CART Deployment Guide

CyberArk Integration

Version 1.0.0

Jan 2021

Prepared by:

CLANGO

Contents

1 Overview

This guide provides instructions for deploying CART for your organization and integrating it with CyberArk. The deployment consists of these main steps:

1. Request and download the CART installation files and license
2. Install and configure the CART web application
3. Install and configure the CART Connector for CyberArk
4. Verify CART can ingest CyberArk data

2 Download CART

To obtain a download link for the CART installation files, fill out and submit the CART request form located here: https://clango.com/request-download-cart/

The download link will contain the CART installation files, the CART user manual and a trial license.

3 Install CART Web Application

The CART web application is designed to run on a Linux VM. The following deployment instructions assume a Red Hat Enterprise Linux 8 VM is provisioned for CART at your organization. Deployment instructions for an OS other than RHEL 8 are available upon request.

3.1 Configure Linux VM

3.1.1 Unzip

The CART installation files are delivered as a ZIP file. Included within the ZIP is cart-linux.zip which must be placed on the Linux VM and unzipped. To install **unzip**, run:

```
sudo yum install unzip -y
```

Then you must unzip the CART ZIP by running **unzip**:

```
unzip /tmp/cart-linux.zip -d /tmp/cart
```

Note in the above line, the cart-linuz.zip file is assumed to be located in **/tmp** and **/tmp/cart** is the desintation folder for the unzipped files.

3.1.2 SSL Certificates

Before running the installer, you must prepare the SSL certificate files. CART requires both a public key (.crt, .cer) and an unencrypted private key (.key). If you have both of these, you can place them on the Linux VM and skip this section. If you are given a pfx file or an encrypted private key, you will need to convert.

1. If you do not have openssl installed and will need to convert, install via:

```
sudo yum install openssl -y
```

2. Converting pfx to encrypted key:

   ```
   openssl pkcs12 -in [pfxfile].pfx -nocerts -out key.pem
   ```

3. You will be asked to enter the password the pfx is protected by as well as a password to protect the pem.
4. Converting encrypted key to unencrypted key:

   ```
   openssl rsa -in key.pem -out server.key
   ```

5. You will be asked to enter the password protecting the pem file.
6. Converting pfx to crt:

   ```
   openssl pkcs12 -in [pfxfile].pfx -clcerts -nokeys -out certfile.crt
   ```

7. If you installed openssl, you may uninstall it now.

The installer will ask for the paths of **certfile.crt** (public SSL certificate) and **server.key** (SSL certificate private key) created in steps 4 and 6.

3.2 Run Installer

Navigate to the unzipped directory, then run:

```
bash cartinstaller.sh
```

The installer allows for flexibility in installations, but the recommended trial version installation steps are as follows:

1. Assuming the unzipped directory is located in **/tmp**, run:

   ```
   bash /tmp/cart/cartinstaller.sh
   ```

2. When prompted if you'd like to install dependencies, answer **y** for yes.
3. When prompted to install Docker, answer **y** for yes.
4. When the script exits, disconnect and reconnect to the VM.
5. Assuming the unzipped directory is located in **/tmp**, run:

   ```
   bash /tmp/cart/cartinstaller.sh
   ```

6. When prompted if you'd like to install dependencies, answer **n** for no.
7. When prompted if the installation requires a new user for SCP, answer **y** for yes.
8. When prompted for CART data user username, enter **cart-data**.
9. When prompted for cart-data password, make note of what you enter.
10. When prompted for the cart-data SSH public key, paste in the contents of **cart-data-public.txt**.
11. When prompted to run setup, answer **y** for yes.
12. When prompted for to enter the CART install directory, press Enter to use the default of **/opt/cart**.

13. When prompted to install PostgreSQL, answer **y** for yes.
14. When prompted for database port, press Enter to use the default of **5432**.
15. When prompted for database name, press Enter to use the default of **cart**.
16. When prompted for database username, press Enter to use the default of **postgres**.
17. When prompted for database password, take note of what you enter.
18. When prompted for the path to the public SSL certificate, enter it.
19. When prompted for the path to the SSL certificate private key, enter it.
20. When the script completes, run:

```
sudo mkdir /var/lib/docker/volumes/cart_ingest/_data/1
```

21. Then run:

```
sudo chown cart-data /var/lib/docker/volumes/cart_ingest/_data/1
```

The CART web application should now be accessible at **https://<linux_vm_address>**.

3.3 Configure CART Web Application

Complete the CART configuration wizard to configure the authentication method, authorized users, email settings and data ingest settings.

1. In a web browser, navigate to **https://<linux_vm_address>**. You should see the configuration wizard.
2. For the server admin password, enter **coldfusion** then click **Next Step**. This default password will be changed in a later step.
3. For the Datasource Settings, use the following the click **Next Step**:
   - Select **PostgreSQL** for Driver.
   - Enter **cart** for Database.
   - Enter the internal IP of the Linux VM for Server.
   - Leave port as **5432**.
   - Enter **postgres** as Username.
   - Enter the password you noted during installation.
4. For Data Ingest Settings, click **Choose File for CyberArk License Key**.
5. Choose the **license.txt** file provided to you.
6. For Database Ingest Directory for CyberArk Data, enter **/shared/ingest**.
7. Choose **Manual** as Import Frequency, then click **Next Step**.
8. For Email Settings, fill in Host, Port [587], From Address, etc. as required, then click Next Step.
9. For Authentication Settings, choose **LDAP** for Authentication Method and fill in the rest of the fields, then click **Next Step**.
10. On the Manage Users page, click the **+** menu button to open the Add User form.
11. Start typing a username and you should see suggestions if LDAP is configured correctly. Chose a user to be the Admin and click **Save**.
12. Click **Next Step**.

13. Optionally add groups in the same was as adding users, then click **Finish**.
14. Log in with the Admin user you set up in step 11.
15. Go to **Admin > Manage Access**.
16. Enter a new Admin Password and click **Save**.
17. Go to **Admin > Manage Vaults**.
18. For each vault listed, click the **Edit Row** button, enter a Name and Description, and click the **Save Changes** button in the row.
19. Go to **Admin > Manage Data Ingest Settings**.
20. Choose a frequency and click **Save**. Typically, daily at 1 AM is used.

4 Install CART Connector for CyberArk

The CART Connector for CyberArk is installed as a Windows service. It utilizes CyberArk utilities that require configuration in PrivateArk and PVWA. The Windows VM should be able to connect to the CyberArk vault via the CyberArk port (usually 1858). The Windows VM will also need to be allowed to connect to port 22 of the Linux VM in your firewall.

4.1 Configure Windows VM

4.1.1 CyberArk Utilities

The CART Connector utilizes the following CyberArk utilities which must be present on the Windows VM:

- ExportVaultData utility 9.8
- PACLI version 7.2

These utilities should be obtainable directly from CyberArk. These exact versions must be installed – higher versions are not supported by the CART Connector.

You will need at least two users in CyberArk in order to use the CART Connector – one user to set up the scheduled reports in PVWA and one user used by the ExportVaultData utility and PACLI for authentication. Our recommendation is to set up three users - one user to set up the scheduled reports in PVWA, one user used by the ExportVaultData utility, and one user used by PACLI for authentication.

See *CART Connector - Configuration Instructions v1.0.pdf* in the CART installation files for instructions on setting up those users with the correct permissions and creating scheduled reports.

4.1.2 CART Installation Files

The CART installation files are delivered as a ZIP file which must be placed on the Windows VM and extracted before running the installer.

4.2 Run Installer

Navigate to the extracted CART installation files and double-click the .msi file to start the installer.

During the installation, you may choose to modify the installation path from the default path (C:\CARTConnectorService).

4.3 Configure CART Connector for CyberArk

Navigate to the installation path and update **config.ini** to specify the settings for your environment. The file contains detailed comments for each parameter. The CART Connecter Service must be restarted for changes in this file to take effect.

To confirm the settings are correct, utilize the **bin/Test.exe** file to execute a data export. Check the **logs** directory to help troubleshoot any errors.

5 Verify CART Connector for CyberArk

Once the data has been exported and sent to the CART VM via the CART Connector, we can invoke the first data ingest.

1. Log in to CART as an Admin user.
2. Navigate to **Admin > Manage Data Ingest Settings** and click **Run Ingest Now**.
3. Navigate to **Admin > Audit Log** and click **Search**.
4. Inspect the audit log entries to confirm the reports were ingested successfully.

6 Troubleshooting

Contact Clango's CART Support team via cart-support@clango.com for any questions or issues.