VMware vSphere Replication セキュリティ ガイド

vSphere Replication 8.1

vmware®

最新の技術ドキュメントは VMware の Web サイト（https://docs.vmware.com/jp/）にあります
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware vSphere Replication セキュリティについて 1

『VMware vSphere Replication セキュリティ ガイド』は、vSphere Replication のセキュリティ機能に関して簡潔にまとめられた参照資料です。

vSphere Replication インストール環境の保護に役立てるため、このドキュメントでは vSphere Replication に組み込みのセキュリティ機能と、攻撃から環境を守るためにとれる手段を説明します。

- vSphere Replication の適切な操作に必要な外部インターフェイス、ポート、およびサービス
- セキュリティに影響する構成のオプションと設定
- ログ ファイルの場所とその目的
- システム アカウントの要件
- 最新のセキュリティ パッチを取得するための情報

対象読者

この情報は、vSphere Replication のセキュリティ コンポーネントに習熟する必要のある IT の意思決定者、設計担当者、管理者などを対象にしています。

vSphere Replication セキュリティ リファレンス

2

セキュリティ リファレンスを使用すると、vSphere Replication のセキュリティ機能および環境を攻撃から守るための手段について学習することができます。

この章では次のトピックについて説明します。

- vSphere Replication 仮想アプライアンスが使用するサービス、ポート、外部インターフェイス
- vSphere Replication 構成ファイル
- vSphere Replication プライベート キー、証明書、キーストア
- vSphere Replication ライセンスおよび EULA ファイル
- vSphere Replication ログ ファイル
- vSphere Replication ユーザー アカウント
- vSphere Replication のセキュリティ アップデートおよびパッチ

vSphere Replication 仮想アプライアンスが使用するサービス、ポート、外部インターフェイス

vSphere Replication の操作は特定のサービス、ポート、外部インターフェイスに依存しています。

vSphere Replication サービス

vSphere Replication の操作は vSphere Replication 仮想アプライアンスで実行されているさまざまなサービスに依存しています。

表 2-1. vSphere Replication サービス

サービス名	起動タイプ	説明
HMS	vSphere Replication アプライアンスで自動。 vSphere Replication アドオン アプライアンスで無効。	vSphere Replication 管理サービス
hbrsrv	自動	vSphere Replication サービス
sshd	デフォルトで無効。	SSH サービス

表 2-1. vSphere Replication サービス (続き)

サービス名	起動タイプ	説明
ntp	自動	NTP (Network Time Protocol) によってインターネット タイム サーバと同期するタイム サービス。 注意 vSphere Replication 仮想アプライアンスをインストールまたはアップグレードした後、アプライアンスをタイム サーバと同期する必要があります。
vaos	自動	ネットワーク設定、ホスト名の設定、ssh キーの作成、EULA の同意、起動スクリプトの実行、VAMI の初期化を開始するゲスト OS の初期化。

通信ポート

vSphere Replication は、さまざまな通信ポートおよびプロトコルを使用します。

vSphere Replication アプライアンスでは、特定のポートが開いている必要があります。

注意 vSphere Replication サーバは、NFC トラフィックでターゲット ESXi ホストにアクセスする必要があります。

表 2-2. vSphere Replication アプライアンスが使用するポート

ソース	ターゲット	ポート	プロトコル	説明
vSphere Replication アプライアンス	ローカルおよびリモートの vCenter Server	80	TCP	vSphere Replication アプライアンスへのすべての管理トラフィックは、vCenter Server プロキシ システムのポート 80 を通過します。
vSphere Replication アプライアンスの vSphere Replication サーバ	ESXi ホスト（イントラサイト）	80	HTTP	最初のレプリケーションがスタートする前に接続を確立するために使用されます。
vSphere Replication アプライアンス	ローカルおよびリモートの vCenter Server	443	TCP	vSphere Replication アプライアンスへのすべての管理トラフィック。
vSphere Replication アプライアンスの vSphere Replication サーバ	セカンダリ サイトの ESXi ホスト（イントラ サイトのみ）	902	TCP と UDP	レプリケーション トラフィックをターゲット ESXi ホストに送信するために vSphere Replication サーバにより使用されます。
ブラウザ	vSphere Replication アプライアンス	5480	HTTPS	vSphere Replication 仮想アプライアンス管理インターフェイス （VAMI） の Web UI。
vCenter Server プロキシ	vSphere Replication アプライアンス	8043	SOAP	vCenter Server プロキシから vSphere Replication アプライアンスへのイントラサイト通信。
vSphere Replication アプライアンス	vSphere Replication サーバ	8123	SOAP	環境内の追加の vSphere Replication サーバに対する、vSphere Replication Management Server からのイントラサイト管理トラフィック。
ソース サイトの ESXi ホスト	ターゲット サイトの vSphere Replication サーバ	31031	TCP	ソース サイトの ESXi ホストから vSphere Replication アプライアンスまたはターゲット サイトの vSphere Replication サーバへの最初の発信レプリケーション トラフィック。

追加で vSphere Replication サーバをデプロイする場合、これらのサーバの vSphere Replication が必要とするポートを開く必要があります。

表 2-3. vSphere Replication サーバが使用するポート

ソース	ターゲット	ポート	プロトコル	説明
vSphere Replication アプライアンスの vSphere Replication サーバ	セカンダリ サイトの ESXi ホスト（イントラ サイトのみ）	902	TCP と UDP	同じサイトの vSphere Replication サーバと ESXi ホスト間のトラフィック。具体的には、ターゲット ESXi サーバへの NFC サービスのトラフィックです。
ブラウザ	vSphere Replication サーバ	5480	HTTPS	管理者の Web ブラウザ。
vSphere Replication Management Server	vSphere Replication サーバ	8123	SOAP	vSphere Replication アプライアンスまたは vSphere Replication Management Server から vSphere Replication サーバへのイントラサイト管理トラフィック。
ソース サイトの ESXi ホスト	vSphere Replication サーバ	31031	TCP	ソース サイトの ESXi ホストから vSphere Replication アプライアンスまたはターゲット サイトの vSphere Replication サーバへの最初の正方向レプリケーション トラフィック。

クラウドへの接続を作成する場合、vSphere Replication アプライアンスの vCloud Tunneling Agent がレプリケーション データをクラウド組織へセキュアに転送するトンネルを作成します。

表 2-4. クラウド レプリケーションに必要なポート

ソース	ターゲット	ポート	プロトコル	説明
ソース サイトの ESXi ホスト	ソース サイトの vCenter Server	80	TCP	vCenter Server リバース プロキシは、VIB（vCloud Availability ファイアウォール ルール）のダウンロード要求を vSphere Replication アプライアンスに転送します。
ソース サイトの vSphere Replication アプライアンス	vCloud API	443	REST over HTTPS	vSphere Replication アプライアンスはこのポートに接続してレプリケーション データをクラウド組織に送信します。
ソース サイトの ESXi ホスト	ソース サイトの vSphere Replication アプライアンス	10000–10010	TCP	vCloud Tunneling Agent は、vSphere Replication アプライアンスのこれらのポートのうち 1 つを開きます。ESXi ホストはこのポートに接続してレプリケーション データをクラウド組織に送信します。

オープン ソースとサードパーティ コンポーネント

オープン ソース ライセンスの全文、すべてのオープン ソースおよびサードパーティ コンポーネントのリスト、および vSphere Replication で使用されるオープン ソース コードについては、http://www.vmware.com/download/open_source.html に進み、「VMware vSphere オープン ソース」リンクにある「VMware vSphere Replication のオープン ソースとライセンス」セクションを参照してください。特定のオープン ソース ライセンスでソフトウェア ライブラリを構築および置き換える必要がある場合、vSphere Replication Open Source Disclosure Package (ODP) にはその手順を記載したテキスト ファイルが含まれています。

vSphere Replication 構成ファイル

構成ファイルによっては、vSphere Replication のセキュリティに影響を与える設定が含まれています。

注意　セキュリティに関するすべてのリソースは、正規の権限と所有権によって保護されています。これらのファイルの所有権または権限を変更しないでください。

ファイルの場所	説明
`/opt/vmware/hms/conf/hms-configuration.xml`	vSphere Replication Management Server のデフォルトのシステム構成。
`/opt/vmware/hms/conf/hms-configuration.xml`	組み込みデータベースの構成ファイル。

vSphere Replication プライベート キー、証明書、キーストア

vSphere Replication のプライベート キー、証明書、キーストアは、vSphere Replication Virtual Appliance にあります。

注意　セキュリティに関するすべてのリソースは、正規の権限と所有権によって保護されています。これらのファイルの所有権または権限を変更しないでください。

- `/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 ライセンスおよび EULA ファイル

エンド ユーザー使用許諾契約書 (EULA) およびオープン ソース ライセンス ファイルは、vSphere Replication Virtual Appliance にあります。

ファイル	場所
オープン ソースのライセンス	`/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE`
VMware Postgres ライセンス	`/usr/share/doc/vmware-vspherereplication/VMware_Postgres_9.5.4.0_open_source_licenses.txt`
エンド ユーザー使用許諾契約書	`/opt/vmware/etc/isv/EULA/<language_code>/0`

vSphere Replication ログ ファイル

システム メッセージを含むファイルは、vSphere Replication 仮想アプライアンスにあります。

ファイルの場所	説明
/opt/vmware/hms/logs/hms-configtool.log	仮想アプライアンス管理インターフェイス (VAMI) の構成中に発生するエラーのログを作成するために使用します。
/opt/vmware/hms/logs/hms.<n>.log	vSphere Replication 管理サーバのランタイム情報を追跡するために使用します。最新のログ ファイルは hms.log としてラベル付けされ、hms.<n>.log ファイルには、以前のログ メッセージが含まれています。<n> の値が最も大きいファイルには、最も古いメッセージが含まれています。
/opt/vmware/var/log/lighttpd/error.log	VAMI エラー ログ ファイル。VAMI 操作のエラーを追跡するために使用します。
/var/log/vmware/	このフォルダには、vSphere Replication サーバのログ ファイルが含まれています。レプリケーションの問題を追跡するために使用します。
/var/opt/apache-tomcat/logs/dr.log	Site Recovery ユーザー インターフェイスのログ。

セキュリティ関連のログ メッセージ

/opt/vmware/hms/logs/hms.log ファイルには、ログインおよびログアウト イベント メッセージ、認証エラー メッセージ、証明書の検証エラー メッセージが以下の形式で含まれています。

- ログイン メッセージ

  ```
  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

  ]
  ```

- ログアウト メッセージ

```
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
```

- 認証メッセージ

```
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

}
```

- 証明書の検証エラー メッセージ

```
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 ユーザー アカウント

vSphere Replication のルート アカウントを設定する必要があります。ルート アカウントは、Virtual Appliance コンソールおよび Virtual Appliance Management Interface (VAMI) にアクセスするために使用します。

vSphere Replication は、現在ルート アカウントを VAMI の管理者として使用しています。そのほかにユーザーを作成することはできません。

vSphere Replication Virtual Appliance をデプロイするときは、OVF Deployment ウィザードでルート アカウントのパスワードを設定します。

root パスワードの長さは 8 文字以上である必要があります。

デフォルトのユーザー ロールに割り当てられる権限

vSphere Replication は一連のロールを含んでいます。各ロールには、該当するロールのユーザーが各種アクションを完了するための権限セットが含まれています。

VMware vSphere Replication のインストールと構成ガイドで vSphere Replication のロールと権限に関するトピックを参照してください。

vSphere Replication のセキュリティ アップデートおよびパッチ

vSphere Replication 仮想アプライアンスはゲスト OS として VMware Photon OS 2.0 を使用します。

最新のセキュリティ アップデートやパッチを、関連する ISO ファイルを使用して適用できます。

ゲスト OS にアップデートやパッチを適用する前に、依存関係を考慮する必要があります。「vSphere Replication 仮想アプライアンスが使用するサービス、ポート、外部インターフェイス」 を参照してください。

最新のセキュリティ告知を受け取るために、http://lists.vmware.com/で VMware セキュリティ告知メーリング リストに加入することができます。