



SECRETS MANAGER

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Zenoss, Inc.

Website: <http://www.zenoss.com>

Name of Product: Zenoss Cloud

Version: SaaS based product as of Mar 2021

Date: March 11, 2021

PARTNER SOLUTION OVERVIEW

Zenoss Cloud is a leading cloud-native unified AIOps and IT operations platform providing full-stack modeling, event management, performance metrics, and integrations with third-party IT operations management tools — allowing automatic action to resolve performance issues with enterprise IT infrastructure and services. Zenoss Cloud offers collaborative troubleshooting tools as well as views into utilization trends, capacity planning and infrastructure anomalies that might impact service availability and performance.

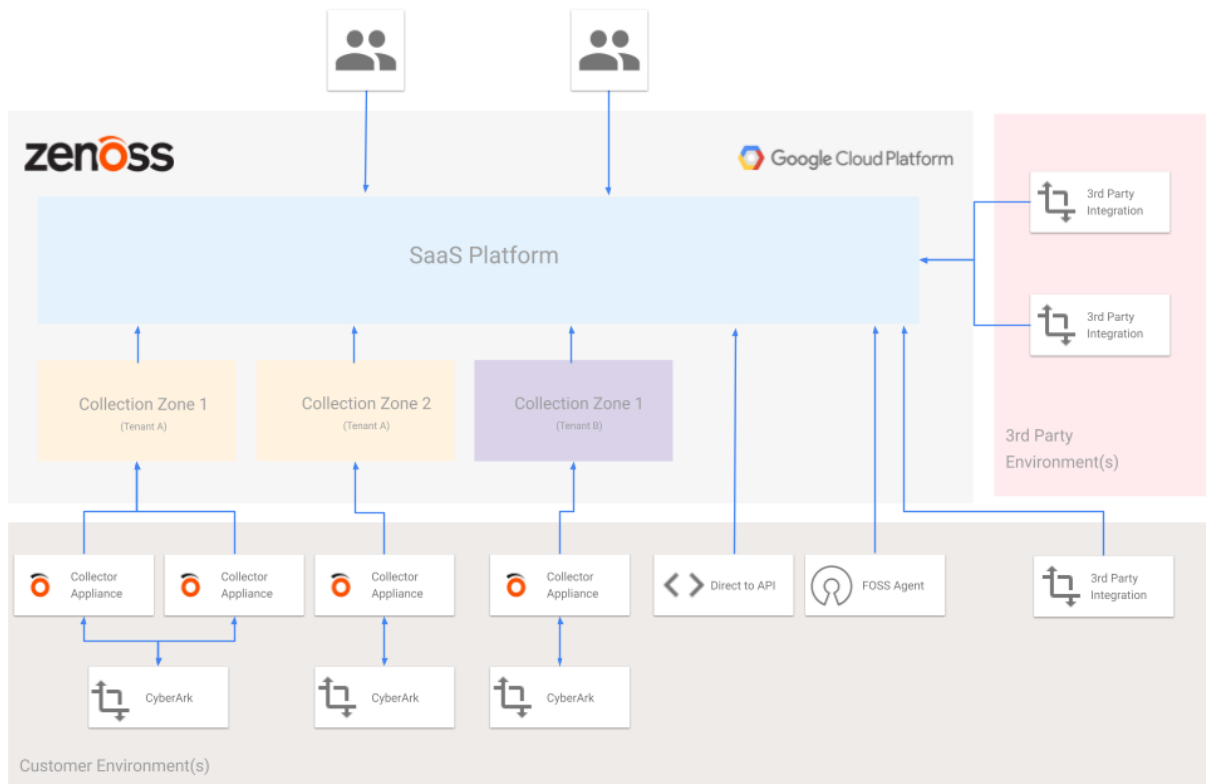
KEY BENEFITS

Zenoss Cloud being a unified AIOps and IT operations platform deals with accessing hundreds and thousands of enterprise IT infrastructure elements like servers, routers, gateways, storage devices, cloud assets. These assets are protected by security credentials and other sensitive security configurations and managing them in a central repository can be a challenge for enterprise security departments. By integrating with CyberArk SECRETS MANAGER Zenoss Cloud can eliminate storing and managing hard coded application credentials embedded in applications, scripts or configuration files (aka Zenoss Cloud), and allows these highly-sensitive config to be centrally stored, logged and managed within the CyberArk Vault (Credentials Provider, Central Credentials Provider)

This will enable organizations to comply with internal and regulatory compliance requirements of periodic security config replacement, and monitor privileged access across all systems, databases and applications.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Zenoss Cloud Architecture



CyberArk and Zenoss Cloud integration Overview:

- **SECRETS MANAGER** is integrated with Collection zone component of Zenoss Cloud. Collection Zone represents a set of **collectors**, which are logical groups of services that gather availability, performance, or model data from IT infrastructure resources and services. Collectors can be used for logical or geographical separation of resources and services within an organization.
- When a user adds a new device for monitoring its performance, the user needs to fill in the credential information. In the case of CyberArk integration, the user fills in the CyberArk query information. The credential retrievals are triggered to collect the device information during the modeling time and during the performance metrics and events collection time. The modeling time is defined in terms of every 6 hours or 12 hours. The collection time is set in terms of 5 minutes. It can be set to a minute at a lower level. In a typical environment, the credential

retrieval is triggered every five minutes. The mechanism does not differentiate between the type of devices and operating systems that zenoss monitors.

SECRETS MANAGER INSTALLATION

Refer to the “Central Credential Provider Implementation guide” for CyberArk Agentless installation and configuration.

SECRETS MANAGER CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.

Add Application

Name: ZenossApp

Description: Zenoss Application Description

Business owner

First Name: Liam

Last Name: Smith

Email: liam.smith@zenoss.com

Phone: +123456789

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

Add Cancel

2. Specify the following information:
 - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: **APP ID = ZenossApp**
 - In the Description, specify a short description of the application that will help you identify it.
 - In the Business owner section, specify contact information about the application's Business owner.
 - In the lowest section, specify the Location of the application in the Vault hierarchy. If a Location is not selected, the application will be added in the same Location as the user who is creating this application.
3. Click **Add**; the application is added and is displayed in the Application Details page.

- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.

4. Specify the application’s **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

- In the Authentication tab, click **Add**; a drop-down list of authentication characteristics is displayed.
- Select the authentication characteristic to specify.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault (Step 1). Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
 - **Manually** – Add accounts manually one at a time, and specify all the account details.
 - **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
 - i. Add the Provider user as a Safe Member with the following authorizations:
 - List accounts
 - Retrieve accounts
 - View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

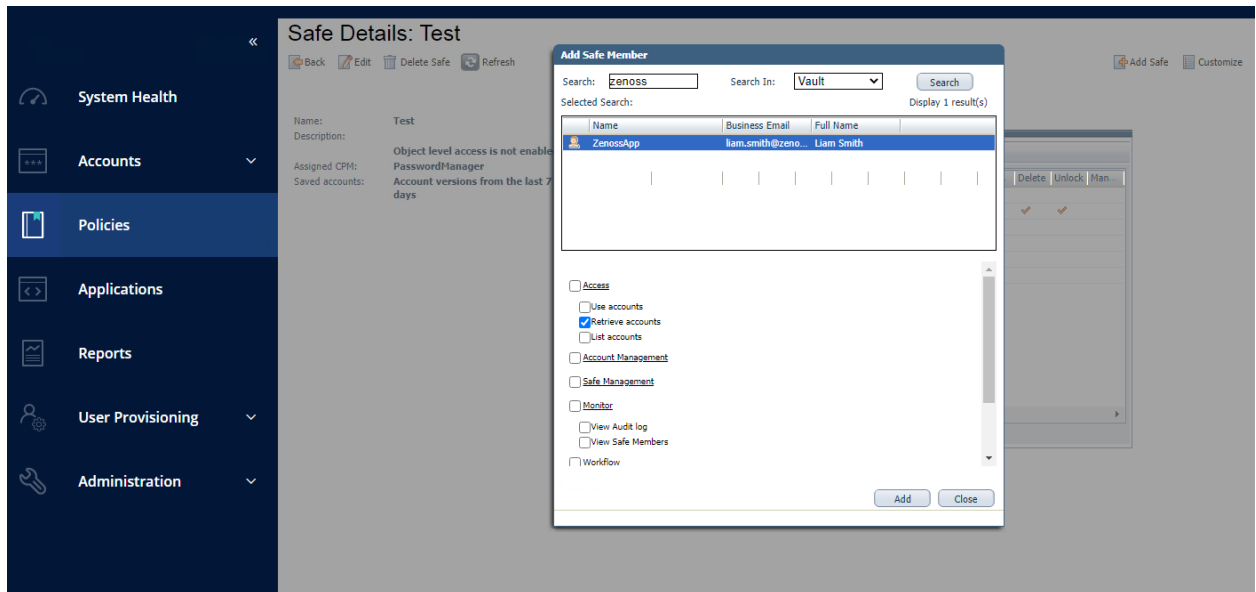
☐ View Audit log

☒ View Safe Members

Add

Close

- ii. Add the application(the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts



- iii. If your environment is configured for dual control:
 - In Privileged Account Security solutions when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- iv. If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

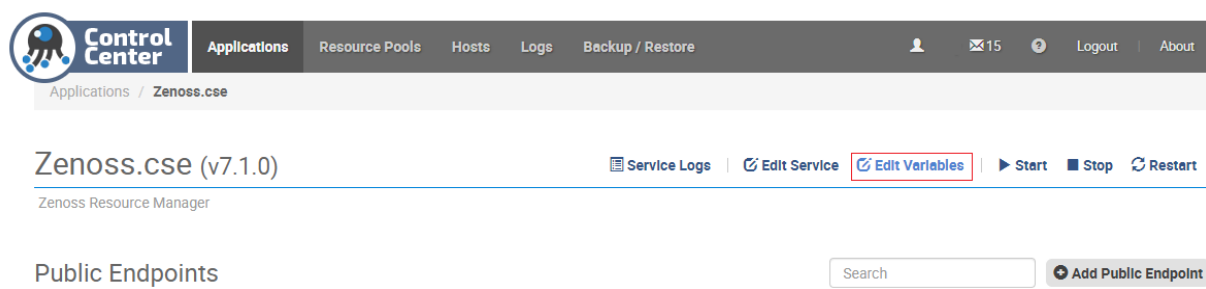
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to help.zenoss.com for zenoss cloud and its components documentation.

Zenoss configuration to work with CyberArk:

- Launch Control Center web based component of collection zone and open settings of the Zenoss Resource Manager



Edit Variables



Enter each key/value pair, separated by a space. One entry per line.

```
1 global.conf.cyberark-cert-path /opt/zenoss/cyberark
2 global.conf.cyberark-port 443
3 global.conf.cyberark-query /AIMWebService/api/Accounts?appid=
4 global.conf.cyberark-cache-ttl 300
5 global.conf.cyberark-url https://example-service.com
6
```

✕ Cancel

✓ Save

- Update global settings of collector daemons configuration properties to provide CyberArk URL, port number, absolute path inside demons containers for security certificate, query format and time to retain credentials in cache in seconds.
 - **global.conf.cyberark-url <e.g example-service.com>**
 - **mandatory, no default value**
 - global.conf.cyberark-port <e.g 13135>
 - optional, default value: 443
 - global.conf.cyberark-cert-path <e.g /some/path/to/certs>
 - optional, default value: /opt/zenoss/cyberark
 - global.conf.cyberark-cache-ttl <e.g 600>
 - optional, default value: 300
 - global.conf.cyberark-query - <e.g /AIMWebService/api/Accounts?appid=>
 - optional, default value: /AIMWebService/api/Accounts?appid=
- Install security certificates on a collector host:
 - Logon to the host using ssh credentials
 - attach to the zope container

- copy certificates (RootCA.crt, client.crt, client.pem) to the folder that are defined in the global.conf.cyberark-cert-path
 - detach from the container
 - commit changes
 - restart all Zenoss services in the Control Center
- Launch zenoss cloud URL
- Select the device that needs to be monitored and provide the CyberArk query information into the fields - username and password.

Add a Single Device

Hostname or IP address:

Device Class:

Collector:

Model Device: ☒

[Less...](#)

Snmp Community:

Snmp Port:

Tag Number:

Rack Slot:

Serial Number:

zCommandUsername:

zCommandPassword:

Title:

Production State:

Device Priority:

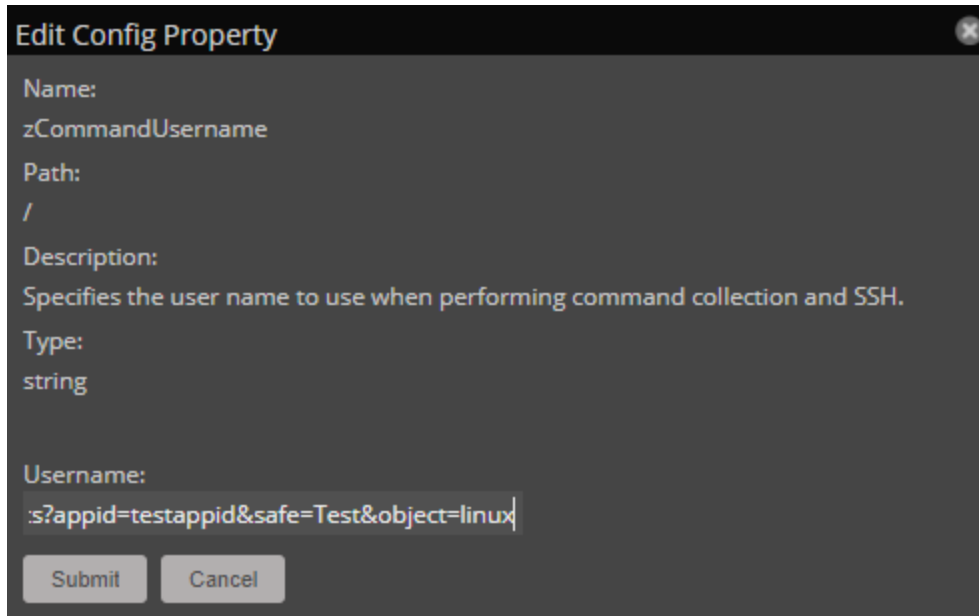
Comments:

Location:

Groups:

Systems:

- In the case if you need to change CyberArk query information after adding a device, you may edit specific zProperty in the device configuration properties



Edit Config Property

Name:
zCommandUsername

Path:
/

Description:
Specifies the user name to use when performing command collection and SSH.

Type:
string

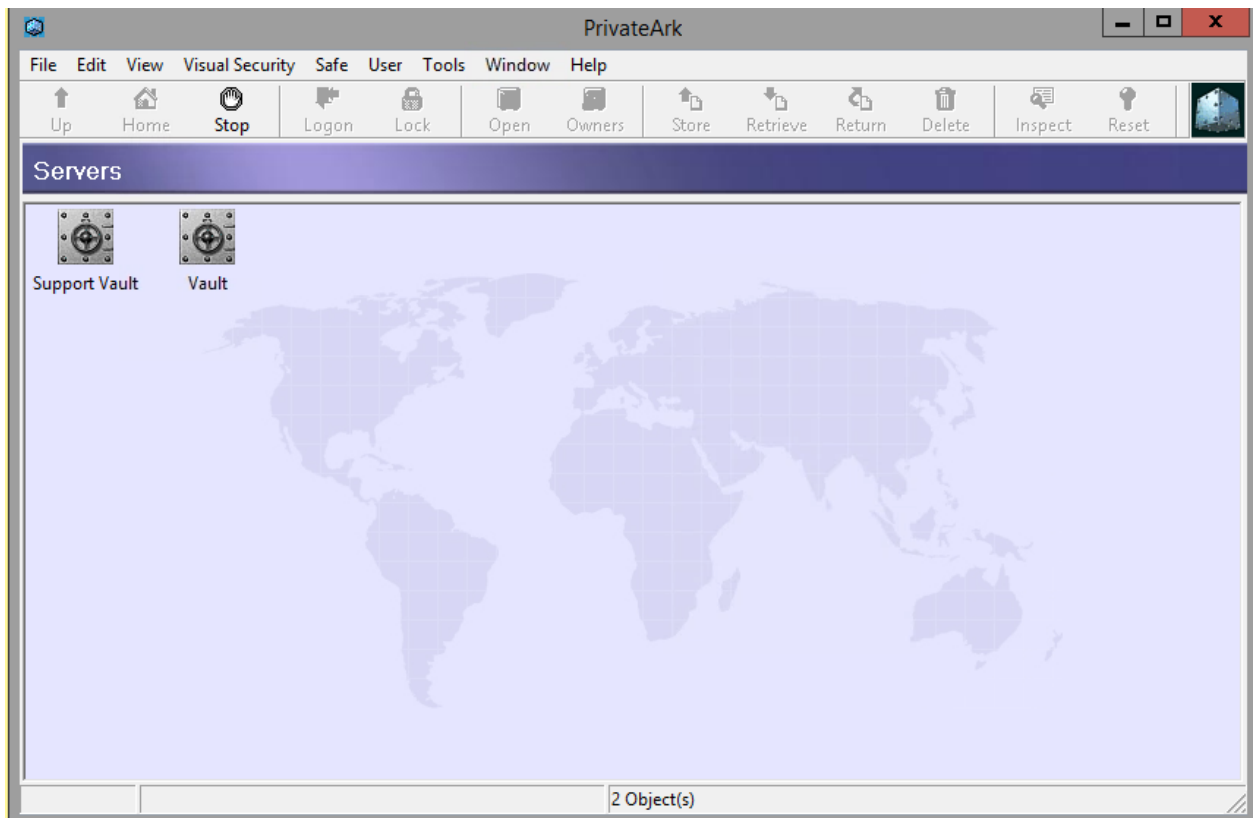
Username:
:s?appid=testappid&safe=Test&object=linux

Submit Cancel

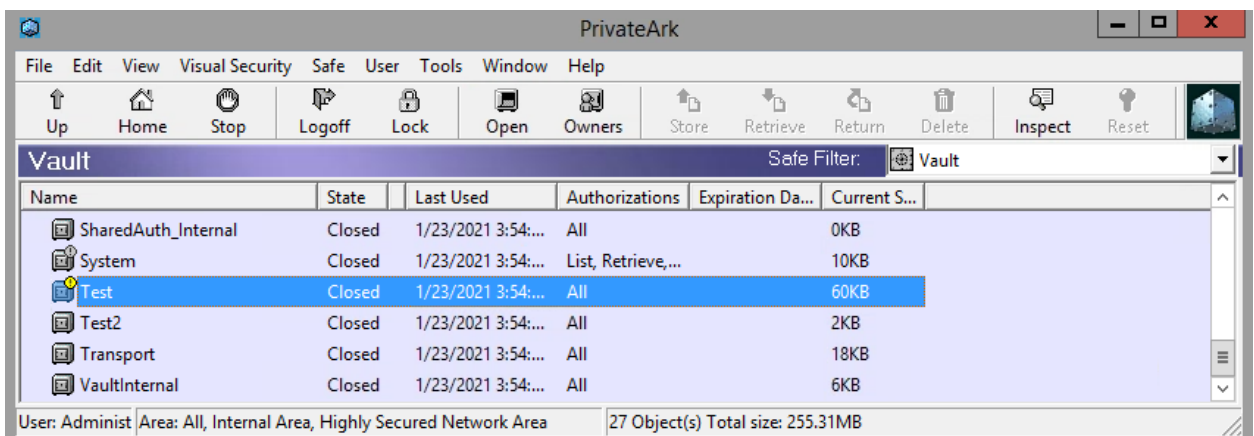
Adding password objects in PrivateArk Application:

The steps 2 and 3 need to be repeated for the devices and/or group of devices to be monitored for their health and performance.

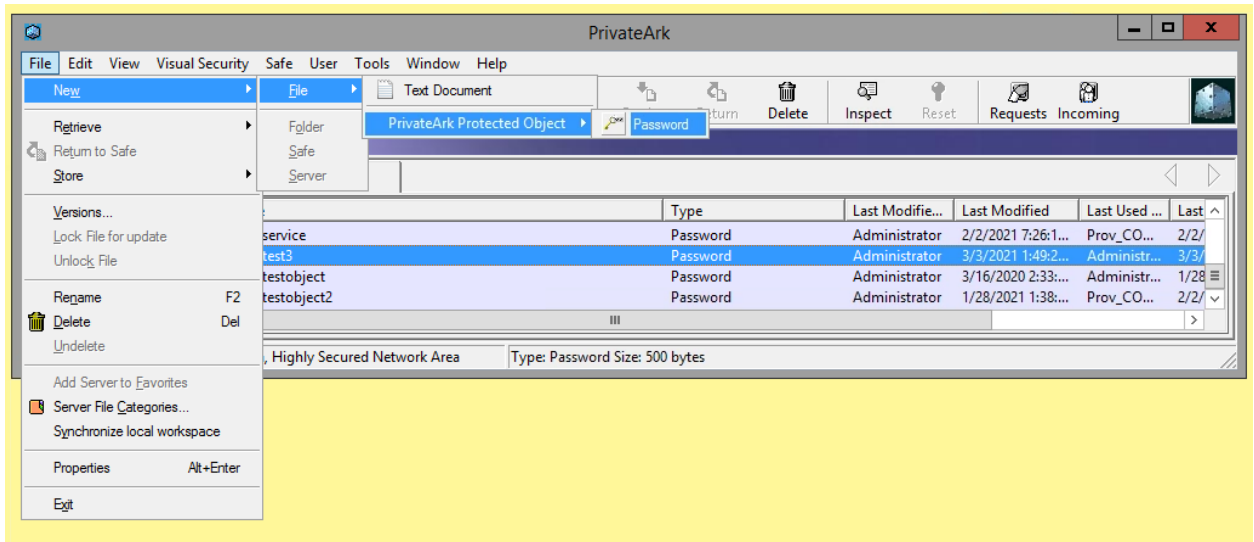
1. Launch the vault in the PrivateArk application.



2. Select Safe for new password



3. Add new password object



Common Use Cases

1. Monitoring Windows Devices

Use the “Add a single Device ...” option from the dropdown menu on the Infrastructure page of Collection Zone UI.

Provided valid CyberArk query information for zWinRMUser and/or zWinRMPasswd (e.g /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=win_user and/or /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=win_password)

Add a Single Device

Hostname or IP address:

win_device

Device Class:

/Server/Microsoft/Windows

Collector:

localhost

Model Device:

☒

Less...

Snmp Community:

Snmp Port:

161

Tag Number:

Rack Slot:

Serial Number:

zWinRMUser:

/AIMWebService/api/Accounts:

Title:

Production State:

Production

Device Priority:

Normal

HW Manufacturer:

HW Product:

OS Manufacturer:

OS Product:

zWinRMPassword:

.....

Comments:

None...

Location:

None...

Groups:

None...

Systems:

None...

zWinKDC:

zWinScheme:

http

zWinRMPort:

5985

Add

Cancel

2. Monitoring Linux Devices

Use the "Add a single Device ..." option from the dropdown menu on the Infrastructure page of Collection Zone UI.

Provide valid CyberArk query information for the fields zCommandUsername and/or zCommandPassword (e.g
 /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=linux_user and/or
 /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=linux_password)

Add a Single Device

Hostname or IP address:
linux_device

Device Class:
/Server/SSH/Linux

Collector:
localhost

Model Device:
☒

Less...

Snmp Community:

Snmp Port:
161

Tag Number:

Rack Slot:

Serial Number:

zCommandUsername:
/AIMWebService/api/Accounts?

Title:

Production State:
Production

Device Priority:
Normal

Comments:
None...

Location:
None...

Groups:
None...

Systems:
None...

zCommandPassword:
.....

Add

Cancel

3. Monitoring Google Cloud Platforms

Use the “Add Google Cloud Project ...” option from the dropdown menu on the Infrastructure page of Collection Zone UI.

Provide the valid values. Note that the private key is validated for integrity and not allowing to enter CyberArk Query information and let the add device process go through.

Alternatively, choose the edit option

Update `zGoogleCloudPlatformPrivateKey` with a valid CyberArk query (e.g. `/AIMWebService/api/Accounts?appid=testappid&safe=Test&object=gcp_key`)

Edit Config Property

Name: zGoogleCloudPlatformPrivateKey

Path: /

Description: Private key to use for monitoring. (private_key)

Type: password

Private Key:

Submit Cancel

4. Monitoring AWS devices

Use the “Add EC2 Account ...” option from the dropdown menu on the Infrastructure page of Collection Zone UI.

Provide the values of valid CyberArk query information for Access Key and/or Secret Key (e.g /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=aws_access_key and/or /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=aws_secret_key)

Add EC2 Account

Device Name: aws_test

Account ID: some_id

Access Key: /AIMWebService/api/Accou

Secret Key:

Collector: localhost

Add Cancel

5. Monitoring Azure targets

Use the “Add Azure Subscription ...” option from the dropdown menu on the Infrastructure page of Collection Zone UI.

Provide a valid CyberArk query information for **Azure AD Application Secret Key** (e.g /AIMWebService/api/Accounts?appid=testappid&safe=Test&object=azure_key)

Add Azure Subscription

Device title (required):

azure_test

Collector:

localhost

Subscription ID (required):

.....

AZURE RESOURCE MANAGEMENT OR CLOUD SOLUTION PROVIDER CREDENTIALS:

Azure AD Application ID (required):

.....

Azure AD Application Secret Key (required):

.....

Azure AD Tenant ID (required):

.....

AZURE SERVICE MANAGEMENT CREDENTIALS:

Certificate file name (optional)
(e.g. /var/zenoss/msazure.pem):

Add

Cancel

PARTNER CONTACT INFO

Business Contact	Name	Padmanand Warriar
	Email	pwarrier@zenoss.com
	Tel	
Technical Contact	Name	Rajan Varathappan
	Email	rvarathappan@zenoss.com
	Tel	512-484-9369
Support Contact	Name	Jean Smith
	Email	jsmith@zenoss.com
	Tel	