Hewlett Packard Enterprise

Technical white paper

Check if the document is available in the language of your choice.

HPE PRIMERA SECURITY GUIDE—SECURE SERVICE ARCHITECTURE OVERVIEW

HPE Primera storage

CONTENTS

EXECUTIVE SUMMARY

Your organization needs to be assured that your infrastructure components, such as your data storage arrays, meet and maintain your organization's security policies. Such policies can be guided by available industry standards, requirements set forth by your industry or government, or just simply the knowledge your team has from years of experience.

Many organizations consider security to just be an issue associated with computer networking. However, security concerns all aspects of the IT infrastructure from the very smallest component of a machine up through the collection of computing devices in the data center, their connectivity, and how all of these components are managed. Developers and manufacturers must be of a frame of mind that product security is a tenet within the organization to develop products and services that will not allow for this diverse environment to be compromised.

Hewlett Packard Enterprise (HPE) requires that its products be able to operate in secure environments and not allow a compromise of information due to product capabilities, quality, or operation. Such requirements have driven HPE products to have superior product quality and capabilities.

HPE also offers industry-leading service capabilities that encompass the requirements for security. HPE provides on-premises monitoring coupled with multi-device rollup of information to the HPE InfoSight portal for customer configurable analysis of an enterprise. HPE InfoSight was designed to deliver as much capability to the customer as they want or do not want, in the case of "dark" sites.

HPE also understands that organizations cannot have unbridled access to their environment. All machinery is configured using a least-privilege level of access and all access is controlled by the customer. Thus, the customer can control which service personnel have access to their machinery and when that access may occur.

Target Audience

This paper is intended for corporate security personnel, risk planners, and array administrative personnel who will be working with the HPE Primera storage array.

This paper gives management the ability to understand the quality drivers for product development. It provides to security personnel and risk planners the information associated with the standards used to develop the product, and lastly it offers administrative personnel an overview of the details of how the HPE Primera array is accessed and how it can share access and configuration information to management tools.

The reader should have reasonable knowledge of computer concepts associated with computer management, networking, security, and data storage arrays.

Document purpose

This paper offers an overview of how HPE has developed the HPE Primera storage array, and its associated products to meet your security needs. It is not intended to replace product manuals but rather to offer an overview of how HPE Primera storage provides a secure platform on which sensitive data can be stored.

The flow of this paper will take a building block approach from concept to actual use of the HPE Primera array. The major areas covered include:

- HPE policies towards product development and information privacy
- Administrative and operational users of the array and their roles
- Types of information exchanged with HPE
- Methods and services that provide access to the HPE Primera array
- Architecture of the HPE Primera array with respect to security

This paper focuses on the use of the HPE Primera array's Graphical User Interface, or GUI, as the primary method to manage the array. The HPE Primera array does not require an external service processor for management. It includes some references to the command line interface, or CLI, as some procedures cannot be executed through the GUI.

Topics such as Data-at-Rest encryption or recovery from Ransomware are not covered.

You will have a good understanding of how the HPE Primera array's security capabilities are enabled after reading this paper. Please do not hesitate to contact your HPE representative if you have additional questions or observations relative to this paper.

HPE SECURITY ARCHITECTURAL STANDARDS

Back doors and Malware avoidance

HPE takes steps to help ensure that its factories have stringent access security measures and physical security procedures to protect both physical and informational resources from unauthorized access. Malware scanning, code signing, and backdoor analysis are broadly implemented as matters of policy. Per HPE policy, (i) HPE manufacturing facilities are scanned for Malware, and all software is scanned prior to manufacturing; (ii) HPE code delivered to customers is digitally signed; (iii) no HPE product may contain a known backdoor or known unauthorized communication channel mechanism that would allow product access by any individuals who are not authorized by the customer; (iv) HPE-developed and third-party applications are transmitted to HPE factories through secured channels and hosted in a secured environment running regular virus scans (running automatic updates with the latest virus definitions on systems that are patched regularly); and (v) all firmware including system BIOS are signed with a digital signature at the development stage as part of the release to manufacturing process.

Federal certifications and validations

HPE has an ongoing program dedicated to ensure encryption algorithms meet Federal Information Processing Standard (FIPS) 140-2, and soon FIPS 140-3, validated and where applicable; select HPE products are Common Criteria (CC) certified.

HPE Anti-counterfeiting program

HPE protects its intellectual property, trademarks, and brand by means of intelligence and investigations spanning international borders to detect and disrupt the global trade of illicit products. HPE Anti-counterfeit (ACF) Investigation and Enforcement (I&E) confront all touch-points of the counterfeit business—from the smallest of vendors to the largest fabricators, distributors, and producers of counterfeit packaging and components.

HPE I&E partners with law enforcement agencies and customs officials around the world to combat the production, distribution, and sale of counterfeit goods by employing strategy experts and accomplished ex-law enforcement professionals internationally, and draws on the expertise of current law enforcement officials in local markets and experts in investigating the traffic of illicit products.

HPE's counterfeit intelligence team deploys highly skilled, experienced investigators into the field to infiltrate counterfeiting activity around the globe. Working with intelligence provided by HPE, law enforcement agencies perform seizures on the ground and local governments press for arrests and appropriate penalties through the criminal justice system. In addition to criminal seizures, HPE seeks additional penalties through civil litigation.

HPE is a member of Business Action to Stop Counterfeiting and Piracy (BASCAP), a global leadership group under the auspices of the International Chamber of Commerce to help strengthen the fight to protect intellectual property and to deter counterfeiting.

Mechanisms used to prevent threats and address them before HPE or its customers suffer negative consequences

Secure Development including:

- HPE performs Malware scanning using an approved automated anti-Malware tool prior to delivery to customers.
- Digital code signing with capability to validate digital signatures or utilize native signature validation capabilities, backdoor, and unauthorized communication channel controls.
- Detailed system inventory check of installed software for customers with pre-installed software that is installed at an HPE-owned or contracted factory.
- HPE-developed and third-party applications are transmitted to HPE factories through secured channels and hosted in a secured environment with regular virus scans.
- When using drivers approved by Microsoft through their Windows Hardware Quality Labs (WHQL), those drivers are signed by Microsoft.
- When loading a customer-developed image through our Custom Integration Service (CIS), CIS performs a virus scan and SHA256 hash verification prior to the image being loaded onto the HPE manufacturing systems and is then transferred to appropriate HPE factory locations through encrypted channels.
- All software loads are validated using hashing before they are loaded into the HPE transmission pipeline and again after they arrive at the factory site.

- Secure Hash Algorithms Value Comparison – This alpha-numeric value is created as a "fingerprint" of the code. Any changes to the code, even as slight as a line space added or removed, would change the value. This process assures that what is delivered by the lab is what goes to production. The SHA256 value is validated automatically by our software code repository (SMTA2), then by Supply Chain Product Engineering during the Quality Verification Check process (post-lab release), and finally during manufacturing First Article Inspection sample review (prior to manufacturing release).
- Malware Checking – Our software code repository, through which our software flows to manufacturing, checks software for viruses/Malware on a weekly basis.
- System BIOS are signed with a digital signature at the development stage as part of the Release-to-Manufacturing (RTM) process. At run-time, digital signatures of firmware components are verified on the systems for assurance that the code legitimately came from HPE and has not been tampered with. Signing keys are protected in hardware security modules (HSMs) with limited and gated access to prevent unauthorized use.
- Server BIOS (Gen 8 server product thru Gen 10) were developed and maintained in the USA. Going forward the design and architectural control of the BIOS and HPE iLO is in the USA including all code reviews, all source code check-in acceptances, building, and code signing.
- The software/firmware security lifecycle for HPE-developed components includes having the design and code go through detailed reviews, some of which includes independent third-party code inspection.

Customer notifications for critical information security vulnerabilities

HPE has processes in place to track component security vulnerabilities or other defects throughout the lifecycle of our products. HPE strongly encourages customers to sign up to receive automatic notifications of future HPE Security Bulletins at: connect.hpe.com/mypreferences/?language=EN.

HPE packaging and labeling authentication

HPE uses security labels with high-tech features that enable authentication of products with a very high degree of confidence. Product packaging can be, and is often, sealed with a tamper-evident security label to ensure package integrity during transport. The packaging tape affixed to the outside of the shipping box is a tamper-evident tape. Some features allow customers to authenticate products themselves.

For HPE validate information, see: hpe.com/products/validate/.

HPE PRIMERA ARCHITECTURAL OVERVIEW

The HPE Primera Secure Service architecture is a large ecosystem comprised of many different components. The HPE Primera array consists of hardware with controllers and disks, virtualization with common provisioning groups (CPG), and virtual volumes—all designed to take advantage of highly redundant hardware. The combination of all these components provides customers with a highly available world-class storage system designed to deliver optimum performance at the lowest cost possible.

A unique OS in its class, the HPE Primera OS is a modular, service-centric design, which is one of the key enablers for the 100% Availability Guarantee. Features such as the I/O stack, RAID, cluster communication, HBA drivers, Remote Copy, and data reduction are implemented as independent services within the HPE Primera OS. This means that unlike traditional monolithic storage platforms, the HPE Primera OS can be updated, upgraded, and extended without the need to reboot the controllers. This enables faster, more frequent updates that are easier to install and significantly less risky to perform than on other high-end storage systems. This radically simplified update process enables HPE Primera to provide a pipeline of innovation that can easily be tapped, so that as new features become available, they can be added in minutes.

HPE Primera OS structure

The HPE Primera OS architecture is structured around a Linux®-based OS. The kernel itself is isolated from users. The command structure uses a sophisticated command line interface (CLI) architecture to manage the HPE Primera array. Each command in the CLI is a captive command, which maintains a barrier from the internal structure of Linux.

Network port usage

The first part of the communication interaction with HPE Primera storage that needs to be understood are the network ports used by the HPE Primera OS. The HPE Primera OS utilizes several network ports by default and several optional network ports based upon services that are running on the array. TABLE 1 shows the characteristics of the network ports that the HPE Primera OS utilizes.

TABLE 1. HPE Primera OS port assignments

Port	Protocol(s)	Inbound/Outbound	Service
22	tcp / udp	inbound / outbound	SSH server listener
80	tcp / udp / http	inbound / outbound	Permanent forward to port 443
123	udp	inbound	NTP peer (configured as strictly a consumer)
161	udp	inbound	SNMP agent listener
162	udp / udp	outbound	SNMP trap originator (v2/v3)
427	tcp / udp	inbound / outbound	CIM SLP listener
443	tcp / udp / http	NA	Permanent forward to port 8443
514	tcp / udp	outbound	syslog
5783	tcp	inbound / outbound	tdpdtcl TLS listener / CLI
5988	tcp / http	inbound / outbound	CIMserver TLS listener
5989	tcp / https	inbound / outbound	CIMserver TLS listener
8443	tcp	inbound / outbound	WSAPI / UI TLS listener Quorum Witness
9997	tcp	inbound / outbound	VASA vvol TLS listener

Transport Layer Security

The HPE Primera OS communicates through Transport Layer Security (TLS) 1.2 as its standard. TLS clients that are configured for older TLS versions cannot connect to the HPE Primera array. Therefore, you will need to inventory your clients that connect to the HPE Primera array and be sure they can connect via TLS v1.2.

CLI cipher suites

The following ciphers are used by the CLI:

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

CIM and WSAPI cipher suites

The following ciphers are used by both CIM and WSAPI:

- Preferred 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
- Accepted 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
- Accepted 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
- Accepted 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256

SSH cipher suites

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

- Key Exchange Algorithms (used to exchange the key for the Encryption Algorithms):
  - diffie-hellman-group-exchange-sha256
- Encryption Algorithms (one-time symmetric keys/ciphers used to encrypt a socket):
  - aes256-gcm@openssh.com,
  - aes128-gcm@openssh.com
  - aes256-ctr

  - aes192-ctr
  - aes128-ctr
- MAC (message authentication code) algorithms, used for data integrity:
  - hmac-sha2-512-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512
  - hmac-sha2-256

Strong password protection

HPE Primera storage uses either a time-based password or encryption-based password system for all privileged accounts. The two types of password generation are as follows.

Time-based passwords

Time-based passwords are unique to each service user account and HPE Primera array. 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.

Encryption-based passwords

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

Remote Device Access – Customer Access Service

HPE Remote Device Access (RDA) is a remote connectivity solution that enables connection to devices on customer networks, such as the HPE Primera array, for remote service delivery, support automation, real-time monitoring, and quality feedback. HPE RDA provides secure connectivity between Hewlett Packard Enterprise and HPE Primera storage using forward and reverse proxy technology.

To ensure secure data transfer, HPE RDA incorporates:

- Authenticated endpoint identification. This is endpoint identity, which provides an easy method for HPE support engineers to find customer devices and connect to them securely.
- Layered security protocol with a meet-in-the-middle architecture. This provides two-point authority, which enables user access control at the HPE midway servers and at the HPE Primera array's Customer Access Service (CAS). CAS provides remote access for HPE support, data transfer of device telemetry to HPE, and diagnostic or update packages from HPE to the HPE Primera array.

The enabling of this service is optional but highly recommended for optimal service from HPE.

FIPS mode

FIPS mode is the use of cryptographic modules for storage system communication with external systems. When FIPS mode is enabled, the storage system uses FIPS 140-2-compliant modules for encrypted communication with external systems.

Examples of storage system communication interfaces that use FIPS mode include UI to server, SMI-S CIM, CLI, EKM, LDAP, QW, SNMP, SSH, SYSLOG, WSAPI, RDA, and VASA.

Changing the FIPS mode setting causes the storage system communication interfaces with external systems to restart and enter the new mode.

Data-at-Rest encryption

Data on drives can be encrypted using a software key such that it can only be decrypted using that same key. Encryption of data only occurs on self-encrypting drives (SEDs). Data-at-Rest is a reference to the data as it resides on the drive and not while the data is in flight; HPE Primera 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-validated self-encrypting drives. 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 removed from the array, because a malicious actor will not know the unlock key and be able to read data from the drive.

Data-at-Rest key management

HPE Primera supports both Local Key Management (LKM) and Enterprise Key Management (EKM). Local Key Management (LKM) is managed by the HPE Primera array and is included in the Primera OS. If LKM is enabled, all key management is local to the HPE Primera array and is controlled by an internal process of the HPE Primera OS. Conversely, if EKM is enabled, the locking key will be managed by and stored on the EKM, with the key retrieved as needed to unlock SEDs in the array.

The file in which the encryption 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 Primera array. LKM encryption key backup actions are available in the HPE Primera UI or HPE StoreServ Management Console (SSMC).

HPE Primera supports several Enterprise Key Managers (EKMs) that are FIPS 140-2 compliant. EKMs provide 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.

HPE Primera supports EKMs from other vendors. Both solutions are validated for FIPS 140-2-level certification.

The table below shows the supported versions of the various EKMs.

TABLE 2. HPE Primera Enterprise Key Manager support matrix

EKM Product	EKM Product Model	EKM Product Version	KMIP Version	IPv6 Support
Gemalto (Safenet)	KeySecure K460(R320), K460(R33)	8.1.2, 8.1.1, 8.1.0, 8.9.0, 8.5.0, 8.4.3	KMIP 1.3	Not Supported
Utimaco ESKM	ESKM 4.1.5.0	5.0.6, 5.0.8, 5.0.9, 5.3	KMIP 1.4	Supported

NOTE
Always confirm supported versions of the above information with your HPE representative.

ACCESS HPE PRIMERA STORAGE

This section of the document is intended to help the user understand the ways in which HPE Primera storage may be accessed and the standard services that may be coupled to the array, thus providing information about the array configuration. Access to the HPE Primera array is provided through user interfaces, programmatically through Application Programming Interfaces, and granted to other services in the environment. Access may include the ability to change objects on the array or view information about the operation of the array.

The areas for HPE Primera access are as follows:

- User Interface (UI)
- Command Line Interface (CLI)
- Secure Shell (SSH)
- HPE StoreServ Management Console (SSMC)
- Web Services Application Programming Interface (WSAPI)
- Common Information Model (CIM)
- Enterprise Key Managers (EKMs)
- Quorum Witness (QW)
- SYSLOG
- Simple Network Management Protocol (SNMP)
- VASA

UI

The HPE Primera array has an integrated browser-based GUI for management, which is referred to as the UI. The HPE Primera UI application software is included in each HPE Primera storage system. You browse directly to the storage system that you want to manage.

The HPE Primera UI Procedures assume the following:

- The HPE Primera storage system has been initialized.
- The HPE Primera UI for the storage system is accessible from a supported browser.
- The user will log in to the HPE Primera UI with a role that is appropriate to the actions to be performed.

See the HPE Primera UI 1.1 User Guide for more information.

LDAP

User access can be authenticated using Lightweight Directory Access Protocol (LDAP). LDAP is a protocol that is used to access directory services. LDAP servers typically provide a directory for storing user names and passwords. The directory enables different applications and services to validate users. You can use supported LDAP servers to authenticate logins to the storage system by nonlocal users. If your environment uses LDAP for authentication and authorization, you can specify an LDAP configuration for the HPE Primera storage system.

HPE Primera storage systems support the following LDAP servers:

- Microsoft Active Directory
- Open LDAP
- Red Hat® Directory Server

See Operating the HPE Primera 600 for more information.

CLI

When you receive your HPE Primera storage system, the installed HPE Primera OS includes the HPE Primera CLI. You can access the HPE Primera CLI from supported host systems using either Secure Shell (SSH) or the HPE Primera CLI remote client. Hewlett Packard Enterprise recommends using SSH to access the HPE Primera CLI for HPE Primera storage management purposes.

See the HPE Primera OS 4.2 Command Line Interface Installation and Reference Guide for more information.

SSH

Most HPE Primera-supported host operating systems include an SSH client application that you can use to access the HPE Primera CLI. The exception is Microsoft Windows, which requires installing an SSH client. Using SSH requires no additional installation or set up of the HPE Primera CLI.

Other benefits of SSH access include the following:

- Security:
  - Encryption: SSH uses strong, symmetric encryption to encrypt all information exchanged between the client and the server. SSH also allows the use of encrypted passwords.
  - Server authentication: SSH supports the use of public or private keys for server authentication. In addition, SSH supports storing the public key on client machines, allowing the SSH client to compare the key presented by the server before allowing access.
  - User authentication: SSH supports the use of public or private keys for user authentication.
- Data integrity: SSH uses integrity checking to verify that no alteration of data occurs during transmission from sender to receiver.
- Compatibility: SSH removes compatibility issues between client and server because you have no HPE Primera CLI client installed.

See the HPE Primera OS 4.2 Command Line Interface Installation and Reference Guide for more information.

HPE SSMC

The HPE StoreServ Management Console (SSMC) is deployed as an appliance. HPE SSMC provides contemporary, browser-based interfaces, including a Management Console and an Administrator Console.

The Management Console includes the following key features:

- Login access to the Main Console can be configured based on HPE Primera and HPE 3PAR storage user accounts and roles.
- General screens are for monitoring and managing the dashboard, activities, schedules, and settings.
- Block Persona screens are for monitoring and managing hosts, host sets, virtual volumes, app volume sets, virtual volume sets, common provisioning groups, and policies.
- Federations screens are for monitoring and managing storage federation configurations and Peer Motion actions.
- Data Protection screens are for monitoring and managing Remote Copy configurations, Remote Copy groups, HPE Recovery Manager Central instances, and restore points.
- Security screens are for managing storage system user accounts, LDAP, user roles, storage system connections, and virtual domains.
- Storage Systems screens are for managing and monitoring storage system licenses and hardware components, such as controller nodes, ports, drive enclosures, and physical drives.
- VMware screens are for monitoring and managing VMware® storage containers and virtual machines.

The Administrator Console includes the following key features:

- Log in is restricted to the HPE SSMC administrator user account.
- Storage Systems screens are for managing the storage systems that are connected to the HPE SSMC server.

See the HPE SSMC 3.7 Administrator Guide for more information.

WSAPI

The Web Services Application Programming Interface (WSAPI) uses the HTTPS protocol to enable programmatic management of HPE Primera storage and provides client access to web services at specified HTTPS locations. Clients communicate with the WSAPI server using HTTPS methods and data structures represented with JSON.

The Quorum Witness server is installed at a third site that would not be impacted by failure of the source or backup sites, and connects to the source and backup storage systems using non-Remote Copy links

See the HPE Primera Web Services 1.8 API Developer Guide for more information.

CIM

The Common Information Model (CIM) standard is the data model for WBEM. CIM provides a conceptual framework for describing management data for systems, networks, applications, and services; and allows for vendor extensions. SMI-S uses CIM to model those objects and relationships that comprise a SAN.

CIM-XML is a method of exchanging CIM management data. CIM-XML uses an xmlCIM payload and HTTP(s) as the transport mechanism.

This protocol is defined by the following specifications:

- Security:
  - Encryption: CIM uses strong, symmetric encryption to encrypt all information exchanged between the client and the server. CIM also allows the use of encrypted passwords.
  - Server authentication: CIM supports the use of public or private keys for server authentication. In addition, CIM supports storing the public key on client machines, allowing the CIM client to compare the key presented by the server before allowing access.
  - User authentication: CIM supports the use of public or private keys for user authentication.
- Data integrity: CIM uses integrity checking to verify that no alteration of data occurs during transmission from sender to receiver.
- Specification for the Representation of CIM in XML: Defines a standard for the representation of Common Information Model (CIM) elements and messages in XML, written in Document Type Definition (DTD).
- CIM Operations over HTTP: Defines a mapping of CIM Messages onto HTTP that allows implementations of CIM to interoperate in an open, standardized manner. It uses the CIM XML DTD that defines the XML Schema for CIM objects and messages.

See the HPE Primera CIM API programming reference guide for more information.

Quorum Witness

Quorum Witness (QW) enables automatic transparent failover (ATF) in a Peer Persistence environment. Quorum Witness is a self-contained application that can be installed on any physical or virtual machine with a supported Linux host OS. Quorum Witness version 4.0.x provides encrypted communication between the QW client and the QW server.

See Installing and Updating HPE Quorum Witness for HPE Primera and HPE 3PAR for more information.

SYSLOG

HPE Primera storage allows for sending messages to two types of syslog servers. The first is a general syslog server.

The second target is a secure syslog server. Messages sent to the secure server are associated with user login actions and changes to encryption management.

The syslog service on the array is not enabled by default.

See Operating the HPE Primera 600 for more information.

VASA

HPE Primera storage is supplied with a VASA provider for interaction with VMware ESX® and VMware ESXi™ for the purpose of managing virtual volumes. The provider can be started and stopped as needed and uses a specific port for communication.

See the HPE Primera VMware ESX/ESXi Implementation Guide for more information.

SNMP

HPE Primera storage supports both SNMP v2 and SNMP v3 trap managers.

The HPE Primera SNMP agent supports the following MIBs:

- SNMPv2-MIB
- Management Information Block-II (MIB-II), system group: For discovery and basic information, the HPE Primera SNMP agent supports the MIB-II system group.
- snmpTrap group, snmpTrapOID only: The authoritative identification of the notification currently being sent. This variable occurs as the second varbind in every SNMPv2 or SNMPv3 trap.
- HPE Primera MIB: This MIB is the HPE Primera proprietary MIB.

The HPE Primera MIB contains proprietary information that defines the configuration and behavior of the system and is useful for network management.

This HPE Primera MIB contains the trap definitions for these traps:

- cpuStatMIB
- alertNotify
- storeServAlerts

See Operating the HPE Primera 600 for more information.

DATA TRANSFERS BETWEEN AN HPE PRIMERA ARRAY AND HPE

The array can communicate with HPE and exchange configuration information and software updates to and from HPE for the purposes of aiding in maintenance and support of the array. Information is also used to assist the HPE InfoSight AI engine with presentation of information used to manage a single array or collection of arrays. The transfer of this information is ultimately controlled by the customer; however, the customer may allow HPE to initiate actions if so required.

It is not a requirement that this service be enabled. It does, however, make it easier for HPE to assist with support issues.

There are three scenarios of data transmission:

- Call home
- Call home with scrubbing
- Call home disabled

It is important to note, that while different telemetry or event information is transferred back to HPE for processing, no customer data is ever transmitted. Customer data is the information that is stored on the array for use by customer applications such as databases. Customer data is always protected from transport. HPE cannot access customer data remotely; any access to this data must be done via customer-assisted transactions.

The data is sent to HPE using multiple files depending on the level and type of data that is being transmitted. The files are configured in such a manner that allows HPE to break them up into its various components after its arrival into the HPE AI engine. Use of multiple files makes it easier for all involved to tell whether the information has been transmitted. The file transmission status can be viewed from the HPE Primera UI. Email notification of transfer of the data can be sent to an authenticated email server if desired. Files can also be downloaded to a user's local device that is accessing the UI, if so desired.

Scenarios of data exchange with HPE InfoSight will require the use of an HPE Passport account. HPE Passport is HPE's Single Sign On mechanism that HPE customers and partners use to exchange various information with HPE that is not available to the general public. The Passport Account information that will be required is a user passport email ID.

HPE also uses this communication to send HPE Primera OS updates and update recommendations to the customer array. The updates are not installed on the array but are staged for installation at a time determined by the customer.

The following is a summary of the information exchanged with HPE and the frequency of collection.

- Weekly data that includes:
  - Alerts
  - Config data
  - Environmental data
  - Event data
  - Event log
  - Mem data
  - Performance data
  - Status data
- Generated data
  - InSplore data: collection of all registers and other important data from the HPE Primera array
  - Performance: on-demand generated array performance analysis data collected some number of intervals over some amount of time
- Existing files: files that had been previously generated, typically due to an issue on the array
  - Application core files
  - System crash dump files

Information that is sent to HPE can be scrubbed of sensitive configuration data. A dictionary is maintained on the HPE Primera array in situations where the customer chooses to scrub the data. This dictionary is needed to assist HPE support in working with problems on the array as it offers support the ability to "unscrub" the data. Of course, scrubbing the data prolongs the resolution of support issues due to the need to translate the scrubbed data. Data scrubbing is not enabled by default.

If call home with scrubbing is enabled, the following information will be scrubbed from the data transmitted to HPE:

- Storage Objects: virtual volume names, logical disk names, and common provisioning group names
- Connected Host Objects: hostnames defined in the `showhost` command output

- Networking Objects: IPv4 and IPv6 addresses, MAC addresses, domain names shown in the `showdomain` command output, iSCSI names, and node names
- Fibre Channel Objects: worldwide names (WWNs) reported in the `showhost`, `showportdev all`, and `showpd -i` commands output
- Replication Objects: remote virtual volume names and remote copy group names

NOTE
Internally generated HPE Primera pseudo WWNs are not scrubbed because this information can assist troubleshooting efforts. These can be identified by the presence of "02AC" in specific locations in the WWN.

SUMMARY

Your organization needs to be assured that your infrastructure components, such as your data storage arrays, meet and maintain your organization's security policies. Security concerns all aspects of the IT infrastructure from the very smallest component of a machine up through the collection of computing devices in the data center, their connectivity, and how all of these components are managed

Hewlett Packard Enterprise (HPE) requires that its products be able to operate in secure environments and not allow a compromise of information due to product capabilities, quality, or operation. Such requirements have driven HPE products to have superior product quality and capabilities. HPE has developed the HPE Primera storage array and its associated products to meet your security needs.

HPE additionally offers industry-leading service capabilities that encompass the requirements for security. HPE provides on-premises monitoring coupled with multi-device rollup of information to the HPE InfoSight portal for customer configurable analysis of an enterprise. HPE InfoSight was designed to deliver as much capability to the customer as they want or do not want, in the case of "dark" sites.

HPE also understands that organizations cannot have unbridled access to their environment. All machinery is configured using a least-privilege level of access and all access is controlled by the customer. Thus, the customer can control which service personnel have access to their machinery and when that access may occur.

RESOURCES AND ADDITIONAL LINKS

HPE Security Bulletins
connect.hpe.com/mypreferences/?language=EN

HPE Primera UI 1.1 User Guide
psnow.ext.hpe.com/doc/a00101446en_us

Operating the HPE Primera 600
psnow.ext.hpe.com/doc/a00098070en_us

HPE Primera OS 4.2 Command Line Interface Installation and Reference Guide
psnow.ext.hpe.com/doc/a00088937en_us

HPE validate information
hpe.com/products/validate/

HPE SSMC 3.7 Administrator Guide
psnow.ext.hpe.com/doc/a00101449en_us

HPE Primera Web Services 1.8 API Developer Guide
psnow.ext.hpe.com/doc/a00088912en_us

HPE Primera CIM API programming reference guide
psnow.ext.hpe.com/doc/a00088913en_us

Installing and Updating HPE Quorum Witness for HPE Primera and HPE 3PAR
psnow.ext.hpe.com/doc/a00089072en_us

HPE Primera VMware ESX/ESXi Implementation Guide
psnow.ext.hpe.com/doc/a00088903en_us

Business Action to Stop Counterfeiting and Piracy (BASCAP)
iccwbo.org/global-issues-trends/bascap-counterfeiting-piracy/#:~:text=ICC%20created%20Business%20Action%20to,protection%20of%20intellectual%20property%20rights.

LEARN MORE AT

HPE Primera Storage

a00109153ENW, December 2020

Hewlett Packard Enterprise