

Sicherheitshandbuch zu VMware vSphere Replication

vSphere Replication 8.2

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2012–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise.](#)

Inhalt

- 1** Informationen zum VMware vSphere Replication-Sicherheitshandbuch 4
- 2** vSphere Replication-Sicherheitsreferenz 5
 - Dienste, Ports und externe Schnittstellen, die von der virtuellen vSphere Replication-Appliance verwendet werden 5
 - vSphere Replication-Konfigurationsdateien 9
 - Privater Schlüssel, Zertifikat und Keystore von vSphere Replication 9
 - vSphere Replication-Lizenz- und EULA-Datei 9
 - vSphere Replication-Protokolldateien 10
 - vSphere Replication-Benutzerkonten 11
 - Sicherheits-Updates und -Patches für vSphere Replication 12

Informationen zum VMware vSphere Replication- Sicherheitshandbuch

1

Das *Sicherheitshandbuch zu VMware vSphere Replication* stellt eine kurz gefasste Referenz zu den Sicherheitsfunktionen von vSphere Replication bereit.

Zum Schutz Ihrer vSphere Replication-Installation beschreibt dieses Handbuch die in vSphere Replication integrierten Sicherheitsfunktionen sowie die Maßnahmen, die Sie ergreifen können, um die Installation vor Angriffen zu schützen.

- Externe Schnittstellen, Ports und Dienste, die für den ordnungsgemäßen Betrieb von vSphere Replication erforderlich sind
- Sicherheitsrelevante Konfigurationsoptionen und Einstellungen
- Speicherort und Zweck von Protokolldateien
- Erforderliche Systemkonten
- Informationen zum Bezug der neuesten Sicherheits-Patches

Zielgruppe

Diese Informationen sind für IT-Entscheidungsträger, -Architekten, -Administratoren und andere Personen bestimmt, die sich mit den Sicherheitskomponenten von vSphere Replication vertraut machen müssen.

vSphere Replication-Sicherheitsreferenz

2

Sie können die Sicherheitsreferenz verwenden, um sich mit den Sicherheitsfunktionen von vSphere Replication und den Maßnahmen zum Schutz Ihrer Umgebung vor Angriffen vertraut zu machen.

Dieses Kapitel enthält die folgenden Themen:

- [Dienste, Ports und externe Schnittstellen, die von der virtuellen vSphere Replication-Appliance verwendet werden](#)
- [vSphere Replication-Konfigurationsdateien](#)
- [Privater Schlüssel, Zertifikat und Keystore von vSphere Replication](#)
- [vSphere Replication-Lizenz- und EULA-Datei](#)
- [vSphere Replication-Protokolldateien](#)
- [vSphere Replication-Benutzerkonten](#)
- [Sicherheits-Updates und -Patches für vSphere Replication](#)

Dienste, Ports und externe Schnittstellen, die von der virtuellen vSphere Replication-Appliance verwendet werden

Der Betrieb von vSphere Replication ist von bestimmten Diensten, Ports und externen Schnittstellen abhängig.

vSphere Replication-Dienste

Der Betrieb von vSphere Replication ist von verschiedenen Diensten abhängig, die auf der virtuellen vSphere Replication-Appliance ausgeführt werden.

Tabelle 2-1. vSphere Replication-Dienste

Dienstname	Starttyp	Beschreibung
HMS	"Automatisch" für die vSphere Replication-Appliance. "Deaktiviert" für die vSphere Replication-Add-On-Appliance.	vSphere Replication-Verwaltungsdienst
hbrsrv	Automatisch	vSphere Replication-Dienst
sshd	Standardmäßig deaktiviert.	SSH-Dienst
NTP	Automatisch	<p>Zeitdienst für die Synchronisierung mit dem Internet-Zeitserver über das Netzwerkzeitprotokoll (NTP).</p> <p>Hinweis Nach der Installation oder dem Upgrade einer virtuellen vSphere Replication-Appliance müssen Sie die Appliance mit einem Zeitserver synchronisieren.</p>
vaos	Automatisch	Gastbetriebssysteminitialisierung, die die Festlegung von Netzwerk- und Hostnameneinstellungen, die Erstellung von SSH-Schlüsseln, die EULA-Annahme, die Ausführung der Startskripte und die VAMI-Initialisierung auslöst.

Kommunikationsports

vSphere Replication verwendet verschiedene Kommunikationsports und -protokolle.

Für die vSphere Replication-Appliance müssen bestimmte Ports geöffnet sein.

Hinweis vSphere Replication-Server müssen über Zugriff auf NFC-Datenverkehr verfügen, um ESXi-Hosts ansprechen zu können.

Tabelle 2-2. Von der vSphere Replication-Appliance verwendete Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
vSphere Replication-Appliance	Lokaler vCenter Server	80	TCP	Der gesamte Verwaltungsdatenverkehr zum lokalen vCenter Server-Proxy-System. vSphere Replication öffnet einen SSL-Tunnel für die Verbindung zu den vCenter Server-Diensten.
vSphere Replication-Appliance	Remote-Lookup-Service	443	TCP	Alle Aufrufe für den Remote-Lookup-Service.
vSphere Replication-Server in der vSphere Replication-Appliance	ESXi-Host (innerhalb der Site)	80	HTTP	Wird verwendet, um die Verbindung herzustellen, bevor die erste Replizierung beginnt.
vSphere Replication-Appliance	Lokaler und Remote-vCenter Server	443	TCP	Der gesamte Verwaltungsdatenverkehr zur vSphere Replication-Appliance.

Tabelle 2-2. Von der vSphere Replication-Appliance verwendete Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
vSphere Replication-Server in der vSphere Replication-Appliance	ESXi-Host (nur innerhalb der Site) auf der sekundären Site	902	TCP und UDP	Dient den vSphere Replication-Servern zur Übertragung des Replizierungsdatenverkehrs an die ESXi-Zielhosts.
Browser	vSphere Replication-Appliance	5480	HTTPS	Web-Benutzeroberfläche der Virtual Appliance Management Interface (VAMI) von vSphere Replication.
vCenter Server-Proxy	vSphere Replication-Appliance	8043	SOAP	Site-interne Kommunikation zwischen den vSphere Replication-Verwaltungsservern der Quelle und der Ziel-Site.
vSphere Replication-Appliance	vSphere Replication-Server	8123	SOAP	Site-interner Verwaltungsdatenverkehr zwischen dem vSphere Replication-Verwaltungsserver und einem weiteren vSphere Replication-Server in der Umgebung.
ESXi-Host auf der Quell-Site	vSphere Replication-Server auf der Ziel-Site	31031	TCP	Erstmaliger und ausgehender Replizierungsdatenverkehr vom ESXi-Host auf der Quell-Site zur vSphere Replication-Appliance oder zum vSphere Replication-Server auf der Ziel-Site für Replizierungsdatenverkehr ohne Netzwerkverschlüsselung.
ESXi-Host auf der Quell-Site	vSphere Replication-Server auf der Ziel-Site	32032	TCP	Erstmaliger und ausgehender Replizierungsdatenverkehr vom ESXi-Host auf der Quell-Site zur vSphere Replication-Appliance oder zum vSphere Replication-Server auf der Ziel-Site für Replizierungsdatenverkehr mit Netzwerkverschlüsselung.

Wenn Sie weitere vSphere Replication-Server bereitstellen, müssen Sie die Ports öffnen, die von vSphere Replication auf diesen Servern benötigt werden.

Tabelle 2-3. Vom vSphere Replication-Server verwendete Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
vSphere Replication-Server in der vSphere Replication-Appliance	ESXi-Host (nur innerhalb der Site) auf der sekundären Site	902	TCP und UDP	Datenverkehr zwischen dem vSphere Replication-Server und den ESXi-Hosts auf derselben Site. Insbesondere der Datenverkehr des NFC-Diensts an die ESXi-Zielserver.
Browser	vSphere Replication-Server	5480	HTTPS	Webbrowser des Administrators.
vSphere Replication-Verwaltungsserver	vSphere Replication-Server	8123	SOAP	Site-interner Verwaltungsdatenverkehr zwischen der vSphere Replication-Appliance oder dem vSphere Replication-Verwaltungsserver und den vSphere Replication-Servern.

Tabelle 2-3. Vom vSphere Replication-Server verwendete Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
ESXi-Host auf der Quell-Site	vSphere Replication-Server	31031	TCP	Erstmaliger und vorwärts gerichteter Replizierungsdatenverkehr vom ESXi-Host auf der Quell-Site an die vSphere Replication-Appliance oder den vSphere Replication-Server auf der Ziel-Site.
ESXi-Host auf der Quell-Site	vSphere Replication-Server auf der Ziel-Site	32032	TCP	Erstmaliger und vorwärts gerichteter Replizierungsdatenverkehr mit Netzwerkverschlüsselung vom ESXi-Host auf der Quell-Site zur vSphere Replication-Appliance oder zum vSphere Replication-Server auf der Ziel-Site.

Wenn Sie eine Verbindung zur Cloud herstellen, erstellt der vCloud Tunneling Agent in der vSphere Replication-Appliance einen Tunnel zum Absichern der Übertragung der Replizierungsdaten an die Cloud-Organisation.

Tabelle 2-4. Für Cloud-Replizierungen erforderliche Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
Der ESXi-Host auf der Quell-Site	Die vCenter Server-Instanz auf der Quell-Site	80	TCP	Der vCenter Server-Reverse-Proxy leitet VIB-Downloadanforderungen (vCloud Availability-Firewallregeln) an die vSphere Replication-Appliance weiter.
Die vSphere Replication-Appliance auf der Quell-Site	vCloud-API	443	REST über HTTPS	Die vSphere Replication-Appliance stellt für den Versand der Replizierungsdaten an eine Cloud-Organisation eine Verbindung mit diesem Port her.
Der ESXi-Host auf der Quell-Site	Die vSphere Replication-Appliance auf der Quell-Site	10000–10010	TCP	Der vCloud Tunneling Agent öffnet einen dieser Ports in der vSphere Replication-Appliance. ESXi-Hosts stellen für den Versand der Replizierungsdaten an eine Cloud-Organisation eine Verbindung mit diesem Port her.

Open Source- und Drittanbieterkomponenten

Ausführliche Informationen zu den Open Source-Lizenzen, eine Aufstellung aller Open Source- und Drittanbieterkomponenten sowie den in vSphere Replication verwendeten Open Source-Code finden Sie unter http://www.vmware.com/download/open_source.html und im Abschnitt *VMware vSphere Replication Open Source und Lizenzen* über den Link *VMware vSphere Open Source*. Falls bestimmte Open Source-Lizenzen dies erfordern, enthält das vSphere Replication Open Source Disclosure Package (ODP) Textdateien mit Anweisungen zum Erstellen und Ersetzen der Softwarebibliotheken.

vSphere Replication-Konfigurationsdateien

Einige Konfigurationsdateien enthalten Einstellungen, die Einfluss auf die Sicherheit von vSphere Replication haben.

Hinweis Alle sicherheitsrelevanten Ressourcen sind durch entsprechende Berechtigungen und Besitzerrechte geschützt. Ändern Sie die Besitzerrechte oder Berechtigungen dieser Dateien nicht.

Dateispeicherort	Beschreibung
/opt/vmware/hms/conf/hms-configuration.xml	Die Standardsystemkonfiguration des vSphere Replication-Verwaltungsservers.
/opt/vmware/hms/conf/embedded_db.cfg	Die Konfigurationsdatei für die eingebettete Datenbank.

Privater Schlüssel, Zertifikat und Keystore von vSphere Replication

Der private Schlüssel, das Zertifikat und der Keystore von vSphere Replication befinden sich in der virtuellen vSphere Replication-Appliance.

Hinweis Alle sicherheitsrelevanten Ressourcen sind durch entsprechende Berechtigungen und Besitzerrechte geschützt. Ändern Sie die Besitzerrechte oder Berechtigungen dieser Dateien nicht.

- /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-Lizenz- und EULA-Datei

Die Endbenutzer-Lizenzvereinbarung (EULA) und die Open Source-Lizenzdateien befinden sich in der virtuellen vSphere Replication-Appliance.

Datei	Speicherort
Open Source-Lizenz	/usr/share/doc/vmware-vsphere-replication/OPEN_SOURCE_LICENSE
VMware Postgres-Lizenz	/usr/share/doc/vmware-vsphere-replication/ VMware_Postgres_9.5.16.0_open_source_licenses.txt
Endbenutzer-Lizenzvereinbarung	/opt/vmware/etc/iso/EULA/ <i>Sprachcode</i> /0

vSphere Replication-Protokolldateien

Die Dateien mit den Systemmeldungen befinden sich in der virtuellen vSphere Replication-Appliance.

Dateispeicherort	Beschreibung
/opt/vmware/hms/logs/hms-configtool.log	Wird zum Protokollieren von Fehlern verwendet, die während der VAMI-Konfiguration (Virtual Appliance Management Interface) auftreten.
/opt/vmware/hms/logs/hms.n.log	Dient zur Verfolgung der Laufzeitinformationen des vSphere Replication Management-Servers. Die neueste Protokolldatei heißt hms.log und hms.n.log-Dateien enthalten ältere Protokolldateien. Die Datei mit dem höchsten n-Wert enthält die ältesten Meldungen.
/opt/vmware/var/log/lighttpd/error.log	Die VAMI-Fehlerprotokolldatei. Dient zum Verfolgen von Fehlern im VAMI-Betrieb.
/var/log/vmware/	Der Ordner enthält die vSphere Replication-Serverprotokolldateien. Dient zum Verfolgen von Replizierungsproblemen.
/var/opt/apache-tomcat/logs/dr.log	Site Recovery-Benutzer-Schnittstelleprotokolle.
/opt/vmware/hms/logs/hms-audit.log	vSphere Replication-Überwachungsprotokolle

Protokollmeldungen im Zusammenhang mit Sicherheit

Die Datei /opt/vmware/hms/logs/hms.log enthält Meldungen zu Anmelde- und Abmeldeereignissen, Autorisierungsfehlern und Zertifikatüberprüfungsfehlern im folgenden Format.

■ Anmeldenachricht

```
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
]
```

- Meldung zur Abmeldung

```
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
```

- Meldung zur Autorisierung

```
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
}
```

- Meldung zu Zertifikatüberprüfungsfehlern

```
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-Benutzerkonten

Sie müssen ein Root-Konto für vSphere Replication einrichten. Das Root-Konto wird für den Zugriff auf die Konsole der virtuellen Appliance und für die VAMI (Virtual Appliance Management Interface) verwendet.

vSphere Replication verwendet das Root-Konto zurzeit als Administrator der VAMI. Es wird kein anderer Benutzer erstellt.

Wenn Sie die virtuelle vSphere Replication-Appliance bereitstellen, legen Sie das Kennwort für das Root-Konto im OVF-Bereitstellungsassistenten fest.

Das Kennwort muss mindestens 8 Zeichen umfassen.

Standardbenutzerrollen zugewiesene Rechte

vSphere Replication enthält mehrere Rollen. Jede Rolle enthält mehrere Rechte, sodass Benutzer mit diesen Rollen verschiedene Aktionen ausführen können.

Weitere Informationen finden Sie unter dem Thema „vSphere Replication-Rollen und -Berechtigungen“ im Handbuch *VMware vSphere Replication – Installation und Konfiguration*.

Sicherheits-Updates und -Patches für vSphere Replication

Die virtuelle Appliance für vSphere Replication verwendet Photon OS 2.0 als Gastbetriebssystem.

Sie können das neueste Sicherheits-Update oder -Patch unter Verwendung der entsprechenden ISO-Datei installieren.

Berücksichtigen Sie die Abhängigkeiten, bevor Sie ein Update oder Patch auf dem Gastbetriebssystem installieren. Weitere Informationen hierzu finden Sie unter [Dienste, Ports und externe Schnittstellen, die von der virtuellen vSphere Replication-Appliance verwendet werden](#).

Um die neuesten Sicherheitsankündigungen zu erhalten, können Sie die VMware Security Announcements-Mailing-Liste unter <http://lists.vmware.com/> abonnieren.