

Sichern und Wiederherstellen von Daten auf CMX 10.5 und höher

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Backup-Prozess](#)

[Erstellen des Backup-Pakets](#)

[Sichern einer Hochverfügbarkeits-Konfiguration](#)

[Verschieben des Pakets von CMX auf einen anderen Computer](#)

[Löschen des Backup-Archivs aus CMX](#)

[Wiederherstellen der Sicherung](#)

[Zusätzliche Informationen](#)

[Einschränkungen des Backup- und Wiederherstellungsprozesses](#)

[Unterschied zwischen Backup und Snapshot des virtuellen Systems](#)

Einleitung

In diesem Dokument wird beschrieben, wie Konfigurations- und Client-Daten auf einem Cisco CMX 10.5 oder höher gesichert und wiederhergestellt werden.

Voraussetzungen

Anforderungen

Allgemeine Kenntnisse über CMX sind erforderlich.

Verwendete Komponenten

Alle Tests wurden auf einem CMX 10.6.0-177 mit MSE 3375-Appliance, MacOS 10.4 und Windows 10 Oktober 2018 Update durchgeführt.

Dies umfasst CMX, das auf einer physischen 3365/3375-Appliance sowie auf einem virtuellen System installiert ist. Die folgenden Komponenten von CMX können gesichert werden:

- Datenbank: Speichert Konfigurationsdaten, z. B. Karten, Controller, Standorte und aggregierte Analysedaten
- Cache - Speicherung von Analysedaten - Wiederholte Besuche
- Cassandra - Speichert Standortverlaufsdaten und Analysen von Besuchen im Rohzustand
- Influxdb - Speichert Kennzahlidaten für Systeme (standardmäßig nicht enthalten)
- Consul - speichert Consul-Konfigurationen

- Floormaps - Speichert Bilder für die Benutzeroberfläche
- Lizenzen - Speichert Cisco CMX-Lizenzinformationen
- Einrichtung - Speichert CMX-Einrichtungsdaten
- Connectimages - Speichern von Bildern auf Connect Captive Portal
- Konf - Speichert Knotenkonfiguration

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

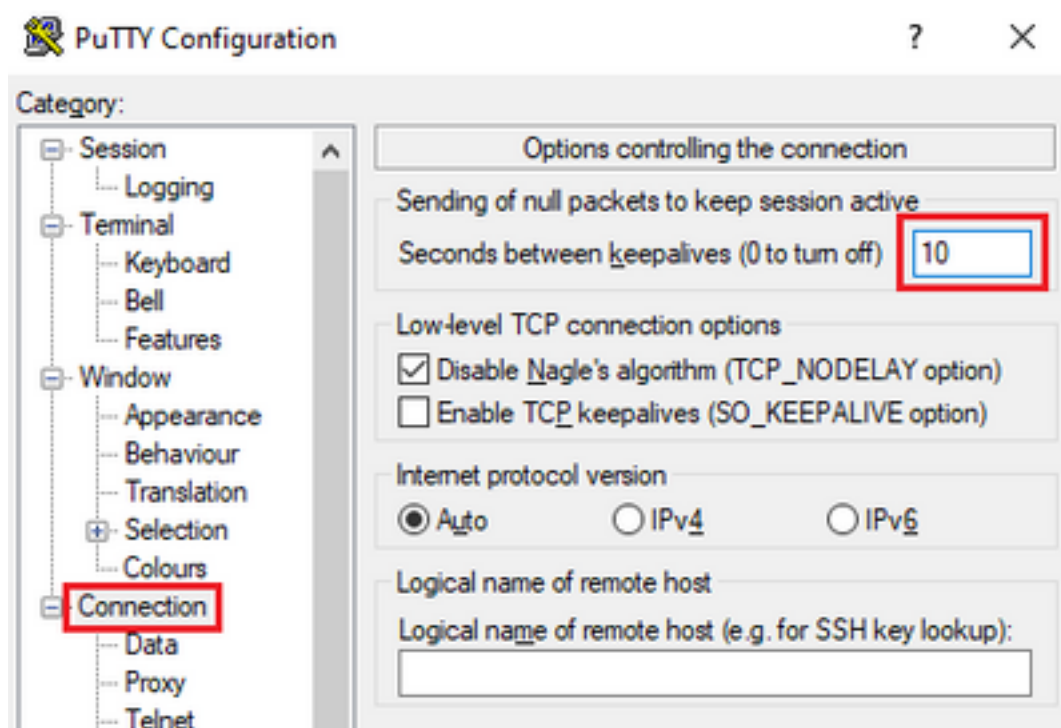
Backup-Prozess

Erstellen des Backup-Pakets

CMX kann unabhängig vom Installationsort mit einem Befehl **cmxos backup** gesichert werden. Standardmäßig umfasst das Backup Datenbank, Cache, Cassandra, Floormaps, Lizenzen, Einrichtung, Verbindungszeiten und Konfiguration. Fügen Sie den Parameter **—all** hinzu, um auch die InfluenzaDB-Daten einzuschließen. Standardmäßig stoppt der Backup-Prozess CMX-Services, während er ausgeführt wird. Fügen Sie den Parameter **online** hinzu, um die Sicherung ohne Anhalten der CMX-Services durchzuführen. Sie werden aufgefordert, das Verzeichnis einzugeben, in dem Sie das Archiv tar.gz sichern möchten. Das Verzeichnis muss über Lese-, Schreib- und Ausführungsberechtigungen verfügen. Es wird empfohlen, das Standardverzeichnis /tmp zu verwenden.

Auf einem frisch installierten CMX dauert der Backup-Prozess ca. 30 Sekunden. Auf einem vollständig geladenen und genutzten CMX kann die Erstellung des Backup-Pakets bis zu eine Stunde dauern.

Stellen Sie sicher, dass Sie Keepalive-Nachrichten in Ihrem SSH-Client aktivieren, damit die Sitzung während der Erstellung des Backups nicht abgelaufen ist. In PuTTY kann dies auf der Registerkarte "Connection" (Verbindung) durchgeführt werden:



```
[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]
```

Am Ende der Ausgabe wird der Name des Backup-Archivs angegeben:

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

Sichern einer Hochverfügbarkeits-Konfiguration

Wenn die Hochverfügbarkeit derzeit verfügbar ist und ausgeführt wird, da alle Datenbanken zwischen primärem und sekundärem System synchronisiert werden, reicht das Sichern von primärem CMX aus, um alle Client-Daten zu speichern. Führen Sie einfach den Befehl **cmxos backup —all —online aus** und übertragen Sie die Dateien vom primären Server.

Wenn derzeit keine hohe Verfügbarkeit zwischen primärem und sekundärem Server besteht, ermitteln Sie zunächst, welches CMX über vollständige und aktuelle Daten verfügt, und erstellen Sie ein Backup davon.

Hinweis: Wenn Hochverfügbarkeit eingerichtet ist, wird Online-Backup nur auf dem primären Server unterstützt. Wenn Hochverfügbarkeit deaktiviert ist, werden Online- und Offline-Backups sowohl auf dem primären als auch auf dem sekundären Gerät unterstützt.

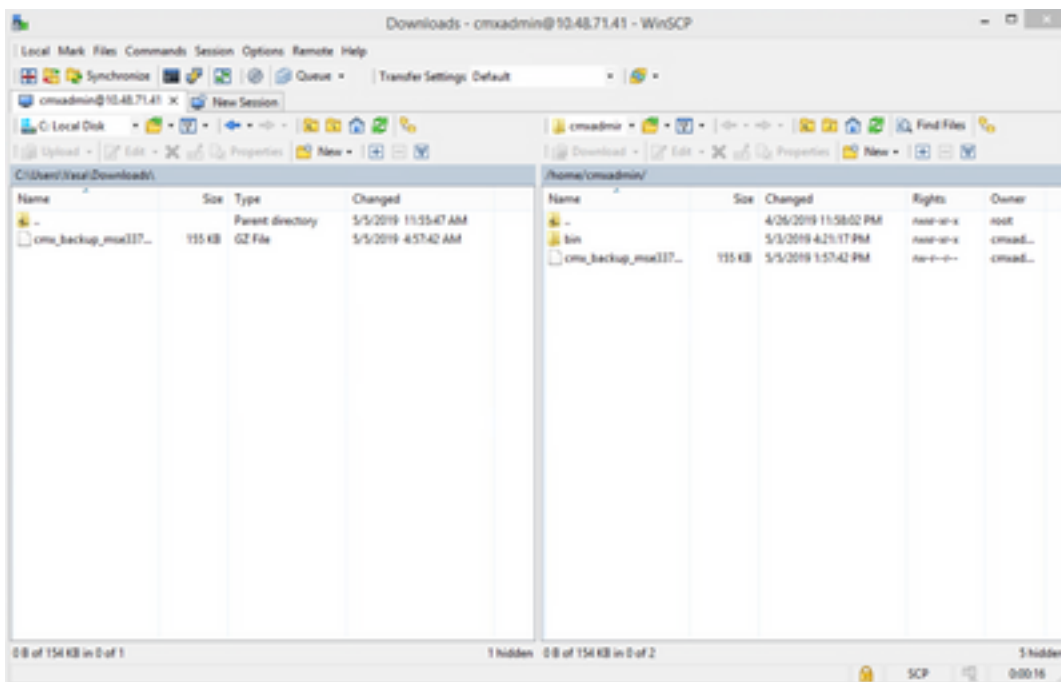
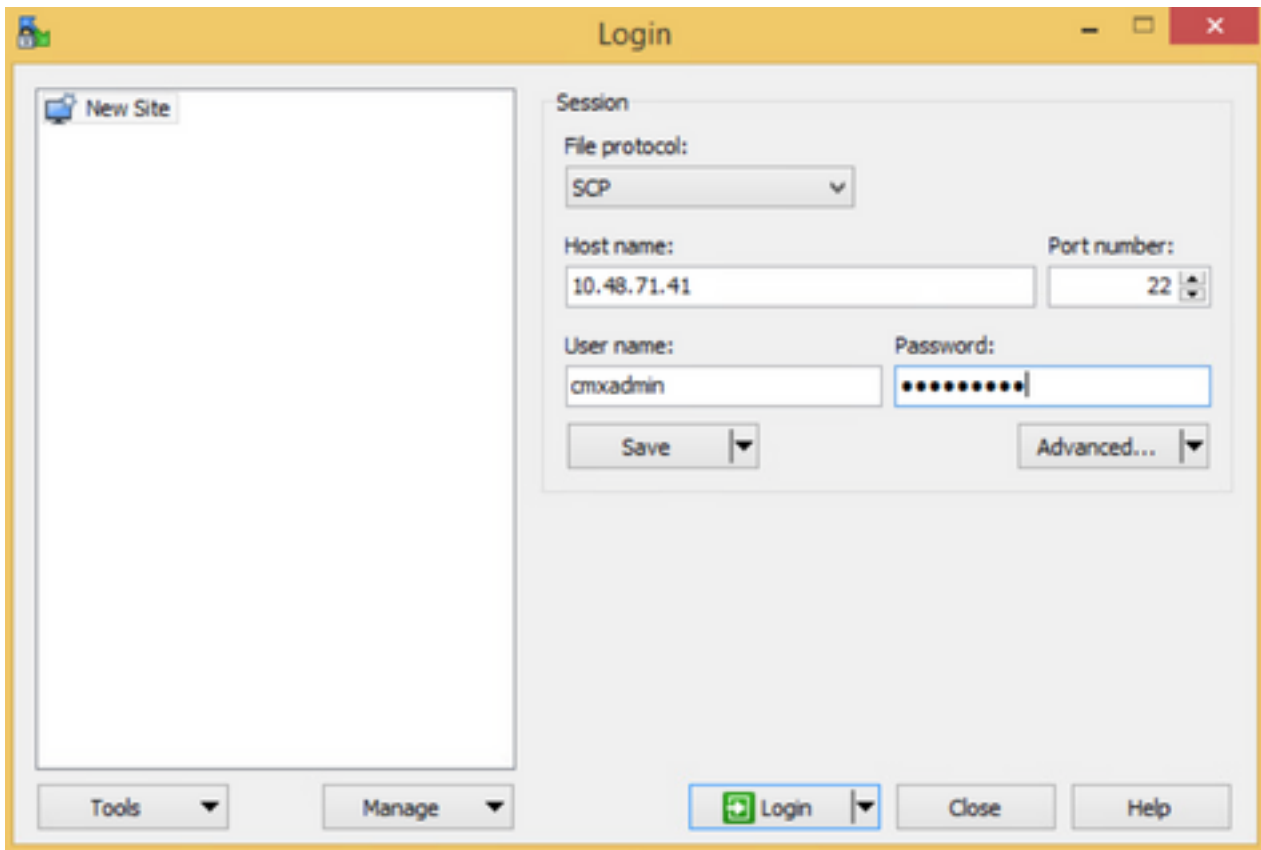
Verschieben des Pakets von CMX auf einen anderen Computer

Wenn etwas mit der Festplatte des CMX passiert oder Dateien während des Upgrade-Vorgangs beschädigt werden, können Backup-Dateien, die auf dem CMX gespeichert sind, verloren gehen. Es wird empfohlen, die Daten mithilfe des Secure Copy Protocol (SCP) von CMX auf einen anderen Computer zu verschieben. Nachstehend finden Sie Beispiele dafür, wie Sie dies auf Windows-, MacOS- und Linux-PCs tun können:

Windows:

Dies ist unter Windows am einfachsten mit dem [WinSCP](#)-Programm. Geben Sie nach der Installation die IP-Adresse und die Anmeldeinformationen des cmxadmin-Benutzers ein, und stellen Sie die SCP-Verbindung her. Navigieren Sie zu dem Ordner, in dem die Sicherung gespeichert ist, suchen Sie die Sicherungsdatei, und ziehen Sie sie an den gewünschten Speicherort auf Ihrem lokalen Computer (linkes Fenster).

Wichtig: Aufgrund von Root-Zugriffsbeschränkungen in CMX 10.6.x ist die Befehl-**CD**, die WinSCP zum Navigieren in Verzeichnissen verwendet, nicht vorhanden. In dieser Situation ist der Einsatz von WinSCP nicht möglich. Wenden Sie sich an das Cisco TAC, wenn Sie Zugriff auf den Root-Patch erhalten oder ein anderes SCP-Dienstprogramm suchen möchten.



MacOS und Linux:

MacOS und die meisten Linux-Distributionen werden mit nativem scp-Client geliefert. Dateien können mit einem einfachen Terminalbefehl verschoben werden:

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

Beispiel:

```
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 zeigt eine Aufforderung zur Eingabe der Anmeldeinformationen des "cmxadmin"-Benutzers an. Anschließend werden die Daten an den angegebenen Speicherort auf dem lokalen Computer übertragen.

Hinweis: Wenn man bedenkt, dass CMX 10.5 und höher auf CentOS 7 ausgeführt wird, kann dieser Befehl verwendet werden, um die Daten von einem CMX in ein neu installiertes CMX zu verschieben. Da ein Wireless-Controller jeweils nur mit einem CMX synchronisiert werden kann, stellen Sie sicher, dass Sie den CMX herunterfahren, von dem das Backup-Paket heruntergeladen wird.

Löschen des Backup-Archivs aus CMX

In CMX, Version 10.5.x, können Dateien gelöscht werden, indem Sie sich als Root-Benutzer über den Befehl **su** anmelden, zum Verzeichnis /tmp navigieren, in dem die Sicherungsdateien gespeichert wurden, und diese über den Befehl **rm -f** löschen:

```
[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
```

Ab Version 10.6.0 wurde der Root-Zugriff eingeschränkt. Ohne einen speziellen Patch, der nur vom Cisco TAC verteilt werden kann, ist ein Löschen der Dateien wie bei 10.5 nicht möglich. Mit dem Befehl **cmxos clean normal --delete** kann etwas Speicherplatz freigegeben werden:

```
[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
```

Wichtig: Wenn nach der Ausführung von **cmxos clean normal --delete** immer noch nicht genügend Speicherplatz für das Backup vorhanden ist, müssen Sie sich an das Cisco TAC wenden, um Zugriff auf den Root zu erhalten und Dateien zu entfernen, die Speicherplatz belegen.

Wiederherstellen der Sicherung

Wenn Sie die Sicherung wiederherstellen möchten, übertragen Sie die Sicherungsdatei vom Remote-Computer auf CMX. In Windows können Sie die Dateien einfach per Drag & Drop mit WinSCP verschieben. Verwenden Sie unter MacOS und Linux den folgenden Befehl:

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

Beispiel:

```
VAPEROVI-M-H1YM:~ vaperovi$ scp /Users/vaperovi/cmxc_backup_mse33752_2019_04_28_19_38.tar.gz
cmxadmin@10.48.71.41:/tmp
cmxadmin@10.48.71.41's password:
cmxc_backup_mse33752_2019_04_28_19_38_copy.tar.gz                               100% 186KB
1.3MB/s   00:00
```

Wichtig: Die Wiederherstellung der Cisco CMX-Daten muss auf einem Gerät mit derselben lokalen Uhrzeit erfolgen. Andernfalls können Sie nicht richtig auf die Analysedaten zugreifen. Darüber hinaus führen die Daten in Berichten zu Fehlern oder Nullwerten.

Um Daten wiederherzustellen, benötigt CMX freien Speicherplatz, der viermal so groß ist wie das Backup-Paket. Wenn nicht genügend Speicherplatz vorhanden ist, können Sie versuchen, den Speicherplatz des virtuellen Rechners zu vergrößern oder den Befehl **cmxos clean normal —delete** auszuführen. Der Wiederherstellungsvorgang kann mit dem Befehl **cmxos restore** initiiert werden. Durch Hinzufügen des **-i**-Parameters können nur bestimmte Elemente gesichert werden (Datenbank, Cache, Cassandra, Floorplans, Lizenzen, Setup, Konf). Es wird empfohlen, vollständige Sicherungen durchzuführen.

Der Wiederherstellungsvorgang erfordert das Beenden aller Dienste. Stellen Sie sicher, genügend Wartungsfenster für diesen Prozess vorzubereiten, da es mehr als eine Stunde dauern kann.

```
[cmxadmin@mse33752 ~]$ cmxos restore
Please enter the backup file path: /tmp/cmxc_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/cmxc_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 ]

```

Zusätzliche Informationen

Einschränkungen des Backup- und Wiederherstellungsprozesses

- Sicherungen von CMX 10.3 oder älter können nicht in CMX 10.5.x oder höher importiert werden. Sicherungen aus 10.5.x können in CMX 10.6.x importiert werden
- Um die Einhaltung der DSGVO zu gewährleisten, muss eine Sicherung der Datenbank, der Grundrisse, der Lizenzen und der Einrichtungskomponenten durchgeführt werden.
- Stellen Sie sicher, dass der Port 22 zwischen CMX und dem Rechner, der für den Zugriff auf CMX verwendet wird, nicht blockiert ist.
- Wenn Sie Backups von einem anderen CMX-Bereitstellungstyp wiederherstellen, überprüfen Sie anhand der Tabelle, ob sie kompatibel sind:

Wiederherstellen von...	Wiederherstellen auf...	Empfehlungen
Gleiche Maschinenspezifikationen	Gleiche Maschinenspezifikationen	OK
Cisco MSE 3365	Cisco 3375-Appliance	OK

Cisco MSE 3365	High-End MSE Virtual (vMSE)	OK
High-End-vMSE	Cisco 3375 und Cisco MSE 3365 Appliances	OK, es sei denn, dem High-End-System ist mehr RAM zugewiesen als empfohlen.
Standard-vMSE	Cisco 3375 und Cisco MSE 3365 Appliances	OK
Standard-vMSE	High-End-vMSE	OK
Low-End-vMSE	Cisco 3375 und Cisco MSE 3365 Appliances	OK
Low-End-vMSE	High-End-vMSE	OK
Low-End-vMSE	Standard-vMSE	OK
Cisco 3375-Appliance	Cisco MSE 3365	Nicht empfohlen
Cisco MSE 3365	Standard-vMSE	Nicht empfohlen
Cisco MSE 3365	Low-End-vMSE	Nicht empfohlen
High-End-vMSE	Standard-vMSE	Nicht empfohlen
High-End-vMSE	Low-End-vMSE	Nicht empfohlen
Standard-vMSE	Low-End-vMSE	Nicht empfohlen

Unterschied zwischen Backup und Snapshot des virtuellen Systems

Snapshots virtueller Maschinen können nicht als Backup-Tool betrachtet werden, da sie nichts tun, um die Integrität der VMDK-Datei zu bewahren, die die virtuelle Maschine für ihre Datenspeicherung verwendet.

Snapshots arbeiten durch "Einfrieren" der ursprünglichen VMDK-Speicherdatei und Erstellen zusätzlicher Snapshot-Dateien, die die an der ursprünglichen VMDK-Datei vorgenommenen Änderungen erfassen (so genannte Disk Chain). Auf diese Weise kann der Status der Datenträgerdatei im Laufe der Zeit beibehalten und nach einigen Änderungen ggf. auf zurückgesetzt werden.

Wenn die ursprüngliche (übergeordnete) VMDK-Datei verloren geht oder in irgendeiner Weise beschädigt ist, können daher keine Snapshot-Daten verwendet werden, um sie in ihren vorherigen Zustand wiederherzustellen, und die gespeicherten Daten gehen effektiv verloren.

Die Best Practices von VMware für die Verwendung von Snapshots in der vSphere-Umgebung umfassen Folgendes:

- **Verwenden Sie keine Snapshots als Backups** (Gründe hierfür)
- VMware empfiehlt, einen einzelnen Snapshot nicht länger als 72 Stunden zu verwenden (Die Größe der Snapshot-Datei wächst weiter, wenn sie über einen längeren Zeitraum aufbewahrt wird. Dies kann dazu führen, dass der Speicherplatz für den Snapshot-Speicher knapp wird und sich dies auf die Systemleistung auswirkt.)
- In einer Kette werden maximal 32 Snapshots unterstützt. Beschränken Sie jedoch zur Verbesserung der Leistung die Verwendung von nur 2 bis 3 Snapshots.

Weitere Informationen finden Sie im [VMware Snapshot Best Practices-Artikel](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.