

Guide de sécurité de VMware vSphere Replication

vSphere Replication 6.5

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur :
<http://www.vmware.com/fr/support/pubs>.

FR-002115-00

vmware[®]

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<http://www.vmware.com/fr/support/>

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

Copyright © 2012–2016 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

| | | |
|----------|---|-----------|
| 1 | À propos du guide de sécurité de VMware vSphere Replication | 5 |
| 2 | Document de référence à propos de la sécurité de vSphere Replication | 7 |
| | Les services, ports et interfaces externes utilisés par le dispositif virtuel vSphere Replication | 7 |
| | Fichiers de configuration vSphere Replication | 11 |
| | Clé privée, certificat et keystore de vSphere Replication | 11 |
| | Licence et fichier CLUF de vSphere Replication | 11 |
| | Fichiers journaux de vSphere Replication | 12 |
| | Comptes d'utilisateurs vSphere Replication | 13 |
| | Correctifs et mises à jour de sécurité pour vSphere Replication | 13 |
| | Index | 15 |

À propos du guide de sécurité de VMware vSphere Replication

1

Le *guide de sécurité de VMware vSphere Replication* constitue un document de référence concis concernant les fonctions de sécurité de vSphere Replication.

Pour vous permettre de protéger votre installation vSphere Replication, ce guide décrit les fonctions de sécurité intégrées à vSphere Replication et les mesures que vous pouvez prendre pour la protéger des attaques.

- Les ports, services et interfaces externes nécessaires au fonctionnement optimal de vSphere Replication
- Les options de configuration et les paramètres qui peuvent engendrer des problèmes de sécurité
- L'emplacement des fichiers journaux et leur fonction
- Les comptes de système requis
- Des informations sur l'obtention des correctifs de sécurité les plus récents

Public cible

Ces informations sont à destination des décideurs informatiques, des architectes, des administrateurs et de ceux qui souhaitent se familiariser avec les composants de sécurité de vSphere Replication.

Document de référence à propos de la sécurité de vSphere Replication

2

Vous pouvez utiliser le document de référence à propos de la sécurité pour en savoir plus à propos des fonctions de sécurité de vSphere Replication et les mesures que vous pouvez prendre pour protéger votre environnement des attaques.

Ce chapitre aborde les rubriques suivantes :

- [« Les services, ports et interfaces externes utilisés par le dispositif virtuel vSphere Replication », page 7](#)
- [« Fichiers de configuration vSphere Replication », page 11](#)
- [« Clé privée, certificat et keystore de vSphere Replication », page 11](#)
- [« Licence et fichier CLUF de vSphere Replication », page 11](#)
- [« Fichiers journaux de vSphere Replication », page 12](#)
- [« Comptes d'utilisateurs vSphere Replication », page 13](#)
- [« Correctifs et mises à jour de sécurité pour vSphere Replication », page 13](#)

Les services, ports et interfaces externes utilisés par le dispositif virtuel vSphere Replication

L'opération de vSphere Replication est dépendante de certains services, ports et interfaces externes.

Services vSphere Replication

L'opération de vSphere Replication est dépendante de différents services qui s'exécutent sur le dispositif virtuel vSphere Replication.

Tableau 2-1. Services vSphere Replication

| Nom du service | Type de démarrage | Description |
|----------------|---|--|
| hms | Automatique pour le dispositif vSphere Replication. Désactivé pour le dispositif additionnel vSphere Replication. | Service de gestion vSphere Replication |
| hbrsrv | Automatique | Service vSphere Replication |
| sshd | Automatique | Désactivé par défaut. |

Tableau 2-1. Services vSphere Replication (suite)

| Nom du service | Type de démarrage | Description |
|----------------|-------------------|--|
| ntp | Automatique | Service de temps pour la synchronisation avec un serveur de temps Internet via NTP. REMARQUE Après l'installation ou la mise à niveau d'un dispositif virtuel vSphere Replication, vous devez synchroniser le dispositif avec un serveur de temps. |
| vaos | Automatique | Initialisation du SE invité qui génère les paramètres réseau, les paramètres de nom d'hôte, la création de clés SSH, l'acceptation du CLUF, l'exécution des scripts de démarrage et l'initialisation VAMI. |

Ports de communication

vSphere Replication utilise différents ports de communication et protocoles.

Le dispositif vSphere Replication nécessite l'ouverture de certains ports.

REMARQUE Les serveurs vSphere Replication doivent disposer d'un accès de trafic NFC à destination des serveurs ESXi cibles.

Tableau 2-2. Ports utilisés par le dispositif vSphere Replication

| Source | Cible | Port | Protocole | Description |
|--|--|------|------------|---|
| Dispositif vSphere Replication | Instance de vCenter Server locale et distante | 80 | TCP | Tout le trafic de gestion vers le dispositif vSphere Replication est envoyé sur le port 80 sur le système proxy vCenter Server. |
| Serveur vSphere Replication dans le dispositif vSphere Replication | Hôte ESXi (intrasite) | 80 | HTTP | Utilisé pour établir la connexion avant le démarrage de la réplication initiale. |
| Dispositif vSphere Replication | Instance de vCenter Server locale et distante | 443 | TCP | Intégralité du trafic de gestion vers le dispositif vSphere Replication. |
| Serveur vSphere Replication dans le dispositif vSphere Replication | Hôte ESXi (intrasite uniquement) sur site secondaire | 902 | TCP et UDP | Utilisé par les serveurs vSphere Replication pour envoyer le trafic de réplication vers les hôtes ESXi de destination. |
| Navigateur | Dispositif vSphere Replication | 5480 | HTTPS | Interface utilisateur Web VAMI (Virtual Appliance Management Interface) vSphere Replication |

Tableau 2-2. Ports utilisés par le dispositif vSphere Replication (suite)

| Source | Cible | Port | Protocole | Description |
|---------------------------------------|--|-------|-----------|---|
| Dispositif vSphere Replication | vCenter Server (intrasite uniquement) | 7444 | TCP | |
| Proxy vCenter Server | Dispositif vSphere Replication | 8043 | SOAP | Communication intrasite du proxy vCenter Server vers le dispositif vSphere Replication. |
| Dispositif vSphere Replication | Serveur vSphere Replication | 8123 | SOAP | Trafic de gestion intrasite du serveur de gestion vSphere Replication vers le serveur additionnel vSphere Replication dans l'environnement. |
| vSphere Web Client sur le site source | vCenter Server Inventory Service sur le site cible | 10443 | HTTPS | L'interface utilisateur vSphere Replication utilise Inventory Service sur vCenter Server distant pour lister les banques de données cibles. |
| Hôte ESXi sur le site source | Serveur vSphere Replication sur le site cible | 31031 | | Trafic de réplication initial et en cours de l'hôte ESXi du site source vers le dispositif vSphere Replication ou le serveur vSphere Replication du site cible. |

Si vous déployez des serveurs vSphere Replication, vous devez ouvrir les ports requis par vSphere Replication sur ces serveurs.

Tableau 2-3. Ports utilisés par le serveur vSphere Replication

| Source | Cible | Port | Protocole | Description |
|--|--|------|------------|--|
| Serveur vSphere Replication dans le dispositif vSphere Replication | Hôte ESXi (intrasite uniquement) sur site secondaire | 902 | TCP et UDP | Trafic entre le serveur vSphere Replication et les hôtes ESXi sur le même site. En particulier le trafic du service NFC vers les serveurs ESXi de destination. |
| Navigateur | Serveur vSphere Replication | 5480 | HTTPS | Navigateur Web de l'administrateur. |

Tableau 2-3. Ports utilisés par le serveur vSphere Replication (suite)

| Source | Cible | Port | Protocole | Description |
|--|-----------------------------|-------|-----------|---|
| Serveur de gestion vSphere Replication | Serveur vSphere Replication | 8123 | SOAP | Trafic de gestion intrasite du dispositif vSphere Replication ou du service de gestion vSphere Replication vers les serveurs vSphere Replication. |
| Hôte ESXi du site source | Serveur vSphere Replication | 31031 | | Trafic de réplication initial et en cours de l'hôte ESXi du site source vers le dispositif vSphere Replication ou le serveur vSphere Replication du site cible. |

Lors de la création d'une connexion vers le cloud, vCloud Tunneling Agent du dispositif vSphere Replication crée un tunnel afin de sécuriser le transfert des données de réplication vers votre organisation cloud.

Tableau 2-4. Ports requis pour les répliquions cloud

| Source | Destination | Port | Protocole | Description |
|--|--|-------------|----------------|---|
| L'hôte ESXi du site source | Le vCenter Server du site source | 80 | TCP | Le proxy inverse vCenter Server transmet la demande de téléchargement du VIB (règles de pare-feu vCloud Air Disaster Recovery) au dispositif vSphere Replication. |
| Le dispositif vSphere Replication du site source | API vCloud | 443 | REST via HTTPS | Le dispositif vSphere Replication se connecte à ce port pour envoyer les données de réplication à une organisation cloud. |
| L'hôte ESXi du site source | Le dispositif vSphere Replication du site source | 10000-10010 | TCP | vCloud Tunneling Agent ouvre un de ces ports au dispositif vSphere Replication. L'hôte ESXi se connecte à ce port pour envoyer les données de réplication à une organisation cloud. |

Composants tiers et Open Source

Pour trouver le texte complet des licences Open Source, une liste de tous les composants tiers et Open Source, ainsi que le code Open Source utilisé dans vSphere Replication, vous pouvez accéder à http://www.vmware.com/download/open_source.html et voir la section *VMware vSphere Replication Open Source and Licenses* sous le lien *VMware vSphere Open Source*. Si certaines licences Open Source le demandent, le package vSphere Replication Open Source Disclosure Package (ODP) contient des fichiers texte avec les instructions concernant la construction et le remplacement des bibliothèques logicielles.

Fichiers de configuration vSphere Replication

Certains fichiers de configuration contiennent des paramètres qui affectent la sécurité de vSphere Replication.

REMARQUE Toutes les ressources de sécurité sont protégées avec la propriété et les permissions adéquates. Ne modifiez pas la propriété ou les permissions de ces fichiers.

| Emplacement du fichier | Description |
|--|---|
| /opt/vmware/hms/conf/hms-configuration.xml | La configuration du système par défaut du serveur de gestion vSphere Replication. |
| /opt/vmware/hms/conf/embedded_db.cfg | Le fichier de configuration pour la base de données intégrée. |

Clé privée, certificat et keystore de vSphere Replication

La clé privée, le certificat et le keystore de vSphere Replication sont situés dans le dispositif virtuel vSphere Replication.

REMARQUE Toutes les ressources de sécurité sont protégées avec la propriété et les permissions adéquates. Ne modifiez pas la propriété ou les permissions de ces fichiers.

- /etc/vmware/ssl/hbrsrv.crt
- /etc/vmware/ssl/hbrsrv.key
- /opt/vmware/hms/security/hms-keystore.jks
- /opt/vmware/hms/security/hms-truststore.jks

Licence et fichier CLUF de vSphere Replication

Le contrat de licence d'utilisateur final (CLUF) et les fichiers de licence open source se situent dans le dispositif virtuel vSphere Replication.

| Fichier | Emplacement |
|--|---|
| Licence Open Source | /usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE |
| Licence VMware Postgres | /usr/share/doc/vmware-vspherereplication/VMware_Postgres_9.5.4.0_open_source_licenses.txt |
| contrat de licence d'utilisateur final | /opt/vmware/etc/iso/EULA/language_code/0 |

Fichiers journaux de vSphere Replication

Les fichiers contenant les messages système situés dans le dispositif virtuel vSphere Replication.

| Emplacement du fichier | Description |
|---|---|
| /opt/vmware/hms/logs/hms-configtool.log | Utilisé pour enregistrer les erreurs qui se produisent lors de la configuration de l'interface VAMI (Virtual Appliance Management Interface). |
| /opt/vmware/hms/logs/hms.n.log | Utilisé pour suivre l'exécution. Informations d'heure du serveur de gestion vSphere Replication. Le fichier journal le plus récent est appelé hms.log et les fichiers hms.n.log contiennent l'historique des messages plus anciens. Le fichier avec la valeur <i>n</i> la plus élevée contient les messages les plus anciens. |
| /opt/vmware/var/log/lighttpd/error.log | Le fichier journal d'erreurs VAMI. Utilisé pour suivre les erreurs dans les opérations VAMI. |
| /var/log/vmware/ | Le dossier contient les fichiers journaux du serveur vSphere Replication. Utilisé pour suivre les problèmes de réplication. |
| /var/log/boot.msg | Utilisé pour suivre le processus de démarrage du dispositif vSphere Replication. |

Historique de messages liés à la sécurité

Le fichier /opt/vmware/hms/logs/hms.log contient les messages d'événements de connexion et de déconnexion, les messages d'erreur d'autorisation et les messages d'erreur de vérification de certificat dans le format suivant.

■ Message de connexion

```
2015-03-23 15:54:05.558 DEBUG jvsl.security.authentication.sessionmap [tcweb-5]
(..security.authentication.SessionMap) operationID=087657ec-ef0f-494c-9739-a4af62a5c049-
HMS-1033 | Ajout d'une nouvelle session à la session
map:com.vmware.hms.security.authentication.HmsUserSession@234f4bed:[
com.vmware.vim.binding.hms.UserSession:
key = site_...1b034,
userName = root,
fullName = root ,
loginTime = ...,
lastActiveTime = ...,
hmsServers = null,
locale = en,
messageLocale = en
]
```

■ Message de déconnexion

```
15-03-23 15:54:05.585 INFO jvsl.security.authorization [tcweb-8]
(..security.authorization.SessionAuthorizer) | HmsSessionManager.HmsSessionManagerLogout
called on session-manager by root@/10.26.233.124:50776 with opId 43263a64-1681-4459-
a921-1d9406308dc8-HMS-1036
```

■ Message d'autorisation

```

2015-06-25 16:10:35.994 INFO jvsl.security.authorization [tcweb-5]
(..security.authorization.SessionAuthorizer) | Authorization for method
"HmsRemoteSiteManager.HmsRemoteSiteManagerFindHmsServer" failed.

(vim.fault.NoPermission) {

  faultCause = null,

  faultMessage = null,

  object = MoRef: type = HmsRemoteSiteManager, value = site-manager, serverGuid = 18327b1a-
dac2-44d9-972e-fa9dd99fce47,

  privilegeId = HmsRemote.com.vmware.vcHms.Hms.View

}

```

■ Message d'erreur de vérification de certificat

```

2015-06-25 16:19:13.794 WARN jvsl.sessions [hms-main-thread-1] (..hms.net.ServerRegistryHms)
| Can not start HMS connection to remote site 'some-address.com'

java.util.concurrent.ExecutionException: com.vmware.vim.vmomi.client.exception.SslException:
javax.net.ssl.SSLHandshakeException:
com.vmware.vim.vmomi.client.exception.VlsiCertificateException: Server certificate chain is
not trusted and thumbprint doesn't match

```

Comptes d'utilisateurs vSphere Replication

Vous devez configurer un compte racine pour vSphere Replication. Le compte racine est utilisé pour accéder à la fois à la console du dispositif virtuel et à l'interface VAMI (Virtual Appliance Management Interface).

vSphere Replication utilise actuellement le compte racine en tant qu'administrateur de l'interface VAMI. Aucun autre utilisateur n'est créé.

Lors du déploiement du dispositif virtuel vSphere Replication, vous définissez le mot de passe du compte racine dans l'assistant de déploiement OVF.

Le mot de passe racine doit comporter au moins 8 caractères.

Privilèges assignés aux rôles d'utilisateur par défaut

vSphere Replication inclut un ensemble de rôles. Chaque rôle comporte un ensemble de privilèges qui autorisent les utilisateurs disposant de ce rôle à effectuer différentes actions.

Consultez la rubrique Rôles et autorisations de vSphere Replication dans le guide *Installation et configuration de VMware vSphere Replication*.

Correctifs et mises à jour de sécurité pour vSphere Replication

Le dispositif virtuel vSphere Replication utilise SUSE Linux Enterprise Server 12 (x86_64), Service Pack 1 comme système d'exploitation invité.

Vous pouvez appliquer la dernière mise à jour de sécurité ou le dernier correctif en utilisant le fichier ISO correspondant.

Avant d'appliquer une mise à jour ou un correctif au système d'exploitation invité, prenez en compte les dépendances. Reportez-vous à « [Les services, ports et interfaces externes utilisés par le dispositif virtuel vSphere Replication](#) », page 7.

Afin de recevoir les dernières annonces de sécurité, vous pouvez vous inscrire à la liste de diffusion Annonces de sécurité VMware à l'adresse <http://lists.vmware.com/>.

Index

C

certificat 11
CLUF 11
comptes d'utilisateurs 13
correctifs 13

D

document de référence à propos de la
sécurité 7

E

embedded_db.cfg 11

F

fichier de licence 11

H

hms-configuration.xml 11
https 7

J

journaux 12
journaux système 12

K

keystore 11

L

licences 11

M

magasin d'approbations 11
mises à jour de sécurité 13
mot de passe racine 13

N

ntp 7

P

ports 7
privilèges 13
public cible 5

S

SE invité 13
services 7

sshd 7

