

Copia de seguridad y restauración de datos en CMX 10.5 y versiones posteriores

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Proceso de backup](#)

[Creación del paquete de copia de seguridad](#)

[Copia de seguridad de una configuración de alta disponibilidad](#)

[Traslado del paquete de CMX a un equipo diferente](#)

[Eliminación del archivo de copia de seguridad de CMX](#)

[Restauración de la copia de seguridad](#)

[Additional Information](#)

[Restricciones del proceso de backup y restauración](#)

[Diferencia entre el backup y la instantánea de máquina virtual](#)

Introducción

Este documento describe cómo realizar una copia de seguridad y restaurar la configuración y los datos del cliente en un Cisco CMX 10.5 y versiones posteriores

Prerequisites

Requirements

Se requiere conocimiento general de CMX.

Componentes Utilizados

Todas las pruebas se realizaron en un CMX 10.6.0-177 que se ejecuta en el dispositivo MSE 3375, MacOS 10.4 y Windows 10 de octubre de 2018, actualización.

Esto incluye CMX instalado en un dispositivo físico 3365/3375, así como en una máquina virtual. Se puede realizar una copia de seguridad de estos componentes de CMX:

- Base de datos: almacena datos de configuración, como mapas, controladores, ubicación y datos de análisis agregados
- Caché: almacena análisis de visitas repetidas
- Cassandra - Almacena datos del historial de ubicación y análisis de visitas crudas
- Influxdb - Almacena datos de métricas para sistemas (no incluidos de forma predeterminada)
- Consul - Tiendas Configuraciones de Consul

- Floormaps - Almacena imágenes de planta para la visualización de IU
- Licencias: almacena la información de licencia de Cisco CMX
- Configuración: almacena los datos de configuración de CMX
- Connectimages - Almacena Imágenes en Connect Captive Portal
- Conf - Almacena la configuración del nodo

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

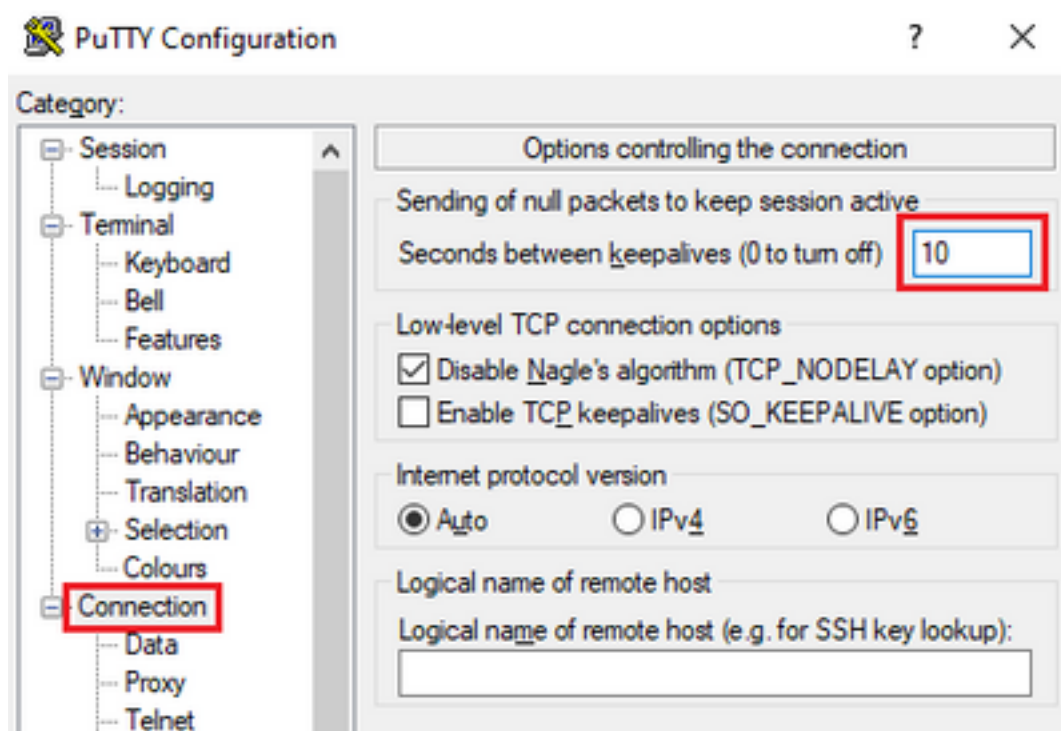
Proceso de backup

Creación del paquete de copia de seguridad

CMX, sin importar dónde esté instalado, se puede realizar una copia de seguridad mediante el comando **cmxos backup**. De forma predeterminada, la copia de seguridad incluye base de datos, caché, cassandra, mapas de planta, licencias, instalación, conexiones, imágenes y configuración. Agregue el parámetro **—all** para incluir también los datos Influxdb. De forma predeterminada, el proceso de copia de seguridad detiene los servicios de CMX mientras se realizan. Agregue el parámetro **—online** para realizar la copia de seguridad sin detener los servicios CMX. Se le solicitará que introduzca el directorio en el que desea guardar el archivo tar.gz de copia de seguridad. El directorio debe tener permisos de lectura, escritura y ejecución. Se recomienda utilizar el directorio /tmp predeterminado.

En un CMX recién instalado, el proceso de copia de seguridad tarda aproximadamente 30 segundos. En un CMX completamente cargado y utilizado, la creación del paquete de copia de seguridad puede tardar hasta una hora.

Asegúrese de habilitar los mensajes keepalive en su cliente SSH para que la sesión no se agote mientras se crea la copia de seguridad. En PuTTY, esto se puede hacer en la pestaña "Conexión":



```
[cmxadmin@mse33752 ~]$ cmxos backup --online --all
Please enter the path for backup file [/tmp]:
backup name: cmx_backup_mse33752_2019_04_28_22_39
backup dir: /tmp/cmx_backup_mse33752_2019_04_28_22_39
tar file: /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz
running: sudo -u cmx /opt/cmx/bin/cmxctl version
```

```
-----
Build Version   : 10.6.0-331
Build Time      : 2019-01-24 13:27:35.937025
-----
```

```
Image Version   : 10.6.0-177
-----
```

```
Preparing backup of following services: ['database', 'cache', 'cassandra', 'influxdb',
'floormaps', 'licenses', 'setup', 'connectimages', 'conf']
```

```
[22:39:56] Preparing for backup...
```

```
Preparing for backup...
```

```
Database size 51226723
```

```
Cache size 7794
```

```
Cassandra size 67462961
```

```
Floormaps size 1014394
```

```
Licenses size 6
```

```
Setup size 1912
```

```
Connectimages size 6
```

```
running: sudo -u cmx /opt/cmx/bin/cmxctl dump
```

```
running locally
```

```
Dumping configuration information...
```

```
[localhost] Executing task 'dump_config_only'
```

```
Done.
```

```
.
.
.
.
.
.
.
```

```
copy snapshot took 0.804718971252 seconds Backup Cassandra DB took: 8.50579595566 seconds
```

```
[22:40:07] Backup InfluxDb... Backup InfluxDb... Backup Influx DB took: 0.0411479473114 seconds
```

```
[22:40:07] Backup Floormaps... Backup Floormaps... Backup floor maps took: 0.055881023407
```

```
seconds [22:40:07] Backup licenses... Backup licenses... Backup licenses took: 0.000136137008667
```

```
seconds [22:40:07] Backup setup... Backup setup... Backup setup took: 0.00061297416687 seconds
```

```
[22:40:07] Backup connect images... Backup connect images... Backup connect images took:
```

```
0.000127077102661 seconds [22:40:07] Backup node configuration... Backup node configuration...
```

```
running: sudo -u cmx /opt/cmx/bin/cmxctl dump running locally Dumping configuration
```

```
information... [localhost] Executing task 'dump_config_only' Done. Backup configuration took:
```

```
0.383893013 seconds [22:40:07] Creating tar file.. Creating tar file.. running: tar -chf
```

```
/tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz --use-compress-program=pigz -C /tmp
```

```
cmx_backup_mse33752_2019_04_28_22_39 running: chmod a+rw
```

```
/tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz running: chown cmxadmin:cmxadmin
```

```
/tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz Post backup took: 0.17880988121 seconds Done
```

```
Backup. Created backup file /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz [22:40:07] Done
```

```
Backup. Created backup file /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz running:
```

```
/opt/apache-cassandra-3.9/bin/nodetool --ssl -h cassandra.service.consul -p 7199 clearsnapshot
```

```
Requested clearing snapshot(s) for [all keyspaces]
```

Al final de la salida, se especifica el nombre del archivo de copia de seguridad:

```
[22:40:07] Done Backup. Created backup file /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz
```

Copia de seguridad de una configuración de alta disponibilidad

Si la alta disponibilidad está activa y en ejecución, ya que todas las bases de datos se sincronizan entre la principal y la secundaria, basta con tomar la copia de seguridad del CMX principal para guardar todos los datos del cliente. Simplemente ejecute el comando **cmxos backup —all —online** y transfiera los archivos desde el servidor principal.

Si actualmente no se ha establecido la alta disponibilidad entre el servidor primario y el secundario, primero determine qué CMX tiene los datos completos y los más recientes y cree una copia de seguridad a partir de ellos.

Nota: Si se establece la alta disponibilidad, la copia de seguridad en línea sólo se admite en el servidor principal. Si se desactiva la alta disponibilidad, se admiten las copias de seguridad en línea y sin conexión tanto en la versión principal como en la secundaria.

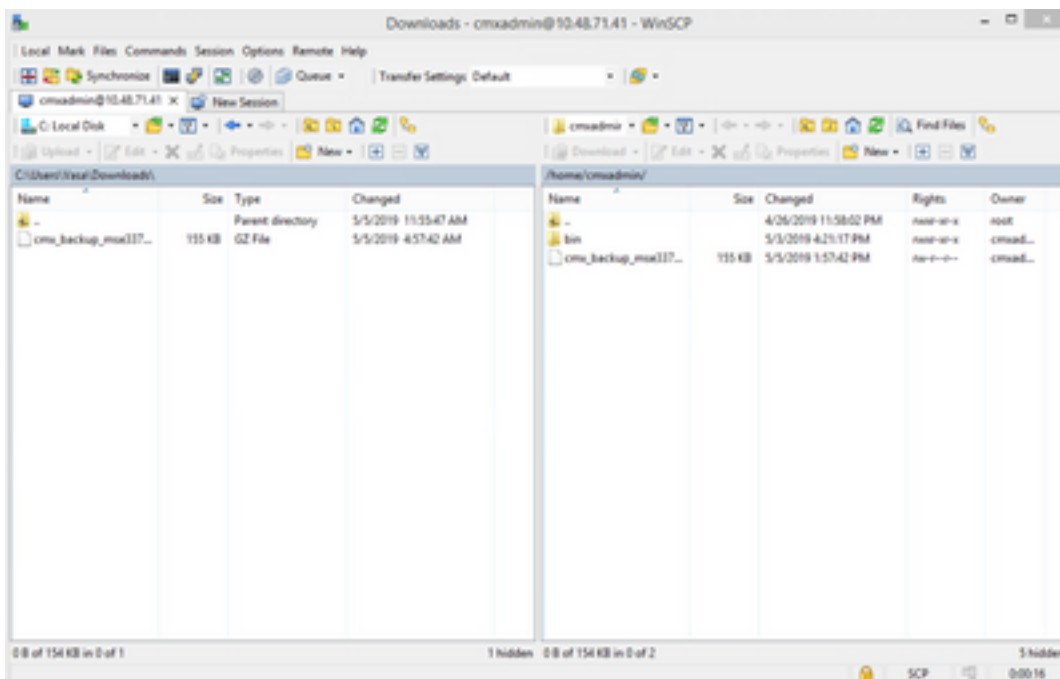
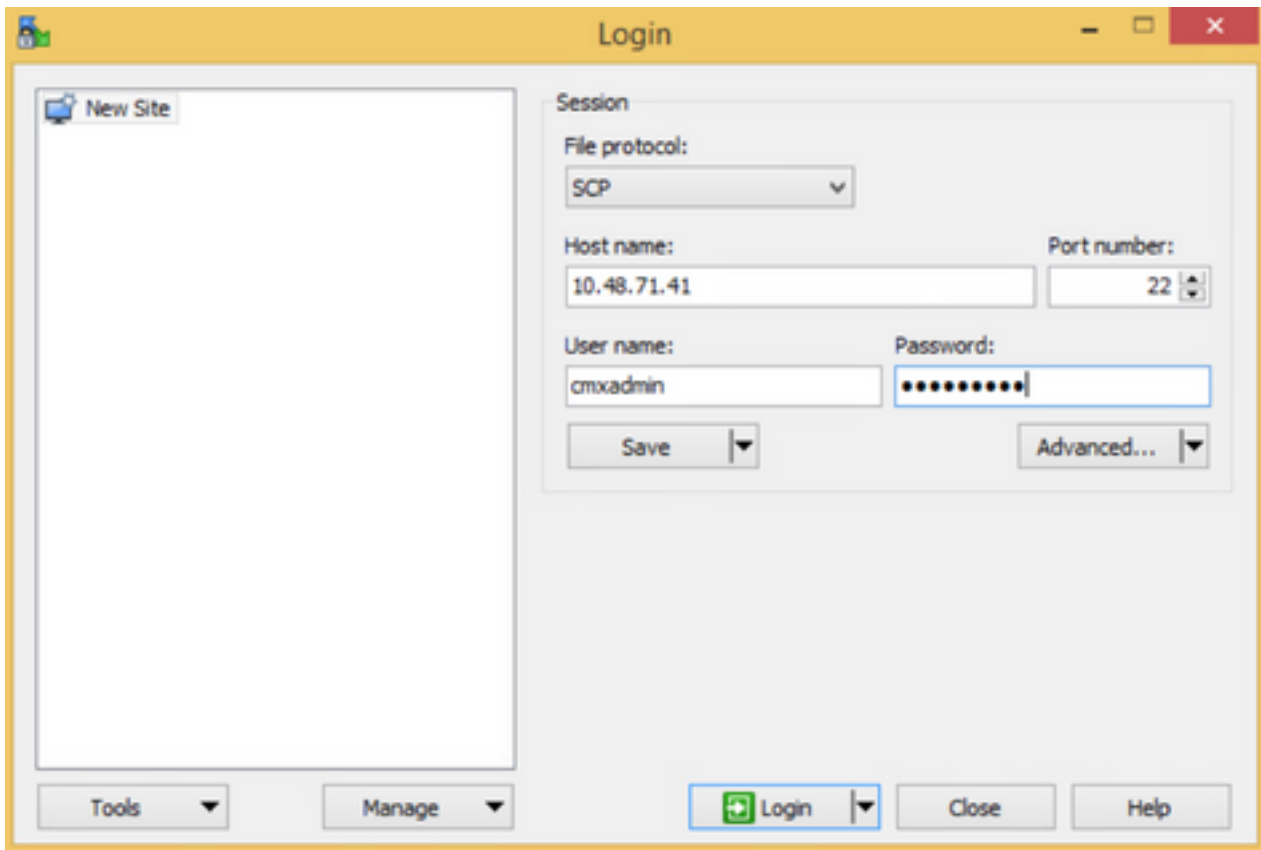
Traslado del paquete de CMX a un equipo diferente

Si algo le sucede al disco duro del CMX o los archivos se dañan durante el proceso de actualización, los archivos de copia de seguridad guardados en el CMX podrían perderse. Se recomienda mover los datos de CMX a otro equipo mediante el protocolo de copia segura (SCP). A continuación encontrará ejemplos de cómo hacerlo en PC con Windows, MacOS y Linux:

Windows:

La manera más fácil de hacer esto en Windows es a través del programa [WinSCP](#). Después de la instalación, introduzca la dirección IP y las credenciales del usuario `cmxadmin` y establezca la conexión SCP. Desplácese hasta la carpeta en la que se ha guardado la copia de seguridad, busque el archivo de copia de seguridad y arrástrelo a la ubicación deseada del equipo local (ventana izquierda).

Importante: Debido a las restricciones de acceso raíz en CMX 10.6.x, el comando **cd** que **WinSCP** utiliza para navegar por los directorios no está presente. En esta situación, no es posible utilizar WinSCP. Póngase en contacto con el TAC de Cisco si desea obtener acceso al parche raíz o buscar una utilidad SCP alternativa.



MacOS y Linux:

MacOS y la mayoría de las distribuciones de Linux vienen con el cliente scp nativo. Los archivos se pueden mover usando un comando simple de terminal:

```
scp cmxadmin@<cmx_ip_address>:<file_path_and_name_on_cmx> <file_path_and_name_on_local_machine>
```

Ejemplo:

```
VAPEROVI-M-H1YM:~ vaperovi$ scp
cmxadmin@10.48.71.41:/tmp/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
```

```
/Users/vaperovi/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
cmxadmin@10.48.71.41's password:
cmx_backup_mse33752_2019_04_28_19_38.tar.gz          100%
186KB  1.4MB/s   00:00
```

CMX muestra una solicitud para introducir las credenciales del usuario cmxadmin, después de lo cual los datos se transfieren a la ubicación especificada en el equipo local.

Nota: Teniendo en cuenta que CMX 10.5 y versiones posteriores se ejecutan en CentOS 7, este comando se puede utilizar para mover los datos de un CMX a uno recién instalado. Dado que sólo se puede sincronizar un controlador inalámbrico con un CMX a la vez, asegúrese de apagar el CMX desde el que se descarga el paquete de respaldo.

Eliminación del archivo de copia de seguridad de CMX

En la versión 10.5.x de CMX, los archivos se pueden eliminar iniciando sesión como usuario raíz mediante el comando **su**, desplazándose al directorio `/tmp` donde se han guardado los archivos de copia de seguridad y eliminándolos mediante el comando **rm -f**:

```
[cmxadmin@mse33752 ~]$ su
Password:
[root@mse33752 cmxadmin]#
[root@mse33752 cmxadmin]# cd /tmp
[root@mse33752 tmp]# rm -f cmx_backup_mse33752_2019_04_28_19_38.tar.gz
```

A partir de la versión 10.6.0, se ha restringido el acceso a la raíz. Sin un parche especial que solo puede ser entregado por el TAC de Cisco, eliminar los archivos como en 10.5 no es posible. Se puede liberar algo de espacio mediante el comando **cmxos clean normal —delete**:

```
[cmxadmin@mse33752 ~]$ cmxos clean normal --delete
Are you sure you wish to remove files? [y/N]: y
Removing files in: /opt/cmx/var/log
Remove: /opt/cmx/var/log/entropy.err
Remove: /opt/cmx/var/log/backup.log.2
Remove: /opt/cmx/var/log/techsupport/cmx_tech_support_2019-04-28.log
Removing files in: /opt/influxdb/shared
Removing files in: /tmp
```

Importante: si aún no hay espacio suficiente para realizar la copia de seguridad después de ejecutar **cmxos clean normal —delete**, debe comunicarse con el TAC de Cisco para obtener acceso a la raíz y eliminar los archivos que están ocupando espacio.

Restauración de la copia de seguridad

Si desea restaurar la copia de seguridad, transfiera el archivo de copia de seguridad desde el equipo remoto a CMX. En Windows, puede simplemente arrastrar y soltar los archivos con WinSCP. En MacOS y Linux, utilice este comando:

```
$ scp <file_path_and_name_on_local_machine> cmxadmin@<cmx_ip_address>:/tmp
```

Ejemplo:

```
VAPERОВI-M-H1YM:~ vaperovi$ scp /Users/vaperovi/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
```

cmxadmin@10.48.71.41:/tmp

cmxadmin@10.48.71.41's password:

cmx_backup_mse33752_2019_04_28_19_38_copy.tar.gz

100% 186KB

1.3MB/s 00:00

Importante: La restauración de los datos de Cisco CMX debe realizarse desde un dispositivo que tenga la misma hora local. De lo contrario, no podrá acceder correctamente a los datos de análisis. Además, los datos producen errores o valores cero en los informes.

Para restaurar los datos, CMX necesita tener espacio libre en el disco 4 veces mayor que el tamaño del paquete de copia de seguridad. Si no hay suficiente espacio, puede intentar aumentar el espacio de la máquina virtual o ejecutar el comando **cmxos clean normal —delete**. El proceso de restauración se puede iniciar con el comando **cmxos restore**. Al agregar el parámetro **-i**, puede realizar una copia de seguridad sólo de determinados elementos (base de datos, caché, cassandra, mapas de planta, licencias, setup, conf). Se recomienda realizar copias de seguridad completas.

El proceso de restauración requiere que se detengan todos los servicios. Asegúrese de preparar una ventana de mantenimiento lo suficientemente grande para este proceso, ya que puede tardar más de una hora.

```
[cmxadmin@mse33752 ~]$ cmxos restore
Please enter the backup file path: /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz
Please enter the path for untar backup file [/tmp]:
Stopping monit (via systemctl): [ OK ]
[23:49:19] Preparing for restore...
Restore size 30383753
Available disk space in /tmp is 1812541169664
Available disk space is 1817753817088
[23:49:19] Untarring backup file...
Backing up existing licenses on the system...
Successfully saved existing licenses
Stopping all services...
Pre restore took: 41.672647953 seconds
[23:50:00] Restoring Database...
Created temporary database temp_mse
Running command /usr/bin/sudo -u postgres pg_restore -j 8 -d temp_mse -Fc
/tmp/cmx_backup_mse33752_2019_04_28_22_39/postgres/mse.dump
Restored temporary database temp_mse
Dropping database mse
Renaming database temp_mse to mse
Restarting database...
Starting database...
Restore database took: 10.2765719891 seconds
[23:50:11] Restoring Cache...
Stopping cache_6378...
Restarting cache_6378...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6385...
Restarting cache_6385...
Stopping cache_6380...
Restarting cache_6380...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6383...
Restarting cache_6383...
```

```

Stopping cache_6384...
Restarting cache_6384...
Restore Cache took: 61.1865711212 seconds
[23:51:12] Restoring Cassandra...
Stopping Cassandra...
Starting Cassandra after wipe...
starting cassandra
Creating empty cassandra schemas
Stopping Cassandra...
Starting Cassandra after restore ...
starting cassandra
Restore Cassandra took: 117.123826981 seconds
[23:53:09] Restoring floormaps...
Restore floor maps took: 0.0736980438232 seconds
[23:53:09] Restoring licenses...
Restore licenses took: 0.000176906585693 seconds
[23:53:09] Restoring setup...
Restore setup took: 0.00758194923401 seconds
[23:53:09] Restoring connect images...
Restore connect images took: 0.000188827514648 seconds
[23:53:09] Running Post Restore Tasks...
[23:53:09] Migrating Schemas...
[23:53:10] Migrating Cassandra Schemas...
stopping cassandra
Local licenses wont be retained.
Running full vacuum command on postgres
Performing cleanup of redis cache 6378 and 6383 to evict bloom filter stale entries.
Performing cleanup of redis cache 6378 to evict stale records by glesspyworker.
Update CMX default certificate
Post restore took: 61.7358779907 seconds
[23:54:11] Starting all services...
[23:56:04] Done
Starting monit (via systemctl): [ OK ]

```

Additional Information

Restricciones del proceso de backup y restauración

- Las copias de seguridad de CMX 10.3 o posterior no se pueden importar a CMX 10.5.x o posterior. Las copias de seguridad de 10.5.x se pueden importar a CMX 10.6.x
- Para cumplir con el RGPD, se debe realizar una copia de seguridad de la base de datos, mapas de planta, licencias y componentes de configuración
- Asegúrese de que el puerto 22 no esté bloqueado entre CMX y la máquina que se utiliza para acceder a él
- Si restaura copias de seguridad de un tipo diferente de implementación de CMX, consulte la tabla para comprobar si son compatibles:

Restaurar desde...	Restaurar en...	Recomendaciones
Mismas especificaciones de la máquina	Mismas especificaciones de la máquina	OK
Dispositivo Cisco MSE 3365	Dispositivo Cisco 3375	OK
Dispositivo Cisco MSE 3365	MSE virtual de gama alta (vMSE)	OK
vMSE de gama alta	Dispositivos Cisco 3375 y Cisco MSE 3365	OK a menos que la máquina de gama alta tenga más asignada que las especificaciones recomendadas

vMSE estándar	Dispositivos Cisco 3375 y Cisco MSE 3365	OK
vMSE estándar	vMSE de gama alta	OK
vMSE de gama baja	Dispositivos Cisco 3375 y Cisco MSE 3365	OK
vMSE de gama baja	vMSE de gama alta	OK
vMSE de gama baja	vMSE estándar	OK
Dispositivo Cisco 3375	Dispositivo Cisco MSE 3365	No recomendado
Dispositivo Cisco MSE 3365	vMSE estándar	No recomendado
Dispositivo Cisco MSE 3365	vMSE de gama baja	No recomendado
vMSE de gama alta	vMSE estándar	No recomendado
vMSE de gama alta	vMSE de gama baja	No recomendado
vMSE estándar	vMSE de gama baja	No recomendado

Diferencia entre el backup y la instantánea de máquina virtual

Las instantáneas de máquinas virtuales no se pueden considerar una herramienta de copia de seguridad, ya que no hacen nada para preservar la integridad del archivo VMDK que la máquina virtual utiliza para su almacenamiento de datos.

Las instantáneas funcionan "congelando" el archivo de almacenamiento VMDK original y creando archivos de instantáneas adicionales que capturan los cambios realizados en el archivo VMDK original (la llamada cadena de disco). De esta forma, el estado del archivo de disco se puede conservar en el tiempo y revertir a si es necesario después de realizar algunos cambios.

Por lo tanto, si el archivo VMDK original (principal) se pierde o está dañado de alguna manera, los datos de instantánea no se pueden utilizar para restaurar su estado anterior y los datos almacenados se pierden de forma efectiva.

Las prácticas recomendadas de VMware para el uso de instantáneas en el entorno vSphere mencionan lo siguiente:

- **No utilice instantáneas como copias de seguridad** (motivos expuestos)
- VMware recomienda no utilizar una sola instantánea durante más de 72 horas (el tamaño del archivo de instantánea sigue aumentando cuando se conserva durante un período más largo). Esto puede hacer que la ubicación de almacenamiento de instantáneas se quede sin espacio y afecte al rendimiento del sistema).
- Se admiten un máximo de 32 instantáneas en una cadena. Sin embargo, para un mejor rendimiento, limite el uso de solo 2 a 3 instantáneas.

Para obtener más información, consulte el [artículo sobre prácticas recomendadas de instantáneas de VMware](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).