**DAP Secrets Retrieval**

**Install and Use DAP Summon to Retrieve Secret Values**

This exercise will install and demonstrate how CyberArk’s DAP Summon utility works to provide another method for retrieving secret/variable values. Summon provides two utilities that operate differently while solving similar secret/variable value retrieval requests.

1. If not already, log into the **Docker-Host1** virtual machine using SSH and authenticate with the **user01 / Cyberark1** credentials
2. Change the working directory to **$HOME/DAPLabs/summon**

**cd $HOME/DAPLabs/summon**

1. Before installing the Summon utilities it should be noted that there are currently 2 separate DAP CLI utilities for the Summon interface:

**summon** (https://github.com/cyberark/summon/)  
- Secrets retrieval utility to return secret/variable values using YAML policy combined with a secret/variable provider utility and output path

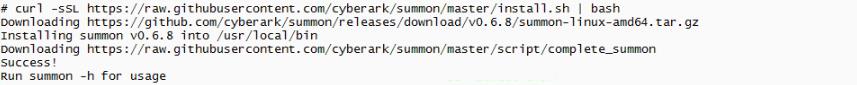
**summon-conjur** (https://github.com/cyberark/summon-conjur)  
- Secrets injection utility to retrieve secret/variable values and inject into environment variables

1. Elevate privilege to the **root/Cyberark1** credentials

**su**

1. Install the summon utility using the following command to download and install automatically.

**curl -sSL https://raw.githubusercontent.com/cyberark/summon/master/install.sh | bash**



1. Once summon is installed, exit back to the user01 user account session

**exit**

1. Open and create a file called **secrets.yml** using vi or nano. This file will define the DAP resource information to have summon retrieve.

**Text to insert (ESC :wq to save)**

DB\_USER: !var dev/db/mysql/cars/username

DB\_PASS: !var dev/db/mysql/cars/secret

1. Open and create a file called **conjurcmd.sh** using vi or nano. This file will define the DAP commands to execute and pass the output to summon.

**Text to insert (ESC :wq to save)**

#!/bin/bash  
conjur variable value $1

**NOTE:** Using **$1** inside the **conjurcmd.sh** script will allow summon to inject the secret/variable declaration found in the **secrets.yml** file and pass into this script as a command-line argument

1. Open and create a file called **output.sh** using vi or nano. This file will be used by summon to inject the secret/variable value into the script through the environment variable(s) declared in the **secrets.yml** file.

**Text to insert (ESC :wq to save)**

#!/bin/bash  
echo "Database Username: $DB\_USER"

echo "Database Password: $DB\_PASS"

**NOTE:** Using **$1** inside the **conjurcmd.sh** script will allow summon to inject the secret/variable declaration found in the **secrets.yml** file and pass into this script as a command-line argument

1. Change the file permissions to allow proper execution

**sudo chmod 755 conjurcmd.sh output.sh**

**sudo chmod 755 secrets.yml**

1. Run summon to retrieve the secret/variable value

**summon -f secrets.yml -p ./conjurcmd.sh ./output.sh**

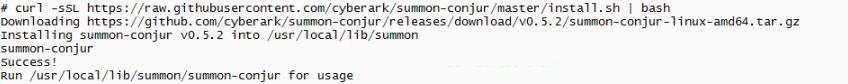
page132image16837808

1. Congratulations! You have successfully retrieved a secret/variable value using summon.
2. Now to compare **summon** to **summon-conjur**, let’s install the summon-conjur utility. Elevate privilege to the **root / Cyberark1** credentials.

**su**

1. Install **summon-conjur**

**curl -sSL https://raw.githubusercontent.com/cyberark/summon-conjur/master/install.sh | bash**



1. Once summon-conjur is installed, exit back to the user01 user account session

**exit**

1. In order to use summon-conjur using relative path the PATH environment variable must be set and initialized. PATH simply provides the user’s shell environment a path to the summon-conjur binary executable.

**export PATH=$PATH:/usr/local/lib/summon**

1. Try to retrieve the secret/variable value using summon-conjur. Did it work?

**summon-conjur dev/db/mysql/cars/secret**

1. Try assigning the secret/variable value to a user defined environment variable. Return the value using the echo command.

**DB\_PASS=$(summon-conjur dev/db/mysql/cars/secret)**

**echo $DB\_PASS**

1. Congratulations! You have successfully retrieved secret/variable values using both Summon utilities for secrets injection.