VERITAS

API Endpoints and Commands on Flex Appliance for CyberArk Integration

Table of Contents

Title: API Endpoints and Commands on Flex Appliance for CyberArk Integration

Introduction

This document describes the API endpoints and the commands that you can leverage to integrate Flex Appliance with a password management solution. This document follows the implementation of a Central Policy Manager (CPM) on CyberArk and can be used to replicate the same functionality on another tool.

The CyberArk integration of Flex Appliance performs the following functions:

1. Verify password: Verifies that the password in the vault is correct.
2. Change password: Changes the user's password.

This document is divided into two main sections. The first section shows the APIs, and the second section shows the commands. The APIs are used to manage the accounts on the Flex Appliance Console. The commands are used to manage the accounts on the Flex Appliance Shell and the instances.

Title: API Endpoints and Commands on Flex Appliance for CyberArk Integration

API endpoints

The following sections detail the API endpoints that are required for the various plug-ins that are available on CyberArk.

Veritas Flex Appliance Console via API GEN2

API: /api/v1/login

Method: POST

Summary: This API signs in the user and returns an access token. It requires that the username and the password be passed in the body of the request as well as a code (totp parameter) if multifactor authentication is enabled.

Headers:

```
<header>
          <Content-Type>
                    application/json
          </Content-Type>
</header>
```

Body:

```
{
"username": "user1",
"password": "passswd",
"totp": "XXXX"
}
```

Response:

```
'200': Successful Operation.
'400': Invalid input.
'401': Invalid credentials, or you do not have permission for this action.
'403': Users from an imported remote user group can't sign in when multifactor authentication is enforced.
'406': The time-to-live parameter must be between 1 and the value of the maximum token validity. You can check the
maximum token validity (token-ttl-limit) with the users API.
'409': You have reached the maximum number of personal API tokens.
'500': Internal server error.
```

API: /api/v1/logout

Method: POST

Summary: Signs out the specified user and revokes the user's token. It requires the authentication and the refresh tokens that were obtained during sign-in to be passed in the header of the request.

Headers:

```
<header>
          <Content-Type>application/json</Content-Type>
          <x-auth-token>insert_auth_token_here</x-auth-token>
          <refresh-token>insert_refresh_token_here</refresh-token>
</header>
```

API: /api/v2/users/{uid}/password

Method: PUT

Summary: This API can be used to change the password of a local user. The {uid} in this API is the ID of the user whose password needs to change. It requires the authentication token that was obtained from a successful login to be passed in the header. The request body must contain the current password and the new password.

Headers:

```
<header>
          <Content-Type>application/json</Content-Type>
          <x-auth-token>insert_auth_token_here</x-auth-token>
</header>
```

Body:

```
{
          "newPassword": "passwd",
          "currentPassword": "newpasswd",
}
```

Response:

```
'200': Successful operation.
'400': Invalid request.
'401': Invalid unlock code.
```

```
'403': You do not have permission to perform this operation, or the account is locked.
'404': User ID not found.
'412': Password does not adhere to password policy, or the new password is the same as the last password.
'500': Internal server error
```

Commands

The verify password process involves entering the password on the password prompt, and then the system looks for the standard prompt to mark it as a successful sign-in.

The change password process uses the commands in the following sections to change the password of the user.

Veritas Flex Appliance Shell via SSH

The command in this section changes the password of the **hostadmin** user in the Flex Appliance Shell.

```
Command: set user password
          Prompt: Current password:
          Action: Sends the current password
          Prompt: New password:
          Action: Sends the newly generated password
          Prompt: Retype new password:
          Action: Sends the newly generated password again
          Responses:
                    Success:
                              Operation completed successfully
                    Failure:
                              Sorry, wrong passwd
                              BAD PASSWORD
```

Veritas Flex Appliance Primary and Media Instance via SSH

The `passwd` command in this section changes the password for a user on a primary or a media server instance. The `sudo passwd <username>` command changes the password with the reconcile operation, which syncs the password between the CyberArk Vault and the instance.

The reconcile operation requires that the user have the same privileges as the **appadmin** user.

```
Command: passwd
          Prompt: Current password:
          Action: Sends the current password
          Prompt: New password:
          Action: Sends the newly generated password
          Prompt: Retype new password:
```

```
          Action: Sends the newly generated password again
          Responses:
                    Success:
                              passwd: all authentication tokens updated successfully
                    Failures:
                              New passwords do not match.
                              Password is invalid.
                              Sorry, wrong passwd
```

```
Command: sudo passwd <username>
          Prompt: New password:
          Action: Sends the newly generated password
          Prompt: Retype new password:
          Action: Sends the newly generated password again
          Responses:
                    Success:
                              passwd: all authentication tokens updated successfully
                    Failure:
                              <extrapass3\username> is not in the sudoers file.
                              New passwords do not match.
                              Password is invalid.
                              Sorry, wrong passwd
```

Veritas Flex Appliance WORM Instance via SSH

The command in this section changes the password for a user on a WORM instance. To run the commands for any user, the system must log in as the **msdpadm** user.

```
Command: setting user change-password username=<username>
          Prompt: Current password:
          Action: Sends the current password
          Prompt: New password:
          Action: Sends the newly generated password
          Prompt: Retype new password:
          Action: Sends the newly generated password again
          Responses:
                    Success:
                              passwd: all authentication tokens updated successfully
                              Operation completed successfully
                    Failure:
                              BAD PASSWORD
                              Password is invalid.
                              Sorry, wrong passwd
```

References

1. CyberArk Plugins for NetBackup Flex Appliances and NetBackup Appliances
2. Veritas plugins on CyberArk marketplace
3. Veritas Appliance Guide for CyberArk Plugin Configuration
4. CyberArk Support for Veritas Appliances