**Emblem Health**

**Cyberark PIM Project**

Requirements Document - Phase 1

Version : 1.0

Date : 04/28/2017

Prepared By : Cognizant Technology Solutions

*All information contained herein is proprietary and shall be kept confidential.*

APPROVALS

Approval denotes acceptance of the business requirements contained herein and serves as authorization to move forward with related documents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Role** | **Date** |
| Seetharaman Jeganathan | Cognizant | Reviewer |  |
| Arjun Sengupta | Cognizant | Reviewer |  |
| Saleem AT | Cognizant | Reviewer |  |
| Sudhir Kumar Panda | Cognizant | Reviewer |  |
| Bhaskar Bhattacharya | Cognizant | Approver |  |
| Randall Dulin | Cognizant | Approver |  |
| Jim Altinay | Emblem Health | Approver |  |

REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Reviewed by** | **Comments** |
| 1.0 | 4/28/2017 | Cognizant |  | Initial Version for Review |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[REVISION HISTORY 3](#_Toc481169960)

[1.0 INTRODUCTION 6](#_Toc481169961)

[1.1 Project Description 6](#_Toc481169962)

[1.2 Purpose of the document 6](#_Toc481169964)

[1.3 Project Vision 6](#_Toc481169965)

[1.4 Project Objectives 7](#_Toc481169966)

[1.5 Definitions and Acronyms 7](#_Toc481169967)

[2.0 PHASE-1 SCOPE 8](#_Toc481169968)

[2.1 In-Scope 8](#_Toc481169969)

[2.1.1 Functional Scope 8](#_Toc481169970)

[2.1.2 Environmental Scope 9](#_Toc481169971)

[2.2 Out of Scope 10](#_Toc481169972)

[2.3 Dependencies 10](#_Toc481169973)

[3.0 PROJECT STAKEHOLDERS & RESPONSIBLITIES 11](#_Toc481169974)

[4.0 FUNCTIONAL REQUIREMENTS 12](#_Toc481169975)

[4.1 End User Login to Cyberark 12](#_Toc481169976)

[4.2 SQL Database Servers 13](#_Toc481169977)

[4.3 Oracle Database Servers 16](#_Toc481169978)

[4.4 DMZ Servers 19](#_Toc481169979)

[4.5 Access Control through Cyberark 21](#_Toc481169980)

[5.0 NON FUNCTIONAL REQUIREMENTS 23](#_Toc481169981)

[5.1 Environment Setup 23](#_Toc481169982)

[5.1.1 Test Environment Setup 23](#_Toc481169983)

[5.1.2 DMZ CPM/PSM Installation & Configuration 23](#_Toc481169984)

[5.2 Security Considerations 23](#_Toc481169985)

[5.3 Licensing Requirements 24](#_Toc481169986)

[5.4 Auditing and Reporting 24](#_Toc481169987)

[6.0 Appendix 25](#_Toc481169988)

[6.1 CyberArk Current State 25](#_Toc481169989)

[6.1.1 Servers 25](#_Toc481169990)

[6.1.2 Architecture 26](#_Toc481169991)

[6.1.3 As Is - Server Sizing-Production 27](#_Toc481169992)

[6.1.4 As Is - Server Sizing-DR 27](#_Toc481169993)

[6.1.5 Data Count 27](#_Toc481169994)

[6.2 To Be - Test Environment 28](#_Toc481169995)

[6.3 Password Policy 28](#_Toc481169996)

[6.4 Inventory 29](#_Toc481169997)

[7.0 OPEN ITEMS 30](#_Toc481169998)

# INTRODUCTION

## Project Description

Emblem Health (“EH” henceforth) is looking for services from Cognizant to enhance Privileged Identity Management (PIM) service/system to address Privileged accounts present in their network and to customize solutions that integrates Cyberark to stay secure.

Below is a list of known issues that must be addressed using Cyberark.

* Currently End users are not using Cyberark for accessing the End Points.
* No Password Management policy is configured in Cyberark currently.
* Though PSM is configured, no session recording is enabled currently and hence no recording is available for audit.
* The decommissioned account are not being removed from Cyberark currently

Cognizant Team envisions addressing these gaps.



## Purpose of the document

The purpose of this document is to capture requirements as they relate to enhance existing Cyberark environment with additional target systems in production environment. Requirements are gathered from project stakeholders, subject matter experts, business and technical stakeholders. Use cases (system and actors specific use cases) were identified for the corresponding requirements with granular details like use case type (system or actor based), pre-conditions, normal flow, alternate flow, post conditions and related use cases. These use cases will act as a basis for design and subsequent SDLC phases of the project implementation such as construction, testing and deployment.

## Project Vision

Cognizant Team envisions to mitigate the risks behind unmanaged privilege accounts by onboarding them for a better visibility and traceability in the Cyberark-PIM environment. This document summarizes.

* Designing and building a non-prod environment in Emblem Health.
* Enhancements to the current production environment as part of Phase1 implementation of this project.
* Enabling PSM to isolate, monitor, record and control privileged sessions, PSM will act as a jump server and single access control point to the target system.
* Enabling CPM to manage password for having Zero Password Age.
* Segregation of accounts on the basis of environment or access. On-boarding the privilege accounts listed in auto discovery with approvals.

## Project Objectives

* Cyberark Enterprise Password Vault will enable Emblem Health to mask privileged credentials from users and ensure that these credentials never reach endpoints.
* Cyberark EPV will protect privileged passwords based on privileged account security policies, it will control who and when these accounts and passwords can be accessed.
* The Central Policy Manager automatically enforces enterprise security policy by automatically changing passwords on remote machines without any human interaction.
* The CPM is capable of generating new random passwords and replacing existing passwords on remote machines, and saving the new passwords in the EPV.
* Privilege Session Manager will isolate, controls, and monitor privilege sessions.
* PSM will isolate connection to the target machine when they login to perform critical administrator activities in Windows, Linux, and UNIX based systems, databases etc.
* PSM will act as a jump server and single access control point to the target system.
* PSM allows Real-time monitoring which enables security teams to track privileged account activity and detect suspicious events in real-time and terminate the session remotely.
* PSM captures and stores detailed session audit logs and video recordings, which can be used to auditing and to find the root cause of any incident that has occurred.

## Definitions and Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AAA | Authorization Authentication and Accounting |
| AD | Active Directory |
| CDW | Corporate Data warehouse |
| CPM | Central Policy Manager |
| DB | Data Base |
| DEV | Development |
| EH | Emblem Health |
| EHDW | Emblem Health data warehouse |
| EPV | Enterprise Password Vault |
| OOTB | Out of the box |
| PACLI | Private Ark Command Line Interface |
| PID | Privilege Identities |
| PIM | Privilege Identity Management |
| PSM | Privilege Session Manager |
| PUUT | Password Upload Utility Tool |
| PVWA | Password Vault Web Access |
| SIT | System Integration Testing |
| UAT | User Acceptance Testing |

# PHASE-1 SCOPE

## In-Scope

The following environments need to be on boarded to Cyberark which relates to Phase-1 deployment of Privilege Identity Management Solution.

* SQL Database
* Oracle Database
* DMZ Servers

The below table describes the details of in scope Servers, Systems and Accounts for each individual Tower

|  |  |
| --- | --- |
| **Tower** | **In scope Servers, Systems and accounts** |
| SQL DB | * Local SQL Admin account like SA or Sys DBA * Any non-individual shared account or generic account not used in any application or automated script |
| Oracle DB | * Local OS level accounts being used to do RDP/SSH to Oracle servers * Local DB admin accounts used to connect to Oracle DB * Any non-individual shared account or generic account not used in any application or automated script |
| DMZ servers | * Local Admin Accounts used to login to DMZ servers hosted in Windows OS |

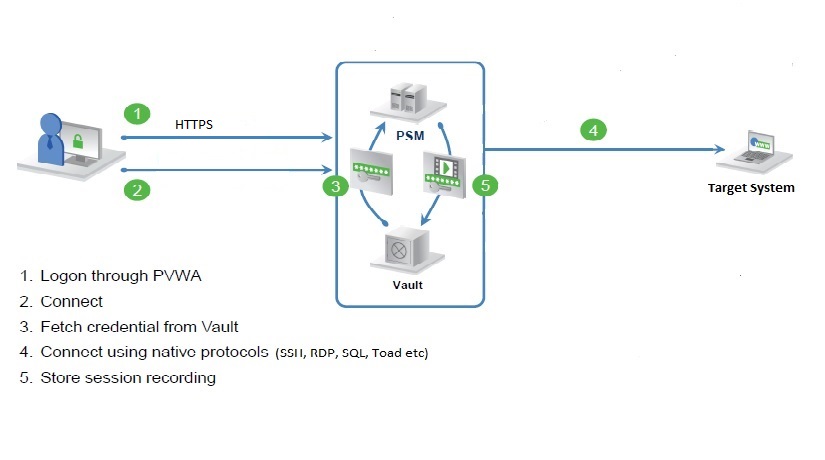
**Note**: The number of servers considered in Phase 1 will be finalized after discussion with different stake holders and EH.

### Functional Scope

Below is a summary of identified functional in-scope activities that are part of the project.

* Identifying list of privileged Accounts which needs to be on-boarded.
* Creating Safes in Cyberark as per EH naming convention.
* Creating Policies based on password change frequency.
* Create the platform based on application by following EH naming convention.
* Configure out-of the box product reports for auditing purpose.
* Testing the privileged accounts to meet the set requirements.
* Configuring Privilege Session manager to isolate, monitor, record and control privileged sessions.

**Privileged Session Manager (PSM) connection overview**



### Environmental Scope

* Co-ordinate with product vendors for procuring required software licenses. Refer to section [License requirements.](#_Licensing_Requirements)
* Additional CPM to be configured in DMZ environment and necessary license to be procured.
* Cyberark –PIM product components are already installed and configured in Production and DR environment, the same setup will be leveraged for this Phase 1 of Cyberark PIM Project
* Coordination with dependent teams to configure networking and load balancing requirements for all the environments. Please refer [Appendix](#_Cyberark_Architecture_in) for the Current Cyberark Architecture in EH.
* Preparing Cyberark Test environment
* Firewall rule for communication are required between Cyberark components and Target systems

Below table can be considered for firewall rule implementation

|  |  |  |  |
| --- | --- | --- | --- |
| **Source** | **Destination** | **Port** | **Reason** |
| CPM & PSM Server | SQL DB Servers | SQL DB Port | If SQL port for the SQL DB servers are restricted |
| CPM & PSM Server | Oracle DB Servers | RDP/SSH and Oracle Port | If SSH/RDP and Oracle port for the Oracle DB servers are restricted |
| Vault | DMZ CPM/PSM | 1858 |  |
| CPM & PSM Server | 1 Test DMZ Server | RDP Port | Need to open Firewall Port to 1 Test DMZ server from Production CPM/PSM |

## Out of Scope

* Any UI customization, customization of core Cyberark functionalities, additional custom connectors.
* Deployment of Cyberark AIM component.
* Dual Control setup and integration with ticketing system
* Any HA configuration
* Any new Cyberark PIM product Installation
* DR configuration for DMZ CPM
* Upgrade of Cyberark environment from version 9.2 to latest version
* The below table describes the details of Accounts and servers that will be out of scope for Phase 1 for individual Towers

|  |  |
| --- | --- |
| **Tower** | **Out Of scope Servers, Systems and accounts** |
| SQL DB | * Individual Network Id being used to connect to SQL DB or to RDP to SQL DB servers * DB Account used to connect to DB from Application/Script |
| Oracle DB | * Individual Network Id to connect to EH CDW or * Oracle DB accounts being used to connect to Oracle DB from Application/Script |
| DMZ servers | * Any DMZ servers other than Windows Operating System |

* Any specific account type not mentioned for any of the towers in the in scope section
* Any specific point not explicitly mentioned in In-Scope.

## Dependencies

* Privileged Identity management policy needs to be defined.
* EH Test environment to be set up for testing purpose.
* On testing phase additional information is required from the four specified towers mentioned in section [In Scope](#_In-Scope). The following table shows the details of the test integration requirement.

|  |  |
| --- | --- |
| **Towers** | **Required items for testing** |
| Database | * Oracle and SQL test admin accounts * Reconciliation accounts * Firewall port open to test database servers from Cyberark * Necessary approvals after demo |
| DMZ | * DMZ server test account * Need to open firewall port from Test Cyberark to one DMZ server to test integration with DMZ server * Necessary approvals after demo |

* Sign-off required from end user, once they are able to login successfully to the target system.

# PROJECT STAKEHOLDERS & RESPONSIBLITIES

Please refer below corresponding project stakeholders.

|  |  |
| --- | --- |
| **Active Directory** | |
| Cognizant SME Names | Malaiarasan Jayaraman (181317) |
| Yogesh Nilajkar (347681) |
| Cognizant SME Roles | AD/ Wintel Administrator |
| Cognizant SME Responsibilities | Participating in UAT |
| EH Distribution list | InternalProdSupport@emblemhealth.com |

|  |  |
| --- | --- |
| **Database – SQL Server and Oracle** | |
| Cognizant SME Names | Lalit Agarwal (567808) |
| Cognizant SME Roles | Database Owner |
| Cognizant SME Responsibilities | Participating in UAT Provide the required data |
| EH Distribution list | Databasesupport@emblemhealth.com |

|  |  |  |
| --- | --- | --- |
| **DMZ Servers** | | |
| Cognizant SME Names | | Yogesh Nilajkar (347681) |
| Cognizant SME Roles | | AD/ Wintel Administrator |
| Cognizant SME Responsibilities | | Participating in UAT Provide the required data |
| EH Distribution list | | InternalProdSupport@emblemhealth.com |
|  |  | |

|  |  |
| --- | --- |
| **EH Stakeholders** | |
| EH Approvers | Jim Altinay, Tom McDermot, Alton Janeway |
| EH Approvers Responsibilities | Review and approve the requirements |
| Review and approve the design |
| Approve build and unit testing phase completion |
| Approve the SIT |
| Approve the UAT |
| Approve the Production Deployment |

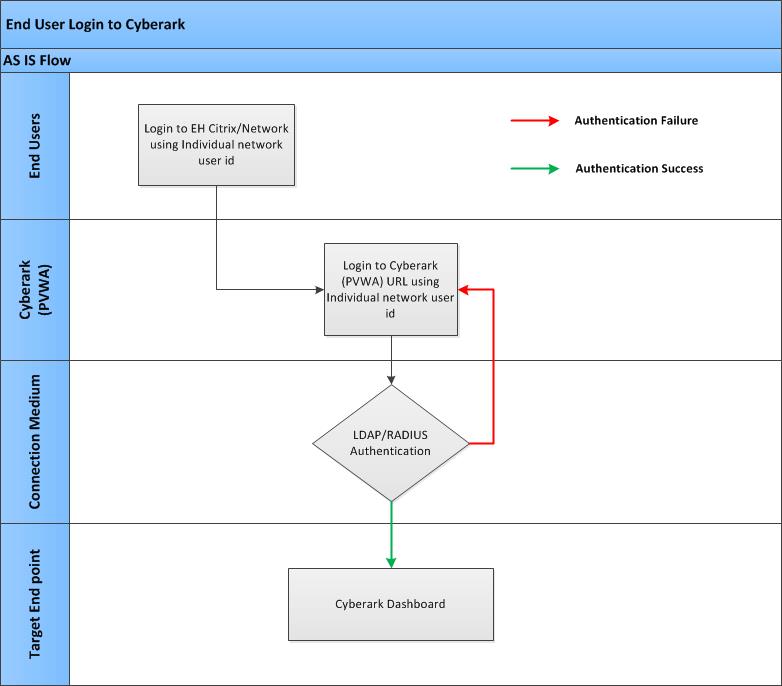
# FUNCTIONAL REQUIREMENTS

## End User Login to Cyberark

Currently, Emblem Health end users login to Cyberark using their network id via Radius authentication. Radius authentication uses DUO.

As this is already implemented, there is no new requirement to implement or enhance the Cyberark login procedure, the below diagram shows the existing login procedure into Cyberark for Emblem Health users.

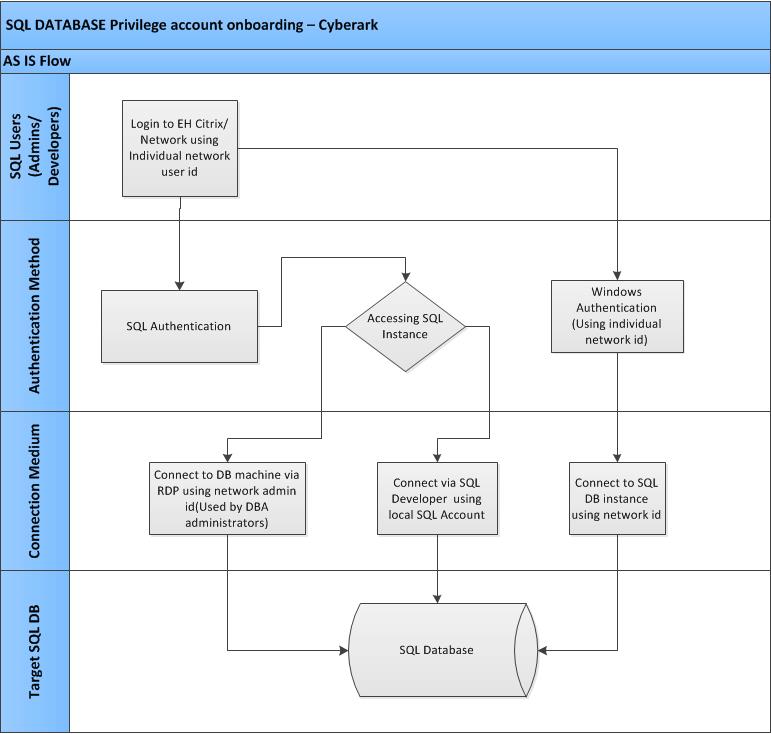
**Note:** All new users requiring access to Cyberark need to have DUO authentication enabled.



## SQL Database Servers

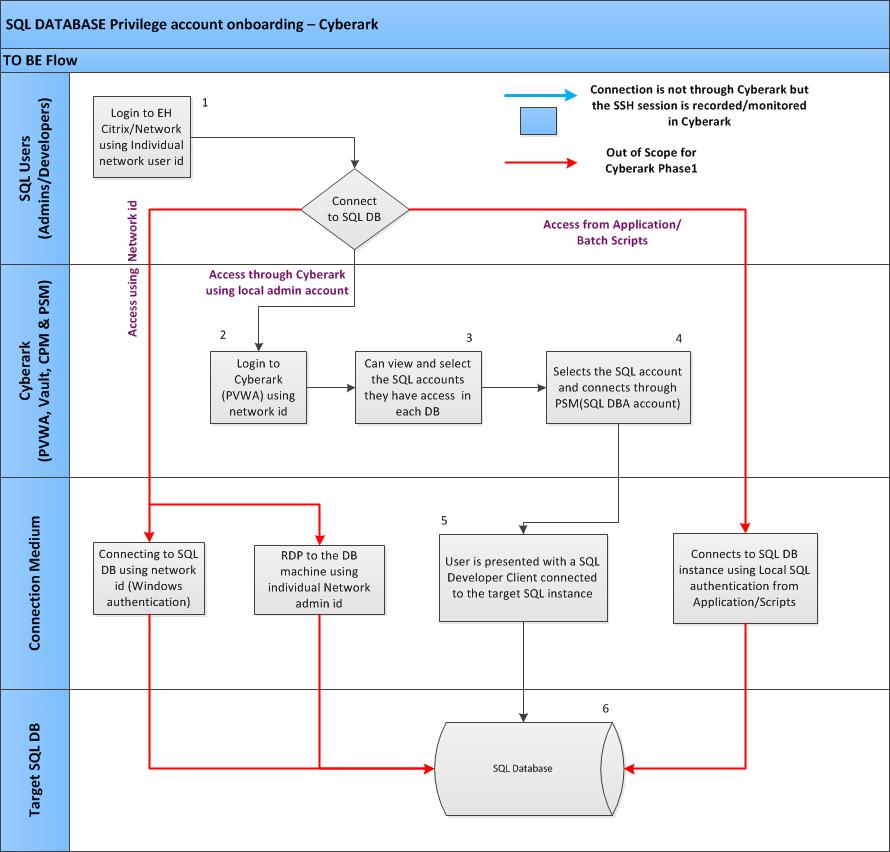
**As Is Flow Diagram:**

The below diagram depict the existing SQL DB connection process:

****

**To be flow diagram:**

The below diagram shows the process flow for accessing Oracle DB using Cyberark

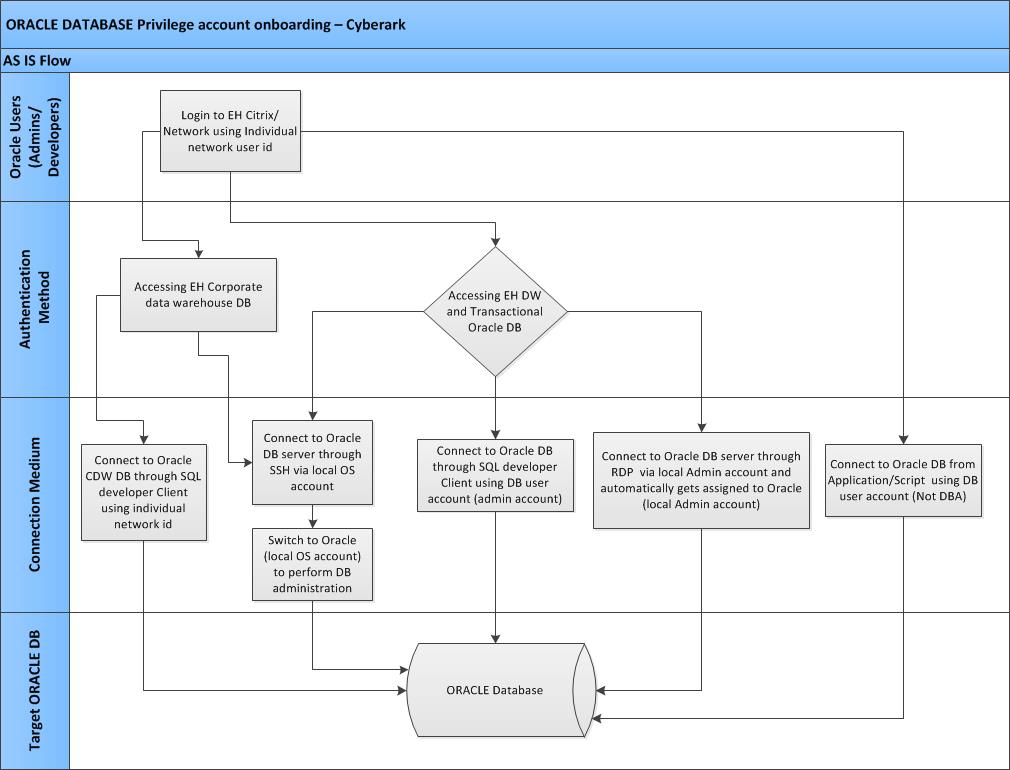
****

|  |  |
| --- | --- |
| **SQL DATABASE** | |
| **Actor** | End User, Cyberark |
| **Prerequisite** | 1. Need the complete inventory of privileged SQL DB accounts 2. Need one Reconciliation account for each DB instances(or single domain account for all DB instances to automatically manage the SQL DB accounts through Cyberark) |
| **Description** | Connectivity to the target SQL Database system will be via Cyberark. The Privilege accounts for the SQL Database systems will be secured in Cyberark. This solution enables organization to secure, provision, control, and monitors all privileged account activities associated with the Database environment. |
| **Use case Requirement** | All SQL database Instances are running on Windows machine. There are three types of SQL accounts which are currently being used to connect to SQL database. Below are the different types of SQL DB accounts and their use:   1. DBA Accounts: Currently there are only two accounts of this type and has the highest privileges to manage SQL DB instances. These users use SQL Authentication methodology to connect to DB. These users do connect to the SQL DB using SQL client and also these users do RDP to the DB machine using there network id and does DB management activity using this DBA local SQL account. These DBA local SQL accounts can be managed through Cyberark and users can be allowed to connect to the DB by PSM 2. Network id/AD Group: These kind of accounts have access to DB with different permissions and login to DB using Windows Authentication Methodology and using SQL Client. As this are individual users account, this will be out of scope for automatic management by Cyberark in this phase 3. Batch login/service accounts: This account are local SQL DB accounts and mostly used in application/scripts (password hard coded). These accounts will be out of scope as Application Identity management is not in scope for this phase.   Now to accomplish the above scenarios below are the process needs to be followed in Cyberark:   1. Safes will be created for different type of SQL DB 2. The in scope accounts will be on boarded into the safes. 3. Cyberark Users or Groups will be provided membership to these safes to use accounts based on their permissions to the safes via PSM |
| **Cyberark To Be Flow** | 1. End user logins to their Emblem Citrix desktop/ EH network 2. Users can login to Cyberark using their Network id into Cyberark, for any incorrect login attempt Cyberark will display error message on screen 3. Once logged in users will be landed in their Cyberark dashboard where they can select the particular SQL DB account they want to use and they have access for 4. Once the account is selected user can chose to connect to the target DB instance 5. Cyberark will connect the user to the DB via PSM and will present a SQL Developer client connected to the DB. 6. Connected to target SQL DB |
|
|
|
|
| **Dual Accounts** | No |
| **PSM Feature** | PSM is available, need to be enabled |
| **Exception flow** | If any error occurs during connection Cyberark will display the OOTB error message on screen. |
| **Inventory** | Please refer [Appendix](#_Inventories) for the inventory list. |
| **Post Conditions** | 1. Post successful connection to the target system, Session must be closed by the end user 2. Once the session is closed Cyberark PSM component will store the session recording in vault. |

## Oracle Database Servers

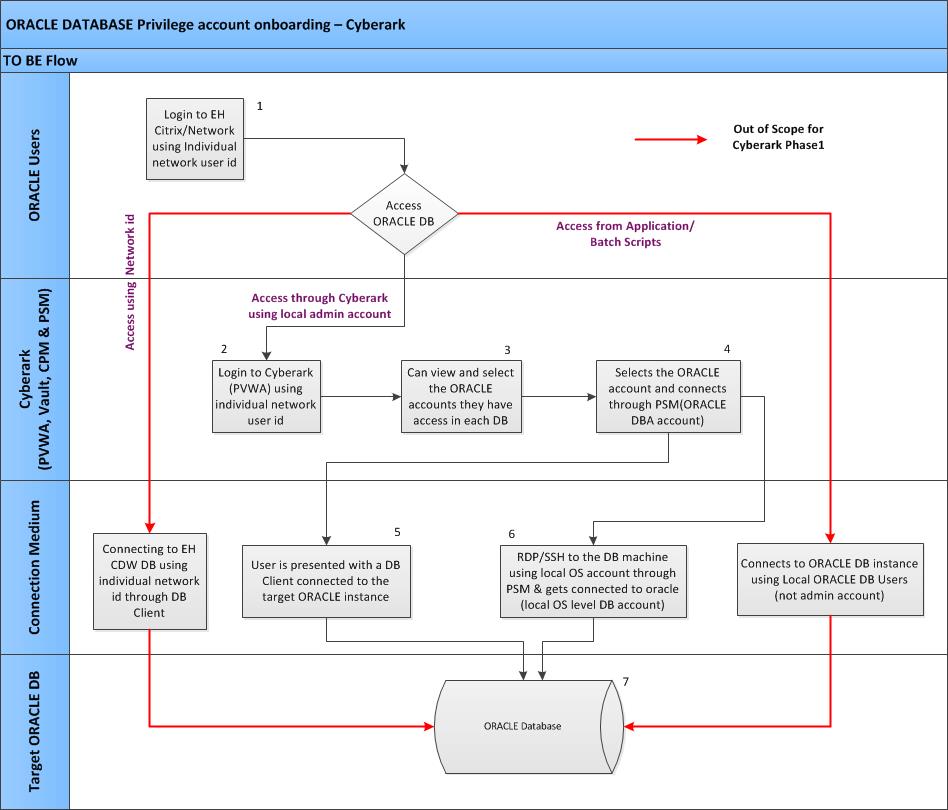
**As Is Flow Diagram:**

The below diagram depict the existing Oracle DB connection process:

****

**To be flow diagram:**

The below diagram shows the process flow for accessing Oracle DB using Cyberark

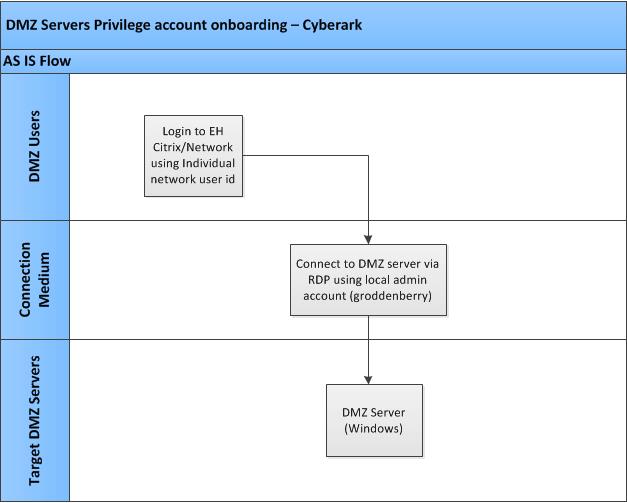


|  |  |
| --- | --- |
| **ORACLE DATABASE** | |
| **Actor** | End User, Cyberark |
| **Prerequisite** | 1. Need the complete inventory of privileged Oracle DB accounts 2. Need one Reconciliation account for each Oracle DB instances(or single domain account for all DB instances to automatically manage the Oracle DB accounts through Cyberark) |
| **Description** | Connectivity to the target Oracle Database system will be via Cyberark. The Privilege accounts for the Oracle Database systems will be secured in Cyberark. This solution enables organization to secure, provision, control, and monitors all privileged account activities associated with the Oracle Database environment. |
| **Use case Requirement** | There are two Oracle data warehouse DB and other transactional Oracle DB. Out of these the EH CDW is integrated with OVD.  User access the CDW DB using there network id through DB client. As these Network ids are individual user accounts these are out of scope for Cyberark for this phase.  The administrators access the EH DW and other transactional oracle database through DB client using local DB user (DBA account). This privileged account will be stored and managed by Cyberark.  Admin users also login to the DB server machine for all type of DB using their local OS level admin account and switch to the Oracle (local OS level DB admin account). These accounts will be managed by Cyberark.  There are DB accounts (Not DBA) used by application team to connect to Oracle DB. These accounts will be out of scope of Cyberark as Application Identity management is out of scope for this phase.  To manage the in scope accounts the below will be configured in Cyberark.   1. Create Safes for Different types of Oracle Database server admin accounts 2. Onboarding the DB privileged accounts in the different safes. 3. Adding users to the safe membership and providing appropriate safe authorization to those safe members 4. Configure any account level access control as required. |
| **Flow** | 1. End user logins to their Emblem Citrix desktop/ EH network 2. Users can login to Cyberark using their Network id into Cyberark, for any incorrect login attempt Cyberark will display error message on screen 3. Once logged in users will be landed in their Cyberark dashboard where they can select the particular Oracle DB account they want to use and they have access for 4. Once the account is selected and user connects to the target system Cyberark will ask for the access reason. 5. **a.** User will be provided with a DB client connected to the target Oracle DB via PSM   **b.** User will be presented with a SSH/RDP console connected to the DB machine and gets connected to Oracle (local OS level DB admin account) via PSM  6. Connected to target Oracle DB |
|
|
|
|
| **Dual Accounts** | No |
| **PSM Feature** | PSM is available, need to be enabled |
| **Exception flow** | If any error occurs during connection Cyberark will display the OOTB error message on screen. |
| **Inventory** | Please refer [Appendix](#_Inventories) for the inventory list. |
| **Post Conditions** | 1. Post successful connection to the target system, Session must be closed by the end user 2. Once the session is closed Cyberark PSM component will store the session recording in vault. |

## DMZ Servers

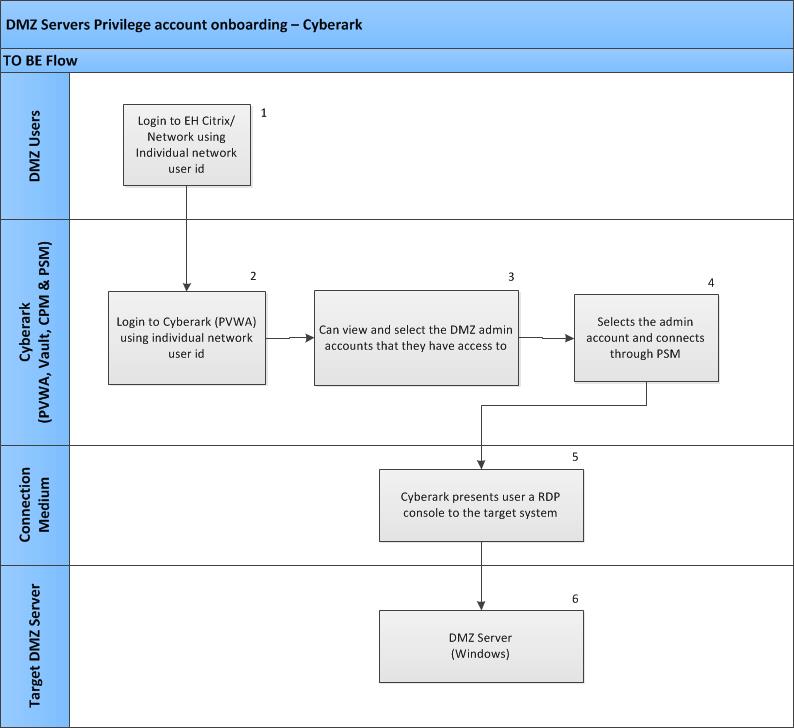
**As Is Flow Diagram:**

The below diagram depict the existing DMZ Server access process:

****

**To be flow diagram:**

The below diagram shows the process flow for accessing DMZ servers using Cyberark

****

|  |  |
| --- | --- |
| **DMZ SERVERS** | |
| **Actor** | End User, Cyberark |
| **Prerequisite** | 1. CPM server to be built in DMZ environment 2. Need the complete inventory of DMZ servers with Privilege accounts 3. Need one Reconciliation account for DMZ servers to automatically manage the DMZ admin accounts through Cyberark |
| **Description** | Connectivity to the target DMZ servers will be via Cyberark. The Privilege accounts in the system will be secured in Cyberark. This solution enables organization to secure, provision, control, and monitor all privileged account activities associated with the DMZ servers. |
| **Use Case Requirement** | Majority of the DMZ servers are Windows servers.  Any DMZ server hosted other than Windows are out of scope for this phase.  Each of these servers has a local admin account (groddenberry) using which the DMZ users do connect through RDP to those DMZ servers. To manage these accounts in Cyberark the following needs to be done:   1. Need to build a CPM server in DMZ environment and configure it in production Cyberark 2. Need to enable firewall rules for Cyberark to connect to DMZ CPM. 3. Need to create safes for DMZ server privilege accounts 4. The in scope accounts will be created into the safes. 5. Cyberark Users or Groups will be provided membership to these safes to use (via PSM) based on their permissions to the safes |
| **Cyberark To Be Flow** | 1. End user logins to their Emblem Citrix desktop/ EH network 2. Users can login to Cyberark using their Network id into Cyberark, for any incorrect login attempt Cyberark will display error message on screen 3. Once logged in users will be landed in their Cyberark dashboard where they can select the particular DMZ server account they want to use and they have access for 4. Once the user selects the account and connection to the target DMZ server is established 5. Cyberark PSM presents the user with a RDP session connected to the server 6. Connected to target DMZ server |
|
|
|
|
| **Dual Accounts** | No |
| **PSM Feature** | PSM is available, need to be enabled |
| **Exception flow** | If any error occurs during connection Cyberark will display the OOTB error message on screen. |
| **Inventory** | Please refer [Appendix](#_Inventories) for the inventory list. |
| **Post Conditions** | 1. Post successful connection to the target system, Session must be closed by the end user 2. Once the session is closed Cyberark PSM component will store the session recording in vault. |

## Access Control through Cyberark

For each tower the access controlled will be based on different type of users (This will be categorized based on access requirement), In Cyberark user groups will be created for different type of users. These groups will be provided with different set of permissions in the account safes.

The following are the three major categories of different type of users in Cyberark.

Approvers/Owners, Users, Developers, Auditors

* Approvers/Owners – Will have permission to approve/reject any access request by users.
* Users – Will have permission to view, use the accounts.
* Developers – Will have permissions only to use the accounts.
* Auditors – Will have permission to view monitor sessions and run reports.

# NON FUNCTIONAL REQUIREMENTS

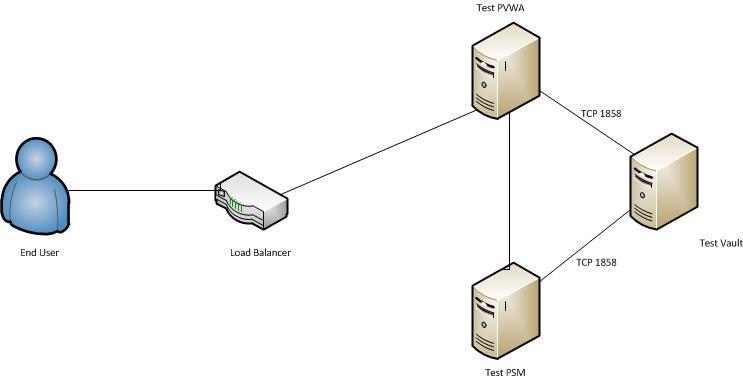
## Environment Setup

EH environment Cyberark PIM will have production environments (PROD/DR) and a non-production (TEST) as per the industry best practice for critical information security systems.

Production and DR environment is already setup. Test environment and an instance of CPM in DMZ needs to be set up in Emblem Health.

### Test Environment Setup

The below image shows the Test environment system architecture



**Note:** Load Balancer is not available now and will be configured in future

### DMZ CPM/PSM Installation & Configuration

Since the DMZ is non-domain joined to manage the DMZ servers in Cyberark with our existing CPM we would require to open multiple firewall ports from CPM to DMZ servers, which is a security risk. Hence it is recommended to place another instance of CPM/PSM in DMZ. This will only require one port, TCP 1858 to be opened to communicate to the Vault. All other ports can talk locally within the DMZ. If there are multiple DMZs, this still limits traffic to the production network.

## Security Considerations

* Use HSM/Keepass to secure the Encryption Key used by Cyberark during installation. (For Future enhancement)
* Secure all the communication from PVWA to any target application by having secure protocol. (For Future enhancement)
* Keep Master/Operator CD securely with limited access and make sure available when ever needed.
* Make sure PAReplicate/PARestore working to recover the Data in real time without any outages whenever needed.
* Retain the ITA/System Log by using SIEM to enhance auditing and forensic need. (For Future enhancement)

## Licensing Requirements

Licenses will be required for the below components for Test environment setup and for upgrading the Production environment in future. Additional components if added in future will require respective license to be purchased.

* Vault-Test
* CPM-Test
* PSM-Test
* CPM-DMZ
* RDS license in the PSM machine and DMZ CPM/PSM machine

## Auditing and Reporting

|  |  |  |
| --- | --- | --- |
| **SL No.** | **Report Name** | **Report Description** |
| 1 | Password Change | Contains the list of accounts whose credentials are not changed as per password policy. |
| 2 | Access Recertification | Contains list of accounts and users whose identity needs to be recertified over a period of time. |
| 3 | Usage Report | Contains the list of accounts with the user details with login log. |

# Appendix

## CyberArk Current State

The following are the current state of Cyberark in Emblem Health environment.

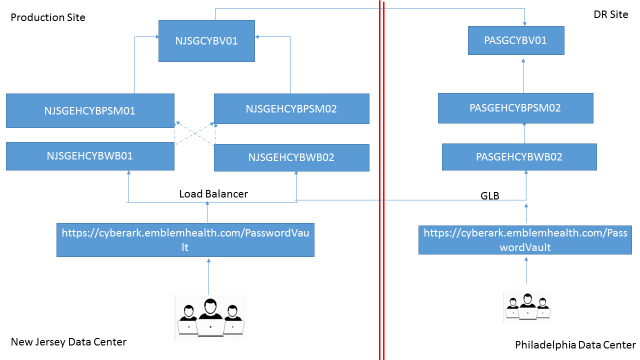
* Cyberark is not being used as a medium to connect with Target Systems i.e. Connection to target systems are handled manually by the respective team or resource administrators
* Privileged Session Manager (PSM) is not enabled, hence monitoring, session recordings and auditing are not possible.
* Password is used and has expired for accounts on boarded but the change did not happen in target system as well as in PVWA.
* Accounts that are de-provisioned in QAR, still exists in Cyberark, hence cleanup is required to free up the space utilization.
* There is no recertification process on decommissioned or disabled accounts.
* Challenges and failures in meeting audit compliance requirements.

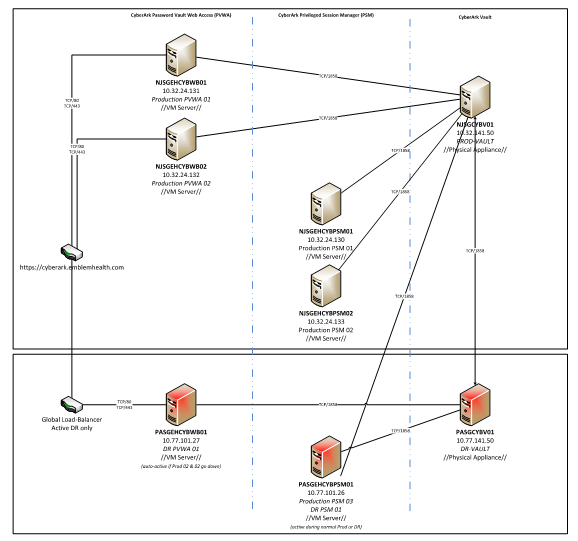
### Servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Cyberark Servers** | | | |
|  |  | **PROD** | **DR** |
| **VAULT** | VAULT Server | NJSGCYBV01 | PASGCYBV01 |
| **PVWA** | PVWA Server 1 | NJSGEHCYBWB01 | NA |
| **CPM** | PVWA Server 2 | NJSGEHCYBWB02 | PASGEHCYBWB01 |
| **PSM** | PSM Server 1 | NJSGEHCYBPSM01 | PASGEHCYBPSM01 |
| PSM Server 2 | NJSGEHCYBPSM02 | PASGEHCYBPSM01 |

### Architecture

The below two pictures shows the current architectural setup of CyberArk components in Production and DR environments.





### As Is - Server Sizing-Production

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Vault** | **PVWA + CPM** | **PSM** |
| **Memory (RAM)** | 32 GB | 16 GB | 16 GB |
| **QTY** | 1 | 2 | 2 |
| **OS** | Windows R2 2008 (64-bit) SP1 | Windows R2 2008 (64-bit) SP1 | Windows R2 2008 (64-bit) SP1 |
| **Storage** | 2x600GB | 80GB | 80 GB |
| **Software (If any)** | .NET Framework 3.5 SP1 | IIS + .NET Framework 3.5 SP1 | IIS + .NET Framework 3.5 SP1 |
| **License** | YES | YES | YES |
| **Database(if any)** | NA | NA | NA |
| **(Physical / Virtual)** | Physical | Virtual | Virtual |

### As Is - Server Sizing-DR

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Vault** | **PVWA + CPM** | **PSM** |
| **Memory (RAM)** | 16 GB | 16 GB | 16 GB |
| **QTY** | 1 | 1 | 1 |
| **OS** | Windows R2 2008 (64-bit) | Windows R2 2008 (64-bit) | Windows R2 2008 (64-bit) |
| **Storage** | 2X 80GB ,2X Network adapter (1Gb),DVD ROM | 40GB | 40GB |
| **Software (If any)** | .NET Framework 3.5 SP1 | IIS + MS Office + .NET Framework 3.5 SP1 | Microsoft Remote Desktop Services (RDS) Session Host |
| **License** | YES | YES | YES |
| **Database(if any)** | NA | NA | NA |
| **(Physical / Virtual)** | Physical | Virtual | Virtual |

### Data Count

|  |  |  |
| --- | --- | --- |
| **Row Labels** | **Count** | **Description** |
| Number of accounts | 11036 | Total No of accounts currently present in Cyberark |
| Number of automated account | 9228 | No of account successfully managed by Cyberark |
| Number of Failed accounts | 1808 | No of accounts failed to be managed by Cyberark for various reasons like:   * End systems not reachable * Locked account in end systems * Decommissioned accounts |
| Number of Safe | 18 | Total numbers of Account containers (Safe) based on different type of accounts present in Cyberark  Example: **Emblem-WinServ-groddenberry** contains the window servers local groddenbery accounts |

## To Be - Test Environment

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Role** | **Vault** | **PVWA + CPM** | **PSM** |
| **CPU , Core** | 2 X 4 core CPU | 2 X 4 core CPU | 2 X 4 core CPU |
| **Memory (RAM)** | 8 GB | 8 GB | 16 GB |
| **QTY** | 1 | 1 | 1 |
| **OS** | Windows 2012 R2(64-bit) | Windows 2012 R2(64-bit) | Windows 2012 R2(64-bit) |
| **Storage** | 80GB | 80 GB | 250 GB |
| **Software(if any)** | .NET Framework | IIS + MS Office + .NET Framework | Microsoft Remote Desktop Services |
| **License** | New License required | New License required | New License required |
| **Database(if any)** | NA | NA | NA |
| **Physical / Virtual** | Physical - Preferable | Virtual | Virtual |

## Password Policy

The Detail password policy for different towers will be updated during the design phase.

## Inventory

|  |  |
| --- | --- |
| **Towers** | **Data** |
| **Database** |  |
| **DMZ** |  |

# OPEN ITEMS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S No.** | **Question** | **Concerned Team** | **Status** | **Actions** |
| 1 | Password Policy for individual towers |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |