Quick Start Guide

Dell EMC VxFlex OS

CloudLink for SDS Devices

P/N 302-002-975
REV 04
June 2018

Quick start and best practice guide for using CloudLink 5.5 D@RE for SDS devices with VxFlex OS. Topics include:

- About this document 2
- Before you begin 2
- Download and install the Linux agent 2
- Add a new approved VxFlex OS network to CloudLink 5
- Adding a new machine group 5
- Encrypt devices 6
- Add encrypted devices to an SDS 8
- Disabling encryption and removing encrypted devices from an SDS 8

DELL EMC

About this document

This document provides a quick start to deploying the software-based CloudLink D@RE solution for VxFlex OS SDS devices in Linux-based physical machines, as well as deployments on virtual machines (specifically, the SVM in a VxFlex OS ESX deployment).

A complete explanation for CloudLink deployment and administration can be found in the documents *CloudLink SecureVM Administration Guide for VxFlex OS* and *CloudLink SecureVM Deployment Guide for VxFlex OS*.

Before you begin

This section describes what you should do before starting to use the CloudLink interface for SDS with VxFlex OS system.

- Read this document in its entirety.
- Ensure that the CloudLink Center is deployed and configured as described in *CloudLink SecureVM Deployment Guide for VxFlex OS*.
- Ensure that there is connectivity between the VxFlex OS system and the CloudLink Center.
- Ensure that you know the CloudLink Center login credentials and IP address.

The following concepts are critical to understand before beginning:

- Devices that are physically installed in a server may (or may not) be part of the VxFlex OS system. In this document, “adding a device” means adding a device to the VxFlex OS system using one of the VxFlex OS management interfaces such as the CLI, the GUI, or the REST API.
- VxFlex OS Devices that have already been added to a VxFlex OS SDS cannot be encrypted by CloudLink until they are first removed from the SDS. Such removal will cause the device's data to be removed and rebalanced to spare capacity. Once all data is removed, the device can be encrypted. Device encryption must be applied prior to adding a device to the SDS.

Process overview:

1. Download and install the Linux agent.
2. Add a VxFlex OS approved network to CloudLink.
3. Add IP addresses to the approved network.
4. Create a Machines group and add SDSs to the group.
5. Encrypt devices, and determine the path of the encrypted devices.
6. Use VxFlex OS to add the encrypted devices to the SDSs.

Download and install the Linux agent

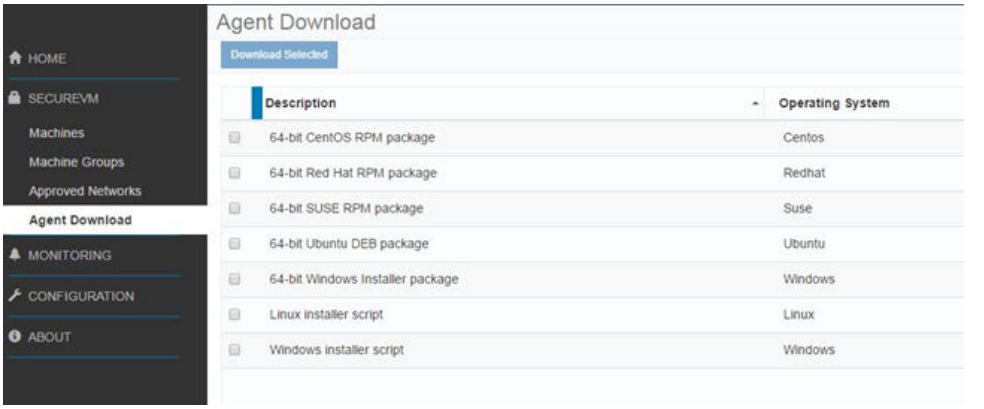
This topic describes how to download the Linux agent (the svm) from the CloudLink Center and install it on the SDS server. You install the svm after installing the VxFlex OS SDS software, but before adding the devices to the SDS.

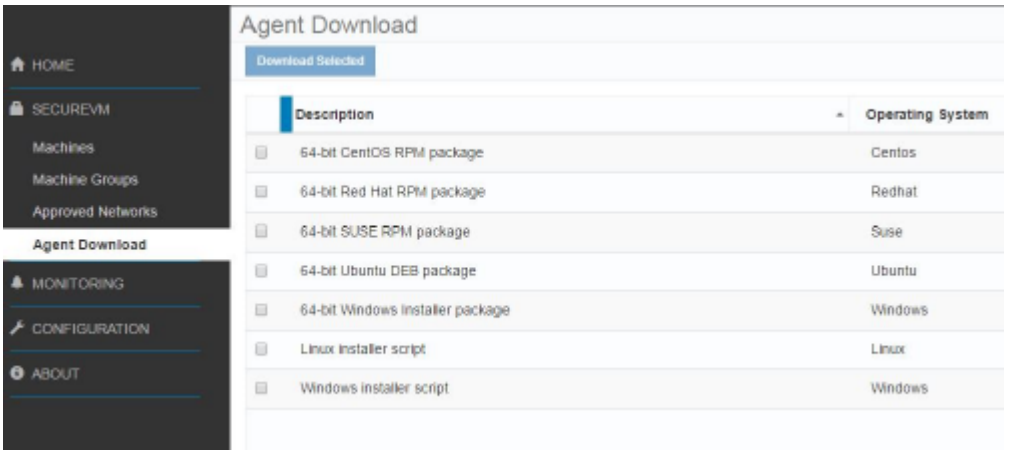
Procedure

1. Download the Linux agent (svm):

a. Log in to **CloudLink Center** and navigate to **SECUREVM** > **Agent Download**.

b. Select and download the **Linux installer script**.





2. Install the svm:

   a. Copy the **Linux installer** to the SDS server.

   b. Run the installation script: `./securevm.sh -S <CLC_IP>`

      where *<CLC_IP>* is the CloudLink Center IP address

   c. Install the svm on all SDS whose devices are to be encrypted.

The Linux agent (svm) is installed. Commands can now be issued to the svm using the command line, REST APIs, or using the CloudLink Center GUI.

Note

To install SDS software after installation of the Linux Agent, or if you are reinstalling the SDS on a server when the Linux Agent is already installed, run the following command sequence after the SDS installation is complete:

```
service svmd stop
```

```
service svmd start
```

Verify that the file `pre_run.sh` was created under `/opt/emc/extra/`.

Verify that the svm recognizes the devices in the SDS servers

This topic describes how to verify that the Linux agent (svm) recognizes the devices in the SDS servers.

Procedure

1. Run the command `svm status`.
2. Verify that the svm is connected to the CloudLink Center's IP address.
   - Initially all newly installed devices are unencrypted.
   - Devices that were not added to the SDS appear as raw.
   - If there are devices that were previously added to the SDS, they will appear with type sds. You can use these devices as they were being used before, but you cannot encrypt them in this state.

```
112CB-9:/tmp # svm status
Connected to 10.136.242.45
/                    unencrypted
/dev/rssda           unencrypted      (raw   SN:949091917673          )
/dev/sdb             unencrypted      (raw   SN:94917674              )
/dev/sdc             unencrypted      (raw   SN:94917675              )
/dev/sdd             unencrypted      (raw   SN:94917676              )
/dev/sde             unencrypted      (raw   SN:94917677              )
/dev/sdf             unencrypted      (sds   SN:94917678              )
/dev/sdg             unencrypted      (sds   SN:94917679              )
/dev/sdh             unencrypted      (sds   SN:94917680              )
/dev/sdi             unencrypted      (sds   SN:94917681              )
/dev/sdj             unencrypted      (sds   SN:94917682              )
/dev/sdk             unencrypted      (raw   SN:94917683              )
/dev/sdl             unencrypted      (raw   SN:94917684              )
/dev/sdm             unencrypted      (raw   SN:94917685              )
/dev/sdn             unencrypted      (raw   SN:94917686              )
Group:  Default
Policy: All Data
```

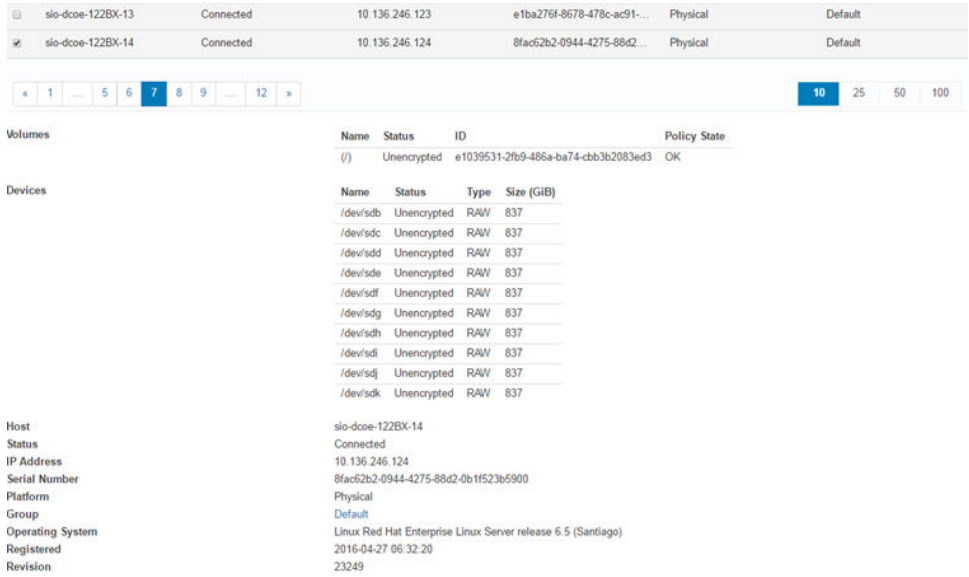
Verify that the SDS servers appear in the CloudLink Center

This topic describes how to verify that the SDS servers appear in the **CloudLink Center**.

All new servers are initially added to the Default group.

Procedure

1. From the CloudLink Center, verify that the platform type (Physical/Virtual Machine) and the operating system are properly recognized.
2. Verify that all the devices appear with correct size, type, and encryption status.



Add a new approved VxFlex OS network to CloudLink

Add a new, approved network to the **CloudLink Center**.

Procedure

1. On the **CloudLink Center** main page, select **Approved Networks** > **Add**.
2. Create a new, approved network for your SDS machines.

Add IP addresses to an approved network

This topic shows you how to add an SDS IP address to an approved network.

You can add IP addresses one by one, using an IP address range, or by CIDR notation.

You can add separate approved networks for SDS machines on different subnets.

Adding a new machine group

Add a new machine group in the **CloudLink Center** interface.

Procedure

1. On the **CloudLink Center** main page, select **Machine Groups** > **Add**.
2. Create a new **Machine Group** for the SDS servers.
3. For **Volume Encryption Policy**, select **All Data**.
4. Add the approved networks that you created and configured in the previous procedures.

   Multiple groups can be created to separate policy and administration of machines.

Move SDS servers to the machines group

Move the SDS servers to a machine group in the **CloudLink Center** interface.

For each SDS server, perform the following steps:

Procedure

1. Select the **Machines** menu on **CloudLink Center**.
2. From the **Actions** menu, select the **Add to Group** option.
3. Select the **Machine Group** that you created earlier for the SDS servers.
4. Click **Move**.
5. Alternatively, you can automate the previous steps by installing the CloudLink Agent using the following command:

```
./securevm.sh  -S <CLC_IP> -G <CLC_Group_Code>
```

where

- *<CLC_IP>* is the CloudLink Center IP address
- *<CLC_Registration_Code>* is the Registration Code shown in CloudLink Center for the group

Encrypt devices

Encrypt devices using the CloudLink GUI.

Note

- Never attempt to encrypt or erase the devices that are currently attached to the SDS. Devices should only be encrypted before they are added to the SDS, or after removing them from the SDS.
- Any existing data on the device will be destroyed as a result of this procedure.

Procedure

1. Encrypt a device, using either of the following methods:

Client	Description
GUI	a. Select the **Machines** menu. b. In the **Machines** list, select the required machine. c. Click **Actions**. d. Select the **Encrypt** option. e. Select the device to be encrypted. f. Click **Encrypt**.
CLI	Run the following command: `svm encrypt <device_name>` where *<device_name>* is a variable

Client	Description
	112CB-9:/tmp # svm encrypt /dev/sdk Using SDS. Encryption started for /dev/sdk.

Verify device encryption and determine the path of the encrypted device

This topics describes how to verify the encryption status of a device and the path to an encrypted device.

The `svm status` command in the Linux Agent CLI will now display the devices' encryption status, and the new path to each of the encrypted devices.

The new device path starts with the string `/dev/mapper/`.

```
112CB-9:/tmp # svm status
Connected to 10.136.242.45
/                   unencrypted
/dev/rssda          unencrypted     (raw   SN:949091917673          )
/dev/sdb            unencrypted     (raw   SN:94917674             )
/dev/sdc            unencrypted     (raw   SN:94917675             )
/dev/sdd            unencrypted     (raw   SN:94917676             )
/dev/sde            unencrypted     (raw   SN:94917677             )
/dev/sdf            unencrypted     (sds   SN:94917678             )
/dev/sdg            unencrypted     (sds   SN:94917679             )
/dev/sdh            unencrypted     (sds   SN:94917680             )
/dev/sdi            unencrypted     (sds   SN:94917681             )
/dev/sdj            unencrypted     (sds   SN:94917682             )
/dev/sdk            encrypted       (raw   SN:94917683            /dev/mapper/svm_sdk)
/dev/sdl            encrypted       (raw   SN:94917684            /dev/mapper/svm_sdl)
/dev/sdm            encrypted       (raw   SN:94917685            /dev/mapper/svm_sdm)
/dev/sdn            encrypted       (raw   SN:94917686            /dev/mapper/svm_sdn)
```

In this example, only the last four devices are encrypted. The same view in **CloudLink Center** GUI is shown in following figure, that also shows the path to each device in the `Name` column.

Volumes

Name	Status	ID	Policy State
(/)	Unencrypted	1467ad0b-693f-4168-a77c-1fa0ab11db0f	OK

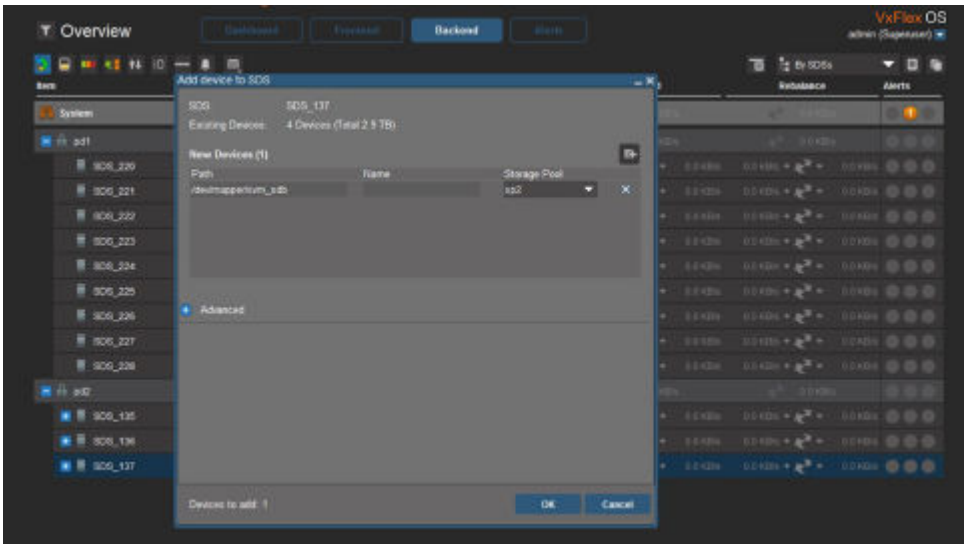
Devices

Name	Status	Type	Size (GiB)
/dev/rssda	Unencrypted	RAW	652
/dev/sdb	Unencrypted	RAW	930
/dev/sdc	Unencrypted	RAW	930
/dev/sdd	Unencrypted	RAW	930
/dev/sde	Unencrypted	RAW	930
/dev/sdf	Unencrypted	SDS	930
/dev/sdg	Unencrypted	SDS	930
/dev/sdh	Unencrypted	SDS	930
/dev/sdi	Unencrypted	SDS	930
/dev/sdj	Unencrypted	SDS	930
/dev/mapper/svm_sdk(/dev/sdk)	Encrypted	SDS	744
/dev/mapper/svm_sdl(/dev/sdl)	Encrypted	SDS	744
/dev/mapper/svm_sdm(/dev/sdm)	Encrypted	SDS	744
/dev/mapper/svm_sdn(/dev/sdn)	Encrypted	SDS	744

Add encrypted devices to an SDS

This topic shows how encrypted devices can be added to an SDS.

Now that the devices have been encrypted, you can add them to the SDS by using their new `/dev/mapper/..` path, as shown in the following figure:



The characters within the parentheses are for your reference only and should not be included when using the path for the mapping purposes.

Note

Do not add a device using its original path (`/dev/...`). Doing so can stop the device encryption (device erasure, in terms of CloudLink) and this could corrupt the data on the device.

Disabling encryption and removing encrypted devices from an SDS

This topic describes how to disable the encryption of a device, and how to remove an encrypted device from an SDS.

Before making any change in a device's encryption status, you must use VxFlex OS management tools to remove the device from the SDS.

Procedure

1. Remove the device from the SDS:
   - Use the SCLI `--remove_sds_command`, for example:

     ```
     scli --remove_sds_device --sds_name MY_SDS --
     device_path /dev/mapper/svm_sdX
     ```

   - From the VxFlex OS GUI **Backend** view, right-click the device and select **Remove Device**.

2. Disable the encryption from the CloudLink Center GUI or using the svm `erase` command.

```
svm erase /dev/sdb
```

3. Confirm the device erase.

Note

Removing (erasing) a device from CloudLink will destroy all data on the device.

Copyright © 2016-2018 Dell Inc. or its subsidiaries. All rights reserved.

Published June 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.