# Obecná dokumentace – Správa a monitoring privilegovaných účtů PIM

## Aktualizace dokumentu

**Provedené revize:**

|  |  |  |  |
| --- | --- | --- | --- |
| Verze | Autor | Datum | Revize |
| 0.5 | Oldřich Štěpánek | 21.4. 2020 | Prvotní verze dokumentace |
| 0.8 | Pavel Pokorný | 4.6.2020 | Doplnění dokumentace |
| 0.9 | Oldřich Štěpánek | 10.6.2020 | Zapracování připomínek |
| 1.0 | Karel Štefl | 12.6.2020 | Akceptační verze dokumentu |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Poznámky: |  |  |  |

Obsah

[Obecná dokumentace – Správa a monitoring privilegovaných účtů PIM 1](#_Toc42594564)

[Aktualizace dokumentu 1](#_Toc42594565)

[1. Účel dokumentu 2](#_Toc42594566)

[2. Architektura řešení 2](#_Toc42594567)

[2.1 Popis PIM řešení 2](#_Toc42594568)

[2.2 Seznam serverů 4](#_Toc42594569)

[3. Systémy integrované do PIM řešené 5](#_Toc42594570)

## Účel dokumentu

Účelem tohoto dokumentu je popis technického řešení správy přístupů a monitoringu privilegovaných účtů založeném na komerčním systému CyberArk Privileged Access Security (dále jako „PIM“) pro seznámení potencionálních dodavatelů s architekturou a nastavením PIM řešení v prostředí MZE. Dokument tak představuje podklad pro získání kvalifikovaného odhadu pracnosti údržby PIM řešení s ohledem na jeho stav a rozsah v rámci SKL příslušné VZ.

## Architektura řešení

### 2.1 Popis PIM řešení

Instalace řešení PIM je realizována ve vyhrazené bezpečnostní infrastruktuře MZE, která je síťově oddělena od provozní části sítě. Řešení je založeno na fyzických serverech a virtuální platformě VMware a je distribuováno přes dvě datová centra (geocluster DC Nagano a DC Chodov) a lokalitu Těšnov. V rámci PIM řešení je použito cca 360 uživatelských licencí s cca 50 současnými uživatelskými relacemi během běžného pracovního dne.

Jak v datových centrech tak v lokalitě Těšnov jsou komponenty síťově rozděleny do tří síťových segmentů:

• Frontend - zajišťuje přístup uživatelů k webovému rozhraní řešení

• Backend - zajišťuje řízení a přístup k EP

• SecureVault – bezpečné uložení nahrávek, účtů, logů, apod.

PIM řešení je nainstalováno ve dvou instancích – produkční a testovací. Produkční instance zajišťují přístup a auditní stopu interních a externích administrátorů spravujících systémy MZe integrované do PIM řešení (dále též jako EP) provozovaných ve všech třech uvedených lokalitách. Veškeré komponenty řešení jsou nainstalovány v režimu vysoké dostupnosti a to tak, že vysoká dostupnost komponent je zajištěna napříč datovými centry (DC Nagano a DC Chodov) a dále je zajištěna vysoká dostupnost komponent v lokalitě Těšnov, viz blokové schéma Obrázek 1 - Architektura produkčního PIM.

Vysoká dostupnost komponent CyberArk Privileged Session Manager, a to CyberArk Privileged Session Manager for Windows (dále též jako PSM for Windows, nebo PSM) a Privileged Session Manager for SSH (dále též jako PSM for SSH, nebo PSMP), a zároveň CyberArk Password Vault Web Access (dále též jako PVWA) je zajištěna balancováním provozu na úrovni sítě. Uvedené komponenty jsou provozovány ve virtuálním prostředí VMware, kromě jedné PSM for Windows komponenty (server PSM5 viz na Obrázek 1 - Architektura produkčního PIM), která je provozována na fyzickém serveru.

Vysoká dostupnost komponenty CyberArk Central Policy Manger (dále též jako CPM) je zajištěna pomocí Microsoft Failover Clusteru společně s vlastní synchronizační službou, která mezi CPM synchronizuje potřebné konfigurace.

Vysoká dostupnost bezpečného úložiště je zajištěna instalací CyberArk Digital Cluster skládající se z dvojice fyzických serverů s CyberArk EPV (dále též jako Vault) se společným úložištěm na diskovém poli. Součástí řešení vysoké dostupnosti je i DR Vault komponenta, která je rovněž provozována na fyzickém serveru s lokálním úložištěm.



Obrázek 1 - Architektura produkčního PIM řešení

Testovací instance PIM řešení je provozována čistě ve virtuálním prostředí VMware v DC Chodov a DC Nagano a komponenty PIM řešení nejsou provozovány v režimu vysoké dostupnosti.



Obrázek 2 – Architektura testovacího PIM řešení

### Seznam serverů

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Server | Komponenta PIM řešení | CyberArk verze | Instance | Server |
| PVWA1 | CyberArk Password Vault Web Access | 10.10 | Produkční | Virtuální |
| PVWA2 | CyberArk Password Vault Web Access | 10.10 | Produkční | Virtuální |
| PVWA3 | CyberArk Password Vault Web Access | 10.10 | Produkční | Virtuální |
| PVWA4 | CyberArk Password Vault Web Access | 10.10 | Produkční | Virtuální |
| PSM1 | CyberArk PSM for Windows | 10.10 | Produkční | Virtuální |
| PSM2 | CyberArk PSM for Windows | 10.10 | Produkční | Virtuální |
| PSM3 | CyberArk PSM for Windows | 10.10 | Produkční | Virtuální |
| PSM4 | CyberArk PSM for Windows | 10.10 | Produkční | Virtuální |
| PSM5 | CyberArk PSM for Windows | 10.10 | Produkční | Fyzický |
| PSMP1 | CyberArk PSM for SSH | 10.10 | Produkční | Virtuální |
| PSMP2 | CyberArk PSM for SSH | 10.10 | Produkční | Virtuální |
| PSMP3 | CyberArk PSM for SSH | 10.10 | Produkční | Virtuální |
| PSMP4 | CyberArk PSM for SSH | 10.10 | Produkční | Virtuální |
| CPM1 | CyberArk Central Policy Manger | 10.10 | Produkční | Virtuální |
| CPM2 | CyberArk Central Policy Manger | 10.10 | Produkční | Virtuální |
| Vault1 | CyberArk Vault | 10.10 | Produkční | Fyzický |
| Vault2 | CyberArk Vault | 10.10 | Produkční | Fyzický |
| DR Vault | CyberArk DR Vault | 10.10 | Produkční | Fyzický |
| PVWA-T | CyberArk Password Vault Web Access | 10.10 | Testovací | Virtuální |
| PSM-T | CyberArk PSM for Windows | 10.10 | Testovací | Virtuální |
| PSMP-T | CyberArk PSM for SSH | 10.10 | Testovací | Virtuální |
| CPM-T | CyberArk Central Policy Manger | 10.10 | Testovací | Virtuální |
| VAULT-T | CyberArk Vault | 10.10 | Testovací | Virtuální |

## Systémy integrované do PIM řešené

V rámci PIM řešení je integrováno cca 3300 privilegovaných účtů, které převážně slouží k přihlášení administrátorů či technických prostředků (nástroj pro skenování zranitelností) pomocí RDP nebo SSH protokolu na EP. V případě RDP se jedná buď o lokální účty nebo doménové účty. V případě SSH se jedná pouze o lokální účty s autentizací pomocí uživatelského jména a hesla nebo pomocí SSH klíče. Dále jsou integrovány jednotky ostatních typů EP, mezi které patří HPE iLO, síťová zařízení HPE a Fortigate. Desítky účtů dále představují technické/aplikační účty, pro které PIM řešení slouží jako bezpečné úložiště jejich hesel. Ve dvou případech je použita integrace pomocí CyberArk AAM Credential Provider.