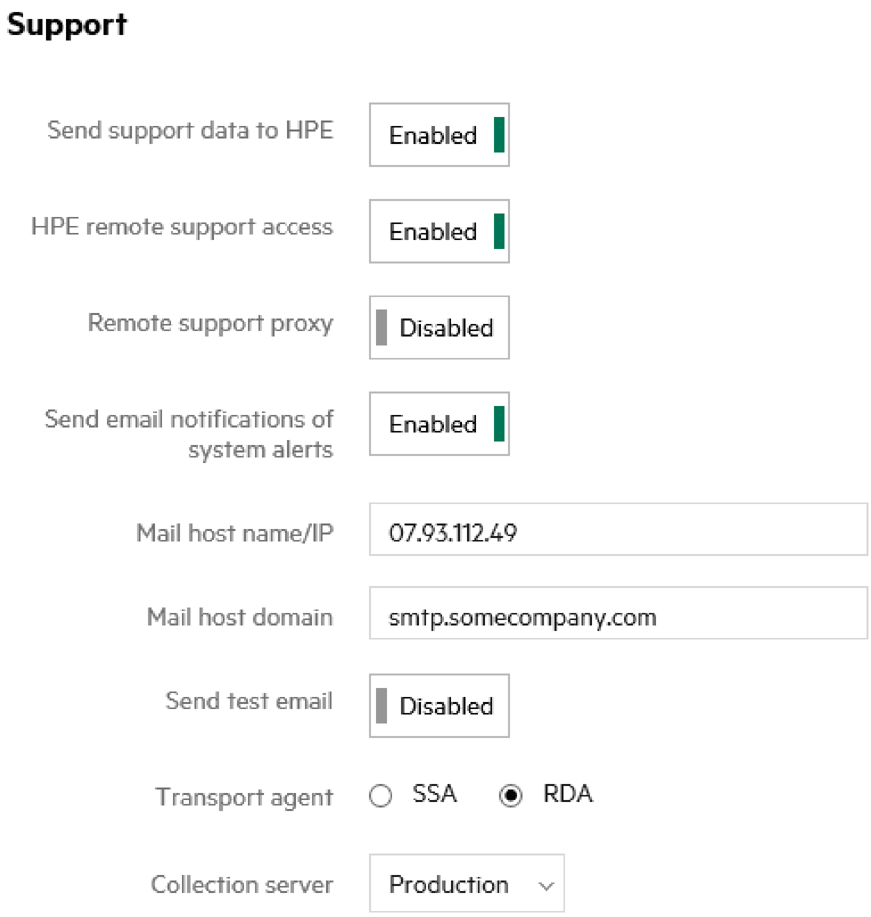
- HPE 3PAR Service Processor initiates all communications in an outbound manner
- Data authentication at HPE 3PAR Central uses a Certificate of Authority authenticated by VeriSign
- Data is NOT transferred in Clear Text

HPE RDA Domino

HPE RDA Domino is designed to be a “Meet in the Middle” connectivity solution. RDA Domino is divided into the following three main components.

RDA Domino Customer Access Server—the custom access server (CAS) is part of the service processor software which is deployed as either a physical or a virtual unit. The CAS server client connects to the Midway server URL embedded as part of the RDA client code and presents a Class 2 Private CA certificate for validation by the Midway server. The RDA client will also provide the Midway server with metadata as to the secure processor for proper identification.

By default, RDA domino is not selected as the transport agent and must be configured either upon the Moment of Birth (MOB) on the service processor or by logging in through the user "hpesupport" and modifying the transport agent identified under the support heading. An illustration of the transport agent setting on the service processor is shown in Figure 3.



Support

Send support data to HPE	Enabled
HPE remote support access	Enabled
Remote support proxy	Disabled
Send email notifications of system alerts	Enabled
Mail host name/IP	07.93.112.49
Mail host domain	smtp.somecompany.com
Send test email	Disabled
Transport agent	○ SSA ● RDA
Collection server	Production

Figure 3. RDA/Axeda modifications page

RDA Domino Midway Servers—the Midway servers are located in the HPE DMZ at HPE 3PAR Central. The servers serve as the master control for all connections. The servers are also responsible for issuing, verifying, and revoking HPE RDA certificates. The Midway servers maintain a list of valid HPE RDA certificates. Midway servers manage connections by issuing one time digital keys that are used to uniquely identify connection pipes. The Midway servers function as a digital switchboard, managing communication paths between the RDA Domino Access Server and the RDA Domino Support clients and other HPE resources.

HPE Axeda

The Axeda platform is a secure and scalable foundation to build and deploy enterprise-grade applications. An Axeda Agent is essentially an application that is capable of representing the devices it is connected to, publishing the data from those devices to the Axeda platform, and allowing the Axeda platform to have some control of the devices. The software itself like the RDA software is incorporated into the Service Processor software.

Axeda uses a Machine 2 Machine (M2M) technology in its deployment of the software. Once data is collected by the Service Processor, a process is initiated to call home with the collected data. The data is transmitted via secure transmission to HPE 3PAR Central whereby the data which has been collected is processed.

Transported Data

Question: What data is collected and sent back to HPE?

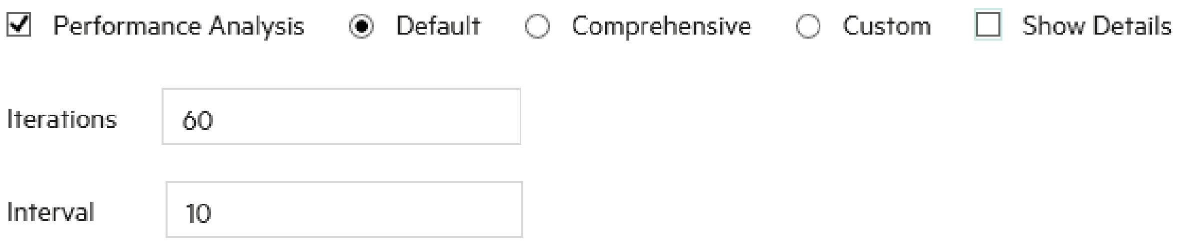
Answer: Data sent back to HPE 3PAR Central includes data from the following categories:

Service Processor:

- Weekly data which includes:
  - Alerts
  - Config data
  - Environmental data
  - Event data
  - Event log
  - Mem data
  - Performance data
  - SP config file
  - Status data
- HPE SPLOR—To collect data to diagnose SP issues, the user can request to run a Service Process Log Out Request (SPLOR)

HPE 3PAR StoreServ Array

- Generated data—data which at that moment the collection will be process
  - InSplore data—collection of all registers and other important data from the HPE 3PAR StoreServ
  - Performance—performance collection is a at time collection and falls into the categories illustrated in Figure 4
- Existing files—files which had been previously generated, typically due to an issue on the array
  - Application core files
  - System crash dump files



☑ Performance Analysis ● Default ○ Comprehensive ○ Custom □ Show Details

Iterations 60

Interval 10

Figure 4. Perf Anal collection files

Transferred Data Contents

It is important to note, that while different telemetry or event data is transferred back to HPE 3PAR Central to be processed, no customer data is ever transmitted. Customer data is always protected from transport and the only information which is transmitted is the serial number of the registered array. HPE 3PAR cannot access customer data remotely, any access to this data must be done via customer assisted transactions. Data sharing is typically done using a WebEx, HPE Virtual Room or some other data sharing method where the customer is logged in and sharing information with HPE 3PAR support personnel.

HPE 3PAR Policy Server

HPE 3PAR Policy Server is designed to ensure only authorized personnel access to, and use of, assets that are running Agent Gateway or Policy Agents. Policy Server is a server-based application that resides on a customer's network. Through the Policy Servers user interface, customers can set and control all permissions for outside access to the HPE 3PAR StoreServ arrays attached to the unit.

Users can use the browser-based user interface of Policy Server to configure policies and monitor requests for operations. Through the Policies component of the application, authenticated users can manage policies and accept or deny requests to perform operations on assets. The Audit component displays a history of actions by Policy Server users and communications with assets managed by Policy Server. Through the Users component, administrators of the Policy Server can assign privileges to profiles, profiles to roles, and roles to user accounts to control access to the components of the Policy Server application.

HSQL Database provides a standalone, open source, Java-based relational database to store and manage the Policy Server configurations. The HSQL database can be installed and set up for use with Policy Server through the installation program for Policy Server. Apache Tomcat provides the web application and file realm component for Policy Server. OpenDS directory server provides an "internal" directory server for managing access to the Policy Server application. Tomcat is installed with Policy Server. You can install the internal OpenDS directory server on the same machine as Policy Server. Alternatively, you can configure an "external" directory server to manage access to the Policy Server application. Policy Server supports the Sun ONE LDAP (Java System) directory server, Microsoft® Active Directory Server, and OpenDS LDAP directory servers for "external" use.

For secure communications with your assets, HPE 3PAR Policy Server supports the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols. Before installation, you need to create the hostname.jks file for the machine where Policy Server will run and make sure that either port 443 or port 8443 is available for Policy Server. During installation, you configure Policy Server to use SSL. You can configure the Agents running on your assets to use SSL when communicating with Policy Server through Agent Builder or Agent Deployment Utility.

Protocol Updates HPE 3PAR OS 3.3.1 Ciphers

What is a Cipher? As defined by Wikipedia, a cipher is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. The operation of a cipher usually depends on a piece of auxiliary information, called a key (or, in traditional NSA parlance, a crypto variable). The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be extremely difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

There are a number of different cipher suites available and differ depending on which the TLS backend was built on. HPE 3PAR continues to evaluate the different ciphers suites and will choose the suite best suited for the environment.

CLI Cipher

Changes were made to the cipher used to secure the connection between the HPE 3PAR StoreServ array and the CLI clients. The Transport Layer Security (TLS) handshake protocol now only supports TLS v1.2. TLS v1.0 & 1.1 were dropped from the supported protocols.

Handshake protocol creates the authentication methodology by which the client responds to a request. During the protocol exchange a certificate is exchanged dependent upon the cipher which is selected during the handshake process. The following ciphers are supported in 3PAR OS 3.3.1

Cipher support:

- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

What is DHE-RSA? DHE is short for Diffie-Hellman ephemeral security modes. In short it is the method for exchanging cryptographic keys over a public channel. In 3PAR OS 3.3.1, the key size was increased from 512 to 2048. This increase in size supports a better security structure.

Once the initial connection is configured using DHE, the RSA cryptosystem creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The RSA algorithm involves four steps: key generation, key distribution, encryption, and decryption.

For more information about the above ciphers and methodologies search the internet, there are many excellent articles with in-depth coverage of all secure transmission concepts.

SSH Cipher

In OS 3.3.1 there is a change to ciphers SSH uses to establish secure connection between the array and clients. The changes to the cipher is as follows.

Three groups of ciphers that are used for SSH are modified as follows:

- Key Exchange Algorithms (Used to exchange the key for the Encryption Algorithms)
  - Drop support for: curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
  - Retain support for: diffie-hellman-group-exchange-sha256
- Encryption Algorithms (One time symmetric keys/ciphers used to encrypt a socket)
  - Drop support for: aes192-cbc, aes256-cbc, aes128-cbc, 3des-cbc
  - Retain support for: chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr
- MAC (message authentication code) Algorithms. Used for data integrity
  - Drop support for: hmac-sha1, hmac-sha1-96
  - Add support for: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-ripemd160-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-512, hmac-sha2-256, hmac-ripemd160, umac-128@openssh.com
  - Customer is not given control of the ciphers used by SSH

HPE 3PAR Security Standards

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes. HPE 3PAR recognizes the importance of this standard and is currently working on ensuring products are secure by design to assist customer in meeting the PCI-DSS compliance requirement, since it's not the storage that can be PCI-DSS compliant, but it's the overall storage data center that needs to be PCI compliant.

Although the PCI-DSS must be implemented by all entities that process, store, or transmit cardholder data, formal validation of PCI-DSS compliance is not mandatory for all entities. The requirements for this standard are very stringent on data transmission through wireless access points and the access to those points. The document further states that the vendors are responsible for running vulnerability tests within their infrastructure and conduct penetration tests both internally and externally.

While the data transmission is outside the scope of the HPE 3PAR StoreServ, the data storage is required to be encrypted. HPE 3PAR StoreServ does support encrypted data at rest through the use of FIPS compliant disks. The HPE 3PAR OS is regularly scanned for vulnerabilities and penetration tests are conducted on all versions of the HPE 3PAR OS on a timely basis.

Pen Testing

Penetration testing (a.k.a. Pen testing) is conducting tests on a computer system, storage array, network of web application for sole purpose of finding vulnerabilities that a hacker could exploit. The main objective of penetration testing is to determine security weaknesses of the tested system. The process of penetration testing may be simplified as two parts:

1. Discover vulnerabilities—combinations of legal operations that let the tester execute an illegal operation
2. Exploit the vulnerabilities—Specify the illegal operation

Once the attacker has exploited one vulnerability they may gain access to other machines so the process repeats i.e., look for new vulnerabilities and attempt to exploit them.

The HPE 3PAR OS is built around the frame of Debian Linux kernel. The kernel is not a full-blown version of the OS but rather uses the shell of the OS structure. Regardless of the structure of the kernel, if the kernel becomes susceptible for hacks from outside sources, HPE 3PAR will work closely with Debian to help mitigate any external attacks. To help identify exposures the software may be exposed to, HPE 3PAR continually performs Pen testing on the HPE 3PAR OS. Figure 5 illustrates pen testing and pushing attacks to access vulnerabilities.

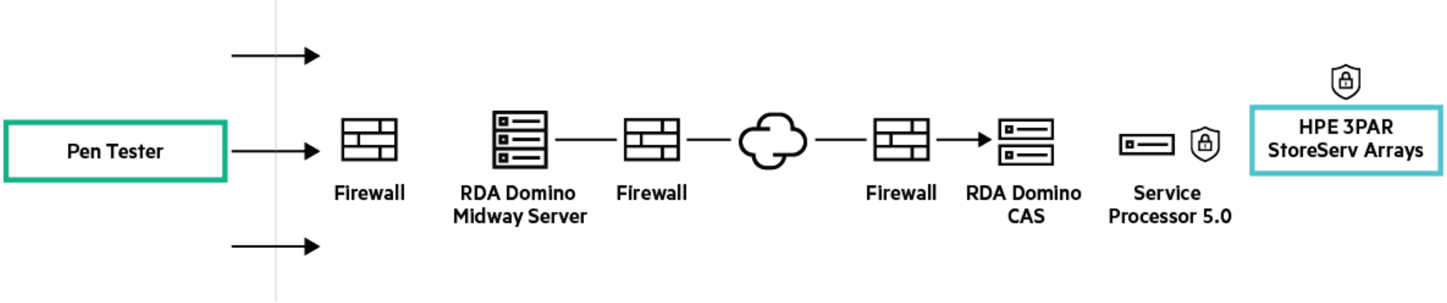


Figure 5. Pen Testing

Pen test strategies for HPE 3PAR OS include the following:

- **Internal HPE testing**—these tests are conducted by HPE 3PAR internal Systems Quality Assurance (SQA) during each build of the HPE 3PAR OS. Testing ensures that no known vulnerabilities are uncovered during the testing process
- **External outside contractor testing**—HPE 3PAR may acquire the service of an outside vendor to conduct intensive pen tests on the HPE 3PAR OS, this extensive testing is either annually done or after a major release of the HPE 3PAR OS

Pen testing methods include the following, HPE may do some or all of the testing dependent on the HPE 3PAR OS lifecycle.

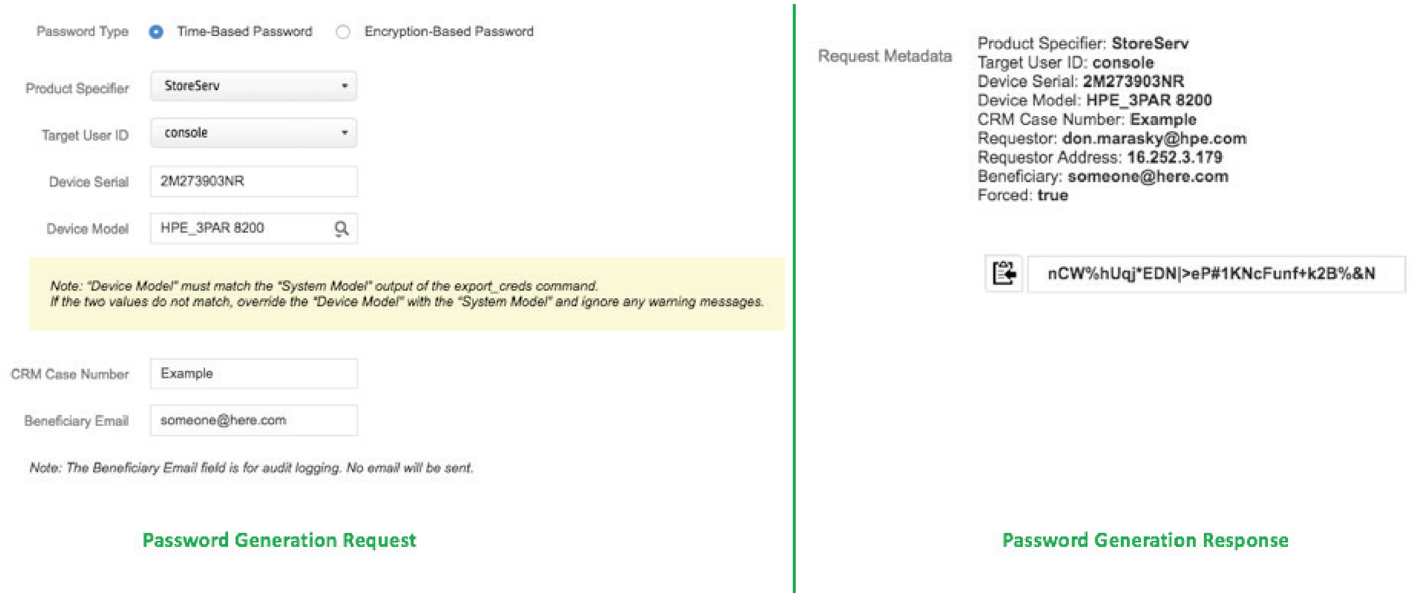
- Targeted testing—testing done by SQA and HPE security team on HPE 3PAR OS, typically looking for a defined or newly defined vulnerability
- External testing—pen tests targets the HPE 3PAR StoreServ array through company servers and external applications. The objective is to identify if an outside attacker can get access and how far they can get in once they've gained access
- Blind testing—a blind test strategy simulates the actions and processes of a real attacker by limiting the information given the team about the structure of the HPE 3PAR StoreServ

Strong Password Protection Schema

Starting with the HPE 3PAR OS 3.2.2 MU2 and above HPE 3PAR will use either a time-based password or encryption based password system for all privileged accounts. Previous privileged accounts will now require the user to call HPE 3PAR support and request one of the two types of generated passwords. The two types of password generation are as follows.

Time-based passwords

Time-based passwords are unique to each service user account and HPE 3PAR StoreServ. They change each hour and can only be generated in the HPE support center to authorized HPE employees and contractors. While operating in time-based mode, passwords cannot be changed since they change automatically each hour. On choosing time-based passwords, you do not need to change your HPE support processes. Figure 6 illustrates the generation of a time-based password on the left and an example of the password generated on the right side.



Password Type ● Time-Based Password ○ Encryption-Based Password

Product Specifier: StoreServ

Target User ID: console

Device Serial: 2M273903NR

Device Model: HPE_3PAR 8200

*Note: "Device Model" must match the "System Model" output of the export_creds command.
If the two values do not match, override the "Device Model" with the "System Model" and ignore any warning messages.*

CRM Case Number: Example

Beneficiary Email: someone@here.com

Note: The Beneficiary Email field is for audit logging. No email will be sent.

Password Generation Request

Request Metadata

Product Specifier: **StoreServ**
Target User ID: **console**
Device Serial: **2M273903NR**
Device Model: **HPE_3PAR 8200**
CRM Case Number: **Example**
Requestor: **don.marasky@hpe.com**
Requestor Address: **16.252.3.179**
Beneficiary: **someone@here.com**
Forced: **true**

nCW%hUqj*EDN|>eP#1KNcFunf+k2B%&N

Password Generation Response

Figure 6. Password generation/time-based

Encrypted ciphertext passwords

Encrypted ciphertext passwords are randomly created on the HPE 3PAR StoreServ for each service user account. You can change these passwords any time; however, the passwords are not known to your or to HPE. Recovery is only possible by exporting the ciphertext for transmission to HPE, where an authorized support center user can decrypt the ciphertext to provide the password to on-site HPE service personnel or contractors. If you choose encrypted ciphertext passwords, you need to export the ciphertext and provide it to the HPE personnel working with you. The ciphertext is pasted into a tool at HPE that can unwrap and decrypt the ciphertext to recover the password. After the support activity is complete, you can change the password so that the recovered password is no longer valid.

Exporting ciphertext

In the encrypted ciphertext mode, use the controlrecoveryauth ciphertext <user> command to export the ciphertext for a service account. This command displays the ciphertext associated with the specified service user account. You can copy and paste that ciphertext into an email to the HPE support center or to the HPE support engineer who is working with you. The ciphertext is protected from exposure if you email it. The random credential contained in the ciphertext is first encrypted and is then wrapped using a public key. This makes the ciphertext secure for transmission, because only the corresponding private key at HPE can unwrap the encrypted credential.

Changing the ciphertext password

To change passwords in encrypted ciphertext mode, use the controlrecoveryauth rollcred <user> command. This causes a new random password to be generated and assigned to the specified service user account. The two accounts that are affected are root and console. On the HPE 3PAR StoreServ, these user accounts are not used for most maintenance actions.

Setting or changing the Password Mode

To query or change the current setting of the strong service account password system, use the 3PAR CLI command controlrecoveryauth (to change the mode from time-based to encrypted ciphertext, for example).

- To query the current mode, use the command controlrecoveryauth status
- To change the mode, use the command controlrecoveryauth setmethod [totp|ciphertext], choosing either totp (time-based passwords) or ciphertext

In version 5.0 the HPE 3PAR Service Processor adopted the use of strong passwords.

Two factor Authentication

Single form of an authentication is starting to fade away as secure locations look to new ways to thwart unwanted cyber entry into data centers and data farms. Recently with HPE 3PAR OS 3.3.1 the Lightweight Directory Access Protocol was rewritten on the HPE 3PAR StoreServ arrays to comply with the latest standards of the protocol. The following changes were made to the LDAP structure:

- Support Active Directory and LDAP authentication via SSH
- Support Active Directory and authentication via WSAPI
- Support Active Directory and LDAP authentication via CLI with UPN username format
- Support Active Directory and LDAP authentication via SSMC and UPN username format

With these changes included in HPE 3PAR OS 3.3.1, this allowed engineering to support using a two factor authentication. Figure 7 simply illustrates the two-step authentication process.

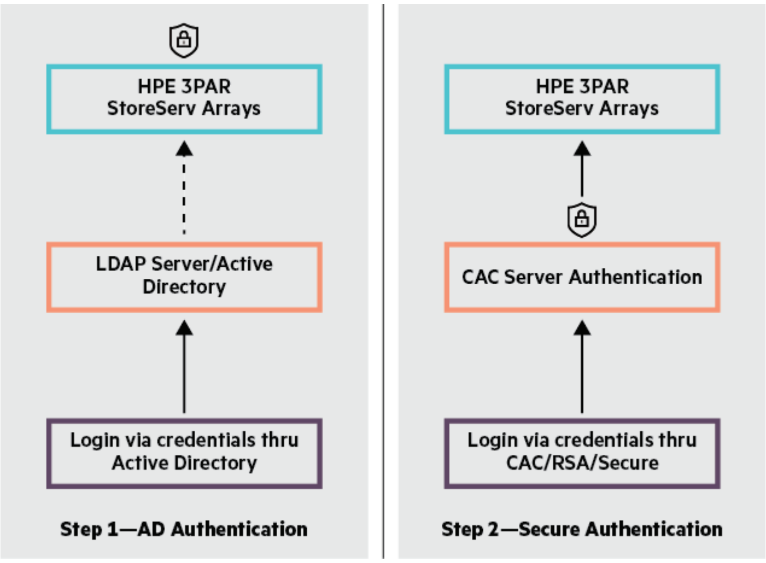

HPE 3PAR StoreServ Arrays
LDAP Server/Active Directory
Login via credentials thru Active Directory
Step 1—AD Authentication
HPE 3PAR StoreServ Arrays
CAC Server Authentication
Login via credentials thru CAC/RSA/Secure
Step 2—Secure Authentication

Figure 7. Two factor authentication

Step 1 illustrates the user will initially authenticate using Active Directory/LDAP to login into the domain, although the user has successfully logged into the domain, they have no access to the HPE 3PAR StoreServ array since additional security remediation must occur.

Step 2 identifies the user then must use a secure methodology to enable login into the HPE 3PAR StoreServ. Login is accomplished via HPE 3PAR SSMC and is not supported using the CLI. Currently the secure methodology would use a Common Access Card (CAC), Virtual Smart Card or some other form of a secure methodology to secure a connection through the SSMC to the array. Although only CAC and Virtual Smart Card have been certified for use, other methods of secure communication could be used.

Feature overview of two factor authentication is as follows:

User action	Card inserted into CAC reader Browser appears to select certificate on the CAC card Pin entered to authenticate to certificate assigned to the card
Outcome	User authenticated for appropriate SSMC/HPE 3PAR usage
LDAP settings	LDAP Service acts as a proxy for user login CAC certificate identifies user mapping to LDAP user name CAC object specifies object in LDAP which user is mapped to… SSMC/HPE 3PAR array

Security Logging

Breaches in security are very disturbing and undermine the environment by which the breach occurred. While a breach in and of itself can be devastating, it would be worse if we could not forensically identify the entry source or the type of breach which occurred. HPE 3PAR understands the need to continually work towards thwarting breaches, it also understands we need to control and provide information which can either identify entry point or help with the logging of attempted security violations. With this in mind the following tools are available to either minimize unauthorized security entries or capture logging data to help identify areas of concern.

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 inbound communications or remote service connections to and from HPE 3PAR StoreServ. 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 managed by the policy server. Looking at Figure 8, we will use the same layout of the data center and call home feature. The difference in this illustration is the addition of the Policy Manager which is installed on a separate server.

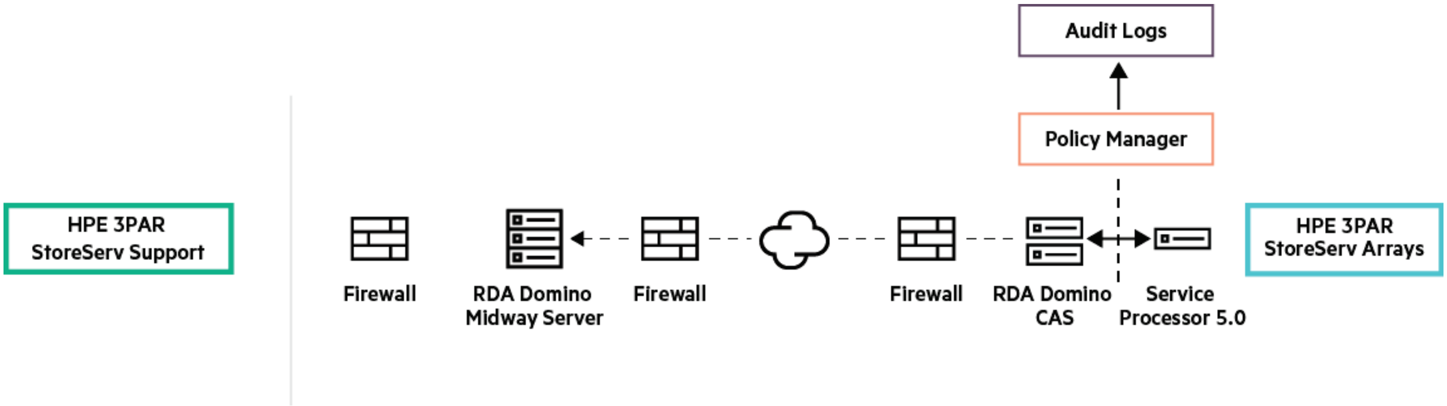


Figure 8. HPE 3PAR Policy Manager

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 StoreServ Management Console and HPE 3PAR Service Processor Audit logging

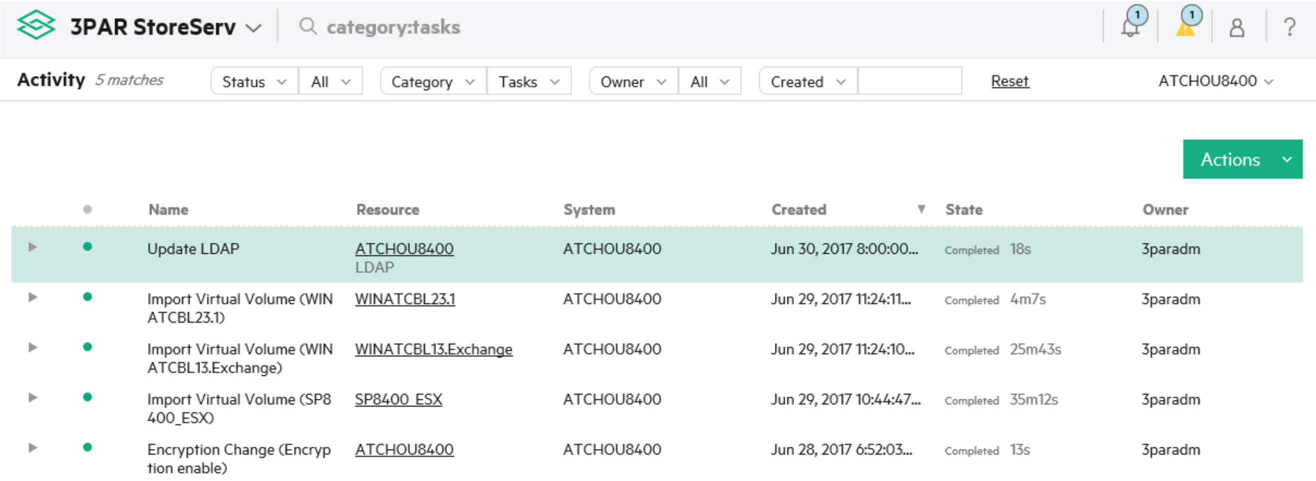
Both the HPE 3PAR Service Processor and the StoreServ Management Console use a common interface. The applications are independent of each other but the interface is common between the two. There are a number of different audit logs which are resident on each of the consoles, the location and the contents of those files are as follows.

HPE 3PAR StoreServ Management Console logs

Location of the log files for the SSMC reside on the server where the tool is installed. To reference the log files user should log into the server and navigate to the following area, “C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data\logs”. Once the user navigates to this area the files listed below can be examined.

- Audit logs
- Event logs
- Fatal logs
- Federation
- Rest history
- Metrics
- SSMC

The user can get information within SSMC which is useful in examining recent user task which were completed on the array. Figure 9 illustrates examining **Activity** → **Status** All → **Category** Tasks → **Owner** All



Activity *5 matches*

Status All | Category Tasks | Owner All | Created | Reset | ATCHOU8400

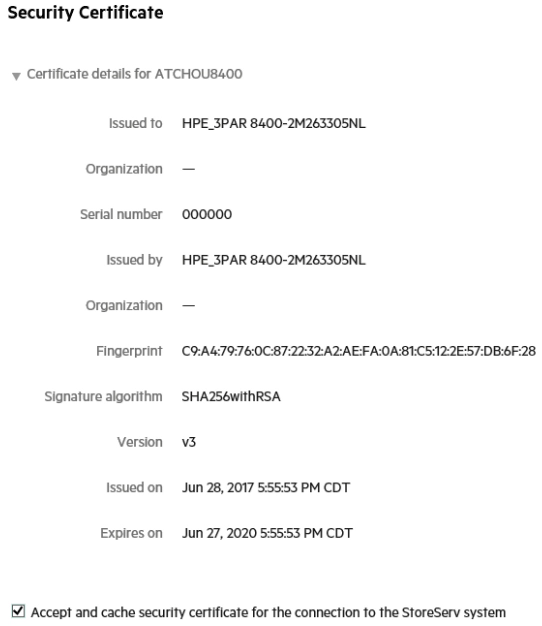
	Name	Resource	System	Created	State		Owner
●	Update LDAP	ATCHOU8400 LDAP	ATCHOU8400	Jun 30, 2017 8:00:00...	Completed	18s	3paradm
●	Import Virtual Volume (WIN ATCBL23.1)	WINATCBL23.1	ATCHOU8400	Jun 29, 2017 11:24:11...	Completed	4m7s	3paradm
●	Import Virtual Volume (WIN ATCBL13.Exchange)	WINATCBL13.Exchange	ATCHOU8400	Jun 29, 2017 11:24:10...	Completed	25m43s	3paradm
●	Import Virtual Volume (SP8 400_ESX)	SP8400_ESX	ATCHOU8400	Jun 29, 2017 10:44:47...	Completed	35m12s	3paradm
●	Encryption Change (Encryp tion enable)	ATCHOU8400	ATCHOU8400	Jun 28, 2017 6:52:03...	Completed	13s	3paradm

Figure 9. SSMC recent tasks

From this example, we have identified that the user 3paradm modified LDAP configuration on the array on June 30th at 08:00. There are other entries in the log file which point to other transactions which were carried out on the array. Using this example there were a number of entries which affected the array such as encryption enablement. The importance here is the user and action they enacted are tracked, it would be easy to then correlate related issues which occurred on the array to an individual.

This should highlight the importance of adding users and assigning proper credentials to the user. Coverage of users and assigning responsibilities is discussed in a separate section of the paper.

Service Processor Certificates



Security Certificate

▾ Certificate details for ATCHOU8400

Issued to	HPE_3PAR 8400-2M263305NL
Organization	—
Serial number	000000
Issued by	HPE_3PAR 8400-2M263305NL
Organization	—
Fingerprint	C9:A4:79:76:0C:87:22:32:A2:AE:FA:0A:81:C5:12:2E:57:DB:6F:28
Signature algorithm	SHA256withRSA
Version	v3
Issued on	Jun 28, 2017 5:55:53 PM CDT
Expires on	Jun 27, 2020 5:55:53 PM CDT

☑ Accept and cache security certificate for the connection to the StoreServ system

Figure 10. Service Processor Security Certificate

As part of the communication between the HPE 3PAR StoreServ array and the HPE 3PAR Service Processor, a certificate is generated and must be accepted prior to any communications between the two devices.

There are a large number of certificates which reside on the Service Processor and there are two which cannot be modified and are as follows:

- Service Processor ←→ HPE 3PAR StoreServ array
- Service Processor ←→ to HPE 3PAR Central

Communications to HPE 3PAR Central as outlined earlier in the paper can be via legacy Axeda or the new RDA technology.

As stated earlier in the paper the base operating system on the HPE 3PAR Service Processor is Debian Linux, no version is included here as with all OS's modifications occur quite frequently to keep up with the need to offer better security. HPE will continually provide the most recent version of the Linux shell which will include all updates at the time the latest HPE Service Processor is generated. For this reason, users should maintain all updates posted to the HPE Service Processor including major release and maintenance updates (MU).

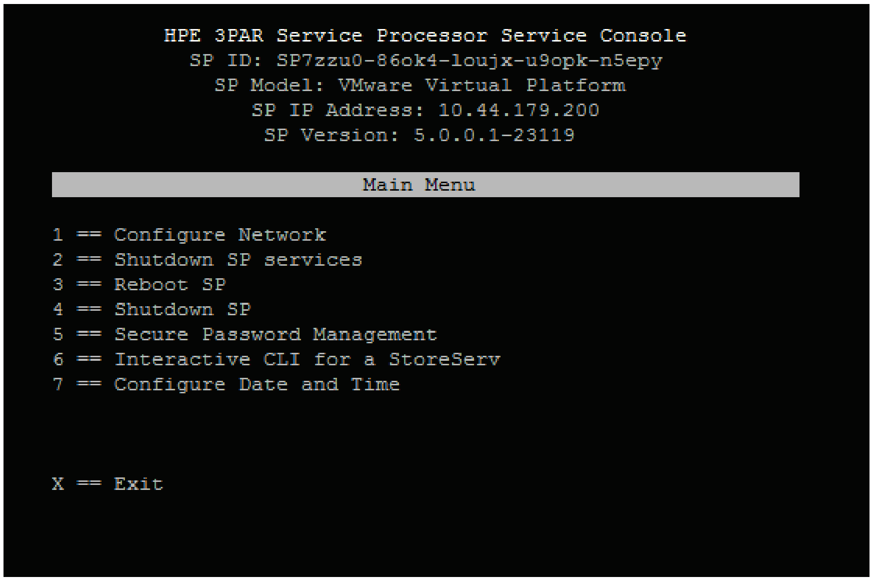
Certificates which pertain to HPE and maintained on the Service Processor are as follows:

- Hewlett Packard Enterprise Company/OU=Remote Device Access/CN=Hewlett Packard Enterprise Remote Device Access Root CA/emailAddress=rda@hpe.com
- Hewlett Packard Enterprise Company/OU=Symantec Trust Network/OU=Class 2 Managed PKI Individual Subscriber CA/CN=Hewlett Packard Enterprise Collaboration CA
- Hewlett Packard Enterprise Company/OU=Infrastructure Services/CN=Hewlett Packard Enterprise Private Root CA
- Hewlett Packard Enterprise Company/OU=Infrastructure Services/CN=Hewlett Packard Enterprise Private SSL CA
- /O=HPE.com/OU=IT Infrastructure/C=US/O=Hewlett-Packard Company/CN=Hewlett-Packard Private Class 2 Certification Authority

Limited command console

One of the major changes to SP 5.0 is the elimination of featured access accounts on the SP. A featured account was an account by which the user when logged in, had the ability to modify the parameters within the SP.

With SP5.0 all user accounts are captive and have limited options available. The screen to the right displays one of the two authorized accounts (admin and hpepartner) and illustrates the limited account options available to the user.



```
            HPE 3PAR Service Processor Service Console
              SP ID: SP7zzu0-86ok4-loujx-u9opk-n5epy
                SP Model: VMware Virtual Platform
                   SP IP Address: 10.44.179.200
                    SP Version: 5.0.0.1-23119

                            Main Menu

1 == Configure Network
2 == Shutdown SP services
3 == Reboot SP
4 == Shutdown SP
5 == Secure Password Management
6 == Interactive CLI for a StoreServ
7 == Configure Date and Time



X == Exit
```

Audit logging (SP)

Audit information which pertains to the HPE 3PAR SP is located under Files section. To gain access to the audit log the user (either admin or hpepartner) navigates through the drop-down menu located under 3PAR Service Console header on the top left side. Under the header is the General category by which the Files section is displayed.

Once the user has navigated to the Files section it is easy to locate the audit log. The audit log is plain ascii text file and can be manipulated with a number of different process. In the following excerpt from the audit log, there is an entry which identifies an unauthorized login attempt.

"13:52:04.870-0500","**16.116.132.162**","n/a","admin","unknown","CREATE","SPUserSession","UNAUTHORIZED","INFO","Session Action","**admin**","**Invalid SP user (admin) or password.**" "2017-07-05 13:52:04.884"

The illegal attempt to login was created by me, and highlighted in the message is the ip address I am assigned currently on my laptop as illustrated below using the ipconfig command from windows.

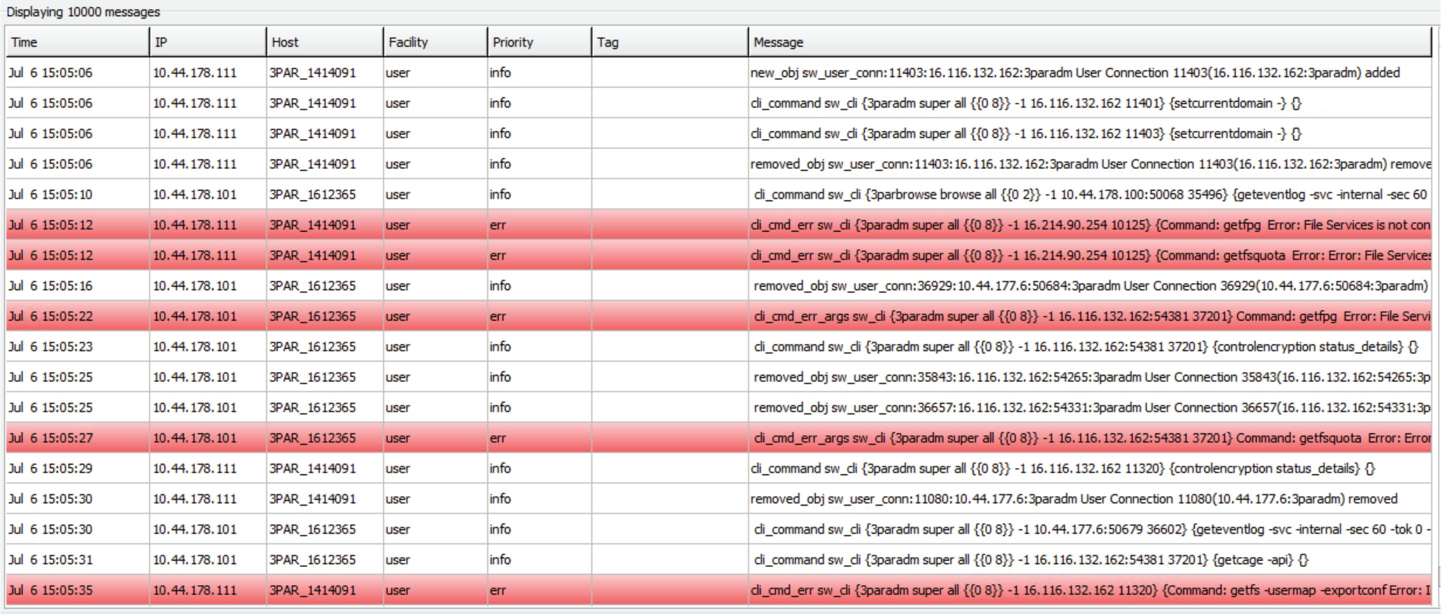
```
Ethernet adapter Local Area Connection* 5:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 16.116.132.162
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :
```

I attempted to login into the admin account with an unauthorized password at the time and date also shown in the capture.

Syslog

The HPE 3PAR StoreServ utilizes the function of syslog to maintain data used for analysis, recording array functions and maintaining a security log of all transactions which occur on the array. Figure 11 illustrates a sample of the data which streams from the array. Output of the data is often considered very chatty and verbose; most users will need some type of a logging tool if data is to be maintained or monitored.



Displaying 10000 messages

Time	IP	Host	Facility	Priority	Tag	Message
Jul 6 15:05:06	10.44.178.111	3PAR_1414091	user	info		new_obj sw_user_conn:11403:16.116.132.162:3paradm User Connection 11403(16.116.132.162:3paradm) added
Jul 6 15:05:06	10.44.178.111	3PAR_1414091	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 16.116.132.162 11401} {setcurrentdomain -} {}
Jul 6 15:05:06	10.44.178.111	3PAR_1414091	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 16.116.132.162 11403} {setcurrentdomain -} {}
Jul 6 15:05:06	10.44.178.111	3PAR_1414091	user	info		removed_obj sw_user_conn:11403:16.116.132.162:3paradm User Connection 11403(16.116.132.162:3paradm) remove
Jul 6 15:05:10	10.44.178.101	3PAR_1612365	user	info		cli_command sw_cli {3parbrowse browse all {{0 2}} -1 10.44.178.100:50068 35496} {geteventlog -svc -internal -sec 60
Jul 6 15:05:12	10.44.178.111	3PAR_1414091	user	err		cli_cmd_err sw_cli {3paradm super all {{0 8}} -1 16.214.90.254 10125} {Command: getfpg Error: File Services is not con
Jul 6 15:05:12	10.44.178.111	3PAR_1414091	user	err		cli_cmd_err sw_cli {3paradm super all {{0 8}} -1 16.214.90.254 10125} {Command: getfsquota Error: Error: File Services
Jul 6 15:05:16	10.44.178.101	3PAR_1612365	user	info		removed_obj sw_user_conn:36929:10.44.177.6:50684:3paradm User Connection 36929(10.44.177.6:50684:3paradm)
Jul 6 15:05:22	10.44.178.101	3PAR_1612365	user	err		cli_cmd_err_args sw_cli {3paradm super all {{0 8}} -1 16.116.132.162:54381 37201} Command: getfpg Error: File Servi
Jul 6 15:05:23	10.44.178.101	3PAR_1612365	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 16.116.132.162:54381 37201} {controlencryption status_details} {}
Jul 6 15:05:25	10.44.178.101	3PAR_1612365	user	info		removed_obj sw_user_conn:35843:16.116.132.162:54265:3paradm User Connection 35843(16.116.132.162:54265:3p
Jul 6 15:05:25	10.44.178.101	3PAR_1612365	user	info		removed_obj sw_user_conn:36657:16.116.132.162:54331:3paradm User Connection 36657(16.116.132.162:54331:3p
Jul 6 15:05:27	10.44.178.101	3PAR_1612365	user	err		cli_cmd_err_args sw_cli {3paradm super all {{0 8}} -1 16.116.132.162:54381 37201} Command: getfsquota Error: Error
Jul 6 15:05:29	10.44.178.111	3PAR_1414091	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 16.116.132.162 11320} {controlencryption status_details} {}
Jul 6 15:05:30	10.44.178.111	3PAR_1414091	user	info		removed_obj sw_user_conn:11080:10.44.177.6:3paradm User Connection 11080(10.44.177.6:3paradm) removed
Jul 6 15:05:30	10.44.178.101	3PAR_1612365	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 10.44.177.6:50679 36602} {geteventlog -svc -internal -sec 60 -tok 0 -
Jul 6 15:05:31	10.44.178.101	3PAR_1612365	user	info		cli_command sw_cli {3paradm super all {{0 8}} -1 16.116.132.162:54381 37201} {getcage -api} {}
Jul 6 15:05:35	10.44.178.111	3PAR_1414091	user	err		cli_cmd_err sw_cli {3paradm super all {{0 8}} -1 16.116.132.162 11320} {Command: getfs -usermap -exportconf Error: I

Figure 11. HPE 3PAR StoreServ Syslog output

The syslog function on the array is not enabled by default, the user must enable to output through enabling parameters with the setsys command.

Remote Syslog Server

The remotes syslog server enables the process of capturing security events from an HPE 3PAR StoreServ to a remote security syslog server. The configurations will use mutually authenticated TLS configuration. The PKI uses x509 (RSA2048) certificates whose trust originates with a customer-provided certificate authority. For simplicity, the base server host operating system used in this example is RHEL6, using rsyslog and gnu-tls. Although we chose to use gnu-tls for the example, there are a wider variety of commercial and open source logging solutions which can be used.

Pre-requisites for installation

1. The HPE 3PAR StoreServ array must have a hostname that is resolvable on the network.
2. The RHEL6 security syslog server must have a hostname that is resolvable on the customer's network.
3. The RHEL6 server must be running rsyslog and gnu-tls must also be installed.
4. The RHEL6 server must have its firewall open for port 6514, TCP 6514 is the default port value for remote security syslog, but the port value is configurable.
5. Networks between the RHEL6 server and the 3PAR StoreServ array must have firewalls open for port 6514, TCP.
6. System clocks must be synchronized to a time server. Mismatched system clocks may result in errors during certificate installation.
7. The 3PAR must be running 3PAR OS version 3.3.1, or later.

RemoteSyslogHost—the remote syslog host captures data output from the array. Remote syslog utilizes UDP port 514 as the transport mechanism to send log information.

RemoteSyslogSecurityHost—is different from RemoteSyslogHost as this setting is used to report strictly on security information on the array. The security information is limited to array access and the monitoring of access points. Monitoring of these dynamics requires the user to change the transport mechanism from UDP to TLS. The use of TLS will require the user to import a CA from the system used in capturing of secure data.

The following tables outline the information gathering for using a RemoteSyslogHost with RHEL6.

Table 3. Summary of steps for configuring HPE 3PAR to use a Remote Security Syslog Server

	Description	HPE 3PAR required steps	RHEL6 required steps
1.	Collect IP addresses and credentials needed	X	X
2.	Create, sign, and install the TLS server certificate and establish CAs		X
3.	Create and export the TLS client certificate request	X	
4.	Sign client request and import the certificates to the client	X	
5.	Configure the remote security syslog feature on 3PAR client	X	
6.	Configure rsyslog on RHEL6 server		X
7.	Enable remote logging and verify operation	X	X

Where to deploy SSMC Syslog

Everywhere! Secure data architecture is paramount to all successful IT organizations. Banks, hospitals, government agencies, corporations, and any IT organization are susceptible to unauthorized access to private data. A remote syslog environment cannot guard against unauthorized entry to a data structure but it is a tool which is part of the overall strategy to securing an environment.

HPE 3PAR continues to work to change the standards for a secure storage architecture by monitoring existing and potential threats, developing new secure measures by which users can manage their environment and publishing standards applicable to today's rapidly changing security. The remote syslog server is another tool HPE 3PAR provides to help users secure their environment.

Data Encryption

Data encryption on the HPE 3PAR StoreServ array is also referred to as Data at Rest. Encryption of data only occurs on disks which are designed with the AES encryption chip internally. Data at Rest is a reference for the data as it resides on the disk drive and not while the data is in flight. HPE 3PAR does not encrypt data while in flight.

Enablement of encryption on the array can only occur when all drives within the array are FIPS 140-2 enabled. Federal Information Processing Standard (FIPS) publication 140-2 is a U.S. government security standard used to approve cryptographic modules. Enabling encryption on the array protects data on the drive if the drive is maliciously removed from the array. Protection of the drives is done through a key mechanism either enabled at the array level or externally from an authorized external key manager. Drives are secured through the exchange of keys controlled by a key manager, unauthorized drive removal locks drive from external access.

Local Key Management

The Local Key Management (LKM) enables key management at the HPE 3PAR StoreServ array. All key management is local to the HPE 3PAR StoreServ array and is controlled by an internal process of the HPE 3PAR OS. The file in which the encrypted key is kept is identified as a keystore, the keystore is kept locally within the array. A backup of the keystore is created when enabling encryption on the HPE 3PAR StoreServ array this file should be securely stored away from the array. The internal HPE 3PAR OS process which interfaces with the encrypted drives is darsvr. Figure 12 illustrates the connection of darsvr to the encrypted drives.

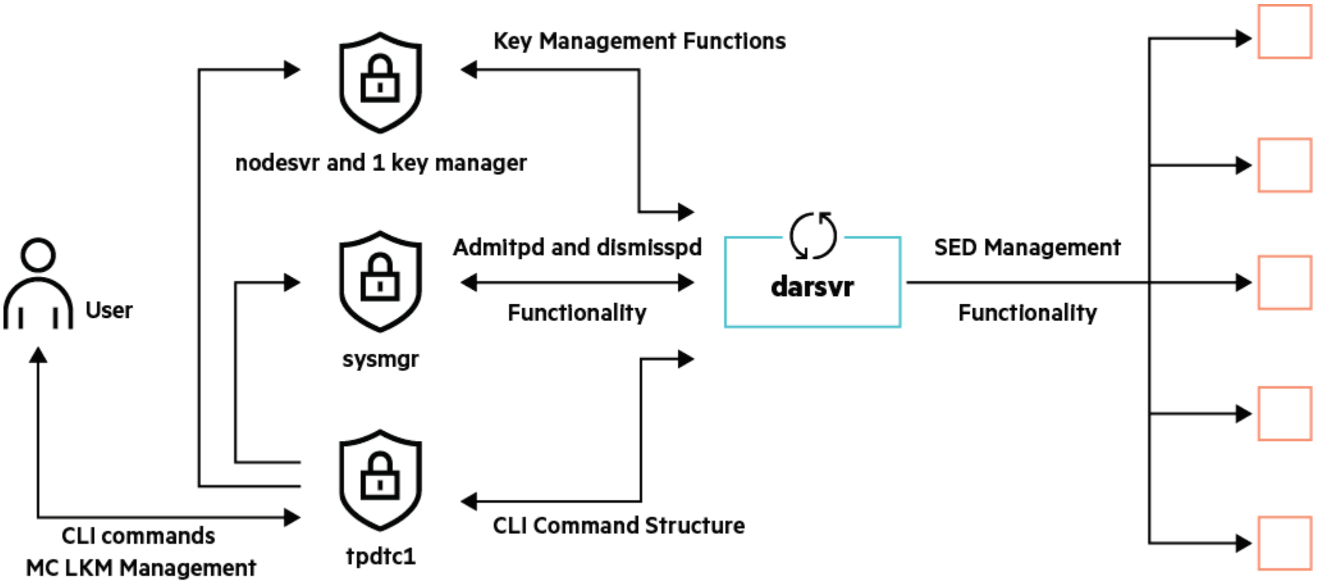


Figure 12. Local Key Management

External Secure Key Manager

As part of FIPS 140-2 compliance, starting from HPE 3PAR OS 3.2.1, HPE 3PAR will supports an External Key Manager (EKM). EKM provides a complete security solution for unifying and automating an organization's encryption controls by securely creating, protecting, serving, controlling, and auditing the encryption keys on a separate server which is only attached to the HPE 3PAR StoreServ array through the internet.

Starting with, HPE 3PAR OS 3.2.1, HPE 3PAR supports the HPE Enterprise Secure Key Manager v4.0 or SafeNet KeySecure k450 and k150. Either solution supports the HPE 3PAR StoreServ Storage arrays which are enabled for encryption. Both solutions meet the NIST Key Management standards and are validated for FIPS 140-2 level certification. As there are many other EKM's in the industry, HPE has only qualified the above EKM's to function with the HPE 3PAR StoreServ Storage array.

Similar to the LKM the EKM will use a single locking key for all drives in the array. The locking key will be managed by the EKM and is not key manager sensitive, meaning whichever HPE key manager the user deploys, EKM will use the same methodology to provide a secure locking key. In order to protect the key, a new process "fipsvr" is deployed and will be the only process which has access to the locking key. The key will only be in resident within the HPE 3PAR OS memory while the array is functioning, otherwise the key is stored in the EKM.

The following two sections will highlight the two EKM's which are supported with HPE 3PAR OS 3.2.1 and after, any further investigation into each of the products is left to the user.

GDPR

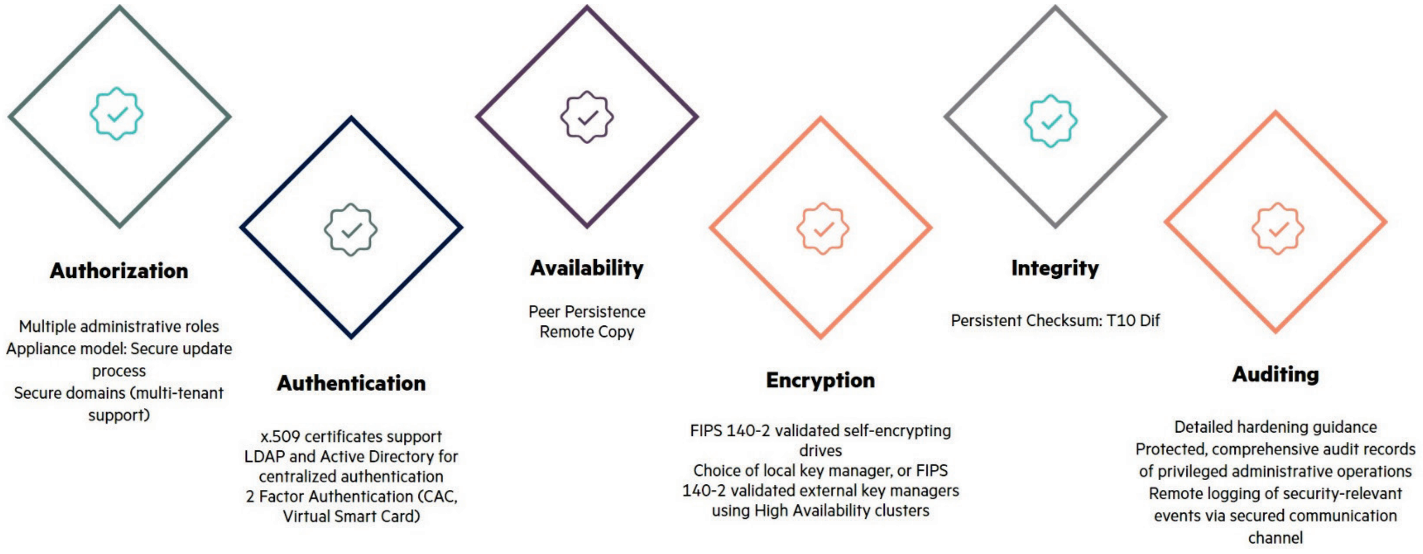
The General Data Protection Regulation (GDPR) is a new European privacy law which comes into force on 25th May 2018 and significantly increases the risks for companies that fail to use and protect personal data in compliance with the law. The GDPR introduces significant monetary penalties of up to a maximum of 20 million Euros or 4% of the annual worldwide turnover of a corporate group.

The GDPR requires organizations to implement appropriate technical and organizational measures to secure data and introduces new breach notification requirements. The HPE StoreServ Storage by its inherent design and architecture with security that is built into the product will assist customers in meeting their GDPR security requirements

HPE 3PAR security categories can be identified as the following:

- Authorization
- Authentication
- Availability
- Encryption
- Integrity
- Auditing

These categories are all fundamental security aspects by which HPE 3PAR StoreServ continues to enhance and harden overall product architecture. HPE 3PAR has already and will continue to adopt security by design into its operating system, appliances and tools which support the array. Figure 13 is an illustration of how HPE 3PAR secure data center architecture design also assists customers with their GDPR compliance security requirements.



Authorization

Multiple administrative roles
Appliance model: Secure update process
Secure domains (multi-tenant support)

Authentication

x.509 certificates support
LDAP and Active Directory for centralized authentication
2 Factor Authentication (CAC, Virtual Smart Card)

Availability

Peer Persistence
Remote Copy

Encryption

FIPS 140-2 validated self-encrypting drives
Choice of local key manager, or FIPS 140-2 validated external key managers using High Availability clusters

Integrity

Persistent Checksum: T10 Dif

Auditing

Detailed hardening guidance
Protected, comprehensive audit records of privileged administrative operations
Remote logging of security-relevant events via secured communication channel

Figure 13. HPE 3PAR secure data center environment

GDPR compliance requires both technology and process changes which HPE is committed to help customers with. Customers own the process of GDPR compliance in their datacenter environment and it is their responsibility to assess what data it possesses, the value that data brings to the organization and how to comply with GDPR. HPE 3PAR StoreServ helps its customers to be GDPR compliant by its inherent design and architecture with security built into the product.

Security resources

Below is a list of security related resources within Hewlett Packard Enterprise

Security Vulnerability Assessment
hpe.com/in/en/services/security-vulnerability.html

STIG
iase.disa.mil/stigs/net_perimeter/network-other/Pages/index.aspx

Common criteria certification
commoncriteriaportal.org/products/

White papers
Secure Analytics in the Cloud for HPE 3PAR StoreServ and HPE StoreOnce devices

HPE 3PAR StoreServ Data-at-Rest Encryption

Blog
community.hpe.com/t5/Around-the-Storage-Block/Where-HPE-3PAR-Fits-into-Your-Data-Center-Security-Plans/ba-p/6909564

Learn more at
hpe.com/info/3par

4AA3-7592ENW, May 2018, Rev. 4