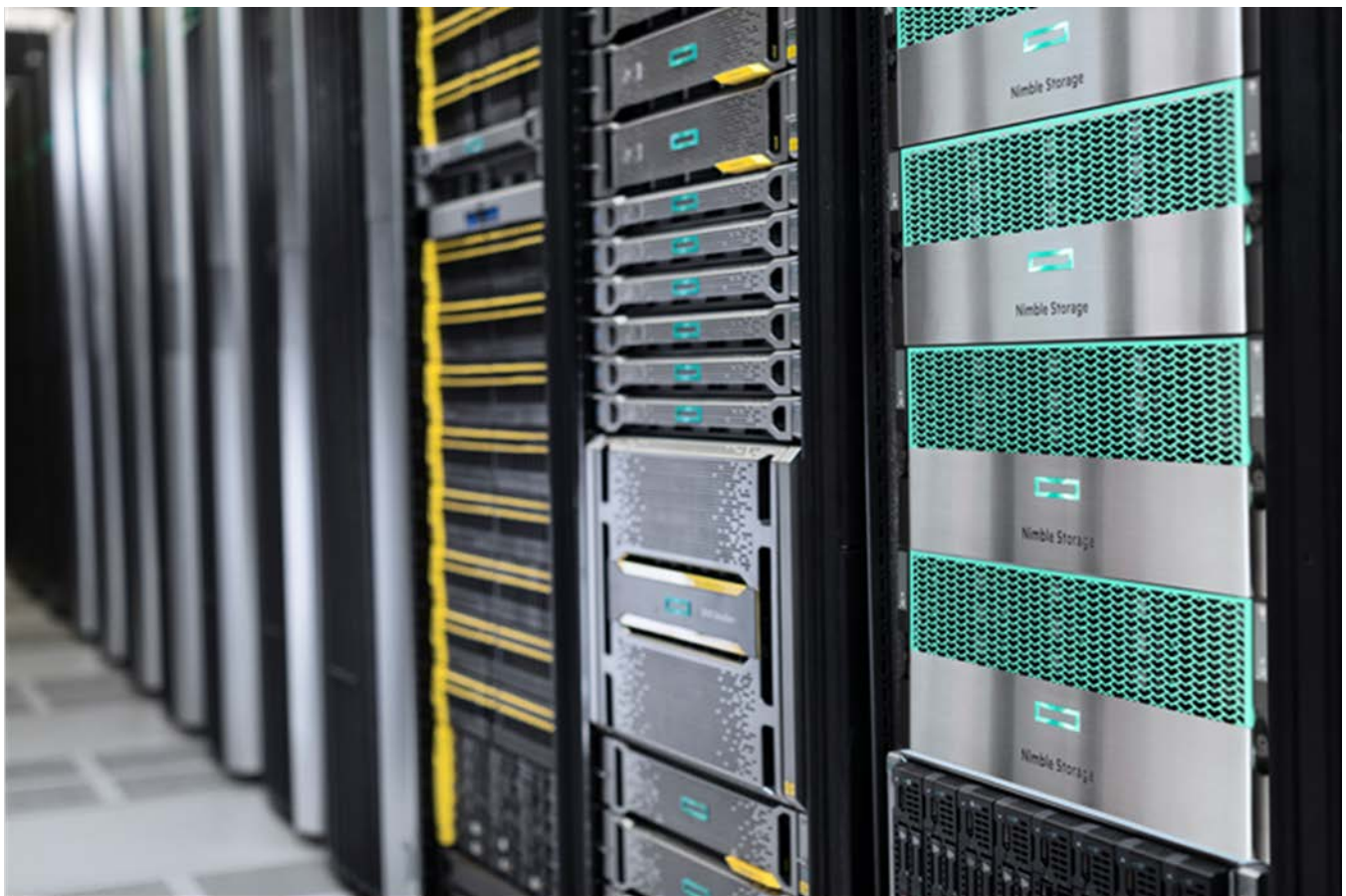




# HPE InfoSight Security for HPE Storage

L'analyse prédictive sécurisée dans le Cloud



# Contenu

Sommaire exécutif.....	3
Présentation de la solution.....	3
Types de données collectées par HPE InfoSight.....	3
Sites sécurisés.....	5
Collecte, traitement et accès aux données.....	5
Collecte et transmission de données.....	6
Traitement des données.....	6
Accès aux données.....	7
Pratiques de sécurité des informations.....	7
HTTPS TLS 1.2.....	7
Accès, surveillance et vérification.....	7
Sécurité et protection du réseau.....	8
Sécurité physique.....	8
Contrôle d'accès basé sur des rôles.....	8
Sommaire.....	9



## Sommaire exécutif

Ce livre blanc fournit aux utilisateurs potentiels ou actuels de systèmes de stockage HPE des informations sur la manière dont les données sont collectées et protégées par [HPE InfoSight](#). Le document part du principe que le lecteur possède une connaissance rudimentaire de HPE InfoSight.

## Présentation de la solution

HPE InfoSight fournit des [analyses prédictives](#) basées sur le cloud pour les baies de [stockage HPE Nimble Storage](#) (100 % Flash, flash adaptatif et flash secondaire), pour [HPE 3PAR StoreServ](#) et pour HPE StoreOnce. Au-delà du stockage, HPE InfoSight a une visibilité à travers la pile technologique sur le réseau, les hôtes et l'infrastructure virtuelle. Hewlett Packard Enterprise estime que l'avenir de [l'infrastructure IT](#) réside dans l'introduction de l'intelligence artificielle dans le data center. HPE InfoSight est un élément clé de l'effort de construction de l'infrastructure du data center autogéré du futur.

## Types de données collectées par HPE InfoSight

Toutes les données collectées par HPE InfoSight concernent la configuration, des statistiques et l'intégrité du système de stockage. HPE InfoSight collecte plusieurs types de données de l'infrastructure d'un client : statistiques de streaming, battements, diagnostics et données de configuration et alertes. Si VMware vCenter® fait partie intégrante de l'infrastructure du client, HPE InfoSight collecte également des données de vCenter.

Selon le type de données, les clients peuvent choisir d'accepter ou de refuser de fournir des jeux de données spécifiques à HPE InfoSight :

- **Statistiques de streaming.** Également connu sous le nom de statistiques de streaming, cet ensemble de données se compose d'informations sur les performances (compteurs et statistiques). Les clients ont la possibilité de ne pas transmettre les statistiques de streaming à HPE InfoSight.
- **Battements.** Les battements permettent à HPE InfoSight de savoir si l'infrastructure est en communication active avec HPE InfoSight ou si la connectivité a été interrompue ou perdue. Le battements consiste en un petit ensemble de paquets qui sont transmis d'une baie de stockage HPE spécifique à HPE InfoSight. Les clients ne peuvent pas refuser de fournir des battements ; la fonction est toujours activée.
- **Diagnostics for HPE Nimble Storage Analytics (DNA).** Les données d'ADN consistent en des données de configuration sur les dispositifs dans l'infrastructure, comme le modèle de la baie de stockage, la capacité rattachée à la baie et la configuration du groupe. Les clients ont la possibilité de refuser de transmettre des données ADN à HPE InfoSight.
- **Alertes.** Les alertes désignent un type de données qui est transmis avec la plus haute priorité à HPE InfoSight. Les alertes peuvent être déclenchées pour de nombreuses raisons. Les clients ont la possibilité de refuser de transmettre des alertes à HPE InfoSight.
- **Cross-Stack Analytics for VMware®.** Précédemment connu sous le nom de VMVision, Cross-Stack Analytics for VMware data est constitué de données sur la configuration et les performances collectées par VMware vCenter. Les clients n'ont pas la possibilité d'accepter ou de refuser la transmission de données VMVision à HPE InfoSight. Ils peuvent contrôler la fonctionnalité à partir de leur compte HPE InfoSight en configurant l'instance vCenter pour activer les données de streaming de la machine virtuelle (VM).

ARRAY	DIAGNOSTICS DELIVERY			DIAGNOSTICS CONTENT
	HEARTBEATS	DAILY	STREAMING	VMWARE
lvs-is-u10-dev33-array-01	13 hours ago	<input checked="" type="checkbox"/>	6 minutes ago	<input checked="" type="checkbox"/>

Schéma1. Activation des données de streaming des machines virtuelles dans HPE InfoSight.

## Important

La sécurité des données créées par les clients est une priorité absolue pour HPE. À aucun moment, les données des clients - les données stockées dans les volumes de stockage ou les LUN - ne sont transmises à HPE InfoSight. La collecte de données par HPE InfoSight est strictement limitée aux données liées à la configuration et aux performances.

À un niveau élevé, pour choisir de transmettre ou non des données à HPE InfoSight, les clients doivent d'abord configurer leurs systèmes de stockage HPE pour activer la communication de données avec HPE InfoSight. Si la communication de données avec HPE InfoSight n'est pas activée, aucune donnée n'est transmise à HPE InfoSight, pour quelque raison que ce soit.

Par exemple, dans les baies de stockage HPE Nimble, la collecte de données est désactivée par défaut. Les utilisateurs peuvent l'activer en cochant la case **Allow Nimble Storage Support pour collecter automatiquement les données analytiques de la baie** sur la page **Administration > Alertes et surveillance** de l'interface de gestion de la baie de stockage. Lorsque cette case est cochée, la baie de stockage commence à transmettre des données à HPE InfoSight via le protocole HTTPS.





Schéma 2. Activation des baies de stockage HPE Nimble Storage pour la transmission des données vers HPE InfoSight.

Les clients peuvent choisir à tout moment de ne pas transmettre certains types de données ou de ne plus transmettre de données à HPE InfoSight.

Pour les systèmes 3PAR, les paramètres de transfert doivent être configurés pour que le processeur de service (SP) transmette des données à HPE InfoSight. Une fois les paramètres configurés dans la console de service 3PAR pour le SP, les analyses de stockage sont transmises à HPE InfoSight par le système 3PAR qui est associé au SP.

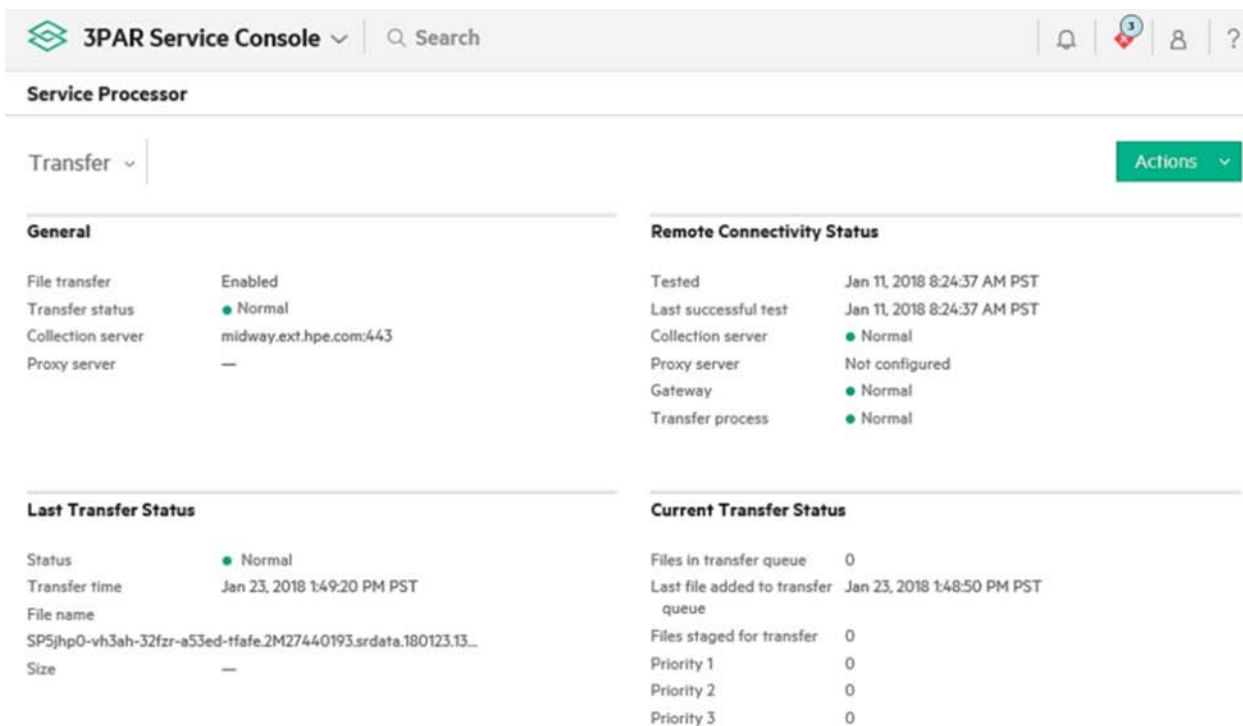
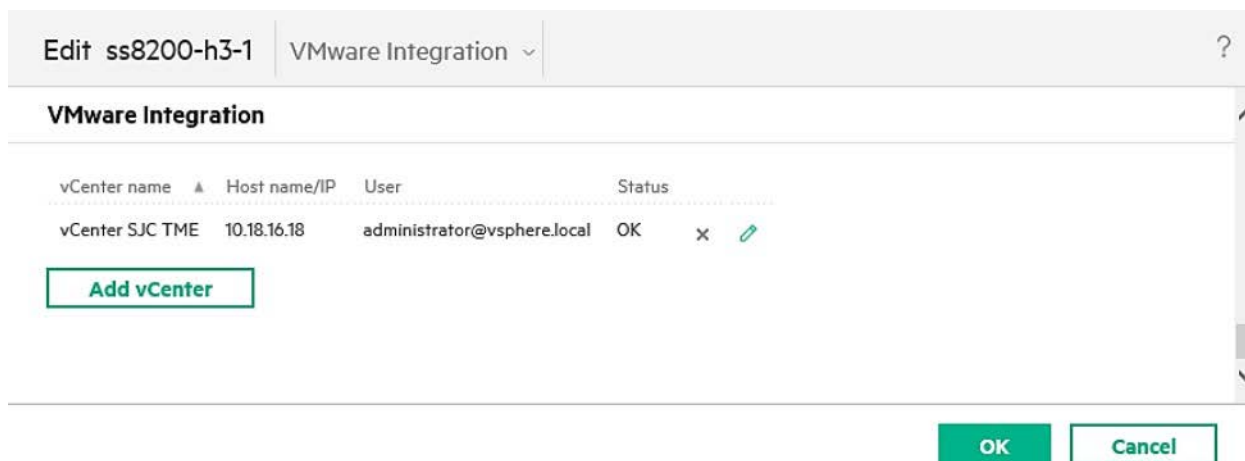


Schéma 3. Activation des systèmes 3PAR pour transmettre des données à HPE InfoSight.

La console de service 3PAR est également utilisée pour ajouter des instances VMware vCenter à la configuration VMware. Pour que les systèmes 3PAR puissent collecter des données pour la fonctionnalité HPE InfoSight Cross-Stack Analytics for VMware (anciennement VMVision), au moins une entrée vCenter doit être ajoutée aux paramètres d'intégration VMware. Une fois ajoutée, les données de streaming des machines virtuelles peuvent être activées sur le portail HPE InfoSight pour la baie qui est configurée.





**Schéma 4.** Paramètres d'intégration VMware de la console de service 3PAR.

### Sites sécurisés

Certains sites de clients sont des sites sécurisés, ce qui signifie que les systèmes ne communiquent pas ni ne peuvent communiquer avec des dispositifs extérieurs au réseau interne. L'ensemble de fonctionnalités de HPE InfoSight ne s'étend pas actuellement aux déploiements locaux tels que ceux nécessaires aux sites sécurisés.

Sur des sites sécurisés, les clients peuvent utiliser l'ensemble de statistiques et d'informations disponibles via l'interface locale de gestion des baies. Pour les clients qui souhaitent ajouter des données dans des outils internes existants, les baies de stockage HPE disposent d'API REST qui peuvent être utilisées pour collecter des données par programmation au sein d'un réseau local. De plus, des alertes peuvent être générées et envoyées au sein du réseau local grâce à l'interface et aux outils de gestion du stockage natifs.

Pour les organismes publics, l'extension de HPE InfoSight à AWS GovCloud ou à des services cloud similaires pourrait être une possibilité pour certains produits de la gamme HPE. Si vous souhaitez explorer les moyens de tirer parti de HPE InfoSight dans votre environnement, contactez votre équipe de conseillers HPE pour obtenir de plus amples informations et les solutions possibles.

### Collecte, traitement et accès aux données

HPE utilise une infrastructure cloud hautement évolutive qui constitue le service Cloud HPE InfoSight. L'architecture complète de HPE InfoSight contient les éléments suivants :

- Des composants qui sont déployés sur le site du client par le biais de baies de stockage HPE (baies de stockage HPE Nimble Storage et systèmes de stockage HPE 3PAR).
- Une infrastructure pour le traitement et l'analyse des données.
- Un portail Internet via lequel les utilisateurs peuvent accéder à leurs données en toute sécurité.

Le schéma suivant présente un aperçu simplifié de la collecte de données et de l'architecture de communication de HPE InfoSight. À haut niveau, les composants peuvent être regroupés dans la collecte et la transmission de données, le traitement de données et l'accès aux données.



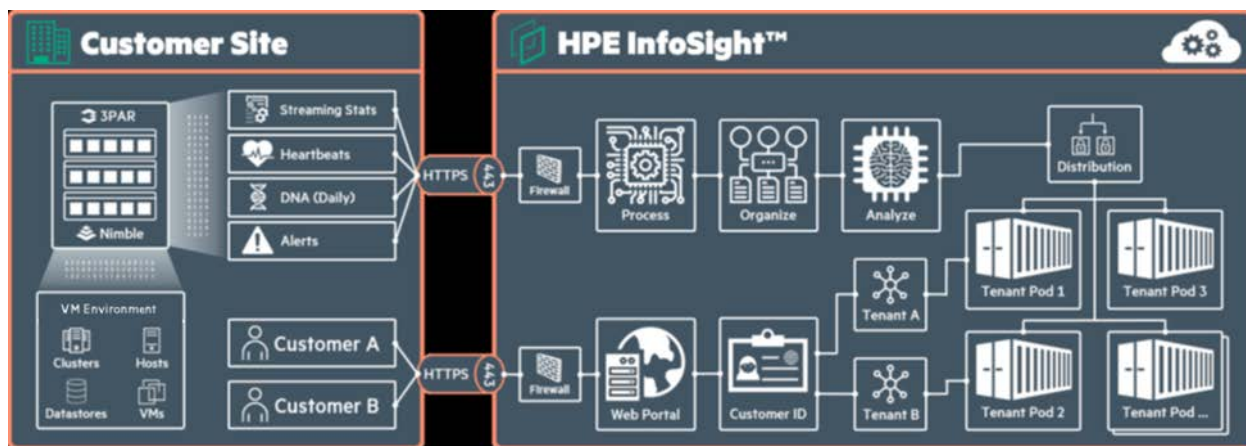


Schéma 5. Architecture de collecte et de communication des données HPE InfoSight.

### Collecte et transmission de données

La baie de stockage est l'élément clé de la collecte de données. Chaque point de données est dénommé capteur de données. Des millions de capteurs de données sont mis en place dans le système d'exploitation de stockage natif. Les capteurs de données ne sont pas des capteurs physiques, tels que des capteurs de chaleur ; ce sont plutôt des compteurs, des statistiques ou un autre point de données fourni par le système d'exploitation de stockage.

---

#### Remarque

Dans certains cas, les capteurs de données peuvent extraire des données de capteurs physiques sur le matériel, mais ils sont généralement des compteurs et des statistiques liés au logiciel.

---

Les capteurs de données de la baie de stockage native transfèrent les données à HPE InfoSight. La fréquence de transmission des données varie selon le type de données qui sont transférées :

- Des alertes sont générées et envoyées instantanément lorsque des événements qui déclenchent les conditions d'alerte se produisent.
- Des battements sont envoyés toutes les cinq minutes.
- Les statistiques de streaming sont envoyées toutes les dix minutes.
- Les données ADN sont envoyées une fois par jour.

Ces intervalles indiqués étaient exactes au moment de la rédaction du présent document. HPE InfoSight est constamment amélioré, l'accent étant mis sur une transmission des données aussi sûre, rapide et efficace que possible.

Lorsque des données doivent être collectées à partir d'autres composants de la pile d'infrastructure, un collecteur natif est intégré au système d'exploitation de stockage. Le collecteur natif est chargé d'extraire ces données du composant de niveau supérieur. Par exemple, lorsque le plugin HPE Nimble Storage VMware vCenter est enregistré sur une instance vCenter, le collecteur dans HPE NimbleOS peut extraire des données de cette instance vCenter spécifique, puis les transférer vers HPE InfoSight.

---

#### Remarque

Plusieurs instances vCenter peuvent être enregistrées pour communiquer des données dans un seul compte HPE InfoSight.

---

Quel que soit le type de données ou la fréquence de transmission, les données sont envoyées à HPE InfoSight par HTTPS (port 443) via TLS 1.2 afin de garantir une protection contre les pirates informatiques malveillants ou tout autre accès non autorisé pendant la transmission.

### Traitement des données

Les données qui sont envoyées à HPE InfoSight doivent être traitées, organisées, analysées et stockées d'une manière accessible via le portail Internet. L'infrastructure cloud qui prend en charge HPE InfoSight utilise des mécanismes de sécurité du réseau standards, tels que des pare-feu, pour empêcher tout accès non autorisé au réseau cloud interne.



Lorsque les données parviennent à HPE InfoSight, elles sont traitées dans le système. Le traitement consiste à reconnaître le type de données qui a été envoyé et le système interne vers lequel ces données doivent être transférées ; par exemple, les battements ne sont pas traités de la même manière que les données ADN. Il est important de savoir que les données doivent être associées à un système, un compte et un client spécifique afin de pouvoir les gérer et les sécuriser pendant leur traitement, puis de les stocker pour y accéder. Avant que les données ne puissent être analysées, elles doivent être organisées de manière structurée, c'est-à-dire qu'un schéma doit être appliqué aux données. L'analyse suppose d'appliquer un vaste ensemble de signatures de données avancées et de vérifications de l'intégrité par rapport à l'ensemble de données. Les données de base et les résultats de l'analyse sont stockés dans une architecture hautement évolutive.

Bien que de nombreuses signatures de données soient appliquées à des ensembles de données spécifiques, de nombreuses autres signatures sont appliquées à l'ensemble des données (la base installée). Ces signatures de données globales ne contiennent jamais l'identification du client ou les détails du système car elles sont appliquées à l'ensemble de données globales pour déterminer les résultats abstraits. Par exemple, HPE InfoSight évalue les taux de modification moyens par minute, par heure et par jour pour les données qui sont affectées à des profils de performance spécifiques. Ces données sont essentielles pour permettre d'identifier les besoins et les attentes en matière de réplication. Seul le résultat de ce type d'analyse est potentiellement visible pour un client, jamais les données qui ont été utilisées pour déterminer le résultat.

### Accès aux données

Pour que HPE InfoSight puisse reconnaître des clients individuels, chaque client se voit attribuer un identifiant unique. Les clients accèdent à leur propre compte HPE InfoSight et le gèrent, y compris en désignant des super-utilisateurs qui peuvent ajouter ou révoquer des autorisations pour permettre à d'autres utilisateurs d'accéder aux données du compte. Du point de vue du traitement des données et de l'accès aux données, chaque client peut être considéré comme un locataire.

Lorsqu'un client se connecte au portail Internet HPE InfoSight pour accéder aux données et les afficher dans l'interface web, HPE InfoSight vérifie l'identifiant du client et récupère les données associées à ce locataire. L'identifiant du client et le processus de vérification garantissent que les clients n'accèdent qu'à leurs données et ne voient ni n'accèdent aux données d'aucun autre locataire. La seule méthode permettant aux clients d'accéder aux données est via le portail Internet HPE InfoSight. Un client ne peut à aucun moment accéder à un système principal.

Un très gros client peut parfois avoir plusieurs comptes HPE InfoSight et, par conséquent, plusieurs identifiants. Ce cas de figure est rare et se produit généralement lorsque le client exploite des filiales ou lorsque la société est exceptionnellement grande et fonctionne comme différentes entités à travers le monde. Le cas échéant, les données sont sécurisées séparément pour chaque identifiant de client et pour chaque compte HPE InfoSight. Les utilisateurs peuvent demander à accéder à d'autres comptes InfoSight HPE, mais les autorisations sont gérées au cas par cas par les propriétaires des comptes HPE, les super-utilisateurs.

### Pratiques de sécurité des informations

HPE utilise plusieurs pratiques courantes pour sécuriser les données HPE InfoSight. HPE InfoSight est un service basé dans le cloud, mais il gère directement l'infrastructure interne.

Les employés qui ne travaillent pas pour HPE n'ont jamais accès à l'infrastructure interne HPE InfoSight. L'accès des employés de HPE est strictement limité à ceux qui ont absolument besoin d'accéder à l'infrastructure. Les clients, les partenaires et la plupart des employés de HPE interagissent avec HPE InfoSight uniquement par le biais du portail Internet.

### HTTPS TLS 1.2

Toutes les données sont transmises à HPE InfoSight via le protocole HTTPS TLS 1.2. En outre, tous les utilisateurs accèdent au portail Internet HPE InfoSight via une connexion HTTPS. Le protocole TLS 1.2 utilise la cryptographie à clé publique et l'authentification mutuelle des clients et des serveurs pour garantir la confidentialité, l'intégrité des messages et l'authentification du trafic transitant sur Internet.

Les certificats TLS pour HPE InfoSight sont signés par une autorité de certification (AC) tierce de confiance, GeoTrust. L'AC est une entité fiable qui valide l'authenticité de HPE InfoSight par le biais d'un certificat numérique. Le certificat comprend la clé publique HPE qui est utilisée pour les communications cryptées vers HPE InfoSight et d'autres informations concernant HPE. La technologie standard du navigateur Internet gère une liste de certificats racines d'AC pour vérifier qu'une AC connue et digne de confiance a signé et validé le certificat numérique.

### Accès, surveillance et vérification

Des listes de contrôle d'accès (ACL) strictes sont établies pour limiter l'accès aux services internes de HPE InfoSight. Seuls les employés de HPE ayant besoin de savoir ont accès aux données InfoSight de HPE. Toutes les conversations réseau et les modifications effectuées sur des comptes HPE InfoSight font l'objet d'un suivi, et la journalisation complète de l'audit est activée.

Les utilisateurs auxquels le rôle d'administrateur a été attribué peuvent accéder aux rapports d'audit sur le portail Internet HPE InfoSight en sélectionnant **Rapports > Rapport d'audit**. Toutes les actions de l'utilisateur sont consignées dans le rapport d'audit, par exemple, lorsque l'autorisation est accordée ou révoquée pour le compte ou lorsqu'une alerte est reconnue pour un dispositif qui transmet des rapports sur le compte. Tout utilisateur qui accède au compte est connecté. Les entrées du journal enregistrent le nom de l'utilisateur, incluent un horodatage et indiquent la catégorie, la description, le statut et d'autres informations sur l'utilisateur. Ces rapports peuvent être exportés si nécessaire.



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

Schéma 6. Exemple de rapport d'audit du portail Internet HPE InfoSight.

### Sécurité et protection du réseau

L'infrastructure réseau HPE InfoSight utilise des pare-feu et une protection antivirus au niveau du réseau. Les signatures de protection contre les virus sont mises à jour régulièrement de sorte que le réseau soit protégé contre les anciens et les nouveaux types de virus et d'attaques.

Les connexions principales entre les sites utilisent des connexions privées et des protocoles sécurisés. La journalisation interne permet de connaître l'identité des employés ou les départements de HPE qui ont accédé aux données et la date d'accès.

### Sécurité physique

Étant donné que HPE InfoSight est un service cloud mondial, l'infrastructure physique de HPE InfoSight est répartie sur plusieurs sites. Certains sites sont des installations qui appartiennent à HPE, mais plusieurs sites de collocation hébergent également l'infrastructure InfoSight de HPE.

La sécurité physique comprend des salles de serveurs verrouillées, une infrastructure protégée dans les collocations, un accès restreint par badge à l'infrastructure physique et un accès consigné aux installations.

### Contrôle d'accès basé sur des rôles

HPE InfoSight utilise le contrôle d'accès basé sur des rôles (RBAC) pour limiter l'accès aux données par le personnel de HPE. Le RBAC s'étend aux utilisateurs de HPE InfoSight et aux partenaires de HPE. Les partenaires et les employés de HPE peuvent demander l'accès aux comptes clients avec lesquels ils travaillent. Un petit nombre de salariés de HPE qui travaillent directement sur HPE InfoSight (par exemple, les ingénieurs) ont un accès super-utilisateur à HPE InfoSight, mais la majorité des salariés de HPE n'ont qu'un accès de base, qui est limité aux comptes et aux données HPE internes (par exemple, le compte IT interne de HPE).

Les utilisateurs ayant des rôles spécifiques peuvent être ajoutés à n'importe quel compte InfoSight HPE. Les comptes d'utilisateurs sont gérés sur le portail Internet via la page **Administration > Utilisateurs**. HPE InfoSight dispose actuellement de deux rôles d'utilisateur : utilisateur standard et super-utilisateur. Les comptes clients doivent avoir au moins un super-utilisateur désigné. Un super-utilisateur a la possibilité de gérer les utilisateurs et les autorisations pour un compte HPE InfoSight ; un utilisateur standard ne peut pas effectuer ces tâches. Les utilisateurs peuvent être créés, activés, désactivés ou modifiés pour que leurs rôles soient changés ou leurs mots de passe soient réinitialisés.

+ Invite User



LOGIN	ROLE
support-tools@nimblestorage.com	Super User ( <a href="#">Change</a>   <a href="#">Delete</a> )

Schéma 7. Gestion des utilisateurs du compte HPE InfoSight et attribution de rôle.

Les utilisateurs qui ne sont pas directement rattachés à un compte InfoSight HPE peuvent demander l'accès à ce compte. Ces demandes d'accès sont gérées à partir du portail Internet via la page **Administration > Autorisations**. Toutes les demandes d'accès sont affichées sur cette page, et un super-utilisateur a la possibilité d'accepter ou de rejeter la demande. Si la demande d'accès est acceptée, l'utilisateur se voit accorder l'accès au compte de base par défaut. Des autorisations supplémentaires peuvent être accordées au cas par cas pour Cross-Stack Analytics for VMware (anciennement VMVision) et pour pouvoir gérer les demandes d'assistance pour le compte. Les autorisations peuvent être modifiées à tout moment.





ORGANIZATION	USER	PERMISSIONS
Nimble Storage - Automation - Reseller1	ns.a.reseller1.contact1@gmail.com	<div data-bbox="821 315 975 344">  <b>Basic Access</b> </div> <div data-bbox="821 351 1190 380">  <b>Support Case Management</b> (🔒 Revoke)                 </div> <div data-bbox="821 387 979 416"> <a href="#">+ Add Permission</a> </div> <div data-bbox="1204 309 1332 353" style="float: right; background-color: red; color: white; padding: 2px 5px; border-radius: 3px;">                     Revoke All                 </div>

**Schéma8.** Gestion des autorisations et des accès HPE InfoSight.

## Sommaire

La sécurité de HPE InfoSight s'étend aux utilisateurs du portail Internet, à la manière dont ils accèdent aux données et à la collecte, à la transmission et au traitement des données dans le cloud HPE InfoSight. HPE a pris des mesures importantes pour sécuriser les données provenant des clients et pour limiter l'accès à ces données aux seuls employés internes appropriés de HPE.



### Ressources

Pour en savoir plus sur HPE InfoSight, consultez les ressources suivantes :

- Architecture de service sécurisée HPE 3PAR  
<https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=4aa3-7592enw>
- HPE InfoSight pour HPE 3PAR StoreServ  
<https://h20195.www2.hpe.com/v2/Getdocument.aspx?docname=a00053623enw&skiphtml=1>
- Prise en main d'InfoSight  
[https://infosight.hpe.com/InfoSight/media/cms/active/pubs\\_InfoSight\\_Getting\\_Started\\_.pdf](https://infosight.hpe.com/InfoSight/media/cms/active/pubs_InfoSight_Getting_Started_.pdf)
- Manuel utilisateur d'InfoSight pour HPE Nimble Storage  
[https://infosight.hpe.com/InfoSight/media/cms/active/pubs\\_InfoSight\\_User\\_Guide\\_for\\_HPE\\_Nimble\\_Storage\\_.pdf](https://infosight.hpe.com/InfoSight/media/cms/active/pubs_InfoSight_User_Guide_for_HPE_Nimble_Storage_.pdf)
- Manuels utilisateur d'InfoSight pour les serveurs HPE  
[https://support.hpe.com/hpsc/public/home/documentHome?sort\\_by=relevance&sp4ts.oid=1011200130](https://support.hpe.com/hpsc/public/home/documentHome?sort_by=relevance&sp4ts.oid=1011200130)

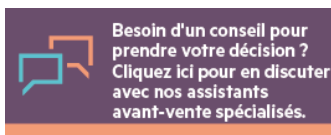
---

### Remarque

Dans certains cas, l'accès à ces ressources nécessite une connexion HPE InfoSight valide. Si vous n'avez pas d'identifiant InfoSight HPE, demandez à votre équipe de compte HPE si des copies de ces documents sont disponibles localement.

---

Pour en savoir plus, rendez-vous sur  
[hpe.com/fr/fr/storage](https://hpe.com/fr/fr/storage)



 **Partagez maintenant**

 **Mises à jour**

---

© Copyright 2020 Hewlett Packard Enterprise Development L.P. Les informations contenues dans ce document sont sujettes à modification sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune déclaration contenue dans le présent document ne peut être interprétée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document.

Aux États-Unis et/ou dans d'autres juridictions, les noms « VMware » et « VMware vCenter », sont des marques ou des marques déposées reconnues comme appartenant à la société VMware, Inc. Toutes les autres marques de tiers sont la propriété de leur(s) propriétaire(s) respectif(s).

a00067516FRE, Février 2020, rév. 1