Hewlett Packard Enterprise

Technical white paper

HPE InfoSight Security for HPE Storage

Secure Predictive Analytics in the Cloud

Contents

Executive summary

This white paper gives prospective or current users of HPE storage systems information about how data is collected and secured by HPE InfoSight. The paper assumes that the reader has a basic understanding of HPE InfoSight.

Solution overview

HPE InfoSight provides cloud-based predictive analytics for HPE Nimble Storage arrays (all-flash, adaptive flash, and secondary flash), for HPE 3PAR StoreServ, and for HPE StoreOnce. Beyond storage, HPE InfoSight has visibility up through the technology stack into the network, the hosts, and the virtual infrastructure. Hewlett Packard Enterprise believes that the future of IT infrastructure lies with bringing artificial intelligence into the data center. HPE InfoSight is a key element of the effort to build the self-managing data center infrastructure of the future.

Types of data collected by HPE InfoSight

All data collected by HPE InfoSight is related to configuration, statistics, and storage system health. HPE InfoSight collects several types of data from a customer's infrastructure: streaming statistics, heartbeats, diagnostics and configuration data, and alerts. If VMware vCenter® is part of the customer's infrastructure, HPE InfoSight collects data from vCenter as well.

Depending on the type of data, customers can choose to opt in or out of providing specific datasets to HPE InfoSight:

- **Streaming statistics.** Also known as streaming stats, this dataset consists of performance information (counters and statistics). Customers can choose to opt out of sending streaming statistics to HPE InfoSight.
- **Heartbeats.** Heartbeat data enables HPE InfoSight to know whether the infrastructure is in active communication with HPE InfoSight or whether connectivity has been interrupted or lost. The heartbeat consists of a small set of packets that are sent from a specific HPE storage array to HPE InfoSight. Customers cannot choose to opt out of providing heartbeats; the feature is always enabled.
- **Diagnostics for HPE Nimble Storage Analytics (DNA).** DNA data consists of configuration data about the devices in the infrastructure, such as the specific storage array model, the capacity attached to the array, and the group configuration. Customers can choose to opt out of sending DNA data to HPE InfoSight.
- **Alerts.** Alerts are a data type that is sent with the highest priority to HPE InfoSight. Alerts can be triggered for many reasons. Customers can choose to opt out of sending alerts to HPE InfoSight.
- **Cross-Stack Analytics for VMware®.** Formerly known as VMVision, Cross-Stack Analytics for VMware data consists of configuration and performance data that is collected from VMware vCenter. Customers do not directly opt in or out of sending VMVision data to HPE InfoSight. They can control the feature from their HPE InfoSight account by configuring the vCenter instance to enable virtual machine (VM) streaming data.

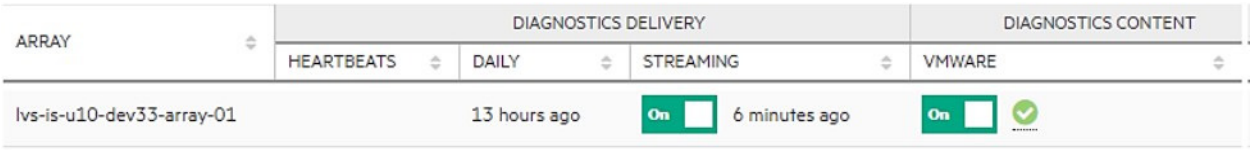

Figure 1. Enabling VM streaming data in HPE InfoSight.

Important

The security of customer-originated data is a top priority for HPE. At no time is customer data—the data stored in storage volumes or LUNs—sent to HPE InfoSight. Data collection by HPE InfoSight is strictly limited to configuration-related and performance-related data.

At a high level, to opt in or out of sending data to HPE InfoSight, customers must first configure their HPE storage systems to enable data communication with HPE InfoSight. If data communication with HPE InfoSight is not enabled, no data is sent to HPE InfoSight at any time, for any reason.

For example, in HPE Nimble Storage arrays, data collection is disabled by default. Users can enable it by selecting the checkbox **Allow Nimble Storage Support to collect analytics data automatically from the array** on the **Administration > Alerts and Monitoring** page of the storage array management interface. When this checkbox is selected, the storage array starts sending data to HPE InfoSight over HTTPS.

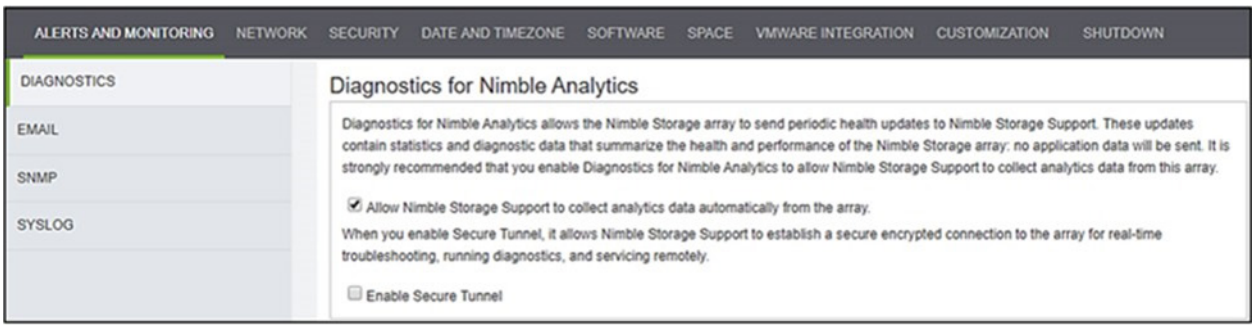

Figure 2. Enabling HPE Nimble Storage arrays to send data to HPE InfoSight.

At any point, customers can choose to opt out of sending specific data types or to stop sending data to HPE InfoSight altogether.

For 3PAR systems, the transfer settings must be configured for the service processor (SP) to send data to HPE InfoSight. After the settings are configured in the 3PAR service console for the SP, storage analytics are sent to HPE InfoSight by the 3PAR system that is associated with the SP.

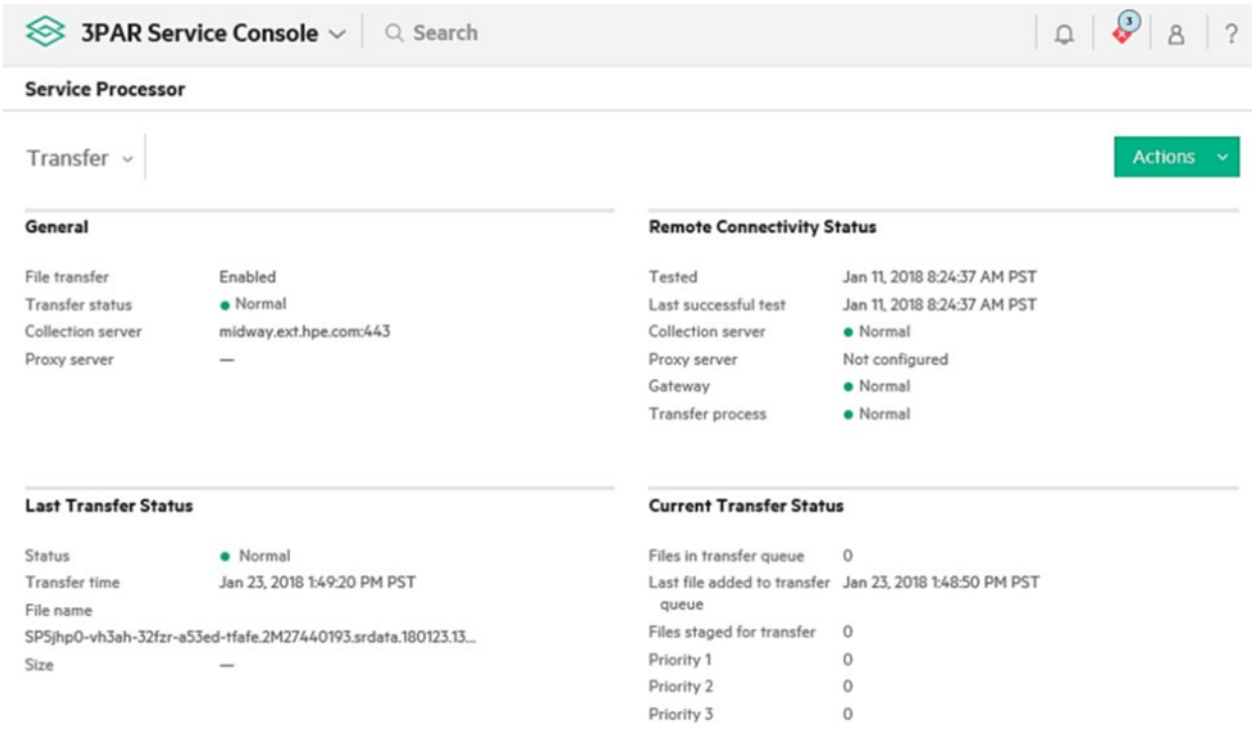

Figure 3. Enabling 3PAR systems to send data to HPE InfoSight.

The 3PAR service console is also used to add VMware vCenter instances to the VMware configuration. In order for 3PAR systems to be able to collect data for the HPE InfoSight Cross-Stack Analytics for VMware feature (formerly VMVision), at least one vCenter entry must be added to the VMware integration settings. After it is added, VM streaming data can be enabled in the HPE InfoSight portal for the specific array that is configured.

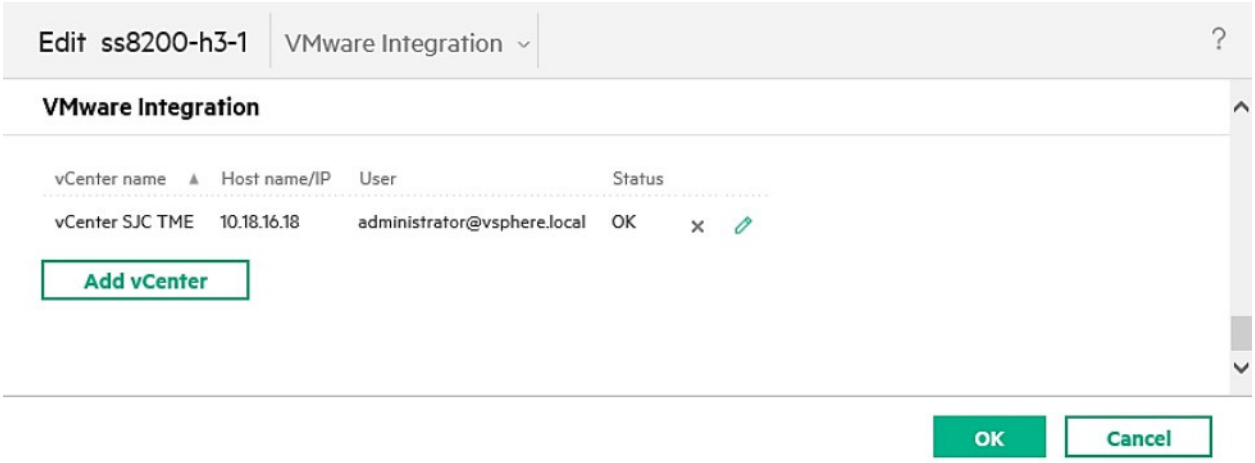

Figure 4. 3PAR service console VMware integration settings.

Secure sites

Some customer sites are secure sites, meaning that the systems do not and cannot communicate with devices outside of the internal network. The HPE InfoSight feature set does not currently extend into local deployments such as those needed for secure sites.

In secure sites, customers can leverage the full range of statistics and information that is available through the local array management interface. For customers who want to pull data into existing internal tools, HPE storage arrays have REST APIs that can be used to programmatically collect data within a local network. In addition, alerts can be generated and sent within the local network through the native storage management interface and tools.

For government agencies, the extension of HPE InfoSight into AWS GovCloud or similar cloud services might be a possibility for certain products in the HPE portfolio. If you want to explore ways to leverage HPE InfoSight in your environment, contact your HPE account team for further information and possible solutions.

Collecting, processing, and accessing data

HPE operates a highly scalable cloud infrastructure that constitutes the HPE InfoSight cloud service. The complete architecture of HPE InfoSight contains the following elements:

- Components that are deployed at the customer site through HPE storage arrays (HPE Nimble Storage arrays and HPE 3PAR storage systems)
- Infrastructure for data processing and analysis
- A web portal front end through which users can securely access their data

The following figure shows a simplified overview of the data collection and communication architecture of HPE InfoSight. At a high level, the components can be grouped into data collection and transmission, data processing, and data access.

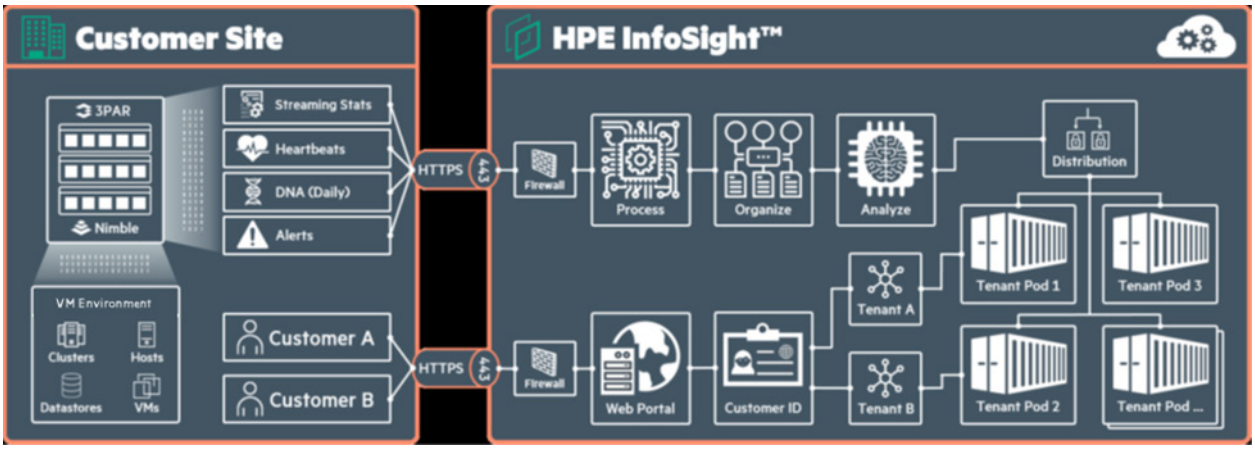

Figure 5. HPE InfoSight data collection and communication architecture.

Data collection and transmission

The focal point for data collection is the storage array. Each data point is referred to as a data sensor. Millions of data sensors are implemented in the native storage OS. Data sensors in this context are not physical sensors, such as heat sensors; rather, they are counters, statistics, or some other soft data point that is provided by the storage OS.

Note
In some cases, data sensors might pull data from physical sensors on the hardware, but most often the sensors are software-related counters and statistics.

Native storage array data sensors push data up to HPE InfoSight. The frequency of data transmission varies by the type of data that is being pushed:

- Alerts are generated and sent instantly as the events that trigger alert conditions occur.
- Heartbeats are sent every five minutes.
- Streaming statistics are sent every ten minutes.
- DNA data is sent once daily.

These stated intervals were accurate at the time that this document was written. HPE InfoSight is constantly being improved with an emphasis on transmitting data as securely, quickly, and efficiently as possible.

When data must be collected from other components of the infrastructure stack, a native collector is built into the storage OS. The native collector is responsible for pulling that data from the higher-level component. For example, when the HPE Nimble Storage VMware vCenter plugin is registered on a vCenter instance, the collector in HPE NimbleOS can pull data from that specific vCenter instance and then push the data to HPE InfoSight.

Note
Multiple vCenter instances can be registered to report data into a single HPE InfoSight account.

Regardless of the type of data or the transmission interval, data is sent to HPE InfoSight through HTTPS (port 443) over TLS 1.2 for protection from malicious hackers or other unauthorized access during transmission.

Data processing

Data that is sent to HPE InfoSight must be processed, organized, analyzed, and stored in a way that is accessible through the web portal. The cloud infrastructure that supports HPE InfoSight uses standard network security practices, such as firewalls, to prevent unauthorized access to the internal cloud network.

When the data reaches HPE InfoSight, it is processed into the system. Processing involves recognizing what data type has been sent and to which internal system that data should be directed; for instance, heartbeats are processed differently from DNA data. More importantly, the data must be associated with a specific system, account, and customer so that it can be handled and secured while it is processed and then stored for access. Before the data can be analyzed, it must be organized in a structured way; in other words, a schema must be applied to the data. Analysis involves applying a large set of advanced data signatures and health checks against the dataset. The core data and the results of the analysis are stored in a highly scalable architecture.

Although many data signatures are applied against specific datasets, many other signatures are applied across the entire dataset (the install base). These global data signatures never contain customer identification or system details because they are applied to the global dataset for determining abstract results. For example, HPE InfoSight assesses the average per-minute, hourly, and daily change rates for data that is assigned to specific performance profiles. This data is critical in helping identify replication needs and expectations. Only the result of this type of analysis is potentially visible to a customer, never the data that was used to determine the result.

Data access

For HPE InfoSight to recognize individual customers, each customer is assigned a unique ID. Customers access and manage their own HPE InfoSight accounts, including designating superusers who can add or revoke permissions for other users to access account data. From the perspective of data processing and data access, each customer can be considered a tenant.

When a customer connects to the HPE InfoSight web portal to access data and display that data in the web interface, HPE InfoSight verifies the customer ID and retrieves the data associated with that tenant. The customer ID and the verification process ensure that customers access only their data and never see or access data from any other tenant. The only method by which customers can access data is through the HPE InfoSight web portal. At no time can a customer access any back-end system.

It is possible for a very large customer to have multiple HPE InfoSight accounts and, consequently, multiple customer IDs. This scenario is rare and usually occurs when the customer operates subsidiary companies or when the company is exceptionally large and operates as different entities across the globe. In this case, data is secured separately for each customer ID and for each HPE InfoSight account. Users can request access to other HPE InfoSight accounts, but permissions are managed on an individual basis by the HPE account owners, the superusers.

Information security practices

HPE uses several common practices to secure HPE InfoSight data. HPE InfoSight is a cloud-based service, but it maintains the internal infrastructure directly.

Non-HPE employees never have access to the internal HPE InfoSight infrastructure. Access by HPE employees is limited strictly to those with an absolute need to access the infrastructure. Customers, partners, and most HPE employees interact with HPE InfoSight only through the web portal.

HTTPS TLS 1.2

All data is transmitted to HPE InfoSight over HTTPS TLS 1.2. In addition, all users access the HPE InfoSight web portal through an HTTPS connection. The TLS 1.2 protocol uses public key cryptography and mutual client and server authentication to provide confidentiality, message integrity, and authentication for traffic passed over the internet.

TLS certificates for HPE InfoSight are signed by a trusted third-party certificate authority (CA), GeoTrust. The CA is a trusted entity that validates the authenticity of HPE InfoSight through a digital certificate. The certificate includes the HPE public key that is used for encrypted communications to HPE InfoSight and other information about HPE. Standard technology in the web browser maintains a list of CA root certificates to verify that a known and trusted CA has signed and validated the digital certificate.

Access, monitoring, and auditing

Strict access control lists (ACLs) are in place to restrict access to HPE InfoSight internal services. Only HPE employees with a need to know are granted access to HPE InfoSight data. All network conversations and changes within HPE InfoSight accounts are tracked, and full audit logging is enabled.

Users who have been assigned the administrator role can access audit reports from the HPE InfoSight web portal by selecting **Reports > Audit Report**. All user actions are logged in the audit report; for example, when permission is granted or revoked to the account or when an alert is acknowledged for a device that is reporting into the account. Any user who accesses the account is logged. Log entries record the user name, include a timestamp, and indicate the category, description, status, and other details about the user. These reports can be exported as needed.

USERNAME	TIMESTAMP	CATEGORIES	DESCRIPTION	STATUS	DETAILS
support-tools@nimblestorage.com	01/23/2018 2:06 PM	VM_Streaming	Streaming enabled	success	Streaming enabled for array: AF-102268
support-tools@nimblestorage.com	01/23/2018 2:04 PM	VM_Streaming	Streaming disabled	success	Streaming disabled for array: AF-124284
esirianni	01/23/2018 1:57 PM	Change_Role	User's role was changed	success	User bajaj.tn@gmail.com role was changed from Super User to Standard User

Figure 6. HPE InfoSight web portal audit report example.

Network security and protection

The HPE InfoSight network infrastructure uses firewalls and network-level virus protection. Virus protection signatures are updated on a regular basis to ensure that the network is protected from old and new types of viruses and attacks.

Back-end connections between sites use private connections and secure protocols. Internal logging tracks which HPE employees or groups have accessed data and when the data was accessed.

Physical security

Because HPE InfoSight is a global cloud service, the physical infrastructure for HPE InfoSight is spread across several sites. Some sites are facilities owned by HPE, but several colocation sites also host HPE InfoSight infrastructure.

Physical security includes locked server rooms, caged infrastructure in colocations, restricted badge access to physical infrastructure, and logged access to facilities.

Role-based access control

HPE InfoSight uses role-based access control (RBAC) to limit data access by HPE personnel. RBAC extends to HPE InfoSight users and HPE partners. HPE partners and HPE employees can request access to the customer accounts with which they are working. A small number of HPE employees who work directly on HPE InfoSight (for example, Engineering personnel) have superuser access to HPE InfoSight, but the majority of HPE employees have only basic access, which is limited to internal HPE accounts and data (for example, the HPE internal IT account).

Users with specific roles can be added to any HPE InfoSight account. User accounts are managed in the web portal through the **Administration > Users** page. Currently, HPE InfoSight has two user roles: standard user and superuser. Customer accounts must have at least one designated superuser. A superuser has the ability to manage users and permissions for an HPE InfoSight account; a standard user cannot perform these tasks. Users can be created, activated, deactivated, or edited to have their roles changed or their passwords reset.

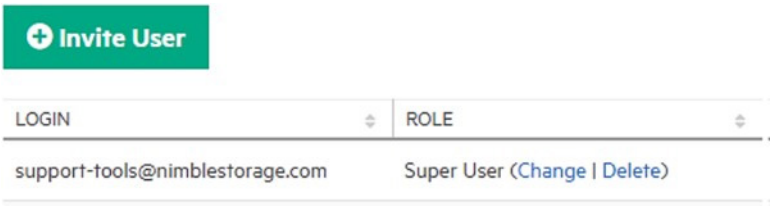

Figure 7. HPE InfoSight account user management and role assignment.

Users who are not directly associated with an HPE InfoSight account can request access to the account. These requests for access are managed from the web portal through the **Administration > Permissions** page. All requests for access are displayed on this page, and a superuser has the ability to accept or reject the request. If the request for access is accepted, the user is granted basic account access by default. Additional permissions can be granted on a per-user basis for Cross-Stack Analytics for VMware (formerly VMVision) and for the ability to manage support cases for the account. Permissions can be modified at any time.

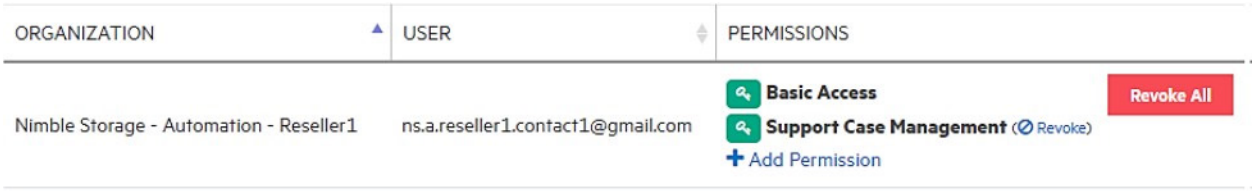

Figure 8. HPE InfoSight permission and access management.

Summary

HPE InfoSight security extends to users of the web portal, to the way they access data, and to the core collection, transmission, and processing of data into the HPE InfoSight cloud. HPE has taken extensive steps to secure customer-originated data and to restrict access to that data to only the appropriate internal HPE employees.

Resources

To learn more about HPE InfoSight, consult the following resources:

- HPE 3PAR Secure Service Architecture
  https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=4aa3-7592enw
- HPE InfoSight for HPE 3PAR StoreServ
  https://h20195.www2.hpe.com/v2/Getdocument.aspx?docname=a00053623enw&skiphtml=1
- InfoSight Getting Started
  https://infosight.hpe.com/InfoSight/media/cms/active/pubs_InfoSight_Getting_Started_.pdf
- InfoSight User Guide for HPE Nimble Storage
  https://infosight.hpe.com/InfoSight/media/cms/active/pubs_InfoSight_User_Guide_for_HPE_Nimble_Storage_.pdf
- InfoSight User Guides for HPE Servers
  https://support.hpe.com/hpesc/public/home/documentHome?sort_by=relevance&sp4ts.oid=1011200130

Note

In some cases, access to these resources requires a valid HPE InfoSight login. If you do not have an HPE InfoSight login, ask your HPE account team whether copies of these documents are available locally.

Learn more at

hpe.com/storage

a00067516ENW, October 2019, Rev. 1