Home
Data Security
Data Security Essentials
Disaster Recovery
AirGap
Introduction
Managing the Solution
What's New
Installation Guide
AirGap Jobs
Common Operations
Airgap Operations
User Help
Dell Cyberstorage
Deprecated Capabilities
Contributor Guide

Version: 2.10.0

How to Install AirGap

Introduction

This guide provides instructions to install and set up the AirGap solution. It includes the hardware requirements, system setup, VM deployment, and other necessary configurations for both the Vault and Production systems. Follow the outlined procedures to ensure proper deployment and functionality of the AirGap environment.

Prerequisites

Vault Cluster Requirements

- **Dedicated Host for Vault Agent VM:** A dedicated host server is required within the Vault environment to deploy the Vault Agent VM.
  - **Hardware Recommendations:**
    - Dual-socket server with 512 GB RAM.
    - 1G and 10G Ethernet interface options.
    - 2–4 TB local flash storage.
    - Future-proof for additional VMs supporting cybersecurity solutions and Windows desktops.
    - Ensure secure OS desktop for recovery operations and Isilon hardware, firmware, and software upgrades.
  - **Time Zone and Time Sync:** Ensure that the time zone and time are correctly set, and ensure the host server is time synced with the Vault Agent.
  - **VM Time Sync:** All VMs need to use the same NTP server, to prevent a time skew that would affect overall functionality.
- **Management and AirGap Replication Pool:** The Vault PowerScale system must have a Management pool and an AirGap replication pool within the System zone. Nodes must be shared between the pools, but different network interfaces are required for each pool to ensure isolation.
- **Network Subnet Segregation:** Use a segregated subnet for all Vault environment components to ensure network isolation.
- **Network Connectivity for Replication:** Establish network connectivity between the replication pool of the Vault PowerScale system and the replication pool of the Source PowerScale system. No password should be required for this communication to ensure successful SyncIQ replication.
- **Firewall and Traffic Control:** Install a firewall or use a dedicated switch to restrict traffic between the production and the Vault environment.
- **Dedicated Switch for Vault Agent VM Connectivity:** Connect the Vault Agent VM to the Management pool of the Vault PowerScale system using a dedicated switch.

Production/Source Cluster Requirements

- **AirGap Replication Pool:** Create a separate AirGap replication pool on the Source PowerScale system within the System zone.
- **Dedicated Subnet for AirGap Replication:** Assign a dedicated subnet specifically for the AirGap replication pool on the Source PowerScale system.
- **Node Availability for High Availability:** Use at least two nodes with separate network interfaces for the AirGap replication pool to ensure high availability. Single-node setups are allowed but will introduce a single point of failure for SyncIQ replication.
- **Optional Dedicated Nodes for AirGap Replication:** You may deploy dedicated nodes specifically for the AirGap replication pools to enhance system isolation and availability.

Hardware Setup

Create Eyeglass Users and Update Sudoer Files

First, you must create the Eyeglass Users and update the Sudoer files on both the Vault and the Production Clusters in order to continue.

It is assumed here that the Service Account for the Production Cluster was created during the Eyeglass VM Installation.

To create the Eyeglass users on the Vault Cluster, SSH into its Eyeglass VM using a Terminal, and use the following string of commands:

```
isi auth roles create --name EyeglassAdmin --description "EyeglassAdmin role Vault"
isi auth users create eyeglass --enabled yes --password YourPassword
isi auth users modify eyeglass --password-expires no
isi auth roles modify EyeglassAdmin --add-user eyeglass
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_LOGIN_PAPI
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_DEVICES
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_NS_IFS_ACCESS
isi auth roles modify EyeglassAdmin --add-priv ISI_PRIV_JOB_ENGINE
isi auth roles modify EyeglassAdmin --add-priv ISI_PRIV_NETWORK
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_LOGIN_SSH
isi auth roles modify EyeglassAdmin --add-priv ISI_PRIV_SYNCIQ
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_EVENT
isi auth roles modify EyeglassAdmin --add-priv-ro ISI_PRIV_STATISTICS
```

Modify the user account using the following commands:

```
isi_visudo
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ? curl *
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ?? curl *
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ? whoami; hostname
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ?? whoami; hostname
```

Next, for the Production Cluster, modify the user account using the following string of commands:

```
isi_visudo
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_classic auth ads*
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_classic domain info*
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ? curl *
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ?? curl *
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ? whoami; hostname
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ?? whoami; hostname
```

Introduction
Prerequisites
Vault Cluster Requirements
Production/Source Cluster Requirements
Hardware Setup
Create Eyeglass Users and Update Sudoer Files
Create Passwordless SSH Tunnel
Environment Setup
Add Airgap Licenses to Eyeglass
Retrieve API Token from Eyeglass
Add Production Cluster to Eyeglass
Deploy and Configure Vault Agent
Deploy the Vault Agent
Edit Vault Agent Config File
Post-Deployment Verification Steps
Add Clusters to the Vault Agent
Next Steps
AirGap Policy Configuration
Operational Procedures

```
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ? ping *
eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array -n ?? ping *
```

Create Passwordless SSH Tunnel

1. SSH into the Production Cluster as the `eyeglass` user.
2. Run the following command:

```
mkdir .ssh
```

3. SSH into to the Vault Cluster as the `eyeglass` Vault user.
4. Create an SSH Key Pair by running the following command:

```
ssh-keygen -t rsa
```

5. After entering the previous command, hit Enter for the default path, and hit Enter again to leave the passphrase blank. An SSH Key Pair should now be created in `/ifs/home/eyeglassvault/.ssh`
6. Copy the public key (`id_rsa.pub`) to the Production Cluster (which will be used for Eyeglass communications) using the following command and replacing the `x.x.x.x` with the IP of the Production Cluster.

```
scp /ifs/home/eyeglass/.ssh/id_rsa.pub
eyeglass@x.x.x.x:/ifs/home/eyeglass/.ssh/id_rsa.pub
```

7. Complete Production Cluster keyless SSH configuration by logging into it through SSH as the eyeglass user, and running the following commands:

```
cd .ssh
cat id_rsa.pub >> authorized_keys
chmod 600 authorized_keys
```

8. Test the Keyless SSH. To do so, SSH into the Vault Cluster as the `eyeglass` user, then SSH again, from the Vault Cluster into the Production Cluster. If no password is requested, the operation was successful.

Environment Setup

Add Airgap Licenses to Eyeglass

After your AirGap Licenses have been generated with the help of the Superna team, add them into Eyeglass using the License Manager.

1. Open License Management.
2. Go to the Manage Licenses tab.
3. Click on Browse to select the License files from your local machine.
4. Click on Upload, and accept the Eyeglass EULA.

Retrieve API Token from Eyeglass

Next, you'll need an API token, used later in the installation process to link the Vault Agent VM to the Eyeglass VM. To get one:

1. Go to Eyeglass Main Menu (on the bottom left of the Eyeglass Web UI).
2. Click on Integrations.
3. Go to the API Tokens tab.
4. Click on Create New Token.
5. Enter a relevant name and click on OK.

Add Production Cluster to Eyeglass

Add the Production Cluster to Eyeglass. When prompted, use the username you created earlier for this Cluster. On the Eyeglass Web UI:

1. Click on Eyeglass Main Menu (bottom left corner).
2. Click on Add Managed Device.
3. Complete the form with the appropriate data. During this step you will be asked for the username and password.
4. Click on Submit.

Deploy and Configure Vault Agent

Deploy the Vault Agent

1. Deploy a dedicated Vault Agent OVF, which you may later upgrade to the latest build. Contact Support if you haven't obtained the download link for the OVF.
2. Cluster Up Vault Agent, check that the required services are running, and then Cluster Down.
3. Upgrade Vault Agent to the desired build, you may use any ECA offline installer for this. If you need help finding one, contact Support.

Edit Vault Agent Config File

1. SSH into the Vault Agent VM.
2. Open the `eca-env-common` configuration file using the following command or your preferred editor:

```
vi /opt/superna/eca/eca-env-common.conf
```

3. Edit the file in the following ways:

```
- export EYEGLASS_LOCATION=*Your Eyeglass IP*
- export EYEGLASS_API_TOKEN=*API Token generated above*
- export RSW_ONLY_CFG=*true* **(this value should be true)**
- export STOP_ON_AUTOMOUNT_FAIL=*false* **(this value should be false)**
```

Post-Deployment Verification Steps

1. Run Cluster Up.
2. Check with the `docker ps` or `ecactl cluster status` commands that all of the required containers are up and running. The results should look something like this:

```
ecaadmin@vltabc-1:~> ecactl cluster status
Checking service status on all cluster nodes.
Connecting to 172.25.11.89...
NAMES         IMAGE                          " " SIZE                   STATUS
ecssync       eca/ecssync:2.5.8.2-22138      " " 90.1kB (virtual 937MB)   Up 21 hours
vaultagent    eca/vaultagent:2.5.8.2-22138   " " 32.8kB (virtual 536MB)   Up 21 hours
taskmaster    eca/taskmaster:2.5.8.2-22138   " " 32.8kB (virtual 508MB)   Up 21 hours
zookeeper     eca/zookeeper:2.5.8.2-22138    " " 35.8kB (virtual 468MB)   Up 21 hours
mariadb       eca/mariadb:2.5.8.2-22138      " " 2B (virtual 414MB)       Up 21 hours
dns           eca/dnsmasq:2.5.8.2-22138      " " 139B (virtual 261MB)     Up 21 hours
Connection to 172.25.11.89 closed.
ecaadmin@vltabc-1:~>
```

Add Clusters to the Vault Agent

Run the following commands, making sure to replace the X.X.X.X with the appropriate IP address corresponding to the selected Cluster.

1. Add the **Vault Cluster** using the following command (this command will prompt for Eyeglass password):

```
ecactl isilons add --vaulthost X.X.X.X --user eyeglass --vaultPoolName (Vault_Cluster_Pool_Name) --vaultsyncio
```

2. Then, add the **Protected Cluster**. This, again, will prompt for the Eyeglass user password:

```
ecactl isilons add --protectedhost X.X.X.X --user eyeglass
```

3. You may also add the Protected Management Node (optional, but recommended). To do this, use the following command (Where X.X.X.X is the IP of the protected Cluster, and Node X is the node from which the source Cluster can reach the Core Eyeglass VM):

```
ecactl isilons add --protectedhost X.X.X.X --user eyeglass --protectedManagementNode X
```

4. Finally, run the Connectivity Check Command:

```
ecactl airgap check --prod isi-prod
```

Next Steps

AirGap Policy Configuration

Create and schedule as many AirGap policies as needed for the environment and use case. See the AirGap Jobs document for more information.

Operational Procedures

For information regarding common AirGap procedures, see the Common Operations document.