Hewlett Packard Enterprise

Technical white paper

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

HPE INFOSIGHT SECURITY FOR HPE STORAGE

Secure predictive analytics in the cloud

CONTENTS

EXECUTIVE SUMMARY

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. This white paper describes how HPE InfoSight collects and secures data.

Target audience: This document is intended for prospective or current users of Hewlett Packard Enterprise storage systems. The paper assumes that the reader has a basic understanding of HPE InfoSight. This guide focuses on HPE Nimble Storage arrays. For information about using HPE 3PAR, HPE Primera, and HPE SimpliVity storage, see Appendix: Setting up HPE InfoSight for HPE 3PAR, HPE Primera, and HPE SimpliVity and the documents listed in Resources and additional links.

SOLUTION OVERVIEW

HPE InfoSight provides cloud-based predictive analytics for HPE Nimble Storage arrays (all-flash, adaptive flash, and secondary flash), as well as for HPE 3PAR StoreServ, HPE StoreOnce, and HPE SimpliVity. Beyond storage, HPE InfoSight has visibility up through the technology stack into the network, the hosts, and the virtual infrastructure.

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 infrastructure, HPE InfoSight collects data from vCenter as well.

Depending on the type of data, customers can choose to opt into 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:** The alert data type is sent to HPE InfoSight with the highest priority. 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 into 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, as shown in Figure 1.

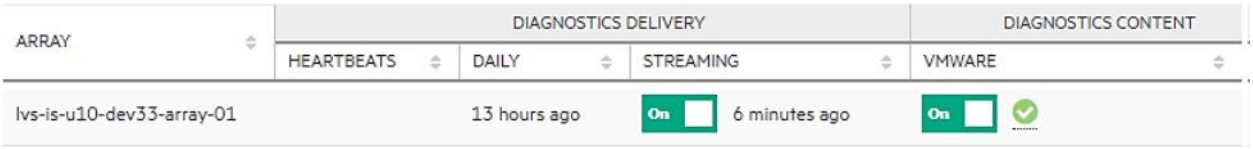

FIGURE 1. Enabling VM streaming data in HPE InfoSight

IMPORTANT

The security of customer-originated data is a top priority for Hewlett Packard Enterprise. Customer data (the data stored in storage volumes or LUNs) is never sent to HPE InfoSight. Data collection by HPE InfoSight is limited strictly to configuration-related and performance-related data.

At a high level, to opt into or out of sending data to HPE InfoSight, customers must first configure their Hewlett Packard Enterprise 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. Customers 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, as shown in Figure 2, the storage array starts sending data to HPE InfoSight over HTTPS.

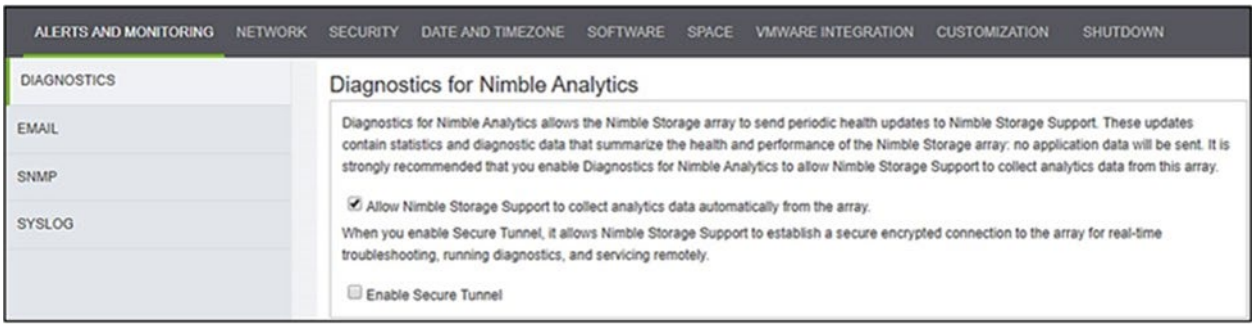

FIGURE 2. Enabling HPE Nimble Storage arrays to send data to HPE InfoSight

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

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 Hewlett Packard Enterprise portfolio. If you want to explore ways to leverage HPE InfoSight in your environment, contact your Hewlett Packard Enterprise account team for further information and possible solutions.

COLLECTING, PROCESSING, AND ACCESSING DATA

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

- Hewlett Packard Enterprise storage arrays
- Infrastructure for data processing and analysis
- A web portal front end through which users can securely access their data

Figure 3 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**.

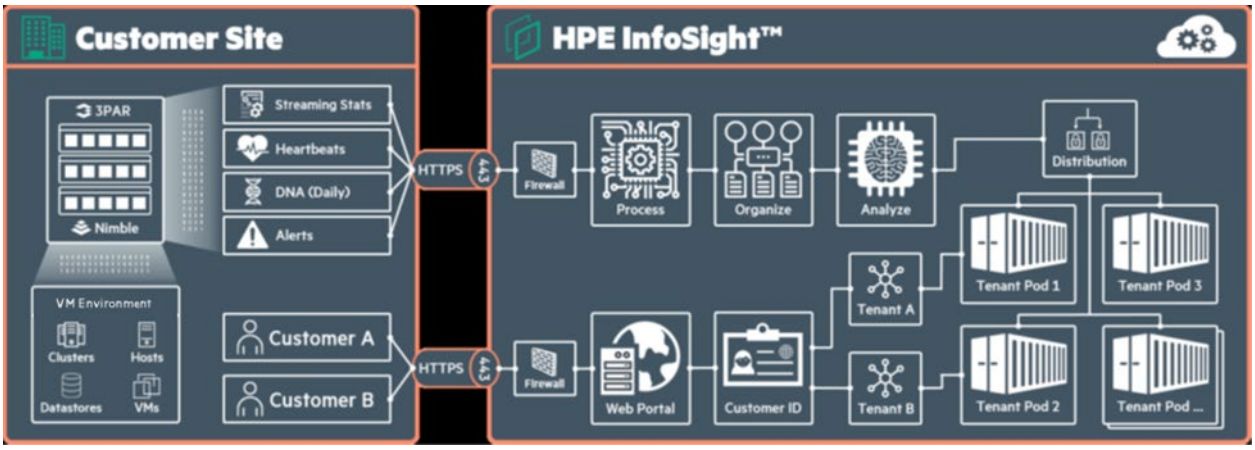

FIGURE 3. HPE InfoSight data collection and communication architecture

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 operating system (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 to 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

To enable HPE InfoSight to recognize individual customers, each customer is assigned a unique ID. Customers access and manage their own HPE InfoSight accounts (referred to as **organizations**), 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 own data and never see or access data from any other tenant.

It is possible for a very large customer to have multiple HPE InfoSight accounts and, consequently, multiple customer IDs. This scenario is rare; it 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

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

No one except Hewlett Packard Enterprise employees ever has access to the internal HPE InfoSight infrastructure, and Hewlett Packard Enterprise employee access is limited strictly to those with an absolute need to access the infrastructure. Customers, partners, and most Hewlett Packard Enterprise 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 that is 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 Hewlett Packard Enterprise. 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 Hewlett Packard Enterprise employees who have 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. Figure 4 shows an example audit report.

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 4. 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 Hewlett Packard Enterprise employees or groups have accessed data and when the data was accessed.

Physical security

Because HPE InfoSight is a global cloud service, its physical infrastructure is spread across several sites. Some sites are facilities owned by Hewlett Packard Enterprise, 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 Hewlett Packard Enterprise personnel. RBAC extends to HPE InfoSight users and Hewlett Packard Enterprise partners. Partners and employees of Hewlett Packard Enterprise can request access to the customer accounts with which they are working. A small number of Hewlett Packard Enterprise employees who work directly on HPE InfoSight (for example, engineering personnel) have superuser access to HPE InfoSight, but most Hewlett Packard Enterprise employees have only basic access, which is limited to internal Hewlett Packard Enterprise accounts and data (for example, the internal IT account for Hewlett Packard Enterprise).

Users with specific roles can be added to any HPE InfoSight account, as the example in Figure 5 shows. 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 those tasks. Users can be created, activated, deactivated, or edited to have their roles changed or their passwords reset.

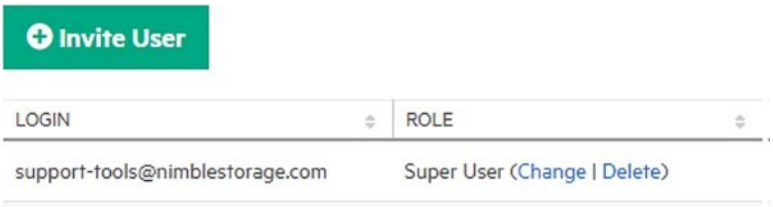

FIGURE 5. HPE InfoSight account user management and role assignment

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, shown in Figure 6. 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.

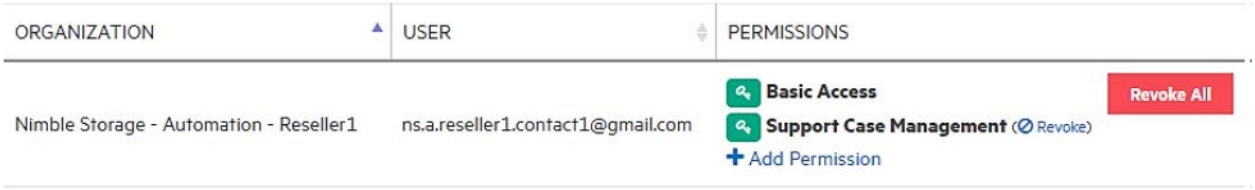

FIGURE 6. HPE InfoSight permission and access management

SUMMARY

HPE InfoSight security extends to all users of the web portal, and it applies not only to the way they access data, but also to the core collection, transmission, and processing of data into the HPE InfoSight cloud. Hewlett Packard Enterprise has taken extensive steps to secure all customer-originated data and to enforce restrictions that allow only the appropriate internal Hewlett Packard Enterprise employees to access it.

APPENDIX: SETTING UP HPE INFOSIGHT FOR HPE 3PAR, HPE PRIMERA, AND HPE SIMPLIVITY

This white paper describes how HPE InfoSight works with HPE Nimble Storage arrays; however, the features of HPE InfoSight are also available for other Hewlett Packard Enterprise products. As a reference, this Appendix provides instructions for enabling HPE InfoSight integration with HPE Primera, HPE 3PAR, and HPE SimpliVity storage.

HPE Primera

For HPE Primera and HPE 3PAR systems, you must have an HPE InfoSight system group to contain your storage arrays. If your company already has an existing system group, you can contact the owner to request an invitation to join it. If no system group exists, as shown in Figure 7, you can create one in HPE InfoSight by going to **Settings → HPE Primera, 3PAR StoreServ & StoreOnce → Register Systems**, clicking **Create Group**, and entering the required information. The system group can contain a combination of HPE Primera and HPE 3PAR arrays.

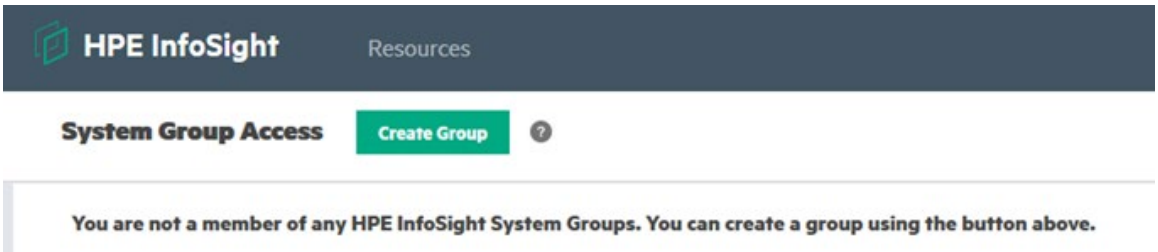

FIGURE 7. Creating an HPE InfoSight system group for your HPE Primera and HPE 3PAR storage arrays

NOTE

An HPE Primera or HPE 3PAR storage array is allowed to be a member of more than one HPE InfoSight system group. For the sake of simplicity, it is a best practice to limit each storage array to membership in only a single system group. If your system already belongs to an HPE InfoSight system group and you want to add it to a second group, you must register it through the HPE SSMC. Registering your system through the Primera UI overwrites any existing system group registrations.

Registering an HPE Primera storage array with HPE InfoSight enables the system to send analytic data to Hewlett Packard Enterprise and to be visible in the HPE InfoSight portal. To register your array through the HPE Primera UI, complete the following steps:

1. Log in to the HPE Primera UI.
2. Complete the **Configuring InfoSight** settings:
   a. In the main menu, select **Settings**.
   b. On the Settings screen, click the **Telemetry** panel.

c. On the Telemetry screen, click **Configure InfoSight** on the InfoSight panel.

3. Follow the instructions in the dialog box that opens:
   a. Authenticate with your HPE Passport ID to retrieve your system group information.
   b. Select your company's system group.
   c. Complete the configuration by selecting **Claim this system in InfoSight**.

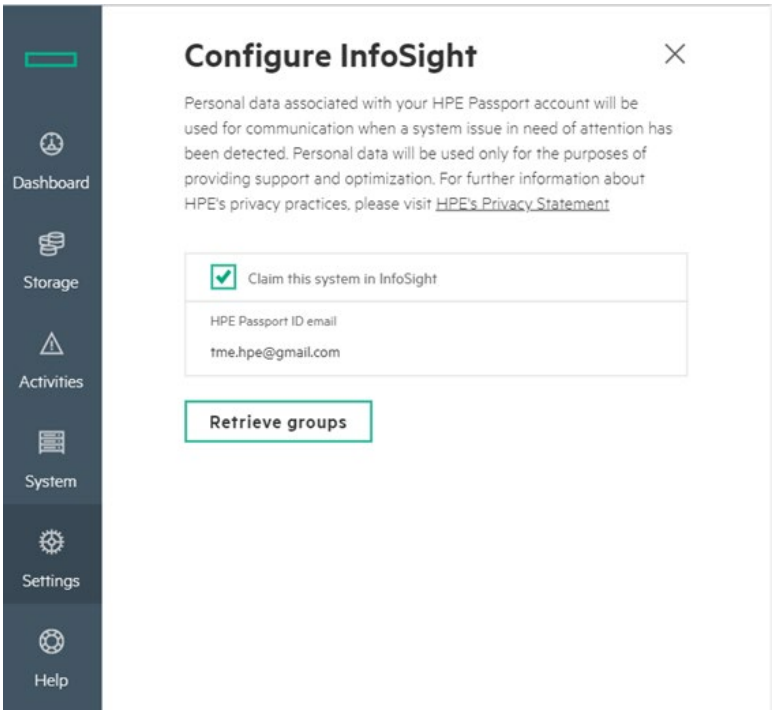

FIGURE 8. Claiming your HPE Primera storage array in HPE InfoSight

The HPE SSMC can also be used to register an HPE Primera system with HPE InfoSight. The process for using the SSMC to register systems is the same for both HPE Primera and HPE 3PAR. If you want to use the SSMC instead of the HPE Primera UI, follow the SSMC instructions in the HPE 3PAR section.

To use the HPE Primera UI to add VMware vCenter instances to the system so that HPE Primera systems can collect data for HPE InfoSight Cross-Stack Analytics for VMware, complete the following steps:

1. In the main menu of the Primera UI, select **Settings**.
2. On the Settings screen, click the **VMware vCenter** panel.
3. Click the plus sign **(+)** in the top right-hand corner of the screen.
4. Add the information for one or more vCenter instances that are associated with the Primera storage array.

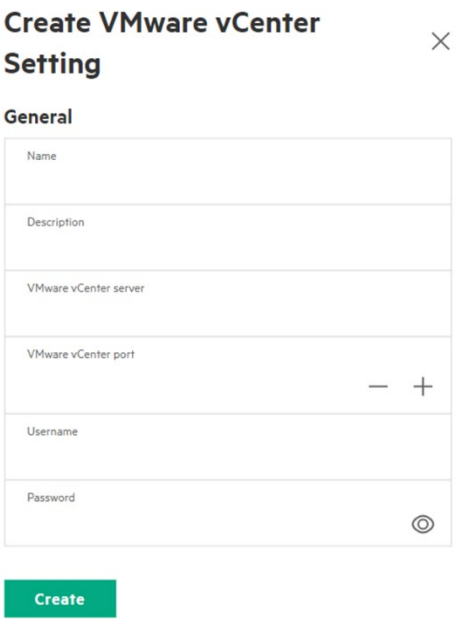

FIGURE 9. Associating a Primera system with an instance of VMware vCenter

HPE 3PAR

For HPE Primera and HPE 3PAR systems, you must have an HPE InfoSight system group to contain your storage arrays. If your company already has an existing system group, you can contact the owner to request an invitation to join it. If no system group exists, as shown in Figure 10, you can create one in HPE InfoSight by going to **Settings → HPE Primera, 3PAR StoreServ & StoreOnce → Register Systems**, clicking **Create Group**, and entering the required information. The system group can contain a combination of HPE Primera and HPE 3PAR arrays.

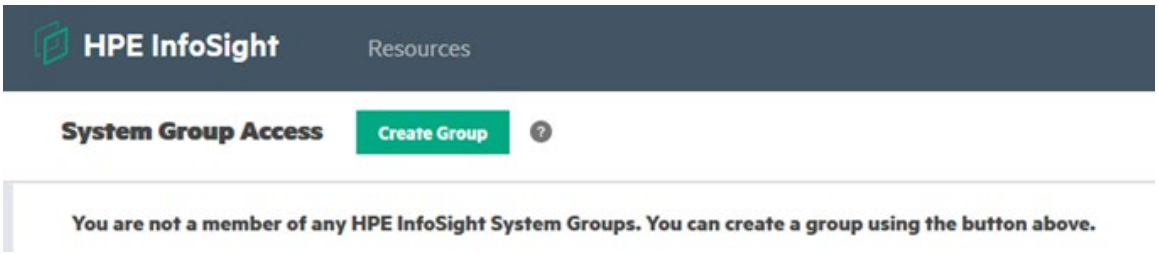

FIGURE 10. Creating an HPE InfoSight system group for your HPE Primera and HPE 3PAR storage arrays

For HPE 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 HPE 3PAR service console for the SP, as shown in Figure 11, the HPE 3PAR system that is associated with the SP sends storage analytics to HPE InfoSight.

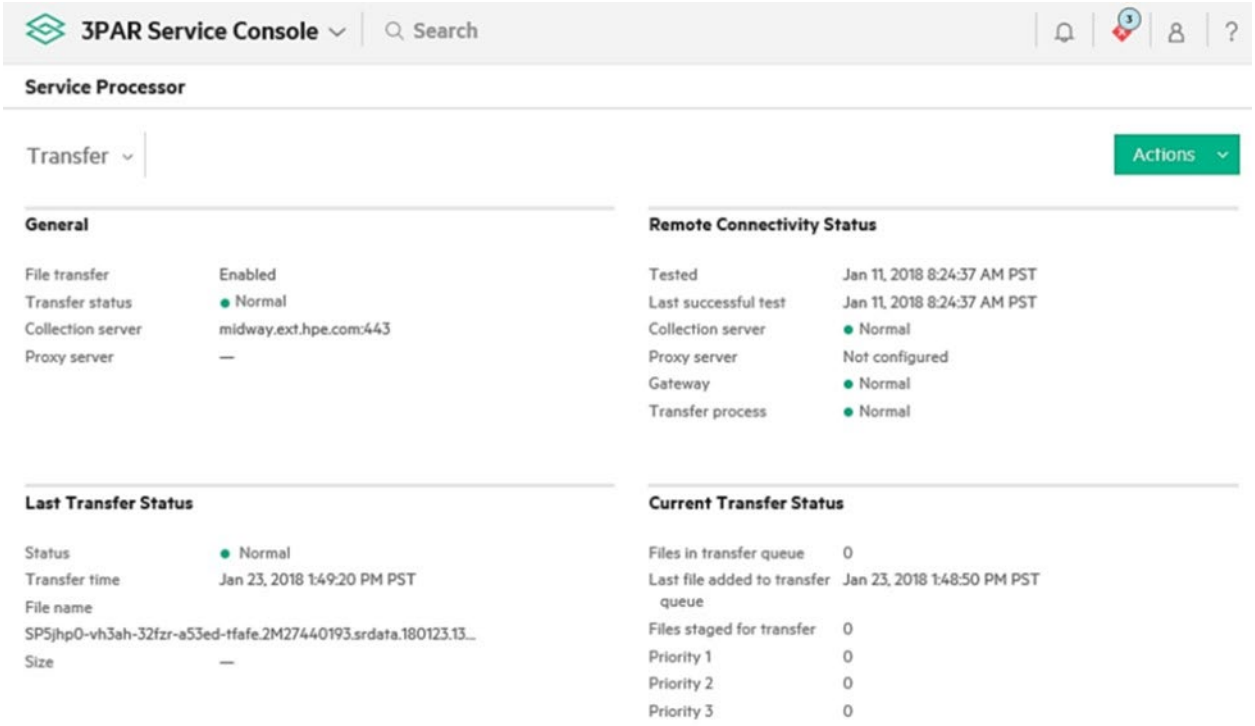

FIGURE 11. Enabling HPE 3PAR systems to send data to HPE InfoSight

The HPE 3PAR service console is also used to add VMware vCenter instances to the VMware configuration, as shown in Figure 12. To enable HPE 3PAR systems to collect data for HPE InfoSight Cross-Stack Analytics for VMware (formerly VMVision), at least one vCenter entry must be added to the VMware integration settings.

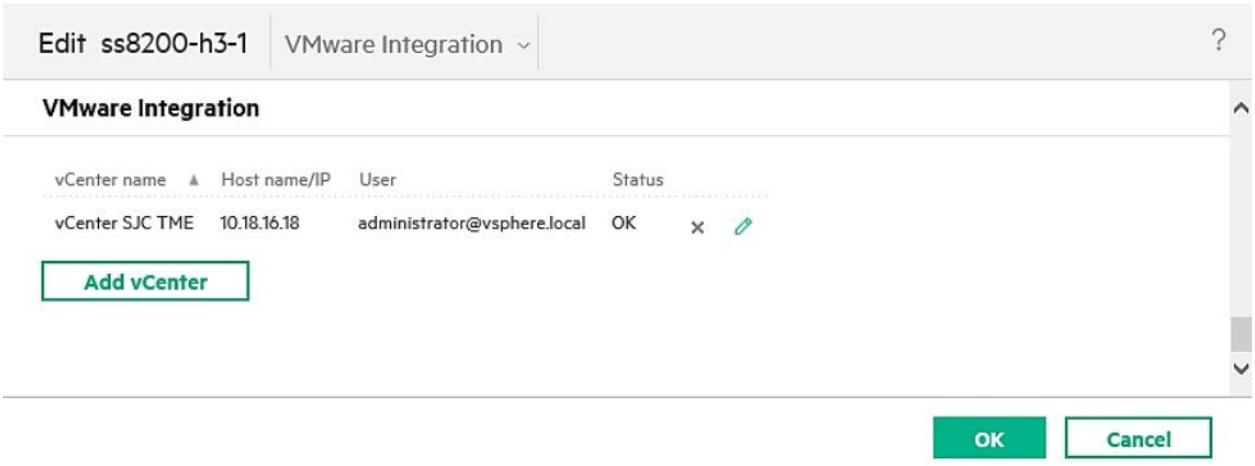

FIGURE 12. HPE 3PAR service console VMware integration settings

To make your HPE 3PAR system visible in the HPE InfoSight portal, you must register it with HPE InfoSight. To register an HPE 3PAR system in the HPE StoreServ Management Console (SSMC), complete the following steps:

1. In the HPE InfoSight portal, copy your company's registration token into **Settings → HPE Primera, 3PAR StoreServ & StoreOnce → Register Systems**.
2. Log in to the HPE SSMC.
3. From the main menu, select **Storage Systems → Systems**.

4. Select the system you want to register.
5. Hover your cursor over the **General** section and click **Edit**.
6. Paste your company's system group registration token into the **Comments** field in the **Descriptors** section.
7. Look for your registration token, which now should be in place in the **Comments** field.

NOTE
This action overwrites any existing comments, including any existing system group registration token. To view the current contents of the **Comments** field in the **Descriptors** section and append your token to them, you can run the CLI command `showsys -d`.

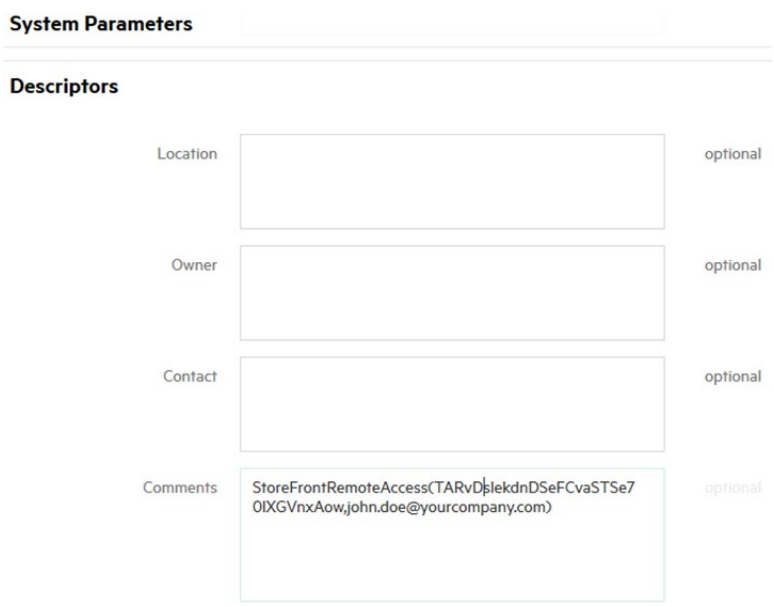

FIGURE 13. Using the HPE SSMC to register an HPE 3PAR system with HPE InfoSight

HPE SimpliVity

At a high level, to opt into or out of sending data to HPE InfoSight, you must first configure your Hewlett Packard Enterprise storage system 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 SimpliVity, data collection is disabled by default. You can enable it by selecting the checkbox **HPE InfoSight host monitor** during the host deployment, as shown in Figure 14, or after deployment from the **Menu** → **HPE SimpliVity Federation** page of the vSphere Client, as shown in Figure 15. When this checkbox is selected, the host starts sending data to HPE InfoSight over HTTPS.

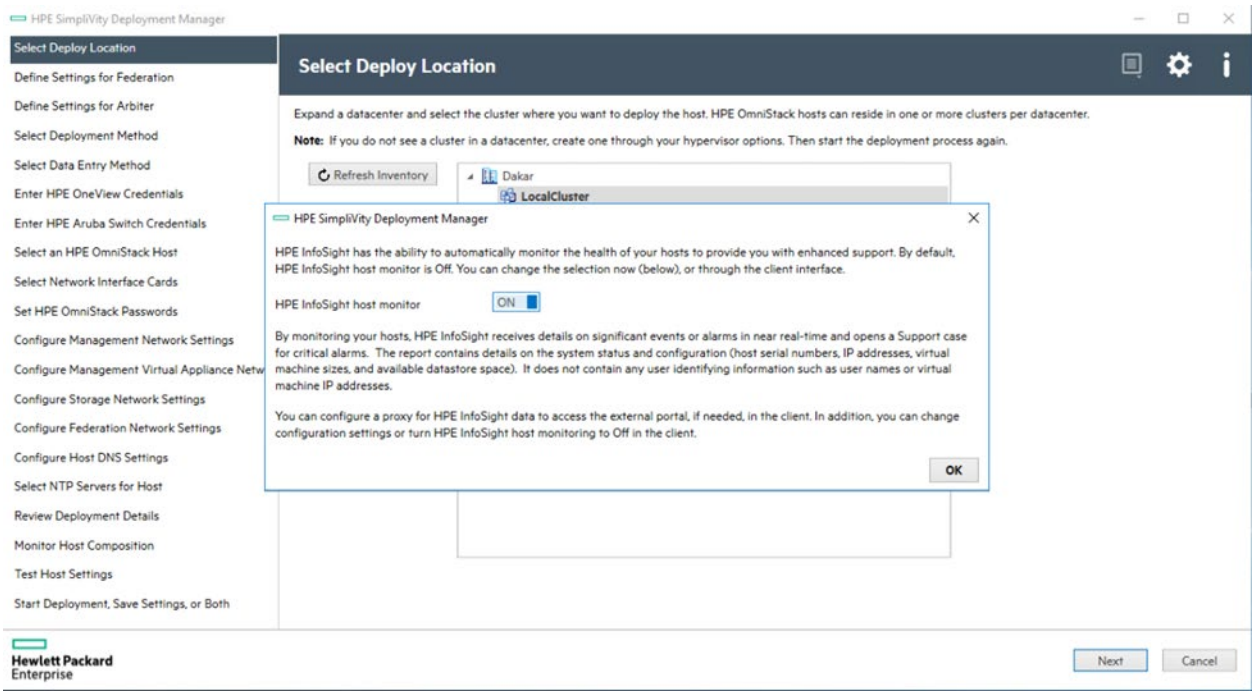

FIGURE 14. Enabling HPE SimpliVity to send data to HPE InfoSight

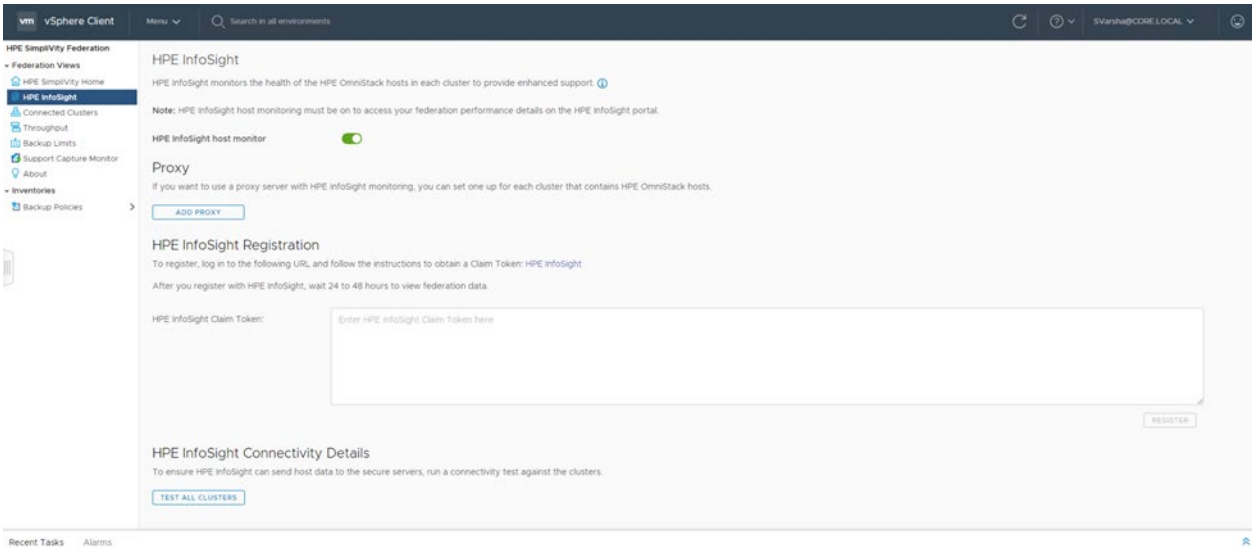

FIGURE 15. Enabling HPE SimpliVity to send data to HPE InfoSight

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

To view clusters, register the hosts with a claim token from the HPE InfoSight portal. To obtain a claim token from the HPE InfoSight page, go to **Settings Icon** → **Device Enrollment** → **HPE SimpliVity** tab, as shown Figure 16.

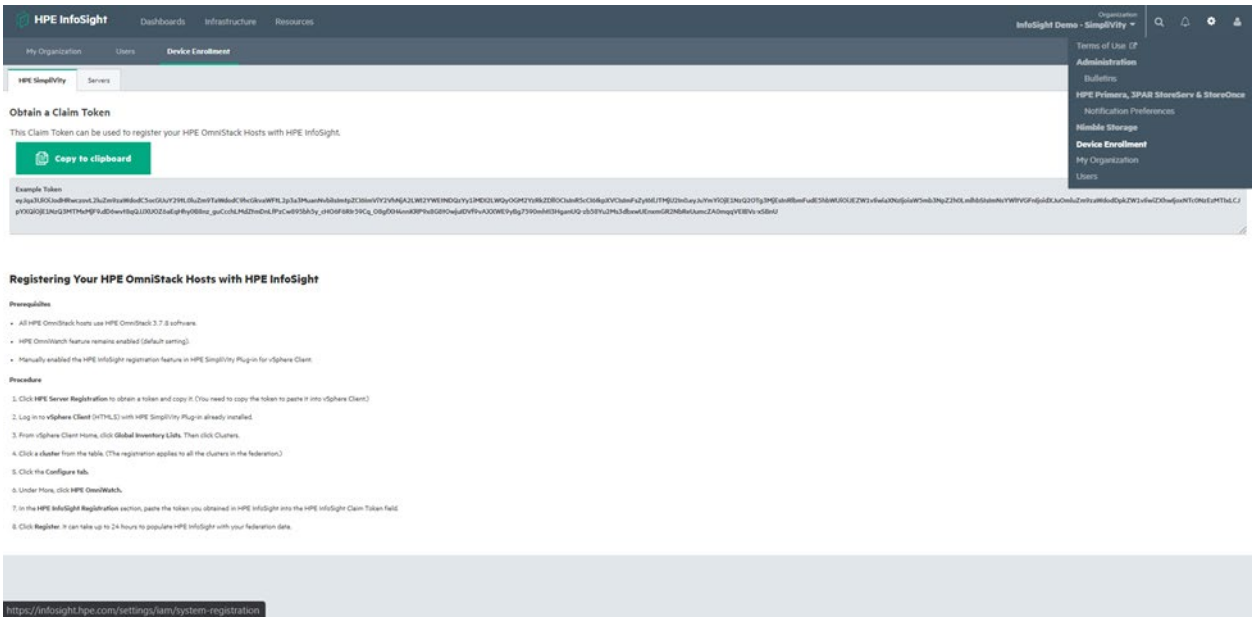

FIGURE 16. Registering HPE SimpliVity hosts on the HPE InfoSight portal

Copy the claim token to the vCenter whose data is to be viewed, as shown in Figure 17.

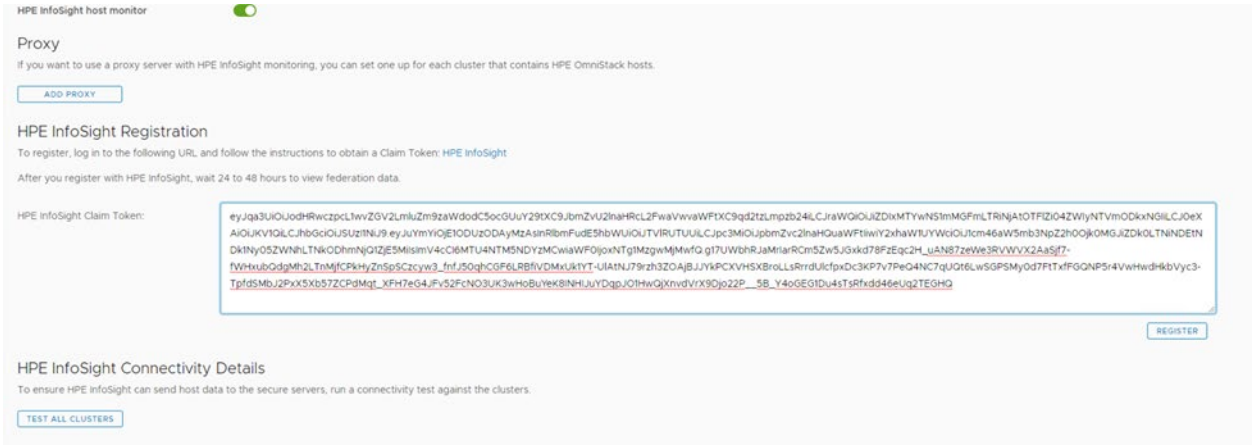

FIGURE 17. Registering HPE SimpliVity hosts on the HPE InfoSight portal

At any point, you can choose to completely unregister your system from HPE InfoSight by clicking the unregister button, as shown in Figure 18 and Figure 19.

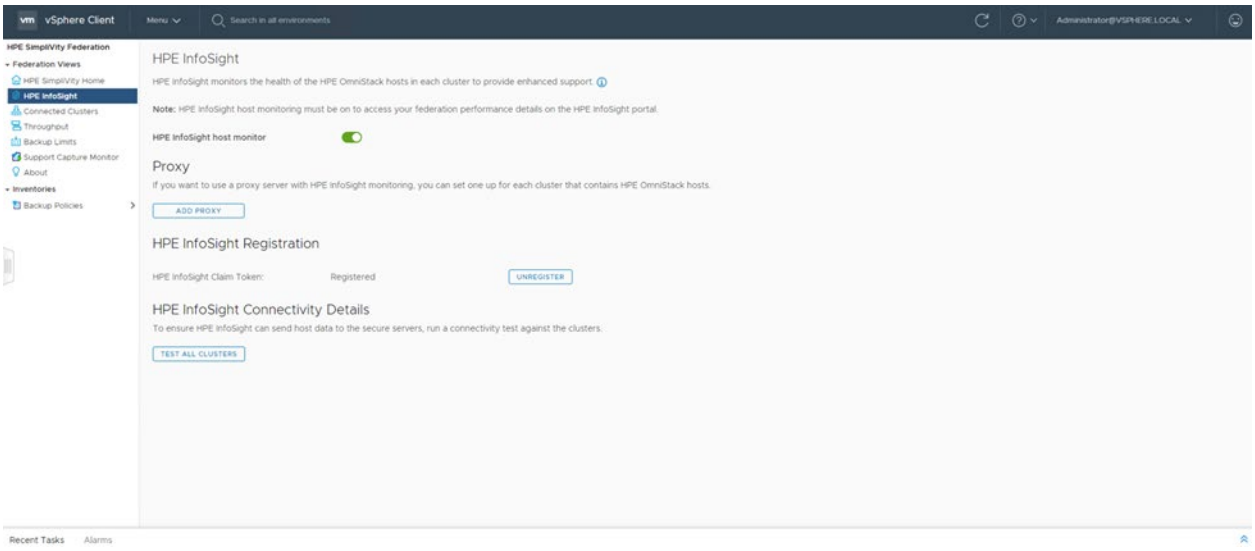

FIGURE 18. Unregistering HPE SimpliVity hosts from the HPE InfoSight portal – Unregister button

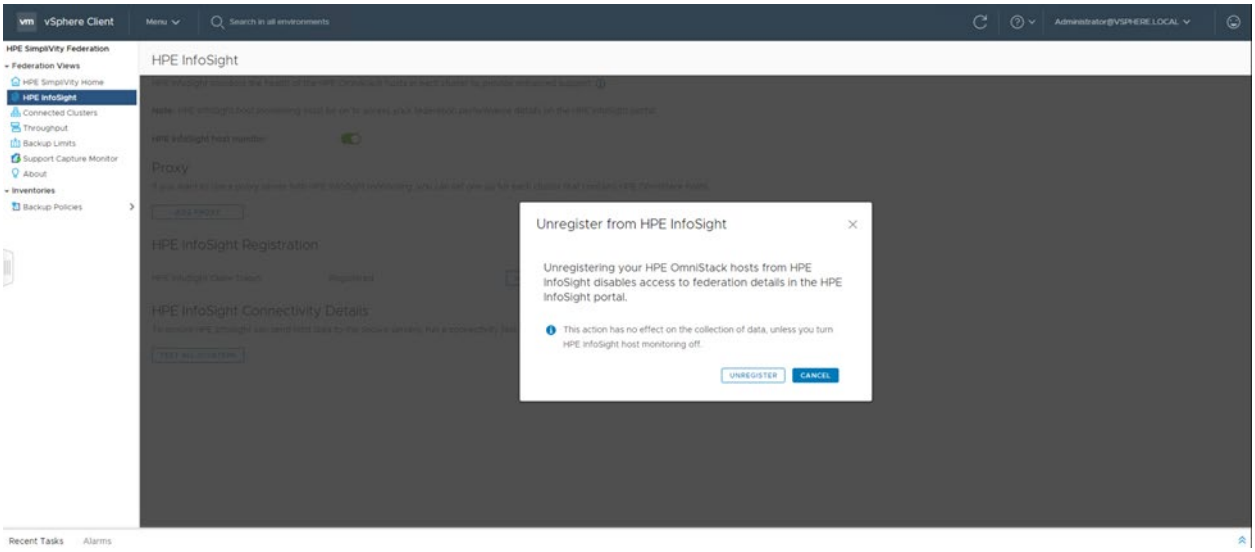

FIGURE 19. Unregistering HPE SimpliVity hosts from the HPE InfoSight portal – Unregister message

RESOURCES AND ADDITIONAL LINKS

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
- HPE InfoSight for HPE SimpliVity Getting Started
  https://support.hpe.com/hpesc/public/docDisplay?docId=a00089726en_us

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 Hewlett Packard Enterprise account team whether copies of these documents are available locally.

LEARN MORE AT

hpe.com/storage

a00067516ENW, April 2021, Rev 3

Hewlett Packard Enterprise