Dell EMC CloudLink 7.0.2

Upgrade Guide

April 2021
Rev. A00

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

About Dell EMC CloudLink

CloudLink secures sensitive information within virtual machines across both public and private clouds. It provides encryption for the boot volume and additional data volumes with pre-startup authorization for cloud-hosted virtual machines. CloudLink provides this encryption by using native operating system encryption features: Microsoft BitLocker for Windows or dm-crypt for Linux.

CloudLink enables you to use native operating system encryption features to encrypt the virtual machine boot and data volumes in a multitenant cloud environment. This encryption helps protect the integrity of the virtual machine itself against unauthorized modifications. CloudLink encrypts the virtual machine boot and data volumes with unique keys that are controlled by enterprise security administrators. Neither cloud administrators nor other tenants in the cloud have access to the keys. Securing the virtual machine lets you define the security policy it must meet before passing pre-startup authorization, including verifying the integrity of the virtual machine's boot chain. This offers protection against tampering.

CloudLink ensures that only trusted and verified virtual machines can run and access sensitive data stored in the cloud. As part of the CloudLink solution, CloudLink Center defines the key release policy, performs prestartup authorization, and monitors all CloudLink Agents, events, and logs.

CloudLink also offers significant benefits for environments that use Dell EMC VxFlex OS resources. VxFlex OS is a software-defined solution that enables you to transform direct-attached storage (DAS) on existing hardware into shared block storage. It offers considerable scalability and extreme performance with flexible and elastic storage capacity and nodes. CloudLink encrypts the SDS devices with unique keys that are controlled by enterprise security administrators.

CloudLink Center—The web-based management interface for CloudLink, is used for managing encryption keys, configuring security policies, and monitoring the security and operation events and logs.

Topics:

About this document

This document describes how to upgrade from Dell EMC CloudLink version 6.9 or 7.0 or 7.0.1. Because of the critical nature of the encryption keys and CloudLink Agent information that is contained in CloudLink Center servers, review the information in this document before starting the upgrade process.

2

Upgrade requirements

Before upgrading to CloudLink version 7.0.2, ensure that the following requirements are met.

Upgrade paths

- You must be using the version **6.9.0 (build 899.7)** or **7.0.0 (build 8.7)** or **7.0.1 (build 12.17)** before upgrading to CloudLink version 7.0.2.
- Log in to the CloudLink Center to verify the CloudLink version and build number. The version and build number is displayed in the **Information** box on the **CloudLink Center Home** panel.
- If CloudLink Center was deployed using a version earlier to CloudLink 6.9, the upgrade includes an update to Ubuntu Server version 16.04. This update increases the time that is required for the upgrade process.
- For Microsoft Azure—If CloudLink Center virtual appliance is running CloudLink version 6.9 or 7.0 or 7.0.1, and Ubuntu version 14.04, then upgrade to CloudLink version 7.0.2 includes an update to Ubuntu Server version 16.04. This update increases the CloudLink 7.0.2 upgrade time.

  NOTE: Wait until the CloudLink version 7.0.2 upgrade is completed. Do not perform any operations during the 7.0.2 upgrade process.
- For Amazon Web Services (AWS)—If CloudLink Center virtual appliance is running CloudLink version 6.9 or 7.0 or 7.0.1, and Ubuntu Server version 14.04, then upgrade to CloudLink version 7.0.2 fails. Contact Dell Technologies Support to upgrade to CloudLink version 7.0.2.
- An active Internet connection is required to download the latest packages for upgrading Ubuntu Server on Microsoft Azure and AWS.

VMs

- Ensure that your CloudLink Center virtual appliance is running the version **6.9.0 (build 899.7)** or **7.0.0 (build 8.7)** or **7.0.1 (build 12.17)**.
- Verify that all CloudLink Center VM must have at least 6 GB of RAM and four vCPUs before you upgrade. If a CloudLink Center VM does not have sufficient resources for the upgrade, a **System does not meet requirements** alarm is triggered.
- To automatically upgrade all CloudLink Agents, ensure that all machines that are registered with CloudLink Center are online and display as **Connected** in CloudLink Center. The `Machine Agent Upgrade` policy must be set to **Auto**.
- If the Machine Agent Upgrade policy is set to **Auto**, any CloudLink Agent that is not connected to CloudLink Center is automatically upgraded the next time the CloudLink Agent connects. Perform the postupgrade verification if machines are online and connected during the upgrade. For more information, see Postupgrade verification.
- If the Machine Agent Upgrade policy is set to **Manual**, then all the machines in the respective machine group that uses Machine Agent Upgrade policy must be upgraded manually.
- Verify that CloudLink Center cluster servers are online and synchronized with each other.

Backups

Ensure that the following critical backup requirements are met:

- It is recommended that you back up CloudLink Center and all VMs before starting the upgrade process. Perform backups by using VM snapshots or traditional backup tools.
- Back up your CloudLink Center configuration data. For more information, see the chapter "Back up and restore CloudLink Center" in the *Dell EMC CloudLink Administration Guide*.
- If you are using Microsoft Active Directory, Amazon S3 external storage, or an S3-compatible bucket, back up your encryption keys by using tools that are specific to those environments.

Keystore

If you are using an external keystore, ensure that the keystore is connected before starting the upgrade process.

CloudLink licenses

Before you start the upgrade process, verify that the CloudLink licenses have not expired.

Licenses that are past their support duration, typically one, two, or three years from the date of purchase, are blocked from being uploaded. If licenses have expired after being uploaded, all the existing CloudLink functionalities will continue to work including releasing of keys. However, new CloudLink Agent installation and encryption of machines and SDS devices cannot be performed. To reenable encryption, purchase a new license and upload it.

Passwords

You require the following:

- CloudLink secadmin password
- CloudLink console password
- One of the CloudLink Vault passwords
- Passwords of the encrypted VMs

CloudLink Center clusters

The upgrade process upgrades all servers in a cluster.

- Ensure that all servers are accessible.
- Upload the upgrade ISO to any server in a cluster.
- Wait until the ISO is uploaded to all servers before you begin the upgrade.

Ports

Before starting the upgrade process, ensure that TCP ports 80 and 1194 and UDP port 1194 are open. For more information, see the section "Software requirements for deploying CloudLink Center" in the *Dell EMC CloudLink 7.0.2 Deployment Guide*.

3

CloudLink upgrade overview

Upgrading CloudLink involves uploading the upgrade ISO file and initiating the upgrade. All servers in a CloudLink Center cluster are automatically upgraded during the upgrade process. Connected CloudLink Agents are automatically upgraded if the Machine Agent Upgrade policy is set to **Auto**. Any CloudLink Agent that is not connected is automatically upgraded the next time it connects to CloudLink Center.

CloudLink enables you to manually upgrade CloudLink Agents after you upgrade CloudLink Center or a CloudLink Center cluster, if the Machine Agent Upgrade policy is set to **Manual**. See Upgrade CloudLink Agents manually for instructions.

Topics:

Group policy and CloudLink agent

If the Group Policy in an Active Directory environment handles the CloudLink agent installation, then the CloudLink Agent Group Policy Object must be updated with the new CloudLink Agent MSI file.

First delete the old CloudLink Agent MSI installer file from its Group Policy Object, upgrade CloudLink Center using the upgrade ISO file, and then add the version 7.0.2 CloudLink Agent MSI installer file to the Group Policy Object.

Change CloudLink Vault unlock modes

Use this procedure to change CloudLink Vault unlock modes.

Prerequisites

The CloudLink Vault must be set to **Auto Unlock** mode before the upgrade begins. This allows CloudLink Center to unlock immediately after the upgrade process begins so that all CloudLink Agents can be upgraded.

About this task

You can also set the CloudLink Vault to **Manual Unlock** before the upgrade. But, you must:

- Enter one of the CloudLink Vault passcodes when prompted.
- Unlock the CloudLink Center after the upgrade process.

NOTE: It is recommended to set the CloudLink Vault to **Auto Unlock** mode before the upgrade begins.

Steps

1. Change the CloudLink Vault to Auto Unlock mode:
   a. Log in to CloudLink Center.
   b. Click **System** > **Vault**.
   c. In the **Vault** page, click **Actions** > **Change Mode**.
   d. In the **Confirm Unlock Mode Change** dialog box, when prompted to confirm the Auto Unlock mode change request, click **Change**.
2. Change the CloudLink Vault to Manual Unlock mode:
   a. Log in to CloudLink Center.
   b. Click **System** > **Vault**.

c. In the **Vault** page, click **Actions** > **Change Mode**.
d. In the **Confirm Unlock Mode Change** dialog box, when prompted with the confirm the Manual Unlock mode change request, click **Change**.

Upgrade CloudLink Agents manually

Use this task if you want to manually upgrade CloudLink Agents in a particular machine group.

Prerequisites

Ensure that your account has the **Update System** permission, which is required to upgrade CloudLink.

Steps

1. Set the **Machine Agent Upgrade** policy to **Manual** for the machine group that contains machines that have CloudLink Agents you want to upgrade manually.
2. Upgrade CloudLink Center to version 7.0.2 by following steps 1 through 6 in Upgrade CloudLink.
3. Log in to CloudLink Center.
4. Click **Agents** > **Machines**.
5. Select a machine in the list, and then click **Actions** > **Upgrade**. Repeat this step for every machine that requires a CloudLink Agent upgrade.

Upgrade CloudLink

Use this procedure to upgrade CloudLink.

Prerequisites

- Ensure that your account has the **Update System** permission, which is required to upgrade CloudLink.
- Set CloudLink Vault to **Auto Unlock** mode before the upgrade begins. This setting allows CloudLink Center to unlock immediately after the upgrade so that all CloudLink Agents can be upgraded. If CloudLink Vault is set to Manual Unlock mode before the upgrade, it remains in Manual Unlock mode after the upgrade and the vault is locked. You can change the vault back to Manual Unlock mode after the upgrade. See Change CloudLink Vault unlock modes for instructions.

Steps

1. Ensure that the CloudLink Vault is set to **Auto Unlock** mode.
2. Log in to CloudLink Center.
3. Click **System** > **Upgrade**.
4. Click **Upload**.
5. In the **Upload ISO** dialog box, click  to go to the upgrade ISO file, and then click **Upload**.
   If you are upgrading a CloudLink Center cluster, it can take several seconds for the ISO file to upload to all nodes in a cluster. Do not attempt to upload the ISO file again during this time.
   NOTE: If for any reason the ISO file is not automatically uploaded to all cluster nodes, manually upload the ISO file to each cluster node.
6. Click **Upgrade** to start the upgrade process.
7. In the **Confirm Host Upgrade** dialog box, click **Upgrade**.
   Your connection to CloudLink Center is lost during the upgrade process. You are returned to the login screen when the upgrade is complete.
8. Log in to CloudLink Center again when the upgrade is complete and perform the Postupgrade verification.

4

Postupgrade verification

Use this task to perform a postupgrade verification.

Prerequisites

Ensure that the upgrade to CloudLink 7.0.2 is completed successfully.

Steps

1. After the CloudLink Center upgrade completes, verify that all virtual machines are connected and stable in CloudLink Center.
   - CloudLink Agents on connected machines attempt to connect to CloudLink Center after the upgrade is complete.
   - If a machine is in a machine group that uses the **Auto** upgrade policy, the CloudLink Agent that is installed on that machine is automatically upgraded to version 7.0.2.
   - If a machine is in a machine group that uses the **Manual** upgrade policy, you must manually upgrade the Agent. See Upgrade CloudLink Agents manually.
2. Verify that all keystores are accessible by CloudLink Center.
3. On all Windows VMs, verify that CloudLink Agent is connected to CloudLink Center and running version 7.0.2.
4. On all Linux virtual machines:
   a. Use the `svm about` command to verify that the CloudLink Agent version appears as "Version 7.0.xxxx".
   b. Use the `svm status` command to verify that the volume encryption type is listed as **dmcrypt**, **ecryptfs**, or **LUKS** volume types in the third column. Those volumes are legacy Linux formats used by CloudLink version 5.0 and earlier, and are no longer supported.

      It is recommended that you contact Dell Technologies support to decrypt the **ecryptfs** or **LUKS** volumes and encrypt them using **dmcrypt**.

      NOTE: Key rotation is not available for **ecryptfs** volumes until they are decrypted and reencrypted.
5. In CloudLink Center, check if these alarms were triggered after the upgrade:
   - If the `Backup file wasn't downloaded/uploaded to store recently` alarm was triggered, download a backup of the new CloudLink 7.0.2.
   - If the `Vault unlock codes are not configured` alarm was triggered, set the CloudLink Vault passcodes as described in the *Dell EMC CloudLink Administration Guide*.
   - If `The keystore is not accessible` alarm was triggered, check the alarm for detailed information. This alarm is cleared when the keystore locations are accessible.
6. If you changed the CloudLink Vault unlock mode from **Manual Unlock** to **Auto Unlock** before the upgrade, change it back to **Manual Unlock**. For more information, see Change CloudLink Vault unlock modes.
7. Restart the VMs to ensure that their boot processes are unaffected by the upgrade.

5

Troubleshooting and getting help

Go to Dell Technologies Online Support and click **MyService360**. You will see several options for contacting Dell Technologies Technical Support. To open a service request, you must have a valid support agreement. Contact your Dell Technologies sales representative for details about obtaining a valid support agreement or with questions about your account.

Dell Technologies support, product, and licensing information can also be obtained from your Dell Technologies account manager.