Technical white paper

HPE SimpliVity for vSphere security guide

Contents

Executive summary

This document discusses the key security features of HPE SimpliVity for vSphere hyperconverged infrastructure. It describes the adherence of HPE SimpliVity to key certifications for federal compliance and other best practices and security features available in the product.

Target audience: This document is aimed at system administrators, infrastructure owners, and system auditors who are responsible for configuration, maintenance, and security of applications that help secure the data center.

Document purpose: This solution guide covers the product security posture, certifications and compliance, and industry-standard best practices adopted by HPE SimpliVity for vSphere. Note that the features discussed in this document pertain to HPE SimpliVity for vSphere and may not be applicable to HPE SimpliVity for HPE Morpheus VM Essentials Software.

Introduction

Managing data and the information derived from it has become one of today's most critical business operations. The acceleration in cybercrimes and ransomware has made securing data a priority for organizations. Cyberattacks are more prevalent today simply because cybercrime is a relatively low-touch attack method for criminals, and it works. Ransomware has real consequences for victims who are affected. Attacked businesses find themselves requiring data recovery, paying the ransom due to a lack of preparedness (or lack of secure backups), or accepting the loss of their data altogether. Some sources estimate the revenue lost from cyberattacks in 2024 will reach $9.5 trillion.

It is now critically important for businesses to always keep their data intact and secure. Data and user account credentials must be protected from unauthorized access to prevent them from being tampered with, destroyed, or disclosed to others. Encryption is key to keeping sensitive data protected. The US government and its National Institute of Standards (NIST) have established guidelines for critical security parameters that vendors must use for encryption before selling to the US government, and many businesses are adopting these as de facto security standards.

Hewlett Packard Enterprise incorporates IT industry best practices during the product development lifecycle to ensure a strong focus on security. HPE engineering and manufacturing practices are designed to meet product security requirements, protect HPE intellectual property, and support HPE product warranty requirements. When a new industry-wide security vulnerability is published, HPE investigates its product line to determine the impact and publishes Security Bulletins for affected products. These bulletins contain impacted product versions and resolution details (patch, upgrade, or configuration change).

You may subscribe to receive real-time notifications about future HPE Security Bulletins and advisories for your products:

- Subscribe to alerts for your products
- Report a security vulnerability
- Review the Security Bulletin archive
- Access Hewlett Packard Enterprise Product Security Vulnerability Alerts

HPE SimpliVity for vSphere security overview

Legacy IT infrastructure composed of silos of computing, storage, and networks is not well suited for today's data protection and security management. HPE SimpliVity collapses the silos into a single software-defined solution with density, resiliency, performance, and data protection. This architecture improves the ability to secure the data from applications and virtualized workloads by using a 3-2-1 data protection strategy. The 3-2-1 data protection rule recommends keeping three copies of your data by storing two copies on different backup media (HDD/SDD)

and storing one copy at an off-site location. HPE SimpliVity increases the protection by providing always-on, inline deduplication and compression of all data.

Several algorithms are available with varying capabilities. As a result, it is a continuous challenge to know which algorithm and security standard to use. To keep up with the growing needs of data security today, security certifications are inevitable.

HPE SimpliVity for vSphere security architecture (high level)

Hardware

HPE offers the first industry-standard servers to include a silicon root of trust built into the hardware. The silicon root of trust provides a series of trusted handshakes, from lowest-level firmware to BIOS and software, to ensure a known good state. HPE SimpliVity runs on HPE servers secured with digital fingerprinting in the silicon, which provides the basis for the hyperconverged platform to natively handle security management. HPE embeds security into the hardware of the HPE ProLiant Gen10 Plus and Gen11 servers. This helps HPE SimpliVity customers prevent, detect, and recover from cyberattacks aimed at the server hardware.

For a full list of security issues resolved and CVEs mitigated in each firmware release, refer to the HPE Support Center.

Software

Ubuntu 22.04

The HPE SimpliVity Virtual Appliance (SVA)—also known as HPE OmniStack Virtual Controller (OVC)—5.3.1 release runs on Ubuntu 22.04 on a Linux® 6.8.0-51-generic kernel.

Patches and updates

Ubuntu system binaries are updated with every release. In addition, Nessus and other tools are used to assess the patch state and exploitability of the system. Kernel updates are performed routinely, although this cadence can be quickened in the event of a major exploit such as Spectre and Meltdown. Although the HPE SimpliVity release cadence is not aligned with Ubuntu releases, HPE makes sure that any security exploits are handled in the subsequent HPE SimpliVity release with necessary updates and patches.

For a list of common vulnerabilities and exposures (CVEs) addressed in the 5.3.1 release of HPE SimpliVity, refer to the HPE SimpliVity 5.3.1 for vSphere release notes.

User authentication

User authentication is based on identities and credentials exposed through VMware vCenter® user management. These identities can be used to access the REST management endpoints, such as through the HPE SimpliVity Client plug-in exposed in the vCenter user interface. Other than this, HPE SimpliVity exposes a pre-created privileged group account, **`svtcli`**, which allows administrative access to the HPE SVA when vCenter is unavailable.

Management actions exposed through the SVT REST interface are access protected by vCenter user authentication. CLI-based management actions, which are available only through an SSH connection, are access protected and available only to members of the vCenter's administrator group and the locally defined **`svtcli`** account.

Authorization

HPE SimpliVity uses two levels of authorization:

- Management APIs, such as those exposed by REST or ones that are modified through an SSH session, are subject to immutable authorization checks based on identities and group memberships managed by vCenter. (Note that HPE SimpliVity native CLI commands that can be run as part of the SSH session do not have access limitations after the user is logged in.) This model is also expanded to include roles by using role-based access control (RBAC) technology.
- In addition, permissions for various vCenter objects are subsequently applied when management calls are made to the vCenter API set. These permissions include actions that are exposed through the API for users based on their roles.

Network profile

HPE SimpliVity is configured to allow only ports that are necessary for the day-to-day operations of the system. For more detailed information, including a full list of required open ports for HPE SimpliVity, refer to the latest HPE SimpliVity 5.3.1 for vSphere Documentation

---

Note

Deployment manager uses the TLS v1.2 protocol to increase privacy of the information communicated over the network. VMware vSphere® 8.0 supports TLS v1.3 and TLS v1.2. VMware vSphere 7.0 supports TLS v1.2 by default, with TLS v1.0 and v1.1 disabled by default. For more information about the TLS v1.2 protocol, see the VMware® Knowledge Base and search for "Status of TLS v1.1/1.2 Enablement and TLS v1.0 Disablement across VMware products (319422)."

OpenSSL

HPE SimpliVity uses the OpenSSL cryptographic libraries for data encryption and secure communication. The 5.3.1 release has updated the OpenSSL version from 3.0.14 to 3.0.15. Refer to the OpenSSL 3.0 Series Release Notes for details of any bug fixes or vulnerability mitigations.

HPE GreenLake for Private Cloud Business Edition

HPE GreenLake for Private Cloud Business Edition is part of Data Services Cloud Console, hosted on the HPE GreenLake cloud, which provides a secure, centralized management platform for managing on-premises and public cloud workloads, including

HPE SimpliVity virtual machines (VMs), and for viewing your HPE SimpliVity infrastructure across all your HPE SimpliVity Federations.

HPE SimpliVity communicates with Data Services Cloud Console services through the Data Services Connector (DSC) VM by a secure mutual TLS tunnel. For further information about Data Services Cloud Console security, refer to the Data Services Cloud Console Security Guide. For firewall requirements for the DSC, refer to the HPE GreenLake for Private Cloud Business Edition Getting Started Guide.

HPE SimpliVity for vSphere federal compliance

FIPS 140-2 on HPE hardware

NIST Federal Information Processing Standard (140-2) specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification, ports and interfaces, roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

HPE SimpliVity SVA supports FIPS for current versions and is Vendor-Affirmed.

For the steps required to enable FIPS mode on HPE SimpliVity hosts, refer to the HPE SimpliVity 5.3.1 for vSphere Documentation.

VMware 7.x and 8.x hardening

VMware publishes guidelines containing those configuration settings, which enable customers to deploy their vCenter instances and VMware ESXi™ hosts more securely. HPE SimpliVity has been qualified to run in a hardened 7.x and 8.x environment, with the exceptions listed in Table 1.

Table 1. VMware hardening exceptions

Category	VMware vSphere guideline	Description
Firewall	`ESXi.firewall-restrict-access`	HPE SimpliVity host requires that certain ports be open. See HPE SimpliVity OmniStack for vSphere Administration Guide for more information on the list of ports that must be opened and how they are used.
SSH	`ESXi.Audit-SSH-Disable`	The ESXi SSH service must be running. Set the ESXi SSH server policy to start and stop with the host.
	`ESXi.set-shell-timeout`	Do not harden this value by setting a specific time-out value. Set the value to 0.
	`ESXi.set-shell-interactive-timeout`	Do not harden this value by setting a specific time-out value. Set the value to 0.
PCI Passthrough	`VM.verify-PCI-Passthrough`	Do not harden this value for the HPE SVA VM. Set this value to TRUE for HPE SVA. This is required for fundamental HPE SimpliVity operations.

PCI-DSS

HPE SimpliVity is designed to comply with several NIST SP 800-53 security control guidelines and meets industry standards security; however, it is not PCI-DSS certified.

GDPR

HPE platforms, on which HPE SimpliVity runs, have been developed in alignment with NIST 800-53 controls—the foundation for accelerating regulatory compliance initiatives such as EU General Data Protection Regulation (EU GDPR).

The HPE cloud-based analytics platform **HPE InfoSight** automatically monitors the health of each registered HPE SimpliVity node in a federation to provide enhanced support. Events/alerts on the HPE SimpliVity system are sent immediately to HPE InfoSight, and HPE InfoSight sends a consolidated report daily that includes information about the system status and significant events.

The report also provides details about:

- Cluster, host, VM, and virtual controller names
- Host serial numbers
- Host IP addresses
- VM sizes
- Datastore details (name, physical capacity, free space, memory size)

The report contains no user-identifying information such as usernames or VM addresses (except for the HPE SVA VM because the IP address of HPE SVA is part of the VM nomenclature), and it complies with GDPR requirements. For more information, refer to the HPE InfoSight for servers Privacy Statement.

DISA STIGs

Although HPE SimpliVity has not yet been qualified against any Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), it has been qualified against several NIST SP 800-53 security guidelines, thus conforming to some of the key industry standard security requirements. It is also qualified against the VMware vSphere 7.0 and 8.0 hardening guides, which contain a subset of the requirements from the VMware vSphere 7.0 STIG and VMware vSphere 8.0 STIG. For more information about the VMware STIGs, go to the DISA STIGs.

These STIGs consist of the following parts:

– VMware vSphere 7.0/8.0 ESXi STIG

– VMware vSphere 7.0/8.0 VM STIG

– VMware vSphere 7.0/8.0 VMware vCenter Server® for Windows STIG

Qualification of HPE SimpliVity against these STIGs is targeted to be available in a future release.

HPE SimpliVity for vSphere security features

HPE SimpliVity RapidDR

HPE SimpliVity RapidDR is a standalone disaster recovery orchestration utility that facilitates the recovery of a failed set of VMs from a source environment to a recovery environment in the event of a site disaster. RapidDR also facilitates restoring VMs back into the source environment after the source environment has been restored. RapidDR enables the creation, testing, and orchestration of recovery plans along with runbooks and reporting on the recovery plan to conform with audit and regulatory requirements.

Data-at-rest encryption and key management

The main architecture of HPE SimpliVity, known as the Data Virtualization Platform, provides persistent data storage (based on the NFS-3) services to customer workloads. HPE SimpliVity is a unique hyperconverged integrated product that stores both primary and secondary storage. It uses inline deduplication and compression to provide the most efficient way to store customers' data. HPE SimpliVity implements data encryption at rest by using the advanced HPE Smart Array encryption technology. HPE Smart Array SR Secure Encryption is a controller-based data-at-rest encryption solution for any drive connected to the HPE Smart Array controller or HPE Smart Host Bus Adapter. HPE Smart Array SR Secure Encryption is a FIPS 140-2 enterprise-class encryption solution that complies with regulations for sensitive data, such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley.

Physical security of the entire data center is the first line of defense, and it is required by several cloud certification standards to receive accreditation. The next level is physical access to the computer stack and the computers themselves. To support system-level or box-level protection of components, the drives that are attached to the HPE Smart Array storage controller might be encrypted. If the drives are encrypted and removed, they are useless without the encryption key that is securely stored. Data is protected by using a series of AES-256 encryption keys that provide layered protection at the volume and drive levels. A primary key, stored either at the controller level or on a remote secure key manager, is required to "unwrap" each successive layer. The HPE Smart Array encryption technology enables management of the keys by using a local, controller-based, key manager or remote enterprise key management software such as Utimaco Enterprise Secure Key Manager, Thales TCT KeySecure for Government G350v, Thales KeySecure k150v or Thales CipherTrust Manager 2.20 virtual (k170v), and physical (k570) appliances.

Beyond the encryption technology, there are situations in which compliance is required to rotate the key used for encryption. Both the local and the remote key management modes support key rotation.

Local and remote key management modes are available for all HPE SimpliVity 380 Gen10 Plus servers. Currently, Gen11 servers with the SR932i-p storage controller support only local data-at-rest encryption through controller-based encryption (CBE) with no controller password set.

For more information, refer to the HPE SimpliVity Data at Rest Encryption Guide.

UEFI Secure Boot

Secure boot is a security standard that ensures that the code launched by a system's UEFI firmware is trusted. It is designed to protect a system from malicious code right from the start of the boot process, before the operating system has been loaded. When the server starts, the firmware checks the digital signature of each component against a set of trusted certificates embedded in the BIOS. When secure boot is in use a system will refuse to load any UEFI driver or application unless its signature matches the trusted list.

With secure boot enabled the HPE SimpliVity bootloader contains a VMware public key. The bootloader uses this key to verify the signature of the kernel and a small subset of the system that includes a secure boot VMware Installation Bundle (VIB) verifier. The VIB verifier then verifies every VIB package installed on the system. Once verified the entire system boots with the root of trust in certificates that are part of the UEFI firmware. Secure boot is one of the best ways to protect the ESXi host from ransomware attacks.

ESXi also contains an advanced boot option to guarantee that the VMkernel runs only those binaries that have been packaged and signed as part of a VIB. The execInstalledOnly option can be enforced on every boot by using the hosts Trusted Platform Module (TPM) after UEFI Secure Boot has been enabled.

HPE SimpliVity provides support for UEFI Secure Boot and execInstalledOnly on ESXi hosts on both fresh deployments and upgrades. Secure boot on HPE SimpliVity hosts requires that the TPM 2.0 to be configured, a minimum server firmware of 2024.0930.02 for Gen11 hosts or 2024.0930.03 for Gen10 hosts, and that no unsigned 3rd party VIBs are in use. This is particularly important to check for when enabling secure boot on upgraded hosts as there may be old VIBs present on the system. HPE recommends enabling both UEFI Secure Boot and execInstalledOnly for all HPE SimpliVity hosts.

All systems shipped from the factory will have secure boot disabled by default and should only be enabled by customers after successful deployments. Secure boot is not supported prior to deployment as there are some elements of the deploy installer that are unsigned.

A simple check from the ESXi shell can confirm the readiness of a system to enable secure boot by running the following command:

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

For the steps required to enable UEFI Secure Boot, refer to the HPE SimpliVity 5.3.1 for vSphere Documentation.

Virtual Trusted Platform Module

Trusted Platform Modules are dedicated microcontrollers designed to secure a system through the use of integrated cryptographic keys. UEFI Secure Boot is a security standard that helps to ensure that the system boots using only software that is trusted by the manufacturer. For certain VM hardware versions and operating systems, a virtual Trusted Platform Module (vTPM) can be enabled, providing the same secure boot functionality as on a physical machine.

HPE SimpliVity has qualified vTPM and enabled secure boot on VMs hosted on HPE SimpliVity Storage. VMs with a compatible guest operating system can use secure boot with minimal loss of deduplication and compression.

The use of secure boot and vTPM on the HPE SVA is not currently supported.

For further information about enabling vTPM for HPE SimpliVity hosted VMs in a VMware environment, refer to the HPE support documentation and the VMware vSphere TPM (vTPM) Questions & Answers.

Role-based access control (RBAC for HPE SimpliVity actions/objects)

As a customer scales up the HPE SimpliVity configuration, the count of nodes and clusters of HPE SimpliVity Federations also scales up. To maximize the return on investment, HPE SimpliVity user count also increases. The challenge is that these users are derived from multiple organizations where their access rights to HPE SimpliVity objects (VM, backups, datastores) are different. This scenario leaves the organization with an overburdened administrator who must respond to the needs of users for any operation related to these HPE SimpliVity objects.

To provide a scalable and efficient method for all users to access HPE SimpliVity objects, it is important to enable a self-service policy with RBAC. Depending on the industry and government for each country, rules to govern who can have access, what they can do, and which objects they can access become crucial. HPE SimpliVity RBAC is designed to meet these requirements.

The HPE SimpliVity 5.3.1 for vSphere Documentation covers RBAC in greater detail.

Penetration testing and security hardening

To assess the potential weakness of HPE SimpliVity software in terms of the ability to maintain integrity, availability, and confidentiality, HPE uses commercial third-party tools in-house to detect and remediate security weaknesses. Every vulnerability discovered is remediated in order of priority as determined by its attack vector and severity. At every release, an independent in-house security team assesses the software for holes in its security posture, leveraging some of the leading commercial tooling. They then prioritize the remediation and deliver a fix for any vulnerability uncovered in the process, in an expedited manner. HPE SimpliVity runs on best-in-class HPE Gen11 servers, which are known for their built-in protection against data loss caused by malicious and man-in-the-middle attacks. The servers ship in high-security mode with security features activated in the factory to reduce the attack surface for cyberattackers, making it more difficult to insert compromised code or malware into the server firmware. For more information about security, see this HPE blog.

Protection from ransomware

Ransomware is particularly troubling and is quite rightly at the forefront of the minds of many security and IT professionals. Ransomware refers to malicious software (malware) that is deployed within an enterprise's infrastructure without the company's knowledge, encrypting data until the attacker chooses an opportune moment to demand a ransom payment. These attacks have evolved in sophistication and in the level of damage they cause, employing methods that make them harder to detect and more difficult to recover from. By encrypting or deleting backup data, attackers attempt to render recovery efforts useless, increasing the chance of the affected party paying the ransom. Unfortunately, paying the ransom does not always guarantee that the data will be released back to the data owner.

There are five aspects to consider in protecting your business from ransomware and parameters to recover from a ransomware attack:

- **Assess your vulnerability.** Consider your backup plans, so that you can gauge the RPOs (how far back you can restore the data) and the RTOs (how quickly you can restore the data). Parameters might include backup windows (time to complete a backup), speed of recovery, and backup success rate.
- **Understand what the business requirement is to recover the data.** Some applications require application awareness to back up and have compliance requirements to ensure that backups are protected to meet the business standard.
- **Follow the 3-2-1 backup strategy.** Ensure that your backup meets data protection requirements: three copies of data, two copies on two different media, one copy off-site.
- **Use purpose-built backup appliances.** Your backup software should rely only on primary storage; however, it should reside on purpose-built backup appliances. That means the interface or the means to transfer the data is not commonly accessible. The special-purpose backup appliances can provide an additional barrier against the instigator to prevent more damage to the business.
- **Educate your teams and implement your plan.** Note that your backup administrator will be able to recognize that the backup deduplication ratio decreased when the ransomware attack happened because encrypted data is ineffective for being deduped and compressed.

HPE SimpliVity secondary data or the backup data is not accessible directly from the user applications. This special-purpose backup can be accessed only by using the HPE SimpliVity API and requires authorization from vCenter or a special service password. Because of this special access, HPE SimpliVity secondary data is safeguarded from ransomware encryption.

Recovering from a ransomware event

Before a ransomware event occurs, it is important to determine two key metrics for recovery. The **recovery point objective (RPO)** refers to the maximum tolerable amount of data loss that an organization is willing to accept during an outage. Determining an appropriate RPO requires considering factors such as data sensitivity, business operations and the cost associated with backup and recovery mechanisms. Critical data and systems typically have lower RPO requirements, whereas non-critical systems might be more flexible. The **recovery time objective (RTO)** defines the acceptable level of downtime and specifies the maximum time needed to recover systems and data and resume normal operations. Many factors are involved in determining the RTO and the impact of

downtime on the organization's operations. For example, customer experience, contractual obligations, and revenue must be assessed. Just as for the RPO, critical systems typically have shorter RTOs, whereas less critical systems might be more flexible.

When responding to a ransomware attack, the administrator must consider the time required to recover all the affected production VMs. If the ESXi and the SVA are impacted, you can assume that all data is completely lost, and the only way out is to redeploy the affected nodes from external backups such as HPE StoreOnce or HPE Zerto Software. This might seem like the most appropriate action, but it is unlikely to fit with the organization's RTO, and it might take several days to begin bringing production systems back into operation.

The HPE SimpliVity ASS3RT team (A Safe & Secure Rapid Response & Recovery Team) is a group of technologists spanning all levels, dedicated to the recovery of data for HPE SimpliVity systems. The ASS3RT team have a deep knowledge of HPE SimpliVity, VMware, Linux, and all the underlying and accompanying technologies as well as a full understanding of the latest research and technical details surrounding the different types of ransomware.

In the event of a ransomware attack, contact HPE Support immediately for assistance.

HPE StoreOnce

Since HPE SimpliVity 4.0.0, HPE SimpliVity introduces the extension of secondary storage to the HPE StoreOnce backup appliance through the HPE Catalyst application. The ability to restore copies of data from completely different types of appliances makes your data exceptionally safe against a ransomware attack.

HPE StoreOnce is a purpose-built backup appliance (or VM) that includes HPE StoreOnce Catalyst stores. These stores effectively isolate critical data where attackers cannot harm it without resorting to direct physical interactions that would ultimately destroy some, or all, of the hardware itself. Even if malware achieves physical destruction at a single location, the more advanced implementation of HPE StoreOnce Catalyst stores (distributed implementation) protects mission-critical data by effectively isolating it from traditional lines of communication and command sets leveraged by ransomware attackers. HPE has "hidden" the HPE StoreOnce Catalyst store from attackers in plain sight, behind an application programming interface (API) that both enhances and simplifies the process of backing up and deduplicating data, while making it practically impossible for ransomware to attack it directly.

HPE StoreOnce further protects backup data by offering data immutability and dual authorization. Data immutability sets a window of time during which the data cannot be modified or deleted, protecting backup data from accidental or malicious deletion. Dual authorization mode requires authorization from both the administrator and a second "security officer" user to approve any action that might lead to the deletion of a volume. Other aspects to consider are the frequency and retention of backups of the workloads in your environment. These factors determine the RPO of recovering the workload. HPE SimpliVity provides a default frequency of a minimum of 10 minutes for backup and recovery of the applications, which can be helpful to enable recovering the business without much discrepancy.

For further information related to backing up HPE SimpliVity to a HPE StoreOnce appliance, refer to the HPE SimpliVity 5.3.1 for vSphere Documentation.

Glossary

Phrase	Meaning
HPE SimpliVity hyperconverged node	An x86 server that is the basic hardware building block of the HPE SimpliVity hyperconverged infrastructure solution
HPE SVA	The software stack is implemented as a single VM per node, which controls all aspects of HPE SimpliVity hyperconverged infrastructure
Data Virtualization Platform (DVP)	A globally aware file system and object store with data optimization techniques that enable a coordinated collection of scalable compute and storage resource pools across multiple sites and provides highly efficient data storage, management, and mobility
HPE SimpliVity cluster	A collection of one or more HPE SimpliVity hyperconverged nodes typically located at the same physical site connected over a standard Ethernet network collectively providing a single storage pool to the hypervisor on each node. An HPE SimpliVity cluster can also be extended across two physical sites, commonly known as a stretched cluster, over low-latency metro networks for disaster recovery and business continuity.
HPE SimpliVity federation	A collection of one or more HPE SimpliVity clusters and the main construct within which data is managed

Resources

HPE SimpliVity 5.3.1 for vSphere Documentation

HPE SimpliVity Data at Rest Encryption Guide

HPE Compute Security

Data Services Cloud Console Security Guide

Learn more at

HPE.com/SimpliVity

Visit HPE.com

Chat now

a50004838ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com