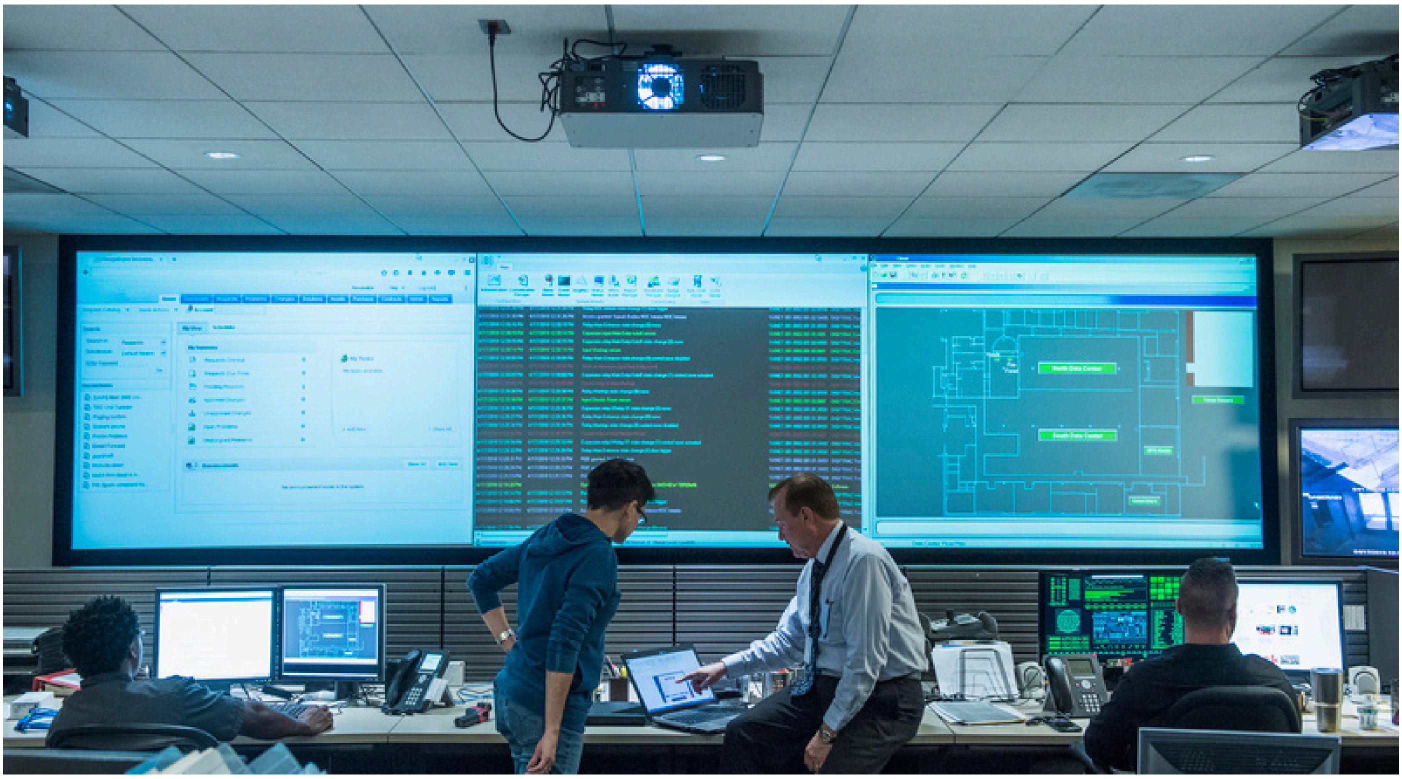
Technical white paper

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

HPE SIMPLIVITY SECURITY BEST PRACTICES



CONTENTS

EXECUTIVE SUMMARY

This document provides the key security features of HPE SimpliVity hyperconverged infrastructure. It describes the adherence of HPE SimpliVity to key certifications for federal compliance and other best practices or 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, which help secure the data center.

Document purpose: This solution guide talks about security concerns, certifications, and industry-standard best practices adopted by HPE SimpliVity.

INTRODUCTION

Managing data and the information derived from it has become one of the most critical operations of businesses today. The acceleration in cybercrimes and ransomware has made securing data a priority within organizations. Cyberattacks are more prevalent today simply because it 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 2021 will reach $6 trillion.[1]

It is now critically important for businesses to always keep their data intact and secure. Data and user account credentials need to 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 vendors must use for encryption before selling into 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 released, HPE investigates its product line to determine the impact. For impacted products, Security Bulletins will be published. These bulletins will contain impacted product versions and the resolution (patch, upgrade, or configuration change).

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

Subscribe to alerts for your products

Report a security vulnerability

Security Bulletin archive

Hewlett Packard Enterprise Product Security Vulnerability Alerts

HPE SIMPLIVITY 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.

There are several algorithms 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.

[1] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, 2020

HPE SIMPLIVITY SECURITY ARCHITECTURE (HIGH LEVEL)

Hardware

HPE offers the first industry-standard servers to include a silicon root of trust built into the hardware.[2] 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. This provides the basis for this hyperconverged platform to natively provide security management. HPE embeds security right into the hardware of the HPE ProLiant Gen10 servers. This helps HPE SimpliVity customers prevent, detect, and recover from cyberattacks aimed at the server hardware.

In addition, the 4.1.0 release of HPE SimpliVity firmware includes resolution for:

- Intel® Q2 IPU UEFI CVE-2019-11136 and BIOS CVE-2019-11137 for HPE SimpliVity 380 Gen10, HPE SimpliVity 380 Gen10 G, HPE SimpliVity 380 Gen10 H, HPE SimpliVity 2600 Gen10, and HPE ProLiant DL325 Gen10 systems.
- BIOS 2.30 for HPE ProLiant DL380 Gen10 and HPE Apollo 2000 Gen10 / HPE ProLiant XL170r / HPE ProLiant XL190r Gen10 servers includes the latest revision for the Intel microcode, which provides mitigation for CVE-2020-0548 and CVE-2020-0549 also known as CacheOut.

Software

Ubuntu 18.04

The HPE OmniStack Virtual Controller (OVC) runs on Ubuntu 18.04 on a Linux® 4.14.113 kernel.

Patches and updates

Ubuntu system binaries are updated every three months. Additionally, 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. Though the HPE SimpliVity release cadence is not in line with Ubuntu releases, it is made sure that any security exploits are handled in the subsequent HPE OmniStack releases with necessary updates and patches whenever required.

User authentication

User authentication is based on identities and credentials exposed via 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. The only exception to this rule is the “svtcli” account, which allows administrative access to the HPE OVC when vCenter is unavailable.

Most management actions are accessible through REST. Others are being migrated to this model, but there are a set of legacy management tools (CLI-based actions native to HPE SimpliVity where commands are executed by the user to perform specific operations), which are only available via SSH by executing commands directly on the HPE OVC. Connecting over SSH is a privileged operation, only available to members of the vCenter administrator’s group or a session established with the emergency (svtcli) account.

Authorization

Two levels of authorization are used on HPE OmniStack. Management APIs, such as those exposed by REST or ones that are modified via an SSH session (Note: HPE SimpliVity native CLI commands that can be executed as part of the SSH session do not have access limitations once the user is logged in.) are subject to immutable authorization checks based on identities and group memberships managed on the vCenter. This model is also expanded to include roles, using role-based access control (RBAC) technology. Additionally, 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 those ports, which are necessary for the day-to-day operations of the system. See port information in Table 1. For more detailed information, see the latest HPE OmniStack 4.1.0 for vSphere Administration Guide.

[2] HPE unveils the world’s most secure industry standard servers

TABLE 1. Port information

Destination port (listening)	Protocol	Source	Destination (listening)	Description
9390	UDP/TCP	Management virtual appliance	HPE OmniStack Virtual Controllers (HPE OmniStack host)	The event manager on the management virtual appliance uses this port to forward the events to HPE OmniStack Virtual Controllers on the HPE OmniStack hosts
9390	TCP	VMware vCenter Server® • Management workstation	Management virtual appliance	SSL ports to access REST endpoint of the management virtual appliance from vCenter Accessing the REST endpoint (aggregator service) on the management virtual appliance
443	TCP	Management virtual appliance	• vCenter Server • HPE OmniStack • Virtual Controllers (HPE OmniStack host)	• SSL ports vCenter Server • SSL ports to access svt-rest service on HPE OmniStack hosts
443	TCP	• vCenter Server • Management workstation	Management virtual appliance	• SSL ports to access REST endpoint of the management virtual appliance from vCenter • Accessing the REST endpoint (aggregator service) on the management virtual appliance
443	TCP	• vCenter Server • Management workstation	• HPE OmniStack • Virtual Controllers (HPE OmniStack host)	• SSL ports to access REST endpoint of the HPE OmniStack Virtual Controllers on the HPE OmniStack hosts
22	SSH	Management workstation	• HPE OmniStack • Virtual Controllers (HPE OmniStack host) • Management virtual appliance	• For remote access, using SSH to the server when the web server is unavailable

NOTE

Deployment manager uses the TLSv1.2 protocol to increase privacy of the information communicated over the network. For more details on the TLSv1.2 protocol, see the VMware® Knowledge Base and search for “Status of TLSv1.1/1.2 Enablement and TLSv1.0 Disablement across VMware products (2145796).”

HPE SIMPLIVITY FEDERAL COMPLIANCE CERTIFICATIONS

FIPS 140-2 (OpenSSL 1.0.2) on HPE hardware

This National Institute of Standards and Technology (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.[3]

FIPS 140-2 support was first introduced with HPE OmniStack 3.7.0 and used the following cryptographic modules:

- HPE OmniStack Crypto Library: Certificate #3303
- Bouncy Castle FIPS Java API (BC-FJA): Certificate #2768

HPE SimpliVity is currently working toward reinstating FIPS for current versions and is targeted to be FIPS compliant in the subsequent release.

[3] csrc.nist.gov/publications/detail/fips/140/2/final

VMware 6.5 and 6.7 Hardening

VMware publishes guidelines containing those configuration settings, which enable a customer to deploy their vCenter more securely and VMware ESXi™ hosts. HPE OmniStack has been qualified to run in a hardened 6.5 and 6.7 environment with the following exceptions:

TABLE 2. Exceptions

Category	VMware vSphere® guideline	Description
Firewall	`ESXi.firewall-restrict-access`	HPE OmniStack host requires that certain ports be open. See HPE OmniStack 4.1.0 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.
PCIPassthrough	`VM.verify-PCI-Passthrough`	Do not harden this value for the HPE OmniStack Virtual Controller (OVC) virtual machine. Set this value to TRUE for HPE OVC. This is required for fundamental HPE OmniStack operations.

PCI-DSS

HPE OmniStack is not PCI-DSS or otherwise accredited since it is not possible to accredit a product. HPE OmniStack has been developed to include features and capabilities that help the end-user customer or systems integrator achieve accreditation such as data-at-rest encryption and the use of TLS for transport security.

GDPR

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

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 once a day, HPE InfoSight sends a consolidated report that includes information on the system status and significant events.

It also contains details on:

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

The report does not contain any user-identifying information such as user names or virtual machine IP addresses (except for the HPE OVC virtual machine, as the IP of HPE OVC is part of the VM nomenclature) and complies with GDPR requirements.

DISA STIGs

Although HPE OmniStack has not yet been qualified against any DISA STIGs, it has been qualified against the VMware vSphere 6.5 and 6.7 hardening guides, and these guides consist of a subset of the requirements from the VMware vSphere 6.5 STIG.

This STIG consists of the following parts:

- VMware vSphere 6.5 ESXi STIG
- VMware vSphere 6.5 Virtual Machine STIG
- VMware vSphere 6.5 vCenter Server for Windows STIG

Qualification of HPE OmniStack against these STIGs is targeted to be available in the subsequent release.

Common Criteria

Common Criteria evaluation is critical for Federal government customers. The first steps toward this are completing the FIPS 140-2 validation process and the STIG qualification, which is in progress.

HPE SIMPLIVITY SECURITY FEATURES

HPE SimpliVity hardware platform security features

The HPE SimpliVity appliance includes HPE Smart Array SR Secure Encryption, which is a controller-based data-at-rest encryption solution for any SAS/SATA 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 Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley.

Physical security of the entire data center is the first line of defense and is required by several cloud certification standards to receive accreditation. The next level is physical access to the actual computer stack and the computers themselves. To support system-/box-level protection of components, the drives that are attached to the HPE Smart Array controller will/may be encrypted. If the drives are encrypted and removed, they are useless without the encryption key that is securely stored.

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

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

To provide a scalable and efficient method for all users to access HPE SimpliVity objects, it's important to enable a self-service policy with role-based access control. Depending on the industry and government for each country, rules to govern who can access, what they can do, and which objects that one can access becomes crucial. HPE SimpliVity RBAC is architected to meet the requirements mentioned previously.

Data-at-rest encryption and support for Enterprise Key Management

The main architecture of HPE SimpliVity, known as Data Virtualization Platform, is providing 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, where using the inline deduplication and compression provides the most efficient way to store customers' data. HPE SimpliVity implements data encryption at rest using the advanced HPE Smart Array encryption technology.

Beyond the encryption technology, there are situations where compliance is required to rotate the key used for encryption. The HPE Smart Array encryption technology allows management of the keys using the remote Enterprise Key Management software such as ESKM. The advantage of using ESKM for a large-scale HPE SimpliVity deployment is secure, efficient, and simple.

Third-party penetration testing and hardening

To assess the potential weakness of HPE SimpliVity software in terms of the ability to maintain integrity, availability, and confidentiality, it uses the third-party commercial software company as advised by the compliance regulation. Every vulnerability that was discovered will go through remediation in the priority that is recommended by the compliance regulation. The vulnerability derives from multiple scenarios such as unnecessary user privilege escalation, circumcision of trust establishment, or exploitation of bugs, and such. HPE SimpliVity will incorporate a penetration testing as part of every release of the code and report any known vulnerabilities that are discovered by documenting them in the form of a knowledge base article to ensure that customer is aware of the remediation required.

HPE SimpliVity runs on best-in-class HPE Gen10 servers, which are known for their built-in protection against data loss due to 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. More details on this can be found in the HPE blog.

HPE SimpliVity security solutions and reference architectures

In the current technological world, the growth of data is unavoidable; the utmost priority is to keep the data secure and healthy wherever it resides. The importance of such phenomena has been understood by HPE SimpliVity and the following are the two unique solutions, which are addressing such requirements.

1. **HyTrust integration with HPE SimpliVity**—Securing application data through encryption on HPE OmniStack.

   HyTrust provides a security and compliance platform for virtualized data centers. A key element of the HyTrust Platform, called HyTrust DataControl ensures organizations avoid becoming the next cyber data breach headline by securing virtual infrastructure throughout the virtual system and data lifecycle. The solution ensures deep security and automates both security and compliance; ensures scalability to be as elastic as the virtual environment it is protecting; and finally, HyTrust DataControl simple operation reduces administrative burden and errors.

Learn more about how this solution works with HPE SimpliVity, benefits and best practices here—hytrust.com/uploads/Simplivity-HyTrust.pdf

2. **Vormetric Transparent Encryption with HPE SimpliVity**—Solution that reduces security risks and helps to ensure compliance with regulatory requirements.

   The Transparent Encryption solution involves the Vormetric Data Security Manager and transparent encryption agents. The software appliance offers centralized capabilities for storing and managing host encryption keys, data access policies, administrative domains, and administrator profiles. Vormetric Transparent Encryption features an agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes. This enables encryption of both structured databases and unstructured files.

   Learn more about how the solution works with HPE SimpliVity, benefits and best practices here—go.thalesesecurity.com/rs/480-LWA-970/images/J496_Vormetric_WP.pdf

Protection from ransomware

Ransomware is an intrusion of data center security to prevent the owner of data to access any of their data until the intruder is compensated. The user data is encrypted or encoded using multiple different encryption technologies such as a combination of asymmetric and symmetric encryption via the malware (malicious and bogus software) that operates like a virus. The intruder can break into your data center through other methods such as breaking administrator login using a weak password, Microsoft Windows vulnerability, and such. Other methods are infection of this virus that happens through downloaded files from spam emails or downloaded files from malicious sites with untrusted sites. So, the intruder works similar to a hijacker to create an economical reason to sell the key to access the original data. Unfortunately, paying the ransom does not always guarantee that the intruder is going to honor the promise.

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

1. **Assess your vulnerability**

   Consider the backup plans, so that you can gauge the RPOs (how far in the past) and the RTOs (how fast can we restore the data). Some parameters are backup windows (time to complete a backup), speed of recovery, and backup success rate.

2. **Understand what the business requirement is to recover the data**

   Some applications require application awareness to back up, compliance requirements to ensure that backups are protected to meet the business standard.

3. **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.

4. **User purpose-built backup appliances**

   Your backup software should not be relying only on primary storage; however, it should be 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 for the instigator to cause more damage to the business.

5. **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 happens because encrypted data is ineffective to be deduped and compressed.

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

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 the copies of data from completely different types of appliances makes your data exceptionally safe against a ransomware attack.

Other aspects to consider are the frequency and retention of backups of the workloads in your environment. This will determine the RPO of recovering the workload. HPE SimpliVity by default provides a minimum frequency of 10 minutes for backup and recovery of the applications, which can be helpful to be able to recover the business without much discrepancy.

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 OmniStack Virtual Controller (OVC)	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 OmniStack Accelerator Card (OAC)	A PCIe-based device that offloads and provides acceleration of data writes and data management functions within the HPE SimpliVity hyperconverged infrastructure solution
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

LEARN MORE AT

hpe.com/simplivity

Make the right purchase decision.
Contact our presales specialists.

Chat **Email** **Call**

Get updates

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel is a trademark of Intel Corporation or its subsidiaries in the U.S. and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. VMware ESXi, VMware vCenter, VMware vCenter Server, VMware vSphere, and VMware are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. Java is a registered trademark of Oracle and/or its affiliates. All third-party marks are property of their respective owners.

a50004838ENW, August 2021

Hewlett Packard
Enterprise