Seguridad de Site Recovery Manager

Site Recovery Manager 6.1

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/es/support/pubs.

ES-001875-01

vmware®

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

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

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

Contenido

Acerca de la seguridad de VMware Site Recovery Manager

Seguridad de Site Recovery Manager proporciona una referencia concisa sobre las características de seguridad de Site Recovery Manager.

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

- Interfaces externas, puertos y servicios necesarios para el funcionamiento correcto de Site Recovery Manager
- 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

Público objetivo

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 Site Recovery Manager.

Información actualizada

Seguridad de Site Recovery Manager se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se brinda el historial de actualizaciones de *Seguridad de Site Recovery Manager*.

Revisión	Descripción
EN-001875-01	Se reemplazó "federado" por "Enhanced Linked Mode" en “Cuentas de Site Recovery Manager,” página 14.
EN-001875-00	Versión inicial.

Referencia de seguridad de Site Recovery Manager 1

Utilice la Referencia de seguridad para obtener información sobre las características de seguridad de la instalación de Site Recovery Manager y de las medidas que puede tomar para proteger su entorno frente a ataques.

Servicios de Site Recovery Manager

La operación de Site Recovery Manager depende de varios servicios que se ejecutan en la máquina host de Site Recovery Manager Server.

Tabla 1-1. Servicios que Site Recovery Manager requiere

Nombre de servicio	Tiempo de inicio	Descripción
VMware vCenter Site Recovery Manager Server	Automático	Brinda las funciones clave de Site Recovery Manager.
Base de datos insertada de VMware vCenter Site Recovery Manager	Automático, si usa la base de datos insertada	El servidor vPostgres para la base de datos insertada Site Recovery Manager.
Servidor	Automático	Servicio de Windows que admite el uso compartido de archivos a través de la red.
Workstation	Automático	Servicio de Windows que crea y mantiene conexiones con servidores remotos.
Almacenamiento protegido	Automático	Servicio de Windows que almacena información confidencial.

Puertos de red de Site Recovery Manager

Site Recovery Manager usa puertos de red, que pueden configurarse para comunicarse con clientes y demás servidores. Debe asegurarse de que no existan firewalls que bloqueen los puertos que Site Recovery Manager usa.

Site Recovery Manager Server recibe todo el tráfico entrante en un puerto de red. El puerto predeterminado es 9086. Si configura Site Recovery Manager para que use una base de datos insertada, la base de datos insertada de Site Recovery Manager recibe el tráfico de red del host local en la interfaz de bucle invertido local. El puerto predeterminado es 5678.

Puede seleccionar otros puertos para el tráfico de la base de datos insertada y Site Recovery Manager durante el proceso de instalación si los puertos predeterminados se bloquean u otras aplicaciones los usan. Debe configurar las directivas de red para habilitar el tráfico en el puerto entrante. Para obtener información acerca de los puertos que puede cambiar después de la instalación, consulte el tema *Modificar una instalación de Site Recovery Manager Server* en la documentación de *Instalación y configuración de Site Recovery Manager*.

Site Recovery Manager Server se comunica con hosts de Platform Services Controller, vCenter Server, ESXi y matrices en el sitio local. Debe comprobar que las directivas de firewall de red permitan el tráfico a los puertos de red de todos los componentes en el sitio local. Para obtener la lista de puertos predeterminados que usan todos los productos VMware, consulte http://kb.vmware.com/kb/1012382.

La conexión entre el sitio local y el remoto de un par de Site Recovery Manager debe ser privada, como VPN. El servidor de Site Recovery Manager Server local se comunica con Site Recovery Manager Server, Platform Services Controller y vCenter Server en el sitio remoto, y el proveedor de red debe garantizar las directivas de red apropiadas para permitir el tráfico.

Para obtener una lista de todos los puertos que deben abrirse para Site Recovery Manager, consulte http://kb.vmware.com/kb/2119329.

Archivos de configuración de Site Recovery Manager

Algunos archivos de configuración de Site Recovery Manager contienen parámetros que pueden afectar la seguridad de su entorno. Los parámetros de configuración inapropiados también pueden tener un impacto en el funcionamiento correcto del entorno de Site Recovery Manager.

Tabla 1-2. Archivos de configuración de Site Recovery Manager

Ubicación de archivo o directorio	Descripción
carpeta_de_instalación\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml	Define la configuración del sistema de Site Recovery Manager Server. **NOTA:** No mueva ni elimine el archivo de configuración. Puede cambiar con tranquilidad los parámetros de configuración del sistema de una instancia de Site Recovery Manager mediante el uso de la pestaña **Advanced Settings** (Configuración avanzada) en la página **Manage** (Administrar) en la interfaz de usuario de vSphere Web Client.
carpeta_de_instalación\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\	Contiene archivos de configuración de la base de datos insertada. **NOTA:** No modifique, mueva ni elimine el archivo de configuración.
carpeta_de_instalación\VMware\VMware vCenter Site Recovery Manager\config\extension.xml	Define la configuración de la extensión de Site Recovery Manager Server. El archivo `extension.xml` contiene las definiciones de los roles de usuario predeterminados y sus privilegios. **NOTA:** No modifique, mueva ni elimine el archivo de configuración.

Certificados y claves de Site Recovery Manager

Site Recovery Manager usa claves privadas y certificados de TLS para proteger la comunicación de red y establecer de forma segura la autenticación con otros servidores.

Certificado CA o clave privada o ambos	Ubicación y descripción
Clave y certificado de TLS para endpoint de Site Recovery Manager Server	El almacén de certificados de Windows y en el archivo *carpeta_de_instalación*\VMware\VMware vCenter Site Recovery Manager\bin*SRM_Server_IP_addressca*.p12 Site Recovery Manager genera el certificado si no brinda un certificado personalizado durante la instalación.
El certificado y la clave de TLS para el usuario de `solution` creado durante la instalación de Site Recovery Manager	Archivo *carpeta_de_instalación*\VMware\VMware vCenter Site Recovery Manager\bin*SRM_Server_IP_addresssu*.p12.

Certificado CA o clave privada o ambos	Ubicación y descripción
El certificado y la clave de TLS para el usuario de `solution` en el sitio remoto	Archivo *`carpeta_de_instalación`*`\VMware\VMware vCenter Site Recovery Manager\bin\`*`extension-s`*`.p12` o archivo `\VMware\VMware vCenter Site Recovery Manager\bin\`*`extension-p`*`.p12`. Site Recovery Manager crea los archivos durante el proceso de emparejamiento.
Certificado CA para Site Recovery Manager Server y certificado de TLS	*`carpeta_de_instalación`*`\VMware\VMware vCenter Site Recovery Manager\bin\`*`SRM_Server_IP_addressca`*`.p7b`. Site Recovery Manager genera el certificado si no brinda un certificado personalizado durante la instalación. Puede importar el certificado en un almacén de claves de confianza de cliente para permitir a los usuarios que confíen implícitamente en el certificado de Site Recovery Manager Server.

IMPORTANTE: Configure las listas de control de acceso para restringir el acceso a los archivos `.p12` según sea apropiado para su entorno.

NOTA: No modifique, elimine ni mueva los archivos `.p12`.

NOTA: No extraiga ni comparta información de clave privada para proteger su instancia de Site Recovery Manager.

Para obtener más información sobre los mecanismos de autenticación de Site Recovery Manager, consulte el tema *Site Recovery Manager Authentication* (Autenticación de Site Recovery Manager) en la *Guía de configuración e instalación de Site Recovery Manager*.

Archivos de CLUF y licencia de Site Recovery Manager

Los archivos de CLUF y licencia de Site Recovery Manager se encuentran ubicados en la máquina host de Site Recovery Manager Server.

Tabla 1-3. Archivos de CLUF y licencia de Site Recovery Manager

Archivo o directorio	Descripción
`carpeta_de_instalación``\VMware\VMware vCenter Site Recovery Manager\en\`	Directorio que contiene los archivos del contrato de licencia del usuario final de Site Recovery Manager.
`carpeta_de_instalación``\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt`	Archivo de licencia de código abierto de Site Recovery Manager.
`carpeta_de_instalación` `\VMware\VMware vCenter Site Recovery Manager\en\ open_source_license_vix.txt`	Archivo de licencia de código abierto de API de Virtual Infrastructure Extension.
`carpeta_de_instalación``\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.doc`	Archivo del contrato de licencia del usuario final de la base de datos insertada de Site Recovery Manager.
`carpeta_de_instalación``\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt`	Archivo de licencia de código abierto de la base de datos insertada de Site Recovery Manager.

Archivos de registro de Site Recovery Manager

Site Recovery Manager registra información operativo en los archivos de registro. Dichos archivos no contienen información confidencial como contraseñas ni claves privadas.

Site Recovery Manager almacena los archivos de registro del sistema en el directorio `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`. Los últimos mensajes de Site Recovery Manager Server se colocan en el archivo `vmware-dr-`*`número`*`.log`.

Si reinicia Site Recovery Manager Server o el archivo actual debe superar el límite del tamaño de archivo establecido, Site Recovery Manager guarda el archivo de registro actual y crea un nuevo archivo de registro.

Para cambiar el directorio del archivo de registro, escriba un nombre de directorio personalizado en el elemento XML de directorio en el archivo de configuración *`directorio_instalación`*`\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml`. También puede cambiar el nivel de log de cada componente actualizando el elemento XML logLevel en el archivo `vmware-dr.xml`. El nivel predeterminado de todos los componentes es verbose (detallado).

IMPORTANTE: Configure las listas de control de acceso para restringir el acceso a los archivos de registro.

Tabla 1-4. Niveles de log

Nivel	Descripción
error (error)	Muestra solo entradas de log de error.
info (información)	Muestra entradas de log de advertencia, error e información.
trivia (variados)	Muestra entradas de log de asuntos varios, detallado, advertencia, error e información.
verbose (detallado)	Muestra entradas de log de detallado, advertencia, error e información.
warning (advertencia)	Muestra entradas de log de error y advertencia.

Site Recovery Manager admite los siguientes componentes.

- App
- Replication
- Recovery
- Storage
- StorageProvider
- Vdb
- Persistence
- SoapAdapter

El archivo `vmware-dr-`*`número`*`.log` contiene mensajes de seguridad respecto del proceso de autenticación y las conexiones con el lado remoto.

Cuentas de Site Recovery Manager

Site Recovery Manager usa certificados de Single Sign-On (SSO) para acceder a Site Recovery Manager Server.

Cuentas de usuario

Los privilegios de administrador de vCenter Server autorizan el acceso de administración a Site Recovery Manager en la configuración predeterminada. Debe usar las credenciales de administrador al intentar iniciar sesión en Site Recovery Manager por primera vez después de la instalación.

Si tiene credenciales de administrador, otorga acceso a Site Recovery Manager a otros usuarios mediante el uso de vSphere Web Client.

Para obtener más información sobre los permisos, privilegios y roles de Site Recovery Manager, consulte *Site Recovery Manager Privileges, Roles, and Permissions* (Permisos, roles y privilegios de Site Recovery Manager) en la documentación de la *administración de Site Recovery Manager* .

Cuenta de usuario de `Solution`

Site Recovery Manager crea un usuario de `solution` durante la instalación y la usa durante la autenticación con vCenter Server. El usuario de `solution` es exclusivo para cada instancia de Site Recovery Manager y está destinado al uso interno por parte de Site Recovery Manager, vCenter Server y Platform Services Controller.

Site Recovery Manager crea un usuario de `solution` adicional en cada sitio remoto durante el proceso de emparejamiento de sitios que no usan Enhanced Linked Mode. Site Recovery Manager usa el usuario de `solution` para realizar las operaciones necesarias en el sitio remoto.

NOTA: Debe eliminar y modificar los roles y privilegios asociados con las cuentas de usuario de `solution`.

Para obtener más información acerca de los usuarios de `solution` y la autenticación entre el sitio local y remoto, consulte el tema *Site Recovery Manager Authentication* (Autenticación de Site Recovery Manager) en la documentación de *Site Recovery Manager Installation and Configuration* (Instalación y configuración de Site Recovery Manager).

Actualizaciones de seguridad y revisiones de Site Recovery Manager

Puede aplicar actualizaciones de seguridad y revisiones de Site Recovery Manager a medida que VMware las ponga a disposición. Puede aplicar actualizaciones de seguridad y revisiones del sistema operativo host a medida que los proveedores de dicho sistema las pongan a disposición.

Versiones de los sistemas operativos host de Site Recovery Manager

Para obtener información acerca de los sistemas operativos host compatibles con Site Recovery Manager Server, consulte *Matrices de compatibilidad para Site Recovery Manager 6.1* en https://www.vmware.com/support/srm/srm-compat-matrix-6-1.html.

Aplicar revisiones y actualizaciones de seguridad de Site Recovery Manager

Las revisiones y las actualizaciones de seguridad de Site Recovery Manager se aplican mediante actualización local en la instalación de Site Recovery Manager existente. Para obtener información acerca de la actualización de Site Recovery Manager, consulte In-Place Upgrade of Site Recovery Manager Server (Actualización local de Site Recovery Manager Server) en *Instalación y configuración de Site Recovery Manager*.

Prácticas recomendadas para configurar Site Recovery Manager Server

Prácticas recomendadas para asegurar que Site Recovery Manager Server pueda proteger el entorno ante posibles problemas de seguridad.

La operación para asegurar Site Recovery Manager depende de una configuración y un mantenimiento adecuados del sistema operativo de Site Recovery Manager Server.

- Ejecute Site Recovery Manager solo en un sistema operativo host, una base de datos y hardware compatibles. Si Site Recovery Manager no está en ejecución en un sistema operativo host compatible, es posible que Site Recovery Manager no se ejecute adecuadamente.
- Aplique las últimas actualizaciones y revisiones de sistema operativo para proteger el sistema operativo host ante ataques malintencionados. Aplique las últimas actualizaciones y revisiones de Site Recovery Manager para abordar los problemas conocidos con Site Recovery Manager.
- Asegure la integridad de la implementación de Site Recovery Manager al ejecutar Site Recovery Manager como una VM. Consulte el tema *Prácticas recomendadas de seguridad de máquina virtual* en la *documentación de vSphere*.
- Limite la instalación de software y deshabilite los servicios que Site Recovery Manager no utilice, para liberar recursos y disminuir las posibilidades de ataques a servidores. Los servicios y el software innecesarios consumen recursos de CPU, almacenamiento, memoria y ancho de banda, además de incrementar las posibilidades de ataques a servidores.
- Permita que solo los administradores accedan al servidor. Para limitar el número de cuentas que un atacante puede utilizar, reduzca la cantidad de cuentas que pueden acceder al servidor.
- Compruebe los puertos de red que Site Recovery Manager utiliza y configure un firewall para proteger el servidor.
- Separe el tráfico de red de administración de Site Recovery Manager del tráfico de carga de trabajo para proteger los servidores de administración ante ataques.

Índice