# CyberArk Outposts Test Plan

**CyberArk AWS Outposts Partner Test Plan**

**Partner name:**  
 CyberArk

<https://cyberark.com>

**Partner and AWS stakeholder names, title, email:**

James Stutes, Alliances Technology Engineer, [james.stutes@cyberark.com](mailto:james.stutes@cyberark.com)  
  
**Brief description of the partner solution:**  
 The CyberArk Privileged Access Security solution provides secure storage and management of privileged accounts while auditing and recording the use of credentials stored in the CyberArk Enterprise Password Vault.  
  
**Summary of customer use case for the partner solution on Outposts:**  
 The CyberArk Enterprise Password Vault (EPV) is a highly encrypted database residing on a hardened Windows OS with a single ingress/egress port. The availability of this instance(s) is paramount to the successful operation of applications throughout the organization’s infrastructure. The use case is to ensure that EPV replication is successful between on-prem, AWS proper and Outpost as well as retrieval of credentials from CyberArk users and applications within the organization.

**Existing AWS Marketplace offering:**  
 CyberArk Privileged Access Security Solution enables enterprises to protect both traditional and modern workloads by providing powerful solutions for securing passwords, credentials, and secrets. The solution enables enterprises to consistently enforce privileged access security policies across cloud, on-premises, and hybrid environments.

Additionally, CyberArk cloud automation tools simplify and accelerate the deployment of CyberArk in cloud environments using AWS CloudFormation templates to deploy the Core PAS solution.

<https://aws.amazon.com/marketplace/pp/B07DHVTDYV?qid=1591903759167&sr=0-3&ref_=srh_res_product_title>

**Has the solution already been tested on EC2?**  
T3, M4, M5, C5  
  
**Which AWS services will the solution require to run locally on Outposts:**  
CloudFormation, EC2, Lambda, VPC, S3, CLI, LogStream, IAM  
  
**Which AWS services will the solution need to access from the AWS Cloud:**  
EC2, VPC, IAM, KMS, SSM  
  
**Is there an architecture diagram of the partner solution?**  
Yes

**Any reason why more than (1) Outpost rack will be needed to perform testing?**

No

**Why is lab testing necessary?**

Testing will confirm the viability of the customer request and allow us to understand how CyberArk can be emplaced to better take advantage of what the Outpost capability can provide. We would like to better understand the advantages of leveraging Outpost through latency testing.

**TEST PLAN**

**Summary of test objectives and success criteria:**  
 CyberArk will perform deployment of the Core PAS solution using CloudFormation templates. We will conduct light configuration modifications to account for the new environment and populate the Enterprise Password Vault with users and account objects. We will test the functionality of the CyberArk EPV by conducting data replications between EPV instances located both on-prem and in AWS cloud in conjunction with testing credential retrieval capabilities from the various environments. All deployment steps will be documented along with configuration steps for implementing test. Success will be declared when we complete data replication from primary EPV to on-prem and AWS cloud and all Core PAS components are functioning properly.   
  
**Test environment details:**

EC2 Instances:

* CPM: c5d.9xlarge
* PSM: m5.4xlarge
* PSMP: m5.4xlarge
* PVWA: m5.4xlarge
* Vault: m5.4xlarge
* DR: m5.4xlarge

IAM Roles:

1 IAM Role allowing CloudFormation templates to be run creating network segments, KMS keys, EC2 instances, Lambda functions, IAM roles and LogStream ARNs.

VPC Subnets:

* Qty (4) subnets
  + Vault
    - Subnet containing Primary Vault instance
    - m5.4xlarge running hardened Windows server 2016
    - /24 subnet
    - External access limited to single port (1858)
  + DR
    - Identical to the Vault subnet with same restrictions
    - Constant data replication between the DR and Primary Vault subnets
  + Components Main
    - Subnet containing all CyberArk Components that communicate with Vault
    - /24 subnet
  + Components Secondary
    - Identical subnet to Main and used to add additional CyberArk Component servers

**Test #1 description:**  
 Initial launch of CloudFormation templates of CyberArk AMIs and smoke tests to validate connectivity

**Test 1 steps:**

* Launch NAT Network CloudFormation template using the AWS Console
* Launch AIO CloudFormation to using the AWS Console to install Primary and DR Vault, CPM, PVWA, PSM, and PSMP
* Populate Primary Vault with User and Account data and ensure proper replication to DR Vault
* Verify CyberArk Component connectivity and functionality.

**Test 1 success criteria:**  
 All CloudFormation templates run to completion with no error. Vault Server service is responsive and PVWA can authenticate. The WebServices SDK functions and accepts requests. Monitored sessions through the PSM can be initiated from the PVWA server. An SSH session can be initiated through the PSMP server

**Test 1 results:**

Templates deployed in the us-west-2 region with no errors and the results were evaluated by the team for anything that could be considered a roadblock.

It was discovered that CyberArk CFN Templates require the use of an AWS Managed Default key to install the Vault and DR servers as well as the requirement to create Lambda functions that create roles that interact with KMS. This required major modification of the CFN Template from the team to work with Customer Managed Keys.

The team was able to manually create IAM roles needed for the instances and the necessary modifications were made to the CFN template to accept the CMK that was provided for this lab environment.

During the deployment stage severe network interruptions were experienced and an internal AWS case was input by the team, and work continued on the deployment of the solution. Once the correct modifications to the CFN template were completed, a successful full deployment of the CyberArk solution into Outpost was achieved.

Once the templates completed, testing authentication and navigation of the PVWA, as well as authenticate to the WebServices SDK was achieved.

Recorded and isolated PSM connections were launched to other instances within the VPC, and the network issues that were experienced have an impact on this workflow. The flow of communications comes from PVWA to Vault to gather data, then PVWA launches an RDP session to the PSM with the data collected, and finally the PSM launches an isolated RDP session to the target, all of this from a bastion host in us-east-2.

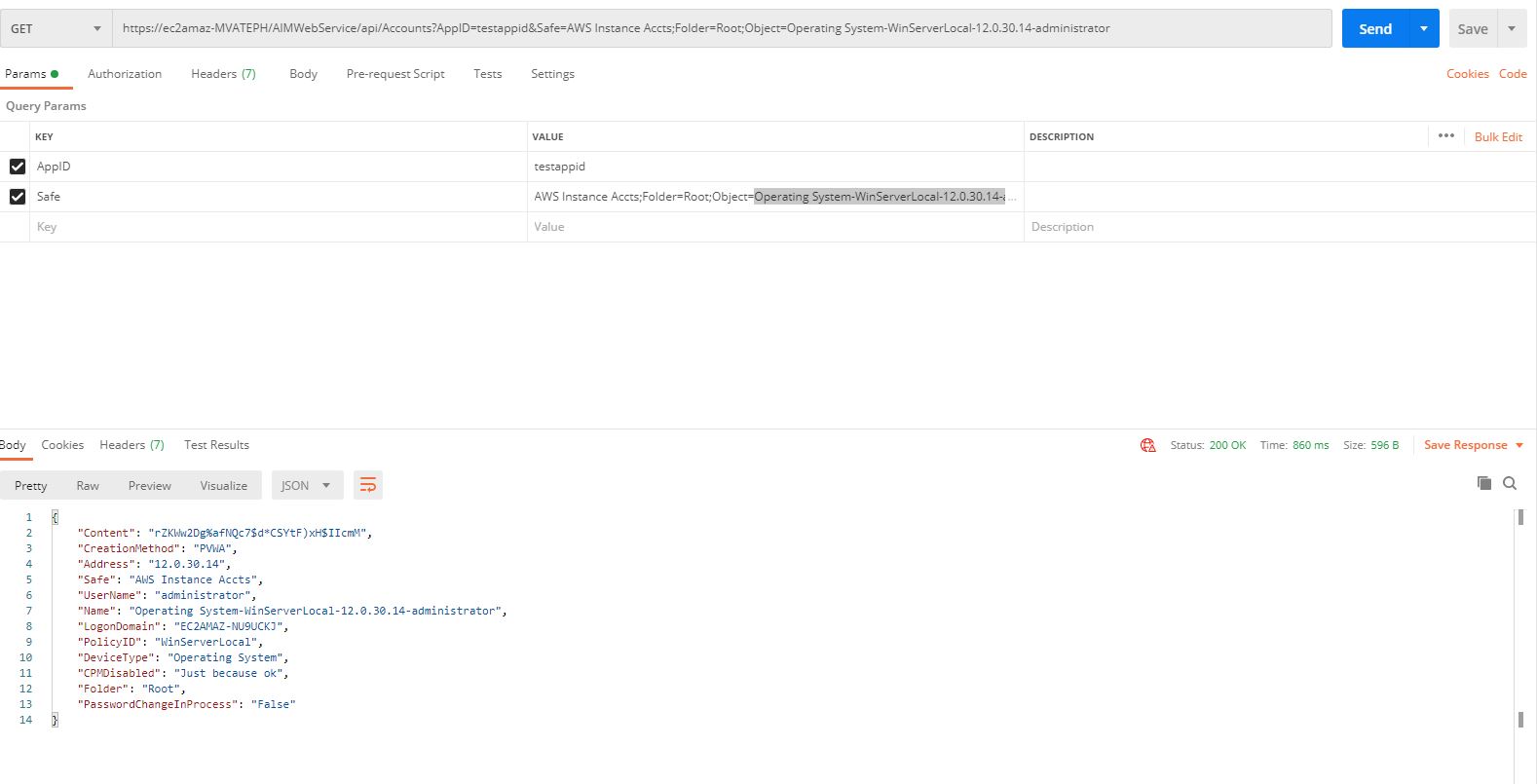
Due to time restrictions, testing of PSMP activity to \*NIX instances was not completed.

**Test 2 description:**  
 Install a CyberArk Application Access Manager credential retrieval agent on the PVWA. Once the Credential Provider (CP) is installed, an IIS plugin is installed to host the AIMWebServices Central Credential Provider service. This exposes a single REST API endpoint for credential retrieval.  
  
**Test 2 steps:**

* Install Credential Provider agent on PVWA
* Install Central Credential Provider on PVWA
* Configure ApplicationID with client certificate authentication
* Ensure that credential can be retrieved from other environments

**Test 2 success criteria:**  
Credentials can be retrieved with no latency from AWS Cloud and on-prem solution.

**Test 2 results:**  
The installation of the CCP on the PVWA presented no issues and the capability was up and running in a short period of time. Once the capability was online, retrieval of credentials from the bastion host located in the us-east-2 region was successful:

[](https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/CCP_postman.JPG?raw=true)

596 bytes at 860ms

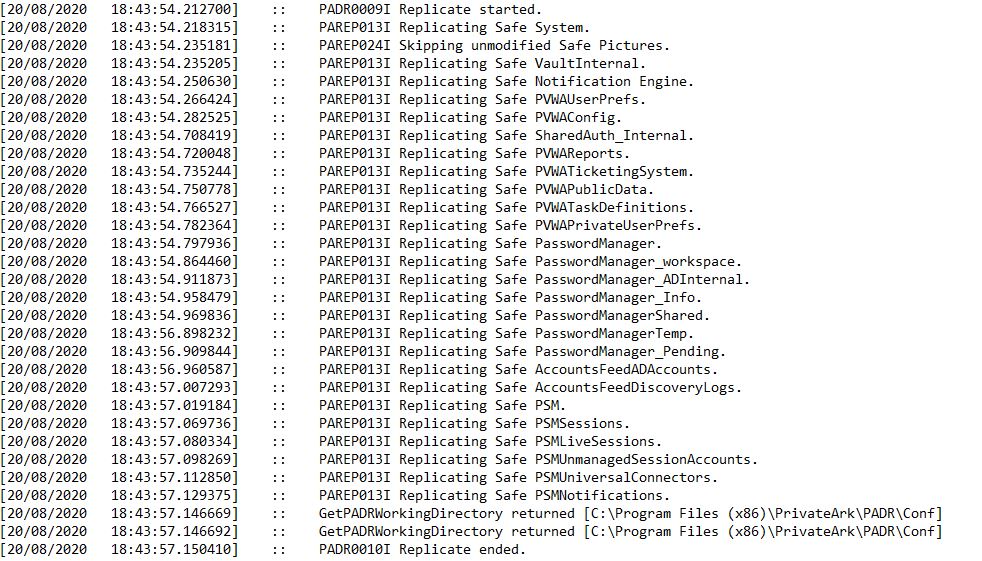
**Test 3 description:**  
 The Vault is at the core of what CyberArk provides as a solution and data replication is something our customers are interested in seeing illustrated. Just as important as the data is getting the data out of the vault to applications that need them to function.  
  
**Test 3 steps:**

* Replicate Vaults
* Retrieve credentials using Application Access Manager components (CP, CCP)

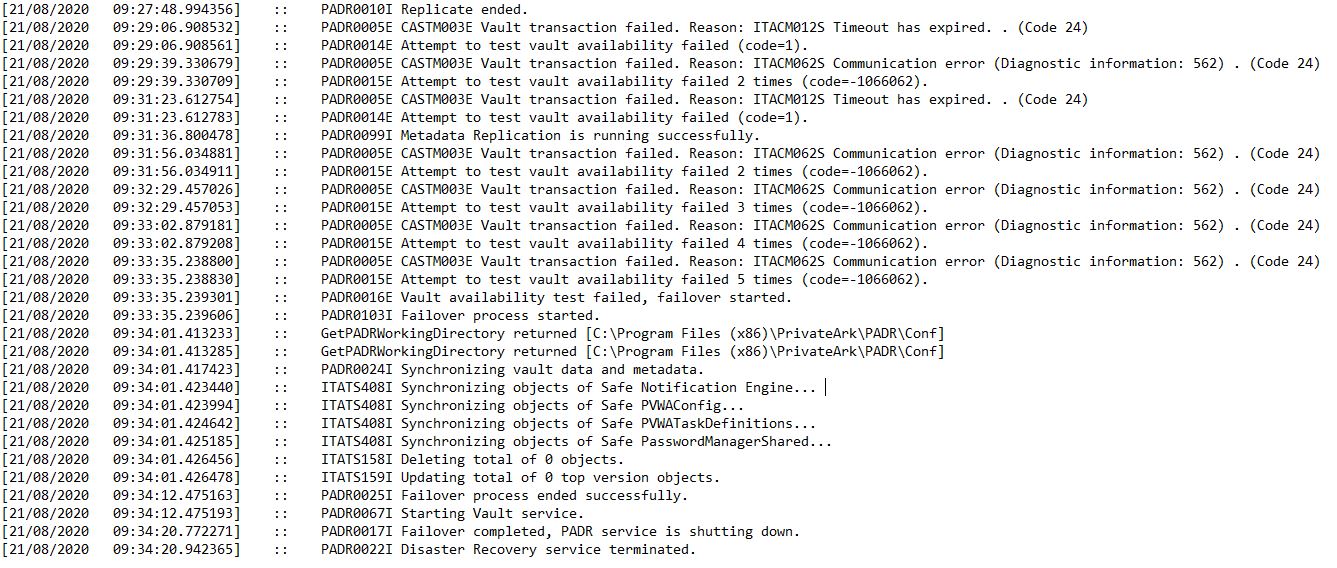
**Test 3 success criteria:**  
 A completion of data replication from multiple sources results in a successful functionality test.

**Test 3 results:**

Successful data replication from the Primary Vault to the DR vault was achieved:

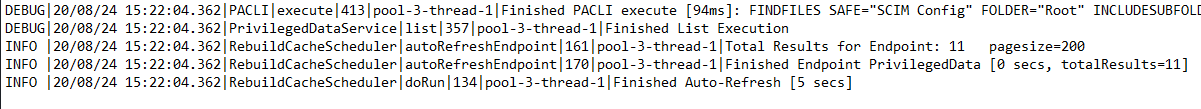
[](https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/replication.JPG?raw=true)

In the DR Vault log collection, the communication issues that were experienced can be observed, and ultimately triggering a successful DR failover due to failed ICMP communication:

[](https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/failover.JPG?raw=true)

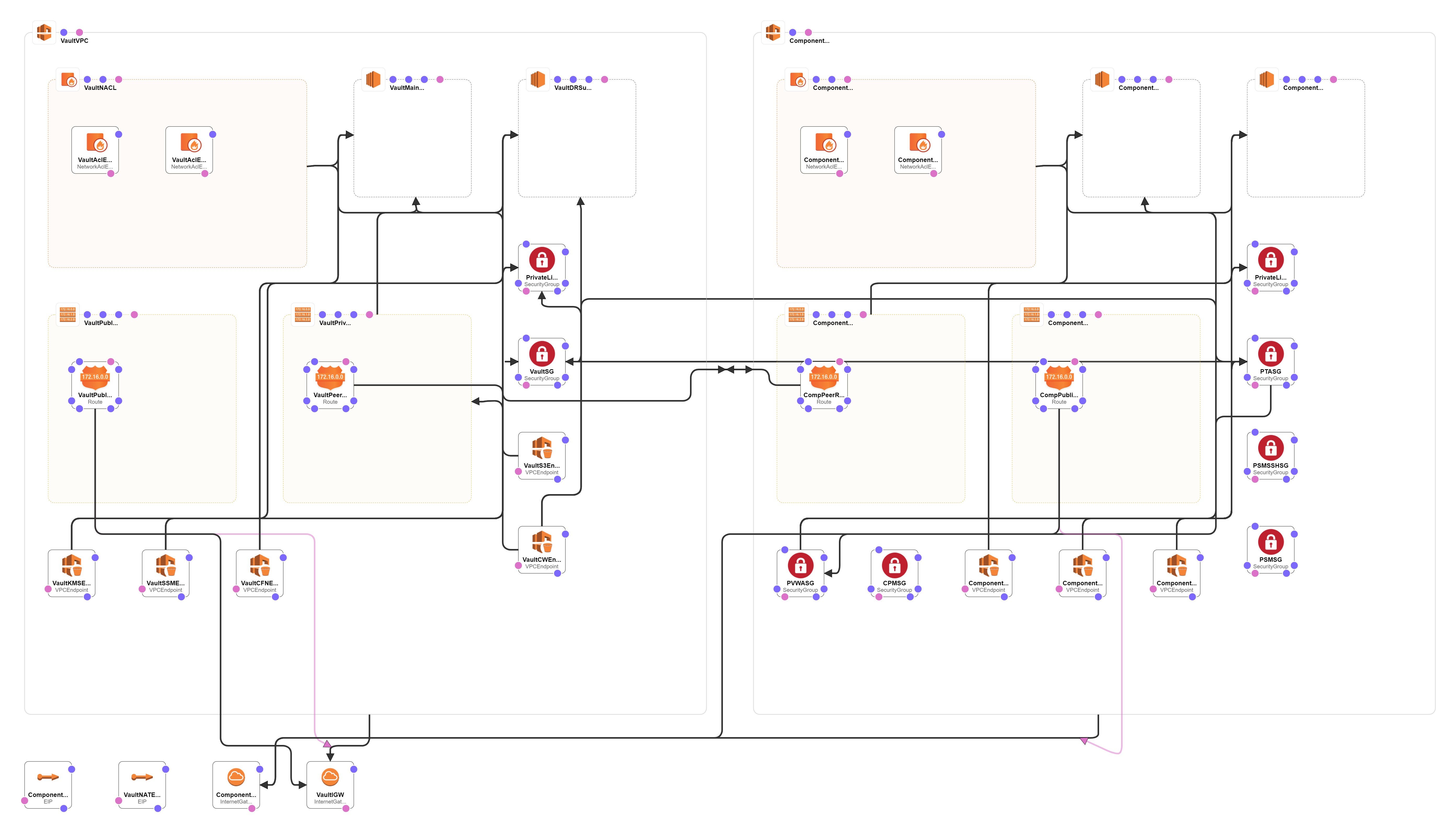
An attempt to stand up a DR instance in another region and connect to Primary Vault on Outpost did not occur due to the DR instance in AWS cloud having a different key than the Primary Vault in Outpost. As a secondary course of action, a data replication was conducted from the Primary Vault to the SCIM server.

The SCIM server queries all data in the Vault (Users, Groups, Safes, Safe Permissions and Privileged Data) and formats all of the Vault contents in a readable format for IAM governance capabilities. This process replicated the Vault contents in 5 seconds.

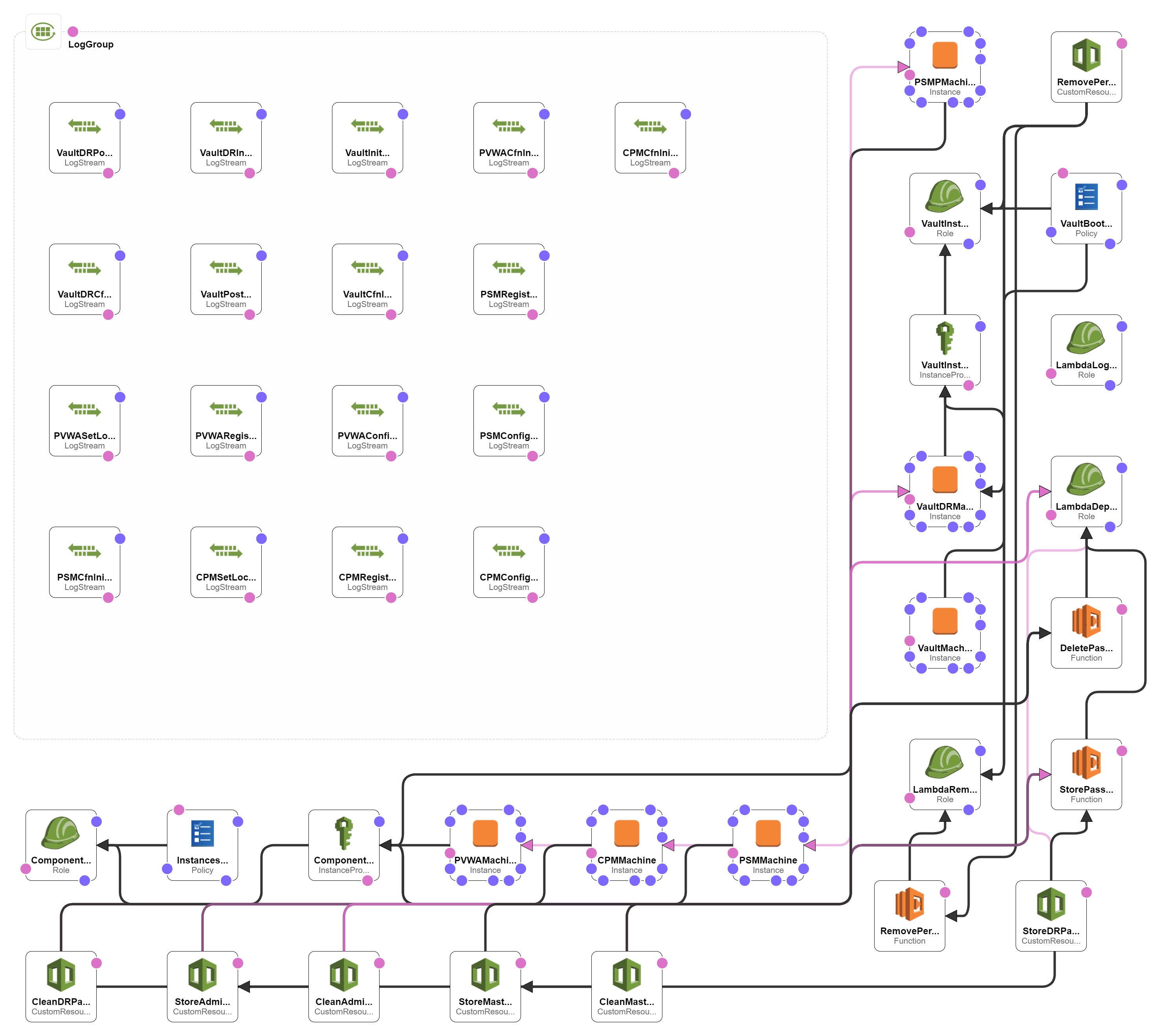


**Test Diagrams**

Network Diagram:

[](https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/Network%20diagram.jpg?raw=true)

Instance Diagram:

[](https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/Architecture%20Diagram.jpg?raw=true)

**APPENDIX**

**Test 1 additional details**

* Link to installation documentation:

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Resources/_TopNav/cc_Home.htm>

**Test 2 additional details**

* Link to AAM implementation documentation:

<https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/Resources/_TopNav/cc_Home.htm>

**Test 3 additional details**

* DR Replication and Failover full logs:

<https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/padr.log>

* SCIM data replication:

<https://github.com/JimmyJamCABD/Documentation_Images/blob/master/AWS%20Outpost/CAScimServer.log>