# CONTENTS

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Introduction</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About this document</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Related documents</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Overview of CloudLink SecureVM</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Deployment Considerations</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CloudLink SecureVM components</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>CloudLink Center server address</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Requirements for CloudLink Center server addresses in clusters</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Pre-startup authorization</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Encryption keys</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Key release policies</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Machine groups</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Encryption key location and protector options</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Key location access control and backup recommendations</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>CloudLink Vault</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Machine IP addresses</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>CloudLink Center clusters</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Deployment scenario</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Deployment workflow</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>System requirements</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>CloudLink Center requirements</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Machine requirements</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Deploying and Configuring CloudLink Center</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Deploying and configuring CloudLink Center for VMware vSphere</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Deploying the CloudLink Center OVF template</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Configuring CloudLink Center</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Deploying and configuring CloudLink Center for Microsoft Hyper-V</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Deploying the CloudLink Center VHD template</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuring CloudLink Center</td>
<td>21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Preparing to Deploy SecureVM Agent</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Access CloudLink Center</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Accessing CloudLink Center</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Initial server configuration</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Configuring the CloudLink Center server</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Configure machine groups and volume encryption policy</td>
<td>25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Deploying CloudLink SecureVM Agent to Machines</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Standard SecureVM Agent deployment</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Downloading SecureVM Agent installer</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Running the installer</td>
<td>30</td>
</tr>
</tbody>
</table>
Chapter 6

Using the CloudLink Center Update Menu

Overview.................................................................................................... 38
Update Menu options................................................................................. 38
CHAPTER 1

Introduction

This chapter presents the following topics:

- About this document ............................................................................................ 6
- Related documents .............................................................................................. 6
- Overview of CloudLink SecureVM ........................................................................ 6
About this document

This guide describes how to deploy and configure Dell EMC™ CloudLink™ SecureVM™. It is intended for IT administrators who are responsible for the deployment and maintenance of machines in the CloudLink Center environment, but not necessarily for the security of data on those machines.

Related documents

The following Dell EMC publications provide additional information:

- CloudLink SecureVM Deployment Guide for Microsoft Azure
- CloudLink SecureVM Administration Guide for Enterprise
- CloudLink SecureVM Release Notes for Enterprise

Overview of CloudLink SecureVM

Cloud computing offers significant benefits for deployment flexibility, infrastructure scalability, and cost-effective use of IT resources. It makes sense to take advantage of these benefits and deploy enterprise workloads in the cloud. However, because cloud computing is based on a shared and multitenant compute, network, and storage architecture, traditional security controls are not sufficient. Data owners must secure sensitive data residing in the cloud to address requirements for privacy and regulatory compliance as well as for data that might remain in the cloud after it is no longer being used.

CloudLink SecureVM 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 SecureVM provides this encryption by using native operating system encryption features: Microsoft BitLocker for Windows or dm-crypt for Linux.

BitLocker and dm-crypt are proven high-performance volume encryption solutions that are widely implemented for physical machines. Before now, customers have not been able to use these solutions in the cloud, where you cannot use these native operating system encryption features alone to encrypt the boot volume. SecureVM is designed to solve this problem.

CloudLink SecureVM 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 against unauthorized modifications. CloudLink SecureVM 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 allows you define the security policy that the virtual machine must meet before passing pre-startup authorization, including verifying the integrity of the virtual machine’s boot chain. These security features protect against data tampering.

CloudLink SecureVM ensures that only trusted and verified virtual machines can run and access sensitive data stored in the cloud. As part of the CloudLink SecureVM solution, CloudLink Center defines the key release policy, performs pre-startup authorization, and monitors all SecureVM Agents, events, and logs.
CHAPTER 2
Deployment Considerations

This chapter presents the following topics:

- CloudLink SecureVM components ................................................................. 8
- CloudLink Center server address ................................................................. 8
- Pre-startup authorization ............................................................................. 8
- Encryption keys ......................................................................................... 9
- Key release policies .................................................................................... 9
- Machine groups ......................................................................................... 10
- Encryption key location and protector options ......................................... 11
- CloudLink Vault ......................................................................................... 12
- Machine IP addresses ................................................................................. 13
- CloudLink Center clusters ........................................................................ 13
- Deployment scenario ................................................................................ 14
- Deployment workflow ................................................................................ 14
- System requirements ............................................................................... 15
CloudLink SecureVM components

CloudLink SecureVM consists of:

- **CloudLink Center**—The web-based interface for CloudLink SecureVM that is used to manage machines that belong to the CloudLink SecureVM environment (those machines on which SecureVM Agent has been installed). CloudLink Center communicates with machines over Transport Layer Security (TLS). It manages the encryption keys used to secure the boot and data volumes for the machines, configures the security policies, monitors the security and operation events, and collects logs.

- **CloudLink SecureVM Agent**—The agent that runs on individual machines. It communicates with CloudLink Center for pre-startup authorization and decryption of BitLocker or dm-crypt encryption keys.

CloudLink Center is packaged as a virtual appliance that can be deployed in the enterprise on VMware ESXi or Microsoft Hyper-V. Download SecureVM Agent from CloudLink Center.

CloudLink Center server address

You use the CloudLink Center server address frequently. For example, you provide the address in the URL used to access the CloudLink Center user interface and in commands used to download installation files.

You can specify the CloudLink Center server address in one of the following formats:

**IP address (default)**

Ensure that a static IP address is used.

**Hostname**

If the Domain Name System (DNS) has an entry for CloudLink Center, Dell EMC recommends that you specify the CloudLink Center server address as a hostname (in fully qualified domain name (FQDN) format, such as clc.example.com). For more information, see *CloudLink SecureVM Administration Guide for Enterprise*.

Requirements for CloudLink Center server addresses in clusters

In a CloudLink Center cluster, servers and SecureVM Agents use the CloudLink Center server address for communication. You define this address, referred to as the *Server Name/Address*, when deploying a new server. You can use either the IP address or hostname (FQDN format).

Ensure that you specify the server address using the preferred format for each CloudLink Center server before creating the cluster. After creating a cluster, you cannot change the server address format.

Pre-startup authorization

Pre-startup authorization allows a machine to start automatically when the machine has been previously registered with CloudLink Center and is able to connect to it.
Note

If a machine's boot volume is not encrypted, but one or more data volumes are encrypted, the machine is allowed to start. After the machine starts, CloudLink Center determines whether encryption keys for encrypted data volumes can be released automatically based on key release policies. If key release policies are not met for the data volume, CloudLink Center puts the machine in the pending state.

If a machine does not pass pre-startup authorization, CloudLink Center puts the machine in the pending state and you must explicitly accept the machine before startup is allowed to continue.

For information about approved networks, removing or blocking a machine, and the pending state, see CloudLink SecureVM Administration Guide for Enterprise.

Encryption keys

CloudLink SecureVM uses the following types of encryption keys to secure machines:

- A volume key encryption key (VKEK) pair that is generated by CloudLink SecureVM. CloudLink SecureVM generates a VKEK for each volume.
- A volume encryption key that is used by native technologies in the machine’s operating system. A unique volume encryption key is generated for each encrypted volume.

These keys can be stored in CloudLink Center or another keystore. For more information, see Encryption key location and protector options on page 11.

For a machine, volume encryption keys secure the boot or data volumes as determined by the key release policy. For more information, see Key release policies on page 9. The VKEK key pair protects the volume encryption keys:

- When CloudLink Center receives a request from SecureVM Agent to encrypt a volume on its machine, CloudLink Center generates a new VKEK in the current keystore and uses it to encrypt the volume encryption key.
- When a volume requires decryption, CloudLink Center decrypts the volume encryption key using the VKEK and sends it to SecureVM Agent.

You must understand the difference between the types of encryption keys used to secure machines. Because volume encryption keys are created and managed by native technologies in machines’ operating systems, CloudLink SecureVM documentation does not discuss keys in detail. Unless specified otherwise, the terms encryption keys and keys in this documentation refer to VKEKs.

Key release policies

Before CloudLink Center automatically releases keys, a machine must:

- Meet key release policies
- Use an IP address that belongs to an approved network
- Not have been previously removed
- Not be in the blocked state

Key release policies may be required to allow:

- A machine to boot as part of the pre-startup authorization process
Access to encrypted data volumes

If a machine does not meet the policies, CloudLink Center puts the machine in the pending state. You must manually choose whether to allow the key release.

Key release policies are set for a machine group. For more information, see Machine groups on page 10.

The following key release policies are available.

**IP Change**
Determines whether CloudLink Center allows a machine to boot automatically when it starts up with an IP address that is different from the one recorded in the CloudLink Center database.
For virtual machines, this policy applies to boot or data volumes on machines with IP addresses that belong to an approved network.

**Machine Clone**
Determines whether CloudLink Center allows a cloned machine to boot automatically.
For virtual machines, this policy applies to boot or data volumes.

**Moved Volume**
Determines whether CloudLink Center allows keys to be released (if any exist) when it detects that a volume is now attached to a different machine than the one recorded in the CloudLink Center database.

**Platform Change**
Determines whether CloudLink Center allows a machine to boot automatically when it starts up with a different platform than the one recorded in the CloudLink Center database.
For virtual machines, this policy applies to boot or data volumes.

**Integrity Change**
Determines whether CloudLink Center allows a machine to boot automatically when it starts up with an integrity value that is different than the one recorded in the CloudLink Center database.
This policy applies only to boot volumes on virtual machines.

You can change these key release policies. For more details and information about approved networks, moved volumes, cloned machines, and the pending state, see CloudLink SecureVM Administration Guide for Enterprise.

### Machine groups

You can organize machines into groups for administrative or operational purposes. For example, you might group machines for your finance department and apply a volume encryption policy that requires encryption of all boot and data volumes. You might also group machines for your development and operations (DevOps) department and apply a volume encryption policy that requires encryption of only boot volumes. Each machine group might have a different administrator.

Each machine must belong to a machine group. A machine is assigned to a machine group during deployment. If you do not specify a group during deployment, the machine is assigned to the built-in machine group named **Default**. You can change the machine group that a machine belongs to after deployment.
All machines in a group use the same:

- Key release policies that determine when CloudLink Center automatically releases keys to a machine. For more information, see Key release policies on page 9.
- Volume encryption policy that determines the types of volumes that must be encrypted (boot, data, or both boot and data). Volume encryption policy applies to virtual machines (boot and data volumes).
- Keystore where encryption keys are stored. For more information, see Encryption key location and protector options on page 11.
- Only users belonging to a managing role for a machine group can view, make changes, and perform operations on the machines belonging to it.
- Approved networks from which machines in the machine group can start up automatically.
- Approved location used to verify a machine is in the correct place.
- Key lifetime that determines how frequently and at what intervals CloudLink Center updates encryption keys for machines in the group.

For information about machine groups, volume encryption policy, managing roles, approved networks, and key lifetimes, see CloudLink SecureVM Administration Guide for Enterprise.

Encryption key location and protector options

Keystores
The term keystore refers to the combination of a key location and a key protector.

Key locations
Encryption keys are stored in a key location and protected by a key protector. CloudLink Center supports several options for the key location:

Local database
An internal key location

Microsoft Active Directory
An external key location

Amazon S3
An external key location. Ensure you have an Amazon Web Services (AWS) account.

Key protectors
Encryption keys are encrypted, or protected, by a key protector. CloudLink Center supports several options for key protectors.

CloudLink Vault
An internal key protector.

SafeNet LunaSA
An external key protector using a hardware security module (HSM) for protection.

Note
The type of available key protector depends on the selected key location.
Microsoft Azure Key Vault
An external key protector using an Azure Key Vault key for external protection.

KMIP server
An external key protector using a Key Management Interoperability Protocol (KMIP) server for protection.

Password
The encryption key is protected using a password.

Key location access control and backup recommendations

You are responsible for your encryption keys and for ensuring that the appropriate access control and backup policies and procedures are in place to protect the keys against loss or theft. If your keys become unavailable, you cannot access any data that was encrypted using those keys.

CloudLink Center backups are critical for restoring CloudLink Center. It is important to have a backup of CloudLink Center so that you can deploy a new server and restore CloudLink Center. If you are using the local database, volume encryption keys are stored in CloudLink Center. Backups are the only method of restoring keys so that you can access encrypted data. For information about VKEKs and volume encryption keys, see CloudLink SecureVM Administration Guide for Enterprise.

The following table identifies which key protectors are available for each type of key location.

Table 1 Key location and key protector options

<table>
<thead>
<tr>
<th>Key protector</th>
<th>Local database</th>
<th>Microsoft Active Directory</th>
<th>Amazon S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudLink Vault</td>
<td>Yes</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>SafeNet LunaSA</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Azure Key Vault</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMIP key manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Password</td>
<td>Not allowed</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note
Ensure that you meet all prerequisites for restoring CloudLink Center from backup; otherwise you cannot access encrypted data after restoring from a backup file.

For more information about CloudLink Center backups and restoring from a backup file, see CloudLink SecureVM Administration Guide for Enterprise.

CloudLink Vault

CloudLink Center includes an encrypted container, CloudLink Vault, that is created during the deployment and configuration of CloudLink SecureVM. CloudLink Vault:

- Encrypts credentials used to access remote resources
For example, CloudLink Vault stores credentials required to access FTP or SFTP servers or external keystores.

- Provides an initial, internal key protector

  You can continue to use this initial CloudLink Vault as the key protector or configure a different key protector. When used as the key protector, CloudLink Vault encrypts volume key encryption keys (VKEKs). For more information, see the CloudLink SecureVM Administration Guide for Enterprise.

When a CloudLink Center server restarts, it must unlock CloudLink Vault before CloudLink Center can authorize machine operations, ensuring that a stolen copy of CloudLink Vault or the disk on which it is stored does not contain any unprotected secrets or encryption keys.

You can configure CloudLink Vault to open:

- Manually by providing a passcode. When configuring CloudLink Vault, you specify up to three passcodes. Only one passcode is required to open the vault.
- Automatically by using a server-specific key.

Dell EMC recommends that you set CloudLink Vault to unlock manually.

**Machine IP addresses**

In some circumstances, the IP address of a machine under CloudLink Center management might change, such as when a Dynamic Host Configuration Protocol (DHCP) server assigns IP addresses. When a machine starts up with a changed IP address, CloudLink Center might put the machine in the pending state. Before startup can continue, you must manually accept the machine. For more information about accepting machines in the pending state, see the CloudLink SecureVM Administration Guide for Enterprise.

To avoid the need to manually accept machines in the pending state because of changed IP addresses, you can:

- Change the key release policies for the machine group to allow CloudLink Center to release keys to machines starting up with changed IP addresses. For information, see Key release policies on page 9.

**CloudLink Center clusters**

A CloudLink Center cluster provides for high availability if one CloudLink Center server in the cluster becomes unavailable, whether due to planned maintenance or an unexpected issue.

A CloudLink Center cluster consists of up to four CloudLink Center servers, where each server is active at all times. There is no master server. The agents can be actively connected to any server in the cluster.

CloudLink Center replicates configuration information between all servers in a cluster. This replication means that all servers contain the same critical configuration information: CloudLink SecureVM licenses, volume encryption policy, user accounts, manual passcodes for unlocking CloudLink Vault, actions, alarms, and security events.

For information about creating a CloudLink Center server cluster, see the CloudLink SecureVM Administration Guide for Enterprise.
Deployment scenario

This guide assumes that CloudLink Center and the encryption keystore are deployed in the private cloud, as shown in the figure below, or in VMware vCloud Air. SecureVM Agent is deployed to individual virtual machines hosted in the private cloud or to virtual machine instances in a supported public or hybrid cloud environment.

When deployed, SecureVM Agent replicates the machine networking configuration as needed, to ensure that it can communicate with CloudLink Center during the startup process. This replication to the preboot environment includes the IP configuration for available network interfaces and any static routing information. For Linux machines, if the networking configuration is changed after deployment, you must refresh the SecureVM Agent service. For more information, see Refreshing the SecureVM Agent service on Linux machines on page 35.

Figure 1 CloudLink deployment scenario

Deployment workflow

The CloudLink SecureVM workflow is as follows:
- Deploy CloudLink Center, as described in Deploying and Configuring CloudLink Center on page 17.
- Prepare to deploy SecureVM Agent to machines, as described in Preparing to Deploy SecureVM Agent on page 23.
- Deploy SecureVM Agent to machines, as described in Deploying CloudLink SecureVM Agent to Machines on page 27.

Encryption (if any) based on the selected volume encryption policy for the machine group begins automatically after you deploy SecureVM Agent to machines. For more information about the volume encryption policy, see CloudLink SecureVM Administration Guide for Enterprise.

### System requirements

This section describes the system requirements for CloudLink Center and for the machines to which SecureVM Agent will be deployed. You must meet these requirements before deployment.

#### CloudLink Center requirements

The system requirements for CloudLink Center are:

- For VMware deployments:
  - vSphere 5.1 or later
- For Microsoft Hyper-V deployments:
  - Hyper-V for Windows Server 2008 or Windows Server 2012
  - 4 GB (minimum) dynamic memory (if used)
- 2 vCPU for up to 500 machines or 4 vCPU for 500 or more machines
- 4 GB vRAM
- Web browser—Google Chrome 38 or higher or Mozilla Firefox 28 or higher

TLS v1.2 must be enabled in your browser settings to connect to CloudLink Center. Some web browsers (such as Google Chrome 30 or higher and Mozilla Firefox 27 or higher) enable this option by default.

The following table lists the network ports used by CloudLink SecureVM for various services.

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Yes</td>
<td></td>
<td>SecureVM Agent download and cluster communication</td>
</tr>
<tr>
<td>443</td>
<td>Yes</td>
<td></td>
<td>CloudLink Center web access and cluster communication</td>
</tr>
<tr>
<td>1194</td>
<td>Yes</td>
<td>Yes</td>
<td>SecureVM Agent communication</td>
</tr>
</tbody>
</table>
### Table 2 CloudLink SecureVM network ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>5696</td>
<td>Yes</td>
<td></td>
<td>Key Management Interoperability Protocol (KMIP)</td>
</tr>
<tr>
<td>8080</td>
<td>Yes</td>
<td></td>
<td>SecureVM Agent download (legacy use)</td>
</tr>
<tr>
<td>8443</td>
<td>Yes</td>
<td></td>
<td>CloudLink Center web access (legacy use)</td>
</tr>
</tbody>
</table>

**Outgoing**

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td></td>
<td>Yes</td>
<td>Network Time Protocol (NTP)</td>
</tr>
<tr>
<td>389</td>
<td>Yes</td>
<td></td>
<td>Microsoft Windows domain integration and Microsoft Active Directory keystore</td>
</tr>
<tr>
<td>443</td>
<td>Yes</td>
<td></td>
<td>External keystores other than Microsoft Active Directory</td>
</tr>
<tr>
<td>464</td>
<td>Yes</td>
<td>Yes</td>
<td>Microsoft Windows domain integration</td>
</tr>
<tr>
<td>514</td>
<td></td>
<td>Yes</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

### Machine requirements

For information about currently supported platforms, see *CloudLink SecureVM Release Notes*. 
CHAPTER 3

Deploying and Configuring CloudLink Center

This chapter presents the following topics:

- Overview ...................................................................................................................... 18
- Deploying and configuring CloudLink Center for VMware vSphere .................... 18
- Deploying and configuring CloudLink Center for Microsoft Hyper-V ............... 20
Overview

This chapter provides instructions for deploying and configuring CloudLink Center on VMware vSphere and Microsoft Hyper-V.

Before deploying CloudLink Center, ensure that you are familiar with all the deployment considerations, including system requirements. For more information, see Deployment Considerations on page 7.

Deploying and configuring CloudLink Center for VMware vSphere

CloudLink SecureVM uses one interface to enable CloudLink Center to communicate with the SecureVM Agent that is installed on individual machines. This interface is supported through a virtual network interface that is included in the Open Virtualization Format (OVF) template used to deploy CloudLink Center. The interface is configured as part of the CloudLink Center configuration process.

Deploying CloudLink Center includes deploying the OVF template and configuring CloudLink Center, as described in the following sections.

Deploying the CloudLink Center OVF template

This procedure assumes that you have obtained the CloudLink Center Open Virtualization Format (OVF) template used for deployment.

Procedure

1. From vSphere Client, select File > Deploy OVF Template.
2. From the Deploy OVF Template window, go to the template folder, select the CloudLink Center template, and click Next.
3. Verify that the OVF template details are correct and click Next.
4. Type a name, select an inventory location for the deployed template, and click Next.
5. Select a host or cluster to run the deployed template and click Next.
6. If a series of warnings is displayed, click Yes to continue with the deployment.
7. Select a resource pool and click Next.
8. Select a storage location for the machine files and click Next.
9. Select the disk format for the virtual disk and click Next.
10. Select a destination network and click Next.
11. In the Deployment Settings panel, review the selected options and click Finish.
12. When you see the Deployment Completed Successfully dialog box, click Close.

Results

The CloudLink Center virtual machine is displayed in the VMware vSphere virtual machine list.
Configuring CloudLink Center

The CloudLink Center virtual machine defaults to Dynamic Host Configuration Protocol (DHCP) and generates a random hostname for CloudLink Center if a DHCP server is available on your network. You are prompted to set static network values if a DHCP server is not available. Use the Update Menu in the CloudLink Center console to change the network or hostname settings. See Update Menu options on page 38 for more information.

Procedure

1. From vSphere Client, right-click CloudLink Center and select Power on.

   **Note**

   Wait until vSphere Client reports that VMware Tools is installed and running before you log in to the CloudLink Center console. Otherwise you might experience network configuration problems.

2. Right-click CloudLink Center and select Open Console.
3. Log in to the CloudLink Center console with the login name cloudlink and the default password cloudlink.

   You are required to change the default password.
4. When prompted, type a new password for the CloudLink Center console.
5. Press down arrow and enter the password again to confirm it.
6. Press Tab and then Enter to accept the password change.

   Subsequent logins to the console prompt for the new password, which you can change at any time from the Update Menu in the CloudLink Center console. For more information, see Using the CloudLink Center Update Menu on page 37.
7. Wait for the configuration to complete.

   This process might take some time.

Results

After the CloudLink Center configuration process is complete, a summary of its settings is displayed, as shown in the following figure. These settings include the URL to access CloudLink Center from a web browser and the default secadmin password for logging in to CloudLink Center for the first time.
Deploying and configuring CloudLink Center for Microsoft Hyper-V

CloudLink SecureVM uses one network interface to allow CloudLink Center to communicate with the SecureVM Agent that is installed on a machine. This interface is supported through a virtual network interface that is included in the virtual hard disk (VHD) template used to deploy CloudLink Center for Microsoft Hyper-V. The interface is configured as part of the CloudLink Center configuration process. SecureVM Agent configures this CloudLink Center network interface server address for authorization purposes.

Deploying CloudLink Center for Microsoft Hyper-V involves deploying the VHD template and configuring CloudLink Center, as described in the following sections.

Deploying the CloudLink Center VHD template

This procedure assumes that you have obtained the CloudLink Center VHD template used for deployment.

Procedure

1. From the Hyper-V Manager, create a CloudLink Center machine by selecting Actions > New > Virtual Machine.
2. Type a name for the virtual machine.
3. Adjust the assigned memory if necessary. Four gigabytes is the recommended amount.
4. Select the **Generation 1** option if it is available.
   This option specifies the generation of virtual machine used and depends on the version of Windows Server that you are using.
5. Select a network to connect to CloudLink Center or leave the **Not Connected** option selected.
   You can connect to the network later.
6. Connect a virtual hard disk by selecting **Use an existing virtual hard disk**, browsing to the copy of the CloudLink Center VHD file, and then clicking **Open**.
   Do not open the master VHD file.
7. Review the configuration and click **Finish**.
8. In the Hyper-V Manager, choose **Settings** and define the network.
9. In the Hyper-V Manager, review your **Hardware** settings for CloudLink Center.
10. Start CloudLink Center.

**Configuring CloudLink Center**

The CloudLink Center virtual machine defaults to Dynamic Host Configuration Protocol (DHCP) and generates a random hostname for CloudLink Center if a DHCP server is available on your network. You are prompted to set static network values if a DHCP server is not available. Use the **Update Menu** in the CloudLink Center console to change the network or hostname settings. See **Update Menu options** on page 38 for more information.

**Procedure**

1. From Hyper-V Manager, right-click CloudLink Center and select **Start**.
2. If the screen is blank, press Alt+F1 to open a new console window.
3. Click **Connect**.
4. Log in to the CloudLink Center console with the login name `cloudlink` and the default password `cloudlink`.
   You are required to change the default password.
5. When prompted, type a new password for the CloudLink Center console.
6. Press **down arrow** and enter the password again to confirm it.
7. Press **Tab** and then **Enter** to accept the password change.
   Subsequent logins to the console prompt for the new password, which you can change at any time from the Update Menu in the CloudLink Center console. For more information about the Update Menu, see **Using the CloudLink Center Update Menu** on page 37.
8. Wait for the configuration to complete.
   This process might take some time.
Results

After the CloudLink Center configuration process is complete, a summary of the settings is displayed, as shown in the following figure. These settings include the URL to access CloudLink Center from a web browser and the default secadmin password for logging in to CloudLink Center for the first time.

Figure 3 CloudLink Center Summary screen for Microsoft Hyper-V

The Update Menu is displayed after you have configured CloudLink Center and every time you log in to the CloudLink Center console. For more information, see Using the CloudLink Center Update Menu on page 37.
CHAPTER 4

Preparing to Deploy SecureVM Agent

This chapter presents the following topics:

- **Overview** .................................................................................................................. 24
- **Access CloudLink Center** .......................................................................................... 24
- **Initial server configuration** ......................................................................................... 24
- **Configure machine groups and volume encryption policy** ..................................... 25
Overview

After deploying and configuring CloudLink Center, prepare to deploy SecureVM Agent to machines by accessing CloudLink Center and setting up CloudLink SecureVM licenses.

Access CloudLink Center

With CloudLink Center deployed, use a web browser to connect to it and log in. Access CloudLink Center from an HTTPS session using a web browser with JavaScript enabled.

You need the following to log in:

- URL for CloudLink Center—The URL is available from the Summary in the Update Menu. For information, see Using the CloudLink Center Update Menu on page 37.

- Password for the secadmin user account—The first time that you log in to CloudLink Center, you are prompted for the default password, and then prompted to change it.
  The default password is available from the Summary in the Update Menu. For more information, see Using the CloudLink Center Update Menu on page 37.

You can change the password for the secadmin user account at any time after the first-time login. For more information, see CloudLink SecureVM Administration Guide for Enterprise.

Dell EMC recommends that you configure Microsoft Windows domain integration so that you can access CloudLink Center with Windows domain credentials. In this case, you do not provide CloudLink Center credentials. The secadmin user account remains a local account. For information about user accounts and configuring Microsoft Windows domain integration, see CloudLink SecureVM Administration Guide for Enterprise.

Accessing CloudLink Center

Procedure

1. In your web browser, type the URL for CloudLink Center in the following format: https://clc_address
   where clc_address represents the CloudLink Center server address. For more information, see CloudLink Center server address on page 8.

2. Type the username secadmin and the default password, and click Login.

3. Type the new password, retype it to confirm, and click Change Password.

Initial server configuration

Configure the server the first time you log in to CloudLink Center by doing the following:

- Accepting or changing the CloudLink Center hostname
• Uploading a CloudLink SecureVM license file

CloudLink SecureVM license files determine the number of machine instances or amount of encrypted storage capacity that your organization can manage with CloudLink Center, and the duration of the license. During initial configuration, you must upload one license. You can upload additional licenses after the initial deployment. For information about CloudLink SecureVM license files, see CloudLink SecureVM Administration Guide for Enterprise.

• Specifying the cluster server name of the server

This information is used primarily for CloudLink Center clusters, but must be specified even if you do not plan to use clusters. For more information, see Requirements for CloudLink Center server addresses in clusters on page 8.

• Generating the RSA-2048 backup key pair and downloading the private key

The public key is saved in CloudLink Center.

• Configuring how CloudLink Center opens the CloudLink Vault on restarts

Dell EMC recommends that you use Manual Unlock mode, which opens CloudLink Vault only when an administrator provides an appropriate passcode. For more information, see CloudLink Vault on page 12.

Configuring the CloudLink Center server

To configure the server:

Procedure

1. From the Deployment Type list, select New Server, and click Next.
2. Accept or change the CloudLink Center hostname.
3. Select the license file and click Upload
   You can browse to the license file.
4. In the Cluster Server Name/Address box, type the DNS name or IP address used to connect to this server.
   For more information, see CloudLink Center server address on page 8.
5. Click Next.
6. Click Generate and Download.
7. Save the private key to an appropriate location.
   By default, the private key is saved to your web browser’s download folder.
8. Click Next.
9. Click I Acknowledge.
10. Select Manual Unlock or Auto Unlock.
11. Enter and confirm at least one passcode.
12. Click Set Codes.

Configure machine groups and volume encryption policy

Before deploying SecureVM Agent to machines, you may want to set up machine groups and their volume encryption policy. For more information, see Machine groups on page 10.
CloudLink Center assigns machines to an existing machine group during SecureVM Agent deployment. Creating machine groups before starting to deploy SecureVM Agent to machines lets you assign a machine to the appropriate group during deployment. The benefit is that, on registration of the machine, encryption begins automatically based on the volume encryption policy for the machine group.

If you do not specify an existing machine group during deployment, CloudLink Center assigns the machine to the Default group. By default, this group uses the Manual volume encryption policy, which does not require encryption of any type of volume on machines in the group.

You can move machines to other groups after deployment. Depending on the volume encryption policy for the original and new group, you may need to manually encrypt volumes so that the machine complies with the new group’s volume encryption policy.

For more information about creating machine groups and defining volume encryption policy, see CloudLink SecureVM Administration Guide for Enterprise.
CHAPTER 5

Deploying CloudLink SecureVM Agent to Machines

This chapter presents the following topics:

- Overview ................................................................. 28
- Standard SecureVM Agent deployment ..................... 29
- Custom SecureVM Agent deployment for Windows .......... 31
- SecureVM Agent for Microsoft SQL Server .................. 33
- Custom SecureVM Agent deployment for Linux ............. 34
- Verifying deployment ............................................... 35
- Refreshing the SecureVM Agent service on Linux machines 35
- Uninstalling SecureVM Agent ..................................... 35
Overview

You can deploy SecureVM Agent using a standard or custom installation.

- The standard installation is an automated method that requires minimal intervention by you.
  
  It is useful for deploying SecureVM Agent to machines on an individual basis.

- The custom installation requires more intervention by you, but it provides more flexibility for deployment. Unlike the standard installation, the custom installation does not automatically register the machine with CloudLink Center.

  A custom installation is useful for the following purposes:
  - Deploying SecureVM Agent to machines before deploying CloudLink Center
  - Deploying SecureVM Agent with configuration management tools

Choose either the standard or custom installation based on the level of automation or points of manual intervention you require. At a high level, deployment includes the following processes:

1. The machine might automatically restart several times to install and configure BitLocker or dm-crypt, and to create a system reserve or boot volume.
2. The machine is registered with CloudLink Center.
3. Encryption (if any) begins based on the volume encryption policy for the specified machine group.

For more information about the pending state and volume encryption policy, see CloudLink SecureVM Administration Guide for Enterprise.

The table below describes the deployment processes for each type of installation and for each operating system. This table is intended to help you determine the appropriate installation based on your deployment requirements.

Table 3 Deployment processes

<table>
<thead>
<tr>
<th>Installation type</th>
<th>SecureVM Agent for Windows</th>
<th>SecureVM Agent for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard installation</td>
<td>Download the online installer. Run the installer to complete installation and configuration.</td>
<td>Download the online installer. Run the installer to complete installation and configuration.</td>
</tr>
<tr>
<td>Custom installation</td>
<td>Download the installer package. Install the package.</td>
<td>Download the operating-system-specific deployment package. Install the package. Configure the CloudLink Center server address.</td>
</tr>
</tbody>
</table>
### Standard SecureVM Agent deployment

Standard SecureVM Agent deployment to Windows or Linux machines involves the following tasks:

- Downloading the installer using the CloudLink Center interface or directly from the server
- Running the installer from the command line to complete installation and configuration

### Downloading SecureVM Agent installer

Download the SecureVM Agent installer from CloudLink Center. For Windows, the installer is provided in the Windows installer script `securevm.bat`. For Linux, the installer is provided in the Linux installer script `securevm.sh`.

You can download the installer in one of the following ways:

- Log in to CloudLink Center and download the installer using the CloudLink Center user interface
- Download the installer from the CloudLink Center server without logging in
- Download the installer using a command line interface

If you are not responsible for completing the installation, provide the downloaded software to the appropriate person.

### CloudLink Center user interface

**Procedure**

1. Log in to CloudLink Center. For more information, see Access CloudLink Center on page 24.
2. From SecureVM, select Agent Download.
3. From the Downloads page, select the Windows installer script or Linux installer script and click Download Selected.
4. Click **Save File**.

**Results**
The installer is downloaded to your download folder.

**Direct from CloudLink Center**

**Procedure**
1. In a web browser, type the following:
   
   ```
   https://clc_address:8080/cloudlink/securevm
   ```
   
   where `clc_address` is the CloudLink Center server address. For more information, see **CloudLink Center server address** on page 8.

2. Click **Save File**.
   
   For Linux, use the file name `securevm.sh`.

**Results**
The installer is downloaded to your download folder.

**Use the command line**

**Procedure**
1. Open a command line client such as PowerShell, wget or curl.
2. Type the following when specifying the installer location.

   ```
   http://clc_address:8080/cloudlink/securevm
   ```
   
   where `clc_address` is the CloudLink Center server address. For more information, see **CloudLink Center server address** on page 8.

**Results**
The installer is downloaded to your download folder.

**Running the installer**

**Before you begin**

After downloading the SecureVM Agent installer from CloudLink Center, run it from the command line, providing the:

- CloudLink Center server address
- Registration code for the machine group to which you want to assign this machine (optional). For more information, see **Machine groups** on page 10. The registration code is available from CloudLink Center on the SecureVM > **Machine Groups** page. For more information, see *CloudLink SecureVM Administration Guide for Enterprise*.

   If you do not provide a registration code, CloudLink Center assigns the machine to the Default machine group.

**Windows**

On Windows virtual machines, SecureVM Agent automatically moves the page file to the boot drive when it is installed.
Dell EMC recommends not moving the page file to an encrypted data drive after SecureVM Agent is installed. Otherwise, Windows uses a temporary page file and is unable to create administrative network shares.

**Procedure**

1. In a command window, go to the folder where you downloaded the SecureVM Agent installer.
   By default, the installer is downloaded to your download folder.
2. Type the following from the command line: `securevm.bat /S clc_address [/g group_code]`
   where
   `/S clc_address` specifies the CloudLink Center server address. For more information, see CloudLink Center server address on page 8.
   `/g group_code` specifies the registration code for the machine group to which you want to assign this machine.

**Linux**

**Procedure**

1. In the command line on the machine, type the following command to run the installer for a Linux machine in the location where the installer was downloaded (by default, to the current folder): `sudo sh securevm -S clc_address [-G group_code]`
   where
   `-S clc_address` specifies the CloudLink Center server address. For more information, see CloudLink Center server address on page 8.
   `-G group_code` specifies the registration code for the machine group to which you want to assign this machine.

**Custom SecureVM Agent deployment for Windows**

Custom SecureVM Agent deployment to Windows machines involves the following tasks:
- Downloading the SecureVM Agent installer
- Running the installer from the command line to complete installation and configuration

**Downloading the SecureVM Agent installer package**

To download the SecureVM Agent installer package for Windows:

**Procedure**

1. Log in to CloudLink Center.
2. From SecureVM, select Agent Download.
3. From the Downloads page, select the 64-bit Windows Installer package (securevm-windows-x64.msi) and click Download Selected.
4. Click **Save File**.
   
   The installer package is downloaded to your Downloads directory.

### Running the SecureVM Agent installer package

After downloading the SecureVM Agent installer package (the `securevm-windows-x64.msi` file) from CloudLink Center, you can run it from the command line or by using Windows Installer tools.

To run the SecureVM Agent installer package:

**Procedure**

1. Go to the folder where the SecureVM Agent installer package is located.
2. From the command line, type the following:

   ```
   msiexec /i securevm-windows-x64.msi
   [CLOUDLINKCENTER=clc_address]
   [GROUPCODE=group_code]
   ```

   where

   - `CLOUDLINKCENTER=clc_address` specifies the CloudLink Center server address. For more information, see CloudLink Center server address on page 8. If you do not specify the CloudLink Center server address, the machine is not registered with CloudLink Center. No automatic encryption occurs after deployment. For information about specifying this address following deployment, see #unique_54.
   
   - `GROUPCODE=group_code` specifies the registration code for the machine group to which you want to assign the machine. If you do not specify a registration code, CloudLink Center assigns the machine to the Default machine group. For more information, see Machine groups on page 10.

   You obtain the machine group registration code from CloudLink Center. The code is displayed on the **SecureVM > Machine Groups** page. For more information, see CloudLink SecureVM Administration Guide for Enterprise.

3. When the SecureVM Setup wizard is displayed, click **Install**.
4. When the wizard completes, click **Finish**.
5. Wait for the installation to complete.
   
   The machine automatically restarts one or more times.

### Adding the CloudLink Center server address or group registration code after deployment

As a deployment option, you might want to omit the CloudLink Center server address when running the MSI file from the command line. Similarly, you might not have access to the group registration code needed to assign a machine to a machine group other than Default. For more information, see Running the SecureVM Agent installer package on page 32.

You can add the CloudLink Center server address or group registration code in the Windows Registry at a later time. If you want the machine to join a group, ensure that you specify the group’s registration code before specifying the server address.

To add SecureVM Agent configuration entries to the Windows Registry:
Procedure

1. On the machine, from a command prompt window, type `regedit`.
2. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\CloudLink Technologies Inc\SecureVM`
3. If you want to add the CloudLink Server address, set the `Server` registry value (`REG_SZ`) to the CloudLink Center server address (for example, 203.0.113.1 or clc.example.com).
4. If you want to add the group registration code, set the `Group` registry value (`REG_SZ`) to the registration code for the machine group.

Save and close the registry.

Results

SecureVM Agent automatically obtains the CloudLink Center server address from the Windows Registry and registers.

SecureVM Agent for Microsoft SQL Server

If SecureVM Agent is installed on a Windows Server running Microsoft SQL Server and the data drive is encrypted, SQL Server cannot load database files because the data is encrypted.

You can set the SQL Server service to start after the data drive is decrypted. SecureVM Agent can start the SQL Server service manually after the data drive is decrypted. After SecureVM Agent receives the decryption key, it decrypts the data drive and starts any SQL Server services that are dependent on CloudLink SecureVM.

When SecureVM Agent is uninstalled, all dependent services revert to their previous state.

Setting Microsoft SQL Server dependencies

Run the following commands in PowerShell to make the SQL Server service dependent on or independent of SecureVM Agent, and to encrypt or decrypt the SQL Server data drive as necessary.

<table>
<thead>
<tr>
<th>Action</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show the volume encryption status</td>
<td><code>svm status</code></td>
</tr>
<tr>
<td>Encrypt [volume letter]</td>
<td><code>svm encrypt [volume letter]</code></td>
</tr>
<tr>
<td>Decrypt [volume letter]</td>
<td><code>svm decrypt [volume letter]</code></td>
</tr>
</tbody>
</table>
| Set the SQL Server service to be dependent on CloudLink SecureVM | `svm setdeps <Microsoft SQL Server service name>`  
Example:  
`svm setdeps MSSQLServer` |
| Show the list of services that are dependent on CloudLink SecureVM | `svm showdeps` |
| Remove the SQL Server service from the CloudLink SecureVM dependency list | `svm cleardeps <Microsoft SQL Server service name>` |
## Custom SecureVM Agent deployment for Linux

Deploying SecureVM Agent using the custom installation involves the following tasks:

- Downloading the SecureVM Agent deployment package
- Installing the SecureVM Agent deployment package
- Configuring SecureVM Agent

### Downloading the SecureVM Agent deployment package for Linux

SecureVM Agent deployment packages are available as DEB or RPM files that you download from CloudLink Center to the current folder.

To download the SecureVM Agent deployment package:

**Procedure**

1. Log in to CloudLink Center.
2. From SecureVM, select Agent Download.
3. From the Downloads page, select the deployment package you want to use and click Download Selected.
4. Select Save File.
   
   The deployment package is downloaded to the current folder.

### Installing the SecureVM Agent deployment package

After downloading the deployment package for your operating system from CloudLink Center, install the package using the package manager for your platform.

### Configuring SecureVM Agent

The deployment package installation installs the SecureVM Agent, which provides the `svm` subcommand for configuring SecureVM Agent. During configuration, the machine is registered with CloudLink Center.

To install SecureVM Agent:

**Procedure**

1. Type the following command:

   ```
   svm [-v ] [-G group_code]-S clc_address
   ```

   where

   - `-v` uses verbose mode.
-G group_code specifies the registration code for the machine group that you want to assign this machine to.

-S clc_address specifies the CloudLink Center server address. For more information, see CloudLink Center server address on page 8.

2. Restart the machine.

Verifying deployment

Confirm that SecureVM Agent has been deployed by logging in to CloudLink Center and viewing the machine status. For information about managing machines, including viewing their status, see CloudLink SecureVM Administration Guide for Enterprise.

You can also confirm deployment from the machine as described in the following sections.

Windows machines

Confirm that SecureVM Agent has successfully installed using the SecureVM Agent Shield icon in the Windows taskbar, as shown in the figure below. The tooltip displays a message indicating that the machine is connected.

Figure 4 SecureVM Agent Shield icon

Linux machines

Confirm deployment from the machine command line and encryption status of volumes by typing the following command:

```
svm status
```

Refreshing the SecureVM Agent service on Linux machines

For Linux machines, if the networking configuration is changed on the client after SecureVM Agent deployment, refresh the SecureVM Agent service.

Refresh the SecureVM Agent service from the machine command line by typing the following command:

```
svm refresh
```

Uninstalling SecureVM Agent

You might need to uninstall SecureVM Agent, such as when you put a machine under management of a different CloudLink Center. For more information about moving a
machine to a different CloudLink Center, see *CloudLink Center Administration Guide for Enterprise*.

**Uninstalling SecureVM Agent for Windows**

**Procedure**

1. Decrypt any encrypted volumes on the machine.
2. Use the Windows tool for uninstalling applications.

**Uninstalling SecureVM Agent for Linux**

**Procedure**

1. Decrypt any encrypted volumes on the machine.
2. Type the following command:

   ```
   svm uninstall
   ```

CHAPTER 6

Using the CloudLink Center Update Menu

This chapter presents the following topics:

- Overview.............................................................................................................38
- Update Menu options..........................................................................................38
Overview

After you have configured CloudLink Center, the Update Menu is displayed every time you log in using the CloudLink Center console, as shown in the figure below.

Figure 5 CloudLink Center Update Menu

Update Menu options

The Update Menu options are:

- **Summary**—Displays a summary of CloudLink Center settings.
- **Password**—Changes the current password used to log in to the CloudLink Center console.
- **Network**—Resets the network settings, after which you can reconfigure them. If you select this option, all current network settings are removed.
- **Routes**—Intended only for use as directed by your Dell EMC representative.
- **Unlock User**—Unlocks the secadmin user account.
- **Diagnostics**—Intended only for use as directed by your Dell EMC representative.