

# Guía sobre seguridad de VMware vSphere Replication

vSphere Replication 8.1



vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware en:

<https://docs.vmware.com/es/>

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware, Inc.**  
Paseo de la Castellana 141. Planta 8.  
28046 Madrid.  
Tel.: + 34 91 418 58 01  
Fax: + 34 91 418 50 55  
[www.vmware.com/es](http://www.vmware.com/es)

Copyright © 2012–2018 VMware, Inc. Todos los derechos reservados. [Copyright e información de marca registrada.](#)

# Contenido

<b>1</b>	<b>Acerca de la Guía sobre seguridad de VMware vSphere Replication</b>	<b>4</b>
<b>2</b>	<b>Referencia sobre seguridad de vSphere Replication</b>	<b>5</b>
	Servicios, puertos e interfaces externas que usa el dispositivo virtual de vSphere Replication	5
	Archivos de configuración de vSphere Replication	8
	Clave privada, certificado y almacén de claves de vSphere Replication	9
	Archivos de CLUF y licencia de vSphere Replication	9
	Archivos de registro de vSphere Replication	9
	Cuentas de usuario de vSphere Replication	11
	Actualizaciones y revisiones de seguridad para vSphere Replication	11

# Acerca de la Guía sobre seguridad de VMware vSphere Replication

# 1

La *Guía sobre seguridad de VMware vSphere Replication* proporciona una referencia concisa acerca de las características sobre seguridad de vSphere Replication.

Para ayudarle a proteger su instalación de vSphere Replication, en esta guía se describen las características de seguridad integradas en vSphere Replication y las medidas que puede tomar para protegerse frente a ataques.

- Interfaces externas, puertos y servicios que se necesitan para el funcionamiento correcto de vSphere Replication.
- Opciones de configuración y ajustes que conciernen a la seguridad.
- Ubicación de los archivos de registro y su propósito.
- Cuentas del sistema obligatorias.
- Información acerca de la obtención de las revisiones de seguridad más recientes.

## Audiencia prevista

Esta información está dirigida a responsables de la toma de decisiones informáticas, arquitectos, administradores y otros usuarios que se deben familiarizar con los componentes de seguridad de vSphere Replication.

# Referencia sobre seguridad de vSphere Replication

## 2

Puede usar la referencia sobre seguridad para conocer las características de seguridad de vSphere Replication y las medidas que puede tomar para proteger su entorno frente a ataques.

Este capítulo cubre los siguientes temas:

- [Servicios, puertos e interfaces externas que usa el dispositivo virtual de vSphere Replication](#)
- [Archivos de configuración de vSphere Replication](#)
- [Clave privada, certificado y almacén de claves de vSphere Replication](#)
- [Archivos de CLUF y licencia devSphere Replication](#)
- [Archivos de registro de vSphere Replication](#)
- [Cuentas de usuario de vSphere Replication](#)
- [Actualizaciones y revisiones de seguridad para vSphere Replication](#)

## Servicios, puertos e interfaces externas que usa el dispositivo virtual de vSphere Replication

La operación de vSphere Replication depende de ciertos servicios, puertos e interfaces externas.

### Servicios de vSphere Replication

La operación de vSphere Replication depende de varios servicios que se ejecutan en el dispositivo virtual de vSphere Replication.

**Tabla 2-1. Servicios de vSphere Replication**

Nombre del servicio	Tipo de inicio	Descripción
hms	Automático para el dispositivo de vSphere Replication. Deshabilitado para el dispositivo de complemento de vSphere Replication.	vSphere Replication Management Service
hbrsrv	Automático	Servicio de vSphere Replication
sshd	Deshabilitado de manera predeterminada.	Servicio SSH

Tabla 2-1. Servicios de vSphere Replication (Continua)

Nombre del servicio	Tipo de inicio	Descripción
ntp	Automático	Servicio de tiempo para la sincronización con el servidor de tiempo de Internet a través del Protocolo de tiempo de red.  <b>NOTA:</b> Luego de instalar o actualizar un dispositivo virtual de vSphere Replication, debe sincronizar el dispositivo con un servidor de tiempo.
vaos	Automático	Inicialización del sistema operativo invitado que conduce la configuración de red, la configuración del nombre de host, la creación de claves ssh, la aceptación del CLUF, la ejecución de scripts de arranque y la inicialización de la VAMI.

## Puertos de comunicación

vSphere Replication utiliza varios puertos de comunicación y protocolos.

El dispositivo de vSphere Replication requiere que ciertos puertos estén abiertos.

**NOTA:** Los servidores de vSphere Replication deben tener acceso de tráfico NFC a los hosts ESXi de destino.

Tabla 2-2. Puertos utilizados por el dispositivo de vSphere Replication

Origen	Destino	Puerto	Protocolo	Descripción
Dispositivo de vSphere Replication	vCenter Server local y remoto	80	TCP	Todo el tráfico de administración del dispositivo de vSphere Replication va hasta el puerto 80 en el sistema proxy vCenter Server.
Servidor de vSphere Replication en el dispositivo de vSphere Replication	Host ESXi (entre sitios)	80	HTTP	Se utiliza para establecer la conexión antes de que comience la replicación inicial.
Dispositivo de vSphere Replication	vCenter Server local y remoto	443	TCP	Todo el tráfico de administración del dispositivo de vSphere Replication.
Servidor de vSphere Replication en el dispositivo de vSphere Replication	Host ESXi (solo entre sitios) en el sitio secundario	902	TCP y UDP	Los utilizan los servidores de vSphere Replication para enviar el tráfico de replicación a los hosts ESXi de destino.
Explorador	Dispositivo de vSphere Replication	5480	HTTPS	UI web de la interfaz de administración de dispositivos virtuales (VAMI) de vSphere Replication
Proxy de vCenter Server	Dispositivo de vSphere Replication	8043	SOAP	Comunicación entre sitios, desde el proxy de vCenter Server hasta el dispositivo de vSphere Replication.

**Tabla 2-2. Puertos utilizados por el dispositivo de vSphere Replication (Continúa)**

Origen	Destino	Puerto	Protocolo	Descripción
Dispositivo de vSphere Replication	Servidor de vSphere Replication	8123	SOAP	Tráfico de administración entre sitios, desde el servidor de vSphere Replication Management a un servidor de vSphere Replication adicional en el entorno.
Host ESXi en el sitio de origen	Servidor de vSphere Replication en el sitio de destino	31031	TCP	Tráfico de replicaciones iniciales y salientes desde el host ESXi en el sitio de origen hasta el dispositivo de vSphere Replication o el servidor de vSphere Replication en el sitio de destino.

Si implementó servidores de vSphere Replication adicionales, debe abrir los puertos que requiere vSphere Replication en dichos servidores.

**Tabla 2-3. Puertos utilizados por el servidor de vSphere Replication**

Origen	Destino	Puerto	Protocolo	Descripción
Servidor de vSphere Replication en el dispositivo de vSphere Replication	Host ESXi (solo entre sitios) en el sitio secundario	902	TCP y UDP	Tráfico entre el servidor de vSphere Replication y los hosts ESXi en el mismo sitio. Específicamente, el tráfico del servicio NFC a los servidores ESXi de destino.
Explorador	Servidor de vSphere Replication	5480	HTTPS	Explorador web del administrador.
Servidor de vSphere Replication Management	Servidor de vSphere Replication	8123	SOAP	Tráfico de administración entre sitios, desde el dispositivo de vSphere Replication o el servidor de vSphere Replication Management hasta los servidores de vSphere Replication.
Host ESXi en el sitio de origen	Servidor de vSphere Replication	31031	TCP	Tráfico de replicación inicial y hacia adelante desde el host ESXi en el sitio de origen hasta el dispositivo de vSphere Replication o el servidor de vSphere Replication en el sitio de destino.

Cuando crea una conexión a la nube, el vCloud Tunneling Agent en el dispositivo de vSphere Replication crea un túnel para garantizar la transferencia de datos de replicación a su organización de nube.

**Tabla 2-4. Puertos requeridos por las replicaciones en nube**

Origen	Destino	Puerto	Protocolo	Descripción
El host ESXi en el sitio de origen	El servidor de vCenter Server en el sitio de origen	80	TCP	El proxy inverso de vCenter Server envía el pedido de descarga del VIB (regla del firewall de vCloud Availability) al dispositivo de vSphere Replication.
El dispositivo de vSphere Replication en el sitio de origen	vCloud API	443	REST over HTTPS	El dispositivo de vSphere Replication se conecta al puerto para enviar los datos de replicación a una organización de nube.
El host ESXi en el sitio de origen	El dispositivo de vSphere Replication en el sitio de origen	10000–10010	TCP	vCloud Tunneling Agent abre uno de esos puertos en el dispositivo de vSphere Replication. Los hosts ESXi se conectan al puerto para enviar datos de replicación a la organización de nube.

## Componentes de terceros y de código abierto

Para obtener el texto completo de las licencias de código abierto, una lista de todos los componentes de terceros y de código abierto, y el código abierto que se usa en vSphere Replication, visite [http://www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html) y consulte la sección *Licencias y código abierto de VMware vSphere Replication*, en el vínculo *Código abierto de VMware vSphere*. Si alguna licencia de código abierto lo requiere, el paquete de divulgación de código abierto (Open Source Disclosure Package, ODP) de vSphere Replication contiene archivos de texto con instrucciones sobre cómo compilar y reemplazar las bibliotecas de software.

## Archivos de configuración de vSphere Replication

Los parámetros de algunos archivos de configuración afectan la seguridad de vSphere Replication

**NOTA:** Todos los recursos relacionados con la seguridad están protegidos con la propiedad y los permisos adecuados. No cambie la propiedad o los permisos de estos archivos.

Ubicación del archivo	Descripción
/opt/vmware/hms/conf/hms-configuration.xml	La configuración predeterminada del sistema para el servidor de vSphere Replication Management.
/opt/vmware/hms/conf/embedded_db.cfg	El archivo de configuración para la base de datos integrada.



## Clave privada, certificado y almacén de claves de vSphere Replication

La clave privada, el certificado y el almacén de claves de vSphere Replication se encuentran en el dispositivo virtual de vSphere Replication.

**NOTA:** Todos los recursos relacionados con la seguridad están protegidos con la propiedad y los permisos adecuados. No cambie la propiedad o los permisos de estos archivos.

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

## Archivos de CLUF y licencia de vSphere Replication

El contrato de licencia para el usuario final (CLUF) y los archivos de licencia de código abierto se encuentran en el dispositivo virtual de vSphere Replication.

Archivo	Ubicación
Licencia de código abierto	/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE
Licencia de Postgres de VMware	/usr/share/doc/vmware-vspherereplication/VMware-Postgres_9.5.4.0_open_source_licenses.txt
Contrato de licencia para el usuario final	/opt/vmware/etc/iso/EULA/language_code/0

## Archivos de registro de vSphere Replication

Los archivos que contienen mensajes de sistema están ubicados en el dispositivo virtual de vSphere Replication.

Ubicación del archivo	Descripción
/opt/vmware/hms/logs/hms-configtool.log	Se utiliza para registrar los errores que se produjeron durante la configuración de la interfaz de administración de dispositivos virtuales (VAMI).
/opt/vmware/hms/logs/hms.n.log	Se usa para realizar un seguimiento de la información de tiempo de ejecución del servidor de vSphere Replication Management. El archivo de registro más reciente recibe las etiquetas hms.log y hms.n.log contienen mensajes de registros más antiguos. El archivo con el valor <i>n</i> más alto contiene los mensajes más antiguos.
/opt/vmware/var/log/lighttpd/error.log	El archivo de registro de errores de la VAMI. Se utiliza para realizar un seguimiento de los errores en las operaciones de la VAMI.

Ubicación del archivo	Descripción
/var/log/vmware/	La carpeta contiene los archivos de registro del servidor de vSphere Replication. Se utiliza para realizar un seguimiento de los problemas de replicación.
/var/opt/apache-tomcat/logs/dr.log	Registros de la interfaz de usuario de Site Recovery.

## Mensajes de registro relacionados con la seguridad

El archivo /opt/vmware/hms/logs/hms.log contiene mensajes de eventos de inicio y cierre de sesión, mensajes de error de autorización y mensajes de error de comprobación de certificado con el siguiente formato.

### ■ Mensaje de inicio de sesión

```
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 | Adding new session to the 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
]
```

### ■ Mensaje de cierre de sesión

```
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
```

### ■ Mensaje de autorización

```
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-fa9dd99f4e47,

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

}
```

- Mensaje de error de comprobación de certificado

```
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
```

## Cuentas de usuario de vSphere Replication

Debe configurar una cuenta raíz para vSphere Replication. La cuenta raíz se utiliza para acceder a la consola del dispositivo virtual y a la interfaz de administración de dispositivos virtuales (VAMI).

Actualmente, vSphere Replication utiliza la cuenta raíz como el administrador de la VAMI. No se crea otro usuario.

Cuando implementa el dispositivo virtual de vSphere Replication, usted configura la contraseña para la cuenta raíz en el asistente de implementación de OVF.

La contraseña raíz debe contener al menos 8 caracteres.

## Privilegios asignados a los roles de usuario predeterminados

vSphere Replication incluye un conjunto de roles. Cada rol incluye un conjunto de privilegios que le permiten a los usuarios con dichos roles completar distintas acciones.

Consulte el tema Permisos y roles de vSphere Replication en la guía de *Instalación y configuración de VMware vSphere Replication*.

## Actualizaciones y revisiones de seguridad para vSphere Replication

El dispositivo virtual de vSphere Replication usa VMware Photon OS 2.0 como sistema operativo invitado.

Se puede aplicar la última actualización de seguridad o revisión mediante el correspondiente archivo ISO.

Antes de aplicar una actualización o revisión para el sistema operativo invitado, tenga en cuenta las dependencias. Consulte [Servicios, puertos e interfaces externas que usa el dispositivo virtual de vSphere Replication](#).

Para recibir los últimos avisos de seguridad, puede suscribirse a la lista de correo VMware Security Announcements en <http://lists.vmware.com/>.