VMware vSphere Replication Security Guide

vSphere Replication 6.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002115-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

About VMware vSphere Replication Security Guide

1

The *VMware vSphere Replication Security Guide* provides a concise reference to the security features of vSphere Replication.

To help you protect your vSphere Replication installation, this guide describes security features built into vSphere Replication and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of vSphere Replication
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information about obtaining the latest security patches

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of vSphere Replication.

vSphere Replication Security Reference

2

You can use the Security Reference to learn about the security features of vSphere Replication and the measures that you can take to safeguard your environment from attack.

This chapter includes the following topics:

Services, Ports, and External Interfaces that the vSphere Replication Virtual Appliance Uses

The operation of vSphere Replication depends on certain services, ports, and external interfaces.

vSphere Replication Services

The operation of vSphere Replication depends on several services that run on the vSphere Replication virtual appliance.

Table 2-1. vSphere Replication Services

Service Name	Startup Type	Description
hms	Automatic for the vSphere Replication appliance. Disabled for the vSphere Replication add-on appliance.	vSphere Replication Management Service
hbrsrv	Automatic	vSphere Replication Service
sshd	Automatic	Disabled by default.

Table 2-1. vSphere Replication Services (Continued)

Service Name	Startup Type	Description
ntp	Automatic	Time service for syncing-up with Internet Time Server through Network Time Protocol. **Note** After you install or upgrade a vSphere Replication virtual appliance, you must synchronize the appliance with a time server.
vaos	Automatic	Guest OS initialization that drives network settings, host name settings, ssh keys creation, EULA acceptance, boot scripts execution, and VAMI initialization.

Communication Ports

vSphere Replication uses several communication ports and protocols.

The vSphere Replication appliance requires certain ports to be open.

Note vSphere Replication servers must have NFC traffic access to target ESXi hosts.

Table 2-2. Ports Used by the vSphere Replication Appliance

Source	Target	Port	Protocol	Description
vSphere Replication appliance	Local and remote vCenter Server	80	TCP	All management traffic to the vSphere Replication appliance goes to port 80 on the vCenter Server proxy system.
vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site)	80	HTTP	Used to establish the connection before initial replication starts.
vSphere Replication appliance	Local and remote vCenter Server	443	TCP	All management traffic to the vSphere Replication appliance.
vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site only) on secondary site	902	TCP and UDP	Used by vSphere Replication servers to send replication traffic to the destination ESXi hosts.
Browser	vSphere Replication appliance	5480	HTTPS	vSphere Replication virtual appliance management interface (VAMI) Web UI.
vSphere Replication appliance	vCenter Server (intra-site only)	7444	TCP	

Table 2-2. Ports Used by the vSphere Replication Appliance (Continued)

Source	Target	Port	Protocol	Description
vCenter Server proxy	vSphere Replication appliance	8043	SOAP	Intra-site communication from the vCenter Server proxy to the vSphere Replication appliance .
vSphere Replication appliance	vSphere Replication server	8123	SOAP	Intra-site management traffic from the vSphere Replication Management server to additional vSphere Replication server in the environment.
vSphere Web Client on the source site	vCenter Server Inventory Service on the target site	10443	HTTPS	ThevSphere Replication UI uses the Inventory Service of the remote vCenter Server to list target datastores.
ESXi host on source site	vSphere Replication server at the target site	31031		Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site.

If you deploy additional vSphere ReplicationvSphere Replication servers, you must open the ports that vSphere Replication requires on those servers.

Table 2-3. Ports Used by the vSphere Replication Server

Source	Target	Port	Protocol	Description
vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site only) on secondary site	902	TCP and UDP	Traffic between the vSphere Replication server and the ESXi hosts on the same site. Specifically the traffic of the NFC service to the destination ESXi servers.
Browser	vSphere Replication server	5480	HTTPS	Administrator's Web browser.

Table 2-3. Ports Used by the vSphere Replication Server (Continued)

Source	Target	Port	Protocol	Description
vSphere Replication Management server	vSphere Replication server	8123	SOAP	Intra-site management traffic from the vSphere Replication appliance or vSphere Replication Management server to the vSphere Replication servers.
ESXi host at the source site	vSphere Replication server	31031		Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site.

When you create a connection to the cloud, the vCloud Tunneling Agent in the vSphere Replication appliance creates a tunnel to secure the transfer of replication data to your cloud organization.

Table 2-4. Ports Required for Cloud Replications

Source	Destination	Port	Protocol	Description
The ESXi host at the source site	The vCenter Server at the source site	80	TCP	The vCenter Server reverse proxy forwards VIB (vCloud Air Disaster Recovery firewall rules) download request to the vSphere Replication appliance.
The vSphere Replication appliance at the source site	vCloud API	443	REST over HTTPS	vSphere Replication appliance connects to this port to send replication data to a cloud organization.
The ESXi host at the source site	The vSphere Replication appliance at the source site	10000-10010	TCP	The vCloud Tunneling Agent opens one of these ports on the vSphere Replication appliance. ESXi hosts connect to that port to send replication data to a cloud organization.

Open Source and Third-Party Components

For the complete text of the open source licenses, a list of all open source and third-party components, and the open source code used in vSphere Replication, you can go to http://www.vmware.com/download/open_source.html and see the *VMware vSphere Replication Open Source and Licenses* section under the *VMware vSphere Open Source* link. If certain open source license requires it, the vSphere Replication Open Source Disclosure Package (ODP) contains text files with instructions how to build and replace the software libraries.

vSphere Replication Configuration Files

Some configuration files contain settings that affect the security of vSphere Replication.

Note All security-related resources are protected with the correct permissions and ownership. Do not change the ownership or permissions of these files.

File Location	Description
`/opt/vmware/hms/conf/hms-configuration.xml`	The default system configuration of the vSphere Replication Management server.
`/opt/vmware/hms/conf/embedded_db.cfg`	The configuration file for the embedded database .

vSphere Replication Private Key, Certificate, and Keystore

The private key, the certificate, and the keystore of vSphere Replication are located on the vSphere Replication virtual appliance.

Note All security-related resources are protected with the correct permissions and ownership. Do not change the ownership or permissions of these files.

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

vSphere Replication License and EULA File

The end-user license agreement (EULA) and open source license files are located in the vSphere Replication virtual appliance.

File	Location
Open Source License	`/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE`
VMware Postgres License	`/usr/share/doc/vmware-vspherereplication/VMware_Postgres_9.5.4.0_open_source_licenses.txt`
End-user license agreement	`/opt/vmware/etc/isv/EULA/`*`language_code`*`/0`

vSphere Replication Log Files

The files that contain system messages are located in the vSphere Replication virtual appliance.

File Location	Description
`/opt/vmware/hms/logs/hms-configtool.log`	Used to log errors that occurred during the Virtual Appliance Management Interface (VAMI) configuration.
`/opt/vmware/hms/logs/hms.`*`n`*`.log`	Used to track the runtime information of vSphere Replication Management server. The most recent log file is labeled `hms.log`, and `hms.`*`n`*`.log` files contain older log messages. The file with the highest *n* value contains the oldest messages.
`/opt/vmware/var/log/lighttpd/error.log`	The VAMI error log file. Used to track errors in the VAMI operations.

File Location	Description
/var/log/vmware/	The folder contains the vSphere Replication server log files. Used to track replication problems.
/var/log/boot.msg	Used to track the startup process of the vSphere Replication appliance.

Log Messages Related to Security

The /opt/vmware/hms/logs/hms.log file contains login and logout event messages, authorization error messages, and certificate verification error messages in the following format.

- Login message

```
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

]
```

- Logout message

```
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
```

- Authorization message

```
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

}
```

- Certificate verification error message

```
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
```

vSphere Replication User Accounts

You must set up a root account for vSphere Replication. The root account is used to access both the virtual appliance console and the Virtual Appliance Management Interface (VAMI).

vSphere Replication currently uses the root account as the administrator of the VAMI. No other user is created.

When you deploy the vSphere Replication virtual appliance, you set the password for the root account in the OVF Deployment wizard.

The root password must be at least 8 characters long.

Privileges Assigned to Default User Roles

vSphere Replication includes a set of roles. Each role includes a set of privileges, which allow users with those roles to complete different actions.

See the topic vSphere Replication Roles and Permissions in the *VMware vSphere Replication Installation and Configuration* Guide.

Security Updates and Patches for vSphere Replication

The vSphere Replication virtual appliance uses SUSE Linux Enterprise Server 12 (x86_64), Service Pack 1 as the guest operating system.

You can apply the latest security update or patch by using the corresponding ISO file.

Before you apply an update or patch to the guest operating system, take into account the dependencies. See "Services, Ports, and External Interfaces that the vSphere Replication Virtual Appliance Uses," on page 7.

To receive the latest security announcements, you can subscribe to the VMware Security Announcements mailing list at http://lists.vmware.com/.

Index