Upgrade CyberArk Core PAS

This note describes the steps you need to take to upgrade a CyberArk Core PAS environment and all of its components in a Primary-DR setup. Clustering and Distributed Vaults are out of scope of this note.

This note is written from experience with real world customer environments, and is written for change management in mind. Official documentation does not cover impact analysis, backup or fallback plans.

We will upgrade the components in the following order:

- Primary Vault
- DR Vault
- PVWA
- CPM
- PSM
- PSMP / PSM for SSH

It's recommended that you validate your backups and checking up on your DR/BC processes before every upgrade.
Not that you can (or should) run a business continuity drill before every upgrade, but test occasionally according to your own (or your customers) risk appetite. Nevertheless, you should have a business continuity plan in case the environment becomes FUBAR.
If there's something that needs amending or adding to the plan, now is the time.

Before upgrading the Primary Vault, I highly recommend taking a full backup using PAReplicate the day before the upgrade.
Another thing I recommend is to take a separate full backup using PAReplicate immediately before the upgrade, by having a separate backup user that is added to the PSMRecordings safe (and any other heavy safe that's not business critical) with no safe authorizations; that way, the user can't read from the safe, reducing the size and time it takes to perform a full backup of the Vault.

When upgrading the Vault, the recommended (and the only supported) approach is to first upgrade the Primary Vault and then the DR Vault. This requires downtime, which must be communicated to the business/customer.
It is also possible to upgrade the DR Vault first, so that you can upgrade the DR Vault during office hours and the Primary Vault during off hours. This is however unsupported and if the database schema has been updated as part of the version upgrade, you risk that the DR Vault is unable to start. If that happens, you need to uninstall the new Vault software and install the older version again.
I will however say that I have upgraded customer prod vaults several times using this approach, saving them downtime. If there's no errors when trying it in a test environment, and you follow the failover/failback process just like on prod, it should (fingers crossed) be safe to do it on prod.

If possible, upgrade the Primary Vault first, because failover/failback is a mess anyway. Saves you hours of work when working on big vaults. Plus, you're following the supported approach and can get help from CyberArk support if stuff breaks.

Format

These are all real-world change requests sent to customers inside of our PSA (Datto AutoTask PSA), and follows the limitations set by the PSA. Change requests inside of AutoTask PSA are divided into six sections:

- Description: Basic rich text formatting
- Impact Analysis: Plain text
- Implementation Plan: Plain text
- Test and Verification Plan: Plain text
- Fall Back Plan: Plain text
- Review Notes: Plain text

As all but the Description section is without text formatting of any sorts aside from line breaks, most of the change requests are written to make it easier to read inside of AutoTask PSA. These notes are in markdown, but it was a priority that they be fully readable without any formatting of any kind.

The change requests are written for techs only. To make it easier to write change requests, we decided on an audience: **Techs who are able to perform an upgrade with supervision.**
That way, we avoid explaining too much and we avoid pigeon-holing you into a specific way to perform a task. Restarting services in PowerShell vs. running services.msc vs. clicking around the places you're used to is not important, what's more important is that the process is reliable.

I'm a fan of PowerShell, but we had the (very relevant) feedback from customers that they couldn't approve a change request that was essentially one big PowerShell script. As such, the process is not fully automated.

CyberArk PAM upgrades are pretty much fully automatable and CyberArk publishes Ansible playbooks on their GitHub for install and upgrades. Inside those Ansible playbooks are just plain PowerShell scripts. While I recommend automating as much as possible, CyberArk PAM upgrades have so many pitfalls and caveats that you really need to know every single customization you've made to your installations and how to redo them after any upgrade. **Let this be a warning, I made customers angry by attempting to automate too much and forget post-upgrade details**.

The format of each upgrade is as such:

- Checklist (Description)
  - Contains a milestone-based checklist that you, the performing tech can check.
    - If the PSA supports timestamping, checking the checklist can help document your time spent on the task.
    - This checklist is split into Pre and Post-actions, with Pre-actions containing actions to perform before the change window and Post-actions containing a mix of post-install configurations and validations.
    - Every checklist item is based on instructions found inside the change request.

        - There's always a final Post-action for a second person to review that the post-actions were completed correctly. That made sense in the PSA we used, as other people could not uncheck your items. Thus, the performing tech will check all of the boxes besides the very last, call in a peer and review the Post-action checklist - if everything was OK, the peer could check their box and give the customer assurance that someone else put their name out there and OK'd your work.
    - Contains boilerplate information about the hostname(s), current version, target version, important IP addresses that will be used to perform the upgrade. This is to generalize the change request such that you don't need to change the sections for every customer. It prevents basic mistakes like pasting other customers' Vault IP addresses into a change request.
    - Contains a description of the sections of the change request. This is to give us and the customer a quick glance over the headlines/phases of the upgrade. This must be updated manually if you write anything new to the change request, and as such can be quite fragile. It's been most useful on Vault upgrades to give myself an overview.
- Impact Analysis
    - A short description of the impact on user productivity or component functionality during the upgrade or if unexpected errors occur during the upgrade.
- Implementation Plan
    - The meat of the change request is in this section. The Implementation Plan is split into at least these three subsections: Pre-Upgrade, Upgrade and Post-Upgrade. I've made headlines that mostly correspond with the Checklist at the top, but it's not a one-to-one mapping.
    - To make it easy to read (and write), a lot of the instructions are standardized. "Ensure that", "Copy the files", "Edit 'FILENAME'", "On the 'X' server", "Restart service 'SERVICENAME'", etc.
    - When you need to test, we'll refer to the Test and Implementation Plan. If the upgrade is complex and multi-step, we'll refer to specific sections in the Test and Implementation Plan.
- Test and Verification Plan
    - Instructions to verify that the upgrade didn't fail, log names are specified for troubleshooting purposes
    - Instructions for validating functionality after the upgrade
- Fall Back Plan
    - When possible, multiple choices are offered. Everything but the Vault is assumed to be a VM, so a snapshot rollback will be recommended in most circumstances.
    - In real life, a snapshot rollback is rarely necessary. CyberArk upgrade packages are notoriously filled with bugs, so in many cases it's enough to just repair the installation if you see errors during the upgrade. Don't be scared to do a repair, because that's what CyberArk support will ultimately recommend you to do.
- Review Notes
    - We filled this section with downtime estimations, change scheduling and "estimated risk" (low/medium/high). This was included to appease a specific customer that needed such estimation, but it was very context-specific to the customer. Don't take it too seriously.

Change - Upgrade Vault with Failover

Important

Upgrading the Vault in this way is not supported. Follow the guide Change - Upgrade Vault[3] instead.
Proceed with caution.

Checklist

1. ○ Pre: Verify that a recent full backup has been taken
2. ○ Pre: Verify that the customer can present the Operator key and Master Key
3. ○ Pre: Copy the files (Vault installation files, Windows Update packages) to the server
4. ○ Pre: Verify that System Locale is set correctly
5. ○ Pre: Validated that prerequisites are installed
6. ○ Pre: Verify that CPMs only connects to the Primary Vault
7. ○ Pre: Verify that all other components point to both vaults
8. ○ Upgrade: Exclude server from monitoring
9. ○ Upgrade: Back up Vault installation folder
10. ○ Upgrade: Acquire the password for the Vault "administrator" user
11. ○ Failover: Failover complete
12. ○ Failover: All components validated
13. ○ Upgrade: Installed prerequisites (if any)
14. ○ Upgrade: Primary Vault upgraded
15. ○ Upgrade: DR Software upgraded
16. ○ Failback: Started replication on Primary
17. ○ Failback: Stopped Vault service on DR
18. ○ Failback: Stopped DR service on Primary
19. ○ Failback: Started Vault service on Primary
20. ○ Upgrade: DR Vault - DR Software upgraded
21. ○ Post: Validate the password for the Vault "administrator" user
22. ○ Post: All components validated
23. ○ Post: Started replication on DR
24. ○ Post: Validated service status on Vault servers
25. ○ Post: Checked all
26. ○ Post: 2nd consultant checked all

Vault IP:
Domain: N/A
Servers:
Failover: YES
Current component version: Vault xx.x
Target component version: Vault xx.x

The upgrade is split into these sections:

- Pre-Upgrade steps
- Upgrade: Primary Vault Server
  - Manual Failover
  - Validate
  - Install Vault Software
  - Validate
  - Install DR Software
  - Validate
  - Manual Failback
  - Validate
- Post-Upgrade steps

Impact Analysis

WRITE THIS SECTION IF YOU WILL NOT PERFORM FAILOVER/FAILBACK:
Throughout the whole upgrade process the vault servers will be rebooted and services taken offline, which will result in PVWA being inaccessible, PSM session already established will not close, but if the connection is lost it cannot be established again before the change is complete.

WRITE THIS SECTION IF YOU WILL PERFORM FAILOVER/FAILBACK:
During the upgrade process for the Primary Vault, the DR site will be active. Software (eg. PAReplicate) that point to the primary vault will fail to run. Under the failover and failback processes, components risk losing connection to the vault for short moments, disrupting user activity.

The CPM will be unable to perform password management tasks and if errors occur during the upgrade, the Vault will be offline until the errors are troubleshooted or the upgrade is rolled back.

Implementation Plan

Pre-Upgrade

- Ensure that a recent full backup of the Vault and metadata has been taken.
- Ensure that the customer can present the Operator and Master key in the case of an emergency.
- Acquire the password for the Prod Vault "administrator" user.
- Ensure that the prerequisites are met for the following software. If they aren't met, follow the "Installing prerequisites for Vault Software" section in the Implementation Plan.

> - Microsoft Visual C++ 2015-2022 (32-bit and 64-bit)
> - Microsoft .NET Framework 4.8

Prepare the setup files on the Vault servers

- Copy the setup files to a server that has PrivateArk Client installed
- Upload the software through PrivateArk Client to a Safe at your control, with a size quota above 5000MB.
- Use PrivateArk Client to download the software on all applicable servers

Ensure that CPM does not connect to the DR Vault during the upgrade.

- Log on to all CPMs
- Edit `C:\Program Files\CyberArk\Password Manager\Vault\Vault.ini`
- Ensure that the IP address of the Primary Vault is the ONLY IP address present in the ADDRESS section.

Ensure that all components (except for CPM) point to the DR Vault in addition to the Primary Vault

- On all component servers, open `vault.ini`
- Take note of the value in ADDRESS
- If any component does not include the DR Vault IP address, add it in the following format `ADDRESS=PRIMARYVAULTIP,DRVAULTIP`

Ensure that the non-Unicode System Locale is set to Danish

This section is only relevant if the system locale has previously been set to Danish (da-DK).

- Open a PowerShell prompt, run the following command
  (Get-WinSystemLocale).name -eq "da-DK"
- If "false", abort the change and arrange a change to set the system locale to Danish and reboot the server.

Back up the installation folders

- `C:\Program Files (x86)\PrivateArk\Server`
- `C:\Program Files (x86)\PrivateArk\Client`

Upgrade

Manual Failover

- On the DR server, edit PADR.ini and set the following:
  EnableFailover=No
  EnableDbsync=Yes
  ActivateManualFailover=Yes
- On the DR server, restart the PADR service and validate in PADR.log that the failover process has started
- On the Primary Vault server, stop the "PrivateArk Server" service

Test using the "Validating component functionality" section of the Test and Verification Plan

Applying Windows Updates | Installing Prerequisites for Vault Software

This section must be followed if the customer has requested Windows Updates to be installed during the change, or if the prerequisites for the Vault Software aren't met.

- Run the following commands as administrator:

```
        $vaultPackagePath = "C:\CA\Core PAS 13.0\Vault"         # change this as needed
        & $vaultPackagePath\WSUS\OpeningServices.ps1
        Set-Service "PrivateArk Server" -StartupType Disabled
```

- Ensure that service "PrivateArk Server" has been set to startup mode Disabled to prevent the Vault from starting automatically after restart
- Restart the server
- Run the wanted update package to install the update
- Install any missing prerequisites
- Restart the server

Test using the Test and Verification Plan before proceeding.

Vault Software upgrade

- Stop services "PrivateArk Database", "CyberArk Logic Container", "Cyber-Ark Event Notification Engine", "PrivateArk Remote Control Agent", "PrivateArk Server" and "CyberArk Vault Disaster Recovery"
- Set service "CyberArk Vault Disaster Recovery" to startup type Manual

Alternatively, with PowerShell:

```
        Get-Service "Cyber-Ark Event Notification Engine", "PrivateArk Remote Control Agent", "PrivateArk Server", "PrivateArk Database", "CyberArk Logic Container" | Stop-Service -Verbose
        Get-Service "CyberArk Vault Disaster Recovery" -ErrorAction SilentlyContinue | Stop-Service -Verbose
        Get-Service "CyberArk Vault Disaster Recovery" -ErrorAction SilentlyContinue | Set-Service -StartupType Manual
```

- Right click Setup.exe and select "Run as Administrator"
- Click Yes to converting data during the upgrade
- Click No to installing RabbitMQ
- Click Finish when the wizard is complete

Test using the "Testing the Primary Vault installation via the PVWA" section of the Test and Verification Plan

DR Software

- Stop service "PrivateArk Server"
- Right click Setup.exe and select "Run as Administrator"
- Click Yes to proceed with the Disaster Recovery application upgrade.

- Click Finish when the wizard is complete
- Set the CyberArk Vault Disaster Recovery service to startup type Manual

PrivateArk Client

- Right click Setup.exe and select "Run as Administrator"
- Click next on the Wizard until completion

Clean up after Windows Update or prerequisite installation

If you applied Windows Updates or installed prerequisites, follow this section.

- Run the following commands as administrator

```
        $vaultPackagePath = "C:\CA\Core PAS 13.0\Vault"            # change this as
needed
        & $vaultPackagePath\WSUS\ClosingServices.ps1
```

- Restart the server

Manual Failback

- DR: Reset the password for the DR user to Cyberark1 (will be automatically changed later)
- Primary: Start the Primary server in DR mode
    1. Stop service "PrivateArk Server" if running
    2. Edit PADR.ini
    3. Set FailoverMode=No
    4. Set NextBinaryLogNumberToStartAt=-1
    5. Save and exit
    6. Create a new credfile for the DR user

    ```
          cd "C:\Program Files (x86)\PrivateArk\PADR"
          del Conf\user.ini*
          createcredfile.exe user.ini /Password /username DR /password Cyberark1
    /DPAPIMachineProtection /EntropyFile
    ```

    7. Start (or restart) service "CyberArk Disaster Recovery"
    8. Wait for replication to end
- DR: Stop service "PrivateArk Server"
- Primary: Perform a manual failover on the Primary Vault server
    1. On the Primary server, edit PADR.ini
    2. Set EnableFailover=No
    3. Set EnableDbsync=Yes
    4. Set ActivateManualFailover=Yes
    5. Save and exit

> 6. Start (or restart) service "CyberArk Disaster Recovery"

- Primary: Edit PADR.ini, set FailoverMode=No to ensure the Vault won't start in DR mode
- Primary: Reset the password for the DR user to Cyberark1 (will be automatically changed later)
- DR: Start the DR server in DR mode

> 1. Stop service "PrivateArk Server" if running
> 2. Edit PADR.ini
> 3. Set FailoverMode=No
> 4. Save and exit
> 5. Create a new credfile for the DR user

```
cd "C:\Program Files (x86)\PrivateArk\PADR"
del Conf\user.ini*
createcredfile.exe user.ini /Password /username DR /password Cyberark1
/DPAPIMachineProtection /EntropyFile.
```

> 6. Start (or restart) service "CyberArk Disaster Recovery"
> 7. Wait for replication to end

If replication was able to run, the password has changed as seen in the message "Leave replication user change password method" in PADR.log
Test using the "Validating component functionality" section of the Test and Verification Plan

Enable DR Replication on DR Vault

- Edit PADR.ini and set the following:
  EnableFailover=Yes
  NextBinaryLogNumberToStartAt=-1
  (delete LastDataReplicationTimestamp)
- Start service "CyberArk Vault Disaster Recovery"
- Set service "CyberArk Vault Disaster Recovery" to startup type Automatic

Validate using the "Validating the DR Service" section of the Test and Verification Plan

Final service validation

- Validate service status using the "Validate service status" section of the Test and Verification Plan

Test and Verification Plan

Validating the DR Vault installation

Review the following logs:

```
    C:\Program Files (x86)\PrivateArk\Server\Server\Logs\VaultConfiguration.log
```

If possible, start the PrivateArk Server service and review `italog.log`. **Do not perform this without approval from the customer.**

Validating the DR service

Review the following logs:

```
        C:\Program Files (x86)\PrivateArk\PADR\Logs\padr.log
```

Tail the log by running `Get-Content -Tail 10 -Wait "C:\Program Files (x86)\PrivateArk\PADR\Logs\padr.log"`

Testing the Vault installation

Review the following logs:

```
        C:\Program Files (x86)\PrivateArk\Server\Server\Logs\VaultConfiguration.log
        C:\Program Files (x86)\PrivateArk\Server\Server\Logs\ITALog.log
```

- Log onto PrivateArk Client with a CyberArk Vault user
- Log onto PVWA with a CyberArk Vault user
- Log onto PVWA with an external directory user

Validate component functionality

Vault/PVWA

- Log onto PVWA with an external directory user using LDAP and RADIUS
- Search for an account
- Log off
- Log onto PVWA with a CyberArk Vault user
- Check System Health, take note of any disconnected components

The PVWA is now validated. If any components are shown as disconnected, review those.

Troubleshooting:

- Run `iisreset` on the PVWA server

CPM

- Check `pmconsole.log` and `pm_error.log` on the CPM server
- Perform a Validate operation in the PVWA

Troubleshooting:

- Restart service `CyberArk Password Manager`

PSM

- Check `psmconsole.log` on the PSM server
- Change a platform to connect to the PSM server and test a Connection Component

Troubleshooting:

- Restart service `CyberArk Privileged Session Manager`

PTA

- Check services on the PTA server as root: `MONIT_STATUS`
- Browse to the Security Events page in the PVWA

Troubleshooting:

- Restart all PTA services: Run `UTILITYDIR`, `./run.sh`, 3, 5, 4, 6

PSMP

- Check service `psmpsrv` on the PSMP server: `systemctl status psmpserv`
- Test an account using the PSMP

Troubleshooting: Restart PSMP service: `systemctl restart psmpsrv`

Validate service status

- DR Vault server:
  - Stopped: CyberArk Event Notification Service
  - Started: CyberArk Logic Container
  - Started: CyberArk Vault Disaster Recovery
  - Started: PrivateArk Database
  - Started: PrivateArk Remote Control Agent
  - Stopped: PrivateArk Server
- Primary Vault server:
  - Stopped: CyberArk Event Notification Service
  - Started: CyberArk Logic Container
  - Stopped: CyberArk Vault Disaster Recovery
  - Started: PrivateArk Database
  - Started: PrivateArk Remote Control Agent
  - Started: PrivateArk Server

Fall Back Plan

Replicate from DR Vault (Recommended)

- Stop service "CyberArk Vault Disaster Recovery" and "PrivateArk Server"
- Perform a full replication and manual failback as detailed in the Implementation Plan
- Validate using the "Testing the Primary Vault installation" section of the Test and Verification Plan

Reinstall Vault (Emergencies)

> **Note**
>
> A common case for Vault software reinstallation is when you upgrade a DR vault and you forgot to turn off the DR service. This will sync a database down from the Primary Vault that's a lower version than the Vault software installed. If there's no database version bump, there's a high chance that it will work fine, but if a particular Vault version happens to bump the schema version, you'll find that the Vault will not be able to start. To revert this, you need to uninstall the new Vault software and install the old one.

- Uninstall Vault
- Reinstall Vault in the same version and with the same Operator key as the currently active Vault
- Replicate from the currently active Vault or restore a full backup
- Validate using the "Testing the Vault installation" section of the Test and Verification Plan

Restore a full backup (Last Resort)

> **Note**
>
> Restoring a full backup is only necessary in absolute emergencies, where the data of both vaults have been corrupted.

- Copy a full backup of the Vault to `C:\PrivateArk\Restored Safes` on the Vault server
- Stop service "CyberArk Vault Disaster Recovery" and "PrivateArk Server"
- Edit `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`
  - Note the current value of BackupFilesDeletion and RecoveryPrvKey
  - Set the following parameters: `BackupFilesDeletion=No` and `RecoveryPrvKey=C:\PathToMasterCD\RecPrv.key`
- From an elevated command prompt, run `cd C:\Program Files (x86)\PrivateArk\Server; CAVaultManager RecoverBackupFiles`
- Run `CAVaultManager RestoreDB`, which will synchronize the Vault Metadata
- Edit `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`, restore to previously noted values
- Start service "PrivateArk Server"

- Validate using the "Testing the Primary Vault installation" section of the Test and Verification Plan

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within 2 hour(s).

Change schedule and time of day of execution

This change is scheduled for XX:XX inside regular business hours.

Estimated risk

Risk is medium.

2

Change - Upgrade Vault

Checklist

1. ○ Pre: Verify that a recent full backup has been taken
2. ○ Pre: Verify that the customer can present the Operator key and Master Key (only applicable if upgrading Primary Vault)
3. ○ Pre: Copy the files (Vault installation files, Windows Update packages) to the server
4. ○ Pre: Verify that System Locale is set correctly
5. ○ Pre: Validated that prerequisites are installed
6. ○ Pre: Verify that CPMs only connects to the Primary Vault
7. ○ Pre: Verify that all other components point to both vaults (only applicable if upgrading Primary Vault)
8. ○ Upgrade: Exclude server from monitoring
9. ○ Upgrade: Back up Vault installation folder
10. ○ Upgrade: Acquire the password for the Vault "administrator" user (only applicable if upgrading Primary Vault)
11. ○ Upgrade: Applied Windows patches (if requested)
12. ○ Upgrade: Installed prerequisites (if any)
13. ○ Upgrade: Vault upgraded
14. ○ Upgrade: DR Software upgraded (if applicable)
15. ○ Post: If DR Server: Started replication
16. ○ Post: Include server in monitoring
17. ○ Post: All components validated (only applicable if upgrading Primary Vault)
18. ○ Post: Validate the password for the Vault "administrator" user (only applicable if upgrading Primary Vault)
19. ○ Post: Validated service status on Vault servers

20. ○ Post: Checked all
21. ○ Post: 2nd consultant checked all

Vault IP:
Domain: N/A
Servers:
Failover: NO
Current component version: Vault xx.x
Target component version: Vault xx.x

The upgrade is split into these sections:

- Pre-Upgrade steps
- Upgrade
  - Install Vault Software
  - Validate
  - Install DR Software
  - Validate
- Post-Upgrade steps

Impact Analysis

If Primary: Throughout the whole upgrade process the vault servers will be rebooted and services taken offline, which will result in PVWA being inaccessible, PSM session already established will not close, but if the connection is lost it cannot be established again before the change is complete. The CPM will be unable to perform password management tasks and if errors occur during the upgrade, the Vault will be offline until the errors are troubleshooted or the upgrade is rolled back.

If DR: Should errors occur during the upgrade, there will be no DR service to fail over to if the Primary Vault experiences problems.

Implementation Plan

Pre-Upgrade

- Ensure that a recent full backup of the Vault and metadata has been taken.
- Ensure that the customer can present the Operator and Master key in the case of an emergency.

Prepare the setup files on the Vault server

- Option 1: Copy the files over RDP to the Vault server
- Option 2: Copy the files over PrivateArk Client
  - Copy the setup files to a server that has PrivateArk Client installed
  - Upload the software through PrivateArk Client to a Safe at your control, with a size quota above 5000MB.
  - Use PrivateArk Client to download the software

Ensure that the non-Unicode System Locale is set to Danish

This section is only relevant if the system locale has previously been set to Danish (da-DK).

- Open a PowerShell prompt, run the following command (Get-WinSystemLocale).name -eq "da-DK"
- If "false", abort the change and arrange a change to set the system locale and reboot the server.

Validate Prerequisites

- Open appwiz.cpl
- If "Microsoft Visual C++ 2015-2022 Redistributable" is installed in x64 and x86 versions, prerequisites are OK
- If not installed, perform the step "Applying Windows Updates | Installing Prerequisites for Vault Software" when performing the change.

Ensure that CPM does not connect to the DR Vault during the upgrade.

- Log on to all CPMs
- Edit `C:\Program Files\CyberArk\Password Manager\Vault\Vault.ini`
- Ensure that the IP address of the Primary Vault is the ONLY IP address present in the ADDRESS section.

Ensure that all components (except for CPM) point to the DR Vault in addition to the Primary Vault

- On all component servers, open `vault.ini`
- Take note of the value in ADDRESS
- If any component does not include the DR Vault IP address, add it in the following format `ADDRESS=PRIMARYVAULTIP,DRVAULTIP`

Upgrade

Exclude server from monitoring

- Exclude the server from monitoring solutions
- Instructions vary by product

Back up the installation folders

- `C:\Program Files (x86)\PrivateArk\Server`
- `C:\Program Files (x86)\PrivateArk\Client`

Applying Windows Updates | Installing Prerequisites for Vault Software

This section must be followed if the customer has requested Windows Updates to be installed during the change, or if the prerequisites for the Vault Software aren't met.
Skip this section if prerequisites are met, and the customer doesn't need Windows Updates applied.

- Run the following PowerShell commands as administrator:

```
        $vaultPackagePath = "C:\CA\Core PAS 13.0\Vault"        # change this as needed
        & $vaultPackagePath\WSUS\OpeningServices.ps1
        Set-Service "PrivateArk Server" -StartupType Disabled
```

- Ensure that service "PrivateArk Server" has been set to startup mode Disabled to prevent the Vault from starting automatically after restart
- Restart the server
- Run the wanted update package to install the update
- Install any missing prerequisites
- Restart the server

Test using the Test and Verification Plan before proceeding.

Vault Software upgrade

- Acquire the password for the Prod Vault "administrator" user.
- Run the following PowerShell commands as administrator to stop all CyberArk related services and set the DR service to not start automatically

```
        Get-Service "Cyber-Ark Event Notification Engine", "PrivateArk Remote Control Agent", "PrivateArk Server", "PrivateArk Database", "CyberArk Logic Container" | Stop-Service -Verbose
        Get-Service "CyberArk Vault Disaster Recovery" -ErrorAction SilentlyContinue | Stop-Service -Verbose
        Get-Service "CyberArk Vault Disaster Recovery" -ErrorAction SilentlyContinue | Set-Service -StartupType Manual
```

- Right click Setup.exe and select "Run as Administrator"
- Click Yes to converting data during the upgrade
- Click No to installing RabbitMQ
- Click Finish when the wizard is complete

Test using the "Testing the Primary Vault installation via the PVWA" section of the Test and Verification Plan

PrivateArk Client

- Right click Setup.exe and select "Run as Administrator"
- Click next on the Wizard until completion

DR Software

- Stop service "PrivateArk Server" if running
- Right click Setup.exe and select "Run as Administrator"
- Click Yes to proceed with the Disaster Recovery application upgrade.
- Click Finish when the wizard is complete
- If the server is a DR Vault, set service "CyberArk Vault Disaster Recovery" to startup type Automatic
- If the server is a DR Vault, start service "CyberArk Vault Disaster Recovery"

Clean up after Windows Update or prerequisite installation

If you applied Windows Updates or installed prerequisites, follow this section.

- Run the following PowerShell commands as administrator:

```
        $vaultPackagePath = "C:\CA\Core PAS 13.0\Vault"            # change this as
needed
        & $vaultPackagePath\WSUS\ClosingServices.ps1
```

- Restart the server

Include server in monitoring

- Include the server in your monitoring solutions
- Instructions vary by product

Final service validation

- Test using the "Validating component functionality" section of the Test and Verification Plan
- Validate service status using the "Validate service status" section of the Test and Verification Plan

Test and Verification Plan

Validating the DR service

Review the following logs:

```
        C:\Program Files (x86)\PrivateArk\PADR\Logs\padr.log
```

Tail the log by running `Get-Content -Tail 10 -Wait "C:\Program Files (x86)\PrivateArk\PADR\Logs\padr.log"`

Validate component functionality

Vault/PVWA

- Log onto PVWA with an external directory user using LDAP and RADIUS
- Search for an account
- Log off
- Log onto PVWA with a CyberArk Vault user
- Check System Health, take note of any disconnected components

The PVWA is now validated. If any components are shown as disconnected, review those.

Troubleshooting:

- Run `iisreset` on the PVWA server

CPM

- Check `pmconsole.log` and `pm_error.log` on the CPM server
- Perform a Validate operation in the PVWA

Troubleshooting:

- Restart service `CyberArk Password Manager`

PSM

- Check `psmconsole.log` on the PSM server
- Change a platform to connect to the PSM server and test a Connection Component

Troubleshooting:

- Restart service `CyberArk Privileged Session Manager`

PTA

- Check services on the PTA server as root: `MONIT_STATUS`
- Browse to the Security Events page in the PVWA

Troubleshooting:

- Restart all PTA services: Run `UTILITYDIR`, `./run.sh`, 3, 5, 4, 6

PSMP

- Check service `psmpsrv` on the PSMP server: `systemctl status psmpserv`
- The customer must verify PSMP functionality

Troubleshooting: Restart PSMP service: `systemctl restart psmpsrv`

Validate service status

- DR Vault server:
  - Stopped: CyberArk Event Notification Service
  - Started: CyberArk Logic Container
  - Started: CyberArk Vault Disaster Recovery
  - Started: PrivateArk Database
  - Started: PrivateArk Remote Control Agent
  - Stopped: PrivateArk Server
- Primary Vault server:
  - Stopped: CyberArk Event Notification Service
  - Started: CyberArk Logic Container
  - Stopped: CyberArk Vault Disaster Recovery
  - Started: PrivateArk Database
  - Started: PrivateArk Remote Control Agent
  - Started: PrivateArk Server

Fall Back Plan

NOTE: Vault reinstallation is only necessary in absolute emergencies, where either both vaults have been corrupted, or the Vault installation itself has been corrupted in the upgrade process.

Replicate from DR Vault (Recommended)

- Stop service "CyberArk Vault Disaster Recovery" and "PrivateArk Server"
- Perform a full replication and manual failback as detailed in the Implementation Plan
- Validate using the "Testing the Primary Vault installation" section of the Test and Verification Plan

Reinstall Vault (Emergencies)

> **Note**
>
> A common case for Vault software reinstallation is when you upgrade a DR vault and you forgot to turn off the DR service. This will sync a database down from the Primary Vault that's a lower version than the Vault software installed. If there's no database version bump, there's a high chance that it will work fine, but if a particular Vault version happens to bump the schema version, you'll find that the Vault will not be able to start. To revert this, you need to uninstall the new Vault software and install the old one.

- Uninstall Vault
- Reinstall Vault in the same version and with the same Operator key as the currently active currently active Vault

- Replicate from the currently active Vault or restore a full backup
- Validate using the "Testing the Vault installation" section of the Test and Verification Plan

Restore a full backup (Last Resort)

> **Note**
>
> Restoring a full backup is only necessary in absolute emergencies, where the data of both vaults have been corrupted.

- Copy a full backup to `C:\PrivateArk\Restored Safes` on the Vault server
- Stop service "CyberArk Vault Disaster Recovery" and "PrivateArk Server"
- Edit `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`
  - Note the current value of BackupFilesDeletion and RecoveryPrvKey
  - Set the following parameters: `BackupFilesDeletion=No` and `RecoveryPrvKey=C:\PathToMasterCD\RecPrv.key`
- From an elevated command prompt, run `cd C:\Program Files (x86)\PrivateArk\Server; CAVaultManager RecoverBackupFiles`
- Run `CAVaultManager RestoreDB`, which will synchronize the Vault Metadata
- Edit `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`, restore to previously noted values
- Start service "PrivateArk Server"
- Validate using the "Testing the Primary Vault installation" section of the Test and Verification Plan

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within 2 hours.

Change schedule and time of day of execution

This change is scheduled for XX:XX inside regular business hours.

Estimated risk

Risk is medium.

3

Change - Upgrade PVWA

Checklist

1. ○ Pre: Ensure that a VM snapshot has been taken for the server
2. ○ Pre: Acquire the password for the Vault "administrator" user
3. ○ Pre: Back up the installation folder and the IIS web site
4. ○ Pre: Note the value of HTTP Redirect in IIS/Default Web Site
5. ○ Pre: Note the value of "Access this computer from the network" in secpol.msc > Local Policies > User Rights Assignment
6. ○ Upgrade: Upgrade complete
7. ○ Upgrade: Performed hardening
8. ○ Post: Test LDAP and RADIUS authentication
9. ○ Post: Check System Health
10. ○ Post: Check the redirect URL in IIS/Default Web Site
11. ○ Post: Check custom MIME types
12. ○ Post: Check the value of "Access this computer from the network" in secpol.msc > Local Policies > User Rights Assignment
13. ○ Post: Checked all
14. ○ Post: 2nd consultant checked all

Vault IP:
Domain:
Servers:
Current component version: PVWA 12.x
Target component version: PVWA 13.0

The upgrade is split into these sections:

- Pre-Upgrade steps
- Upgrade
- Hardening
- Validate

Impact Analysis

During the upgrade, the PVWA service will be down and users connecting to the web portal through this server will experience errors until the upgrade is complete or has been rolled back.

Implementation Plan

PRE-UPGRADE

- Acquire the password for the Prod Vault "administrator" user
- Copy the setup files to the server (ie. `C:\Install\Core PAS 12.6\Password Vault Web Access-Rls-v12.6`)
- Ensure that a VM snapshot has been taken for the server
- Back up the installation folder (`C:\CyberArk\Password Vault Web Access\`) and the IIS web site (`C:\inetpub\wwwroot\`)
- Note the value of HTTP Redirect in IIS/Default Web Site

- Note the value of "Access this computer from the network" in secpol.msc > Local Policies > User Rights Assignment
- Ensure that the server has been excluded from load balancing: `(Get-Counter "\web service(default web site)\current connections").CounterSamples.CookedValue`

Upgrade

- Open a PowerShell prompt as Administrator, navigate to the InstallationAutomation directory under the installation folder

```
        cd "C:\CA\Core PAS 12.6\Password Vault Web Access-Rls-v12.6\InstallationAutomation"
        Set-ExecutionPolicy Bypass -Scope Process -Force
        .\PVWA_Prerequisites.ps1
        cd ..
        .\setup.exe
```

- Click install to the prerequisites. If they fail, they may already be installed in a later version
- Click Next and select Yes to accept the EULA
- Type in the username and password for the Prod Vault "administrator" user.
- Click Finish when the wizard is complete

Adjust the PVWA connection component to work PVWA 13.0

If you have upgraded from PVWA 12.x to PVWA 13.0 or later, follow this section.
Attempt to launch the PVWA Connection Component. If this fails, edit the WebFormFields property on the PVWA Connection Component:

- Copy the value of the WebFormFields property of the Connection Component
- Paste in the following and save:

user_pass_form_username_field>{username}(searchby=id)
user_pass_form_password_field>{password}(searchby=id)
span.p-button-label>(Button)(SearchBy=css)

Test the PVWA Connection Component again.

Hardening

- Run the following PowerShell script: `cd "C:\CA\Core PAS 12.6\Password Vault Web Access-Rls-v12.6\InstallationAutomation"; .\PVWA_Hardening.ps1`
- The hardening script resets the local policy "Access this computer from the network", which may be required for monitoring by an NMS.

> - `secpol.msc`
> - Local Policies, User Rights Assignment

    - Allow this computer from the network: Add `domain\MonitoringAccount`
- The hardening script clears custom MIME types, if those had previously been set
    - `inetmgr`
    - PasswordVault, MIME Types
    - Add
        - File name extension: `.mp4`
        - MIME type: `video/mp4`

Test and Verification Plan

Installation Logs

Review the following logs for errors:

```
        C:\Windows\Temp\PVWAInstall.log
        C:\Windows\Temp\PVWAInstallEnv.log
        C:\Windows\Temp\PVWAInstallError.log
        C:\Windows\Temp\PVWAInstallErrorEnv.log
        C:\CyberArk\Password Vault Web Access\Env\Log\CheckConnection.log
        C:\CyberArk\Password Vault Web Access\Env\Log\ConfigureInstance.log
        C:\CyberArk\Password Vault Web Access\Env\Log\ConfigureVault.log
        C:\CyberArk\Password Vault Web Access\Env\Log\RegisterInstance.log
```

Service health and Validation

- Test Authentication methods using PVWA.
- Check system health on https://SERVERNAME.DOMAIN/PasswordVault
- Check the redirect URL in IIS/Default Web Site
- Check the value of "Access this computer from the network" in secpol.msc > Local Policies > User Rights Assignment

Fall Back Plan

Roll back with snapshot and new Credfile (recommended)

If a snapshot was taken before upgrading, revert to snapshot.
Create a new credfile for the PVWA component user and run `iisreset`.
Test connectivity as noted in the Test and Verification Plan.

Repair the installation

If no snapshot was taken, attempt a repair of the installation.

- Open `appwiz.cpl`
- Select "CyberArk Password Vault Web Access" and click Change/Remove
- Select Repair and click Next

The PVWA server will register itself with the Vault again.
Test connectivity as noted in the Test and Verification Plan.

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within 1 hour.

Change schedule and time of day of execution

This change is scheduled for outside regular office hours dd-mm.

Estimated risk

Risk is medium.

2

Change - Upgrade CPM

Checklist

1. ○ Pre: Ensure that a VM snapshot has been taken for the server
2. ○ Pre: Acquire the password for the Vault "administrator" user
3. ○ Pre: Back up the installation folder
4. ○ Upgrade: Upgrade complete
5. ○ Upgrade: Performed hardening
6. ○ Post: Check System Health
7. ○ Post: Perform a CPM operation (Verify/Change/Reconcile)
8. ○ Post: Checked all
9. ○ Post: 2nd consultant checked all

Vault IP:
Domain:
Servers:
Current component version: CPM xx.x
Target component version: CPM xx.x

The upgrade is split into these sections:

- Pre-Upgrade steps
- Upgrade
- Hardening
- Validate

Impact Analysis

During the upgrade, password management will not function. This affects Password Change, Verify and Reconciliation actions.

If errors occur during the upgrade, password management will not function until the errors have been resolved or the upgrade has been rolled back as per the "Fall Back Plan".
There is no impact on PVWA, users will still be able to access and use their accounts to connect to servers via the PSM.

Implementation Plan

Pre-upgrade

- Acquire the password for the Vault "administrator" user
- Copy the setup files to the server (ie. `C:\CA\Core PAS 12.6\Central Policy Manager-Rls-v12.6\`)
- Ensure that a recent VM snapshot has been taken for the server
- Back up the installation folder (`C:\Program Files (x86)\CyberArk\Password Manager\`)

Upgrade

- Open a PowerShell prompt as Administrator and run the preinstallation script:

```
        cd "C:\CA\Core PAS 12.6\Central Policy Manager-Rls-
v12.6\InstallationAutomation"
        Set-ExecutionPolicy Bypass -Scope Process -Force
        .\CPM_Preinstallation.ps1
        Get-Service "CyberArk Password Manager","CyberArk Central Policy Manager
Scanner" | Stop-Service -Verbose
```

- Right click Setup.exe and select "Run as Administrator"
- Click Yes to start the upgrade
- Confirm the Vault IP address and port 1858 and click Next
- Type in the username and password for the Prod Vault "administrator" user and click Next
- Click Finish when the wizard is complete

Hardening

Run the following PowerShell commands:

```
        Set-ExecutionPolicy Bypass -Scope Process -Force
        cd "C:\CA\Core PAS 12.6\Central Policy Manager-Rls-
v12.6\InstallationAutomation"
        .\CPM_Hardening.ps1
```

- OPTIONAL: Restart the server

Test and Verification Plan

Installation Logs

Review the following logs:

```
        C:\Windows\Temp\CPM\CPMInstall.log
```

Service health and Validation

Review the following logs:

```
    C:\Program Files (x86)\CyberArk\Password Manager\Logs\PMConsole.log
    C:\Program Files (x86)\CyberArk\Password Manager\Logs\pm.log
```

- Check system health in the PVWA
- Perform a CPM operation (Verify/Change/Reconcile)
- Perform a CPM Verify operation in the PVWA
- Perform a CPM Change operation in the PVWA
- Perform a CPM Reconcile operation in the PVWA

Fall Back Plan

Roll back with snapshot and new Credfile (recommended)

- If a snapshot was taken before upgrading, revert to snapshot.
- Stop services "CyberArk Password Manager", "CyberArk Central Policy Manager Scanner"
- In PrivateArk, create a new password for the CPM user
- Run the following command:

```
        cd "C:\Program Files (x86)\CyberArk\Password Manager\Vault"
        CreateCredFile.exe user.ini Password /username PasswordManager /password
Cyberark1 /EntropyFile /DpapiMachineProtection
```

- Start services "CyberArk Password Manager", "CyberArk Central Policy Manager Scanner"
- Test using the "Service health and Validation" procedure in "Test and Verification Plan"

Repair the installation

In the case of errors, a Repair operation can solve the issue.
Repairs can be done either after reverting to snapshot, or on the new version.

- open `appwiz.cpl`
- select "CyberArk Password Manager" and click Change/Remove

- select Repair and click Next
- Click Yes to recreate Vault environment
- click Next
- Type in the username and password for the Prod Vault "administrator" user and click Next
- click Finish when the wizard is complete
- Test using the "Service health and Validation" procedure in "Test and Verification Plan"

Manually reinstall CPM (only in emergencies)

- Open `appwiz.cpl`
- Select "CyberArk Password Manager" and click Remove
- Select Uninstall and click Next
- Restart the server
- In PrivateArk, rename or delete the CPM's previous app user.
- Install the previous version using the "Upgrade CPM" procedure in "Implementation Plan", select "Yes" or "OK" to any additional prompts.
- Restart the server
- Test using the procedure in "Test and Verification Plan"

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within X hours.

Change schedule and time of day of execution

This change is scheduled for XX:XX inside regular business hours.

Estimated risk

Risk is medium.

Change - Upgrade PSM

Checklist

1. ○ Pre: A VM snapshot has been taken for the server
2. ○ Pre: Acquire the password for the Vault "administrator" user
3. ○ Pre: PSM server has been drained of active users before the upgrade
4. ○ Pre: PSM server is not included in Load Balancing during the upgrade
5. ○ Pre: Back up the installation folder
6. ○ Pre: "administrator" is not a safe owner of the "PSMUnmanagedSessionAccounts" safe
7. ○ Pre: Take note of current settings

8. ○ Upgrade: Prerequisites validated
9. ○ Upgrade: Upgrade complete
10. ○ Upgrade: Applied AppLocker and hardening
11. ○ Post: Check System Health
12. ○ Post: Test connection components defined in the description
13. ○ Post: Checked all
14. ○ Post: 2nd consultant checked all

Vault IP:
Domain:
Servers:
Current component version: PSM xx.x
Target component version: PSM xx.x

The following are customizations that need to be made for CUSTOMER1:

CUSTOMER1 T2:

```
PSMHardening.ps1
$PSM_CONNECT_USER                   = "domain\srvpampsmconnect"
$PSM_ADMIN_CONNECT_USER             = "domain\srvpampsmadmconnect"
$SUPPORT_WEB_APPLICATIONS           = $true

PSMConfigureAppLocker.ps1
$PSM_CONNECT                         = "domain\srvpampsmconnect"
$PSM_ADMIN_CONNECT                   = "domain\srvpampsmadmconnect"

basic_psm.ini
PSMServerAdminId="srvpampsmadmconnect"
```

CUSTOMER1 T1:

```
PSMHardening.ps1
$PSM_CONNECT_USER                   = "domain\srvpampsmcon-t1"
$PSM_ADMIN_CONNECT_USER             = "domain\srvpampsmadmcon-t1"
$SUPPORT_WEB_APPLICATIONS           = $true

PSMConfigureAppLocker.ps1
$PSM_CONNECT                         = "domain\srvpampsmcon-t1"
$PSM_ADMIN_CONNECT                   = "domain\srvpampsmadmcon-t1"

basic_psm.ini
PSMServerAdminId="srvpampsmadmcon-t1"
```

The upgrade is split into these sections:

- Pre-Upgrade steps
- Upgrade
- Post-Upgrade steps
  - Customize the PSMConfigureAppLocker.xml file
  - Prepare for hardening with a domain-based PSMConnect and PSMAdminConnect user
  - Applying AppLocker and Hardening
  - Re-applying permissions on PSMSessionAlert.exe

Impact Analysis

During the upgrade, connections through this PSM will fail, causing some users to be unable to launch PSM sessions. Accounts assigned to platforms that are configured to only use this PSM will fail until the upgrade is complete.
Should any errors occur during the upgrade, the PSM server will be out of operation until the errors have been resolved or the upgrade has been rolled back per the Roll Back Plan.

This PSM is part of a Load Balanced setup. During the upgrade, the performance of the other PSM servers in the Load Balanced setup will be degraded due to the higher load.

Implementation Plan

Pre-upgrade

- Acquire the password for the Vault "administrator" user
- Copy the setup files to the server (ie. `C:\CA\Core PAS 12.6\Privileged Session Manager-Rls-v12.6\`)
- Ensure that .NET Framework 4.8 is installed. Reboot the server if necessary.
- Ensure that the PSM server has been drained of active users before the upgrade
- Ensure that the PSM server is not included in Load Balancing during the upgrade
- Back up the installation folder (`C:\Program Files (x86)\CyberArk\PSM`)
- Ensure that a recent VM snapshot has been taken for the server
- Ensure "administrator" is not a safe owner of the "PSMUnmanagedSessionAccounts" safe (https://cyberark-customers.force.com/s/article/00003431)
- Ensure PVWAAppUsers is a safe owner of PSMUnmanagedSessionAccounts with the following permissions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-PSM-in-an-Environment-with-Multiple-PVWAs.htm?tocpath=Installation%7CUpgrade%7CPrivileged%20Session%20Manager%7C_____3)
- Ensure that PSRemoting is enabled, test using this command: `Get-RDServer`
- Take screenshots of the current settings for evidence keeping. Use this PowerShell script to open all relevant files:

```
# take a screenshot of each AppLocker tab
secpol.msc

# take a screenshot of the file
```

```
        notepad "C:\Program Files (x86)\CyberArk\PSM\basic_psm.ini"

        # take a screenshot of $PSM_CONNECT_USER and $PSM_ADMIN_CONNECT_USER
        notepad "C:\Program Files (x86)\CyberArk\PSM\Hardening\PSMHardening.ps1"

        # take a screenshot of $PSM_CONNECT and $PSM_ADMIN_CONNECT
        notepad "C:\Program Files
(x86)\CyberArk\PSM\Hardening\PSMConfigureAppLocker.ps1"

        # take a screenshot of the output and copy out the value for later use
        $psmsessionalertACL = (Get-Acl "C:\Program Files
(x86)\CyberArk\PSM\Components\PSMSessionAlert.exe").Access | where {$_.FileSystemRights
-match "ReadAndExecute" -and $_.AccessControlType -eq "Allow" -and $_.IsInherited -ne
$true -and $_.IdentityReference -notmatch "NT AUTHORITY"} | Sort-Object -Property
IdentityReference
        $psmsessionalertACL.IdentityReference
```

Upgrade

- Open a PowerShell prompt as Administrator, navigate to the setup folder

```
        Set-ExecutionPolicy Bypass -Scope Process -Force
        cd "C:\CA\Core PAS 12.6\Privileged Session Manager-Rls-v12.6"
        Get-ChildItem -Recurse | Unblock-File
        .\setup.exe
```

- Click Install to install the prerequisites.
    - If Visual C++ Redistributable fails to install, verify that a newer version is already installed and continue.
    - If RemoteApp fails to install, verify that local PSRemoting is enabled and that `\\localhost\c$` is accessible. https://cyberark-customers.force.com/s/question/0D52J00006aGhduSAC/upgrade-issue-with-the-psm
    - To enable PSRemoting, run the following PowerShell script and rerun the installer:

```
                # if this registry value has been set by GPO, a "gpupdate /force" or a
restart after installation is recommended
                Remove-ItemProperty
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service" -Name AllowAutoConfig -Verbose
                Configure-SMRemoting.exe -disable
                Configure-SMRemoting.exe -enable
```

- Check Yes to shut down the PSM service
- On the introduction screen, click Next

- Confirm the Configuration Safe name as PVWAConfig and click Next
- Confirm the Vault Address and Port and click Next
- Type in the username and password for the "administrator" Vault user
- Accept the defaults on the API Gateway screen and click Next
- Click Next and do NOT check the box for "PKI authentication for PSM"
- On the Hardening screen, click Advanced and uncheck "Run the Hardening Script" and "Set up AppLocker Rules", click Next
- When the wizard is complete, click Finish to restart the server

Post-Upgrade

- Wait for the PVWA RefreshPeriod interval (20 minutes by default) or run `iisreset` on all PVWA servers

Customize the PSMConfigureAppLocker.xml file

> **Note**
>
> This step is performed because CyberArk may update the contents of PSMConfigureAppLocker.xml from version to version. The important thing is to check if there's any changes between the old default and the new default, and this can be done in a lab or test environment. If nothing important has changed, it's safe to let the old XML be carried into the new version.

- Diff PSMConfigureAppLocker.xml and PSMConfigureAppLocker.bak for changes between versions
- Edit PSMConfigureAppLocker.xml with your desired entries

Prepare for hardening with a domain-based PSMConnect and PSMAdminConnect user

- Edit `C:\Program Files (x86)\CyberArk\PSM\Hardening\PSMHardening.ps1`
  Change the variables `$PSM_CONNECT_USER` and `$PSM_ADMIN_CONNECT_USER` to the values noted in the description.
- Save and exit
- Edit `C:\Program Files (x86)\CyberArk\PSM\Hardening\PSMConfigureAppLocker.ps1`
  Change the variables `$PSM_CONNECT` and `$PSM_ADMIN_CONNECT` to the values noted in the description.
- Save and exit
- Edit `C:\Program Files (x86)\CyberArk\PSM\basic_psm.ini`
  Change the variable `PSMServerAdminId` to the value noted in the description.

Applying AppLocker and Hardening

- Open a PowerShell prompt as administrator, run the following commands:

```
        Set-ExecutionPolicy Bypass -Scope Process -Force
        cd 'C:\Program Files (x86)\CyberArk\PSM\Hardening'
        .\PSMHardening.ps1 -postInstall
        .\PSMConfigureAppLocker.ps1
        Restart-Service "Cyber-Ark Privileged Session Manager"
```

Re-applying permissions on PSMSessionAlert.exe

> **Note**
>
> This is done only if you have accounts that log on directly to the PSM server. CUSTOMER1 has connection components that require this.

- Right click `C:\Program Files (x86)\CyberArk\PSM\Components\PSMSessionAlert.exe`
- Properties, Security, Edit
- Add any needed users with the Read and Execute permissions. Look at the values noted before the upgrade for reference.

Test and Verification Plan

Installation Logs

Review the following logs:

```
    C:\Windows\Temp\PSMInstall.log
```

Service health and Validation

Review the following logs:

```
        C:\Program Files (x86)\CyberArk\PSM\Logs\PSMConsole.log
```

- Validate permissions on PSMSessionAlert.exe
- Check system health on PVWA.
- Test multiple Connection Components, use a platform that uses the upgraded PSM server.
  - PSM-RDP
  - In-box Windows applications (eg. mmc)
  - Web Dispatcher (eg. PVWA)
  - AutoIT-based dispatchers

Troubleshooting

- If AppLocker errors of any kind appear:
    - Run `PSMConfigureApplocker.ps1` again and verify
    - `secpol.msc`, AppLocker, right click, Clear Policy
    - Right click each subgroup, Add Default Policy
    - Run `PSMConfigureApplocker.ps1` again and verify
        - Last resort: Restart the server

Fall Back Plan

Roll back with snapshot and new Credfile (recommended)

- Revert the VM snapshot
- Stop service "CyberArk Privileged Session Manager"
- In PrivateArk, create a new password for the PSM's "PSMApp" and "PSMGW" users
- Open a PowerShell prompt, run the following command to create new credfiles for the PSM's "PSMApp" and "PSMGW" users:

```
        cd "C:\Program Files (x86)\CyberArk\PSM\Vault"
        CreateCredFile.exe psmapp.ini Password /username PSMAppUser /password Cyberark1
/EntropyFile /DpapiMachineProtection
        CreateCredFile.exe psmgw.ini Password /username PSMGWUser /password Cyberark1
/EntropyFile /DpapiMachineProtection
```

- Start service "CyberArk Privileged Session Manager"
- Test using the "Service health and Validation" procedure in "Test and Verification Plan"

Manually reinstall PSM (only in emergencies)

- Open `appwiz.cpl`
- Uninstall "CyberArk Privileged Session Manager"
- Restart the server
- In PrivateArk, rename or delete the PSM's previous "PSMApp" and "PSMGW" users
- Install the previous version using the "Upgrade PSM" procedure in "Implementation Plan", select "Yes" or "OK" to any additional prompts.
- Restart the server
- Test using the procedure in "Test and Verification Plan"

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within 4 hour(s).
30 minutes are allocated for pre-upgrade checks
30 minutes is allocated for upgrading

2 hours is allocated for post-upgrade tasks
1 hour is allocated to test and verification

Change schedule and time of day of execution

This change is scheduled for outside regular office hours.

Estimated risk

Risk is high.

2

Change - Upgrade PSMP

Checklist

1. ○ Pre: Ensure that a VM snapshot has been taken for the server
2. ○ Pre: Acquire the password for the Vault "administrator" user
3. ○ Pre: Prepare the setup files on a Windows machine
4. ○ Pre: Copy over the prepared setup files to the server
5. ○ Upgrade: Upgraded PSMP
6. ○ Post: Validated SSH Proxy functionality
7. ○ Post: Checked all
8. ○ Post: 2nd consultant checked all

Impact Analysis

During the upgrade, users actively using SSH via the PSMP may experience disruptions. Connections through this PSMP will fail, causing some users to be unable to SSH to Linux targets.

Implementation Plan

Pre-Upgrade

- Acquire the password for the Vault "administrator" user in the vault.
- Ensure that a recent VM snapshot has been taken for the server
- Extract the setup files on a Windows machine
- Edit vault.ini, set ADDRESS to the Vault IP
- Edit psmpparms.sample
- Set "InstallationFolder=/home/proxymng/PSMP13_0", "InstallCyberArkSSHD=Yes", "AcceptCyberArkEULA=Yes"
- Rename the folder to "PSMP13_0"
- Use WinSCP to copy over the setup files with the "proxymng" (or similar) user

Upgrade

Semi-Automated

- Use PuTTY to SSH to the server with a user that can run as root (proxymng or root). Adjust the first two lines of the following script and run it on the server:

```
        # EDIT THIS
        PSMPInstallDir="/home/proxymng/PSMP13_0"
        Password="VAULTADMINPASSWORD"

        # DO NOT TOUCH
        PSMPPackage="$(find $PSMPInstallDir -maxdepth 1 -name "CARKpsmp*.rpm")"
        cd $PSMPInstallDir
        /bin/cp psmpparms.sample /var/tmp/psmpparms
        chmod 755 CreateCredFile
        ./CreateCredFile user.cred Password -username administrator -password $Password -entropyfile
        rpm -Uvh $PSMPPackage
        chmod 600 /home/PSMShadowUser/.ssh/config
        service sshd restart
        service psmpsrv restart
```

Post-Upgrade

- Delete the installation folder
- If the PSMP server will target older hosts, algorithms must be enabled as per On PSMP version 12.6 and above - Error when connecting to an account using SSH keys (force.com)
  - Run the following shell code as root:

```
        touch /home/PSMShadowUser/.ssh/config
        cat << EOF > /home/PSMShadowUser/.ssh/config
        Host *
        KexAlgorithms +diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
        PubkeyAcceptedKeyTypes +ssh-rsa
        HostKeyAlgorithms +ssh-rsa
        EOF
        chmod 600 /home/PSMShadowUser/.ssh/config
        chown PSMShadowUser.PSMShadowUsers /home/PSMShadowUser/.ssh/config
```

Test and Verification Plan

Installation Logs

Review the following log for errors related to the upgrade:

```
        /var/tmp/psmp_install.log
        /var/opt/CARKpsmp/temp/EnvManager.log
```

Service health and Validation

Review the following log to ensure the service is running:

```
        /var/opt/CARKpsmp/logs/PSMPConsole.log
```

Check system health on PVWA.
Test an account, either yourself or the customer
Test new and older systems to ensure all Key Exchange algorithms, Public Key algorithms and Host Key algorithms are enabled after the upgrade.

Fall Back Plan

Repair the installation by running "rpm -Uvh --force CARKpsmp...rpm"

Revert to snapshot if necessary. Test by following the Test and Verification Plan.

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within X hours.

Change schedule and time of day of execution

This change is scheduled for XX:XX inside regular business hours.

Estimated risk

Risk is medium.

2

Change - Upgrade AAM CP+CCP

Impact Analysis

During the upgrade, any application that has been integrated with AAM to avoid hardcoded passwords may fail to authenticate.

Implementation Plan

Pre-Upgrade

- Acquire the password for the Vault "administrator" user
- Copy the setup files to the server (ie. `C:\Install\Core PAS 12.6\AAM-Windows64-Rls-v12.6\`)
- Ensure that a recent VM snapshot has been taken for the server

Upgrade CP

- Open a PowerShell prompt as Administrator, run the following:

```
# Define variables
$InstallRoot = "C:\CA"
$InstallFolder = "$InstallRoot\Core PAS 12.6"
$BackupFolder = "$InstallRoot\Backup_before_12.6"
$CP = "AAM-Windows64-Rls-v12.6"
$CCP = "Central Credential Provider-Rld-v12.6.1"

# NO TOUCH SECTION

# Create folders if they don't exist
New-Item -ItemType Directory $InstallFolder
New-Item -ItemType Directory $BackupFolder

# Back up current config
Copy-Item 'C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider' -Recurse -Destination $BackupFolder
Copy-Item 'C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk' -Recurse -Destination $BackupFolder
Copy-Item 'C:\inetpub\wwwroot' -Recurse -Destination $BackupFolder

# Get the current Vault IP address
Get-Content 'C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Vault\Vault.ini' | Select-String -Pattern "^Address"

# Start the installation
Get-Service "CyberArk Application Password Provider" | Stop-Service -Force -Verbose
cd $InstallFolder\$CP
.\setup.exe
```

- Click Yes to confirm and start the upgrade
- Click Next without changing any configurations
- Verify the Vault connection details and click Next (only one Vault address can be written here, if more Vault addresses are needed, do so under the Post-Upgrade section)
- Type the username and password of the Vault "administrator" user
- Click Next to perform the upgrade
- Click Finish to close the wizard

Upgrade CCP

- Open `appwiz.cpl`
- Uninstall "CyberArk AIMWebService"

- Right click the CCP installation setup.exe and select "Run as Administrator"
- Click Next
- Click Finish to close the wizard

Post-Upgrade

- If needed, edit Vault.ini (`C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Vault\Vault.ini`) to add all necessary Vault addresses
- Restart the server

Test and Verification Plan

Installation Logs

Review the following log:

```
        C:\Program Files
(x86)\CyberArk\ApplicationPasswordProvider\Env\Log\CreateEnv.log
```

Service health and Validation

Review the following log:

```
        C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Logs\APPConsole.log
```

- Check system health in the PVWA

Troubleshooting

- CheckConnection fails: Password contains `"`, which makes the command line utility that the installer runs in the background fail.

Fall Back Plan

- Restore the VM snapshot taken for the server
- Run a Repair of CP to register the application with Vault
- Uninstall CP and reinstall CP as per the Implementation Plan
- Restart the server
- Verify using the Test and Verification Plan

Review Notes

Downtime estimation

If no errors occur, the server will be upgraded and operational within 1 hour(s).

Change schedule and time of day of execution

This change is scheduled for DATE, TIME

Estimated risk

Risk is medium.

1