CYBERARK UNIVERSITY

Configuration and Performance Tuning

CyberArk Training

OBJECTIVES

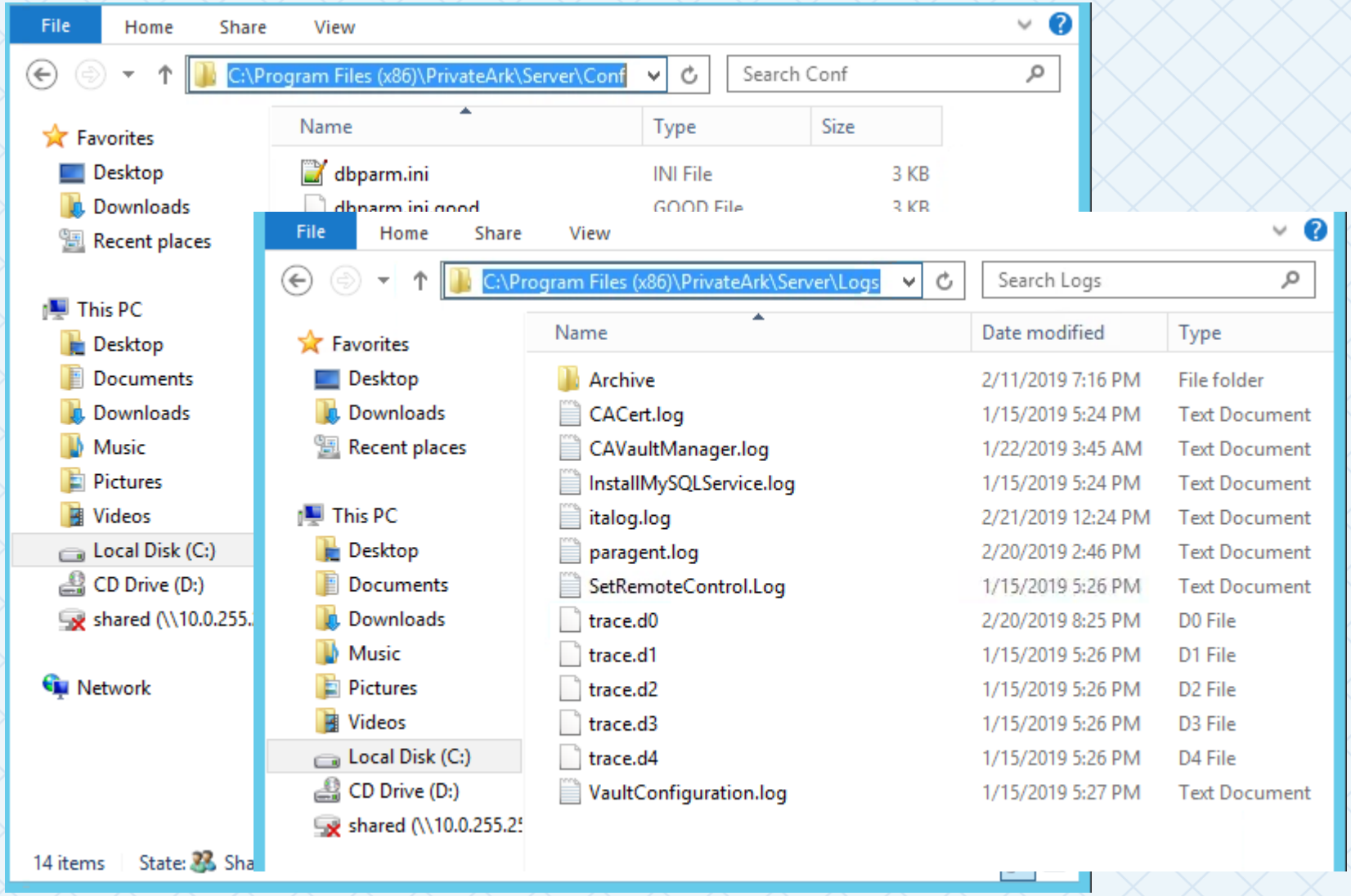
By the end of this session you will be able to:

- Describe Logging and Performance Configurations of Active Components
- Tune component configuration in high demand environments

VAULT

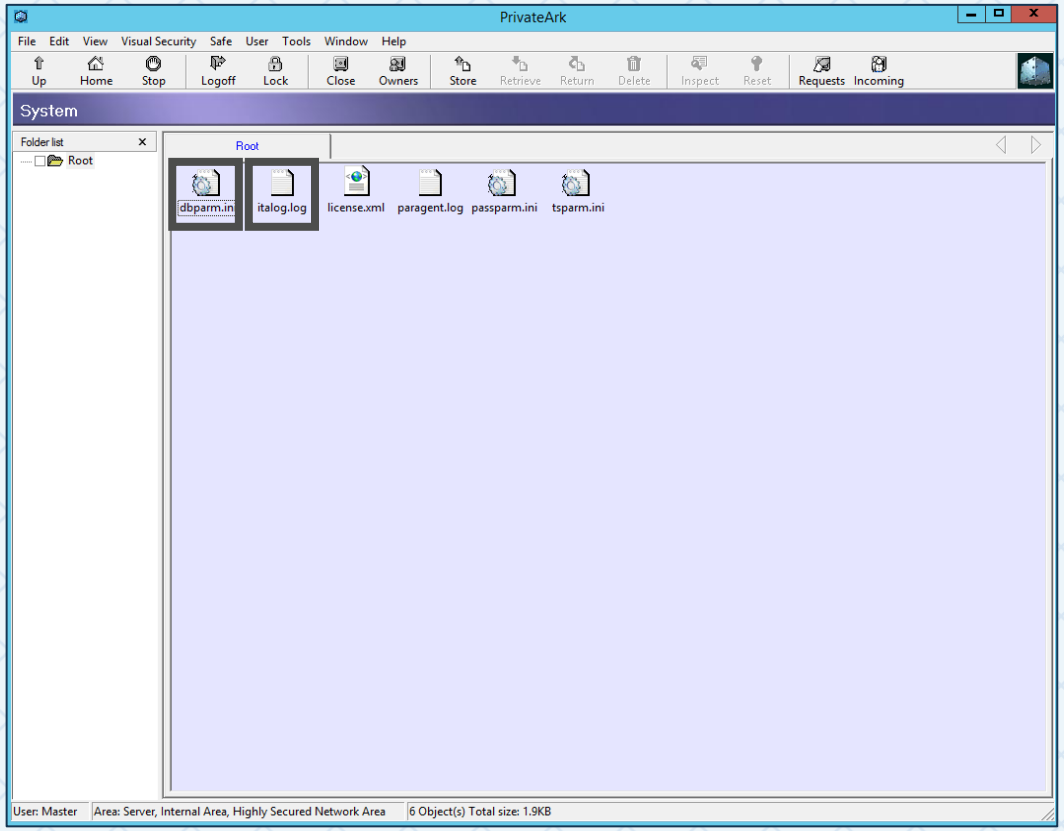
VAULT CONFIGURATION FILES (FILE SYSTEM)

- The **Vaults** configuration and log files can found in subfolders from the Vault's root installation folder;
- PrivateArk\Server\Conf.
  - dbparm.ini
  - license.xml
  - paragent.ini
  - passparm.ini
  - tsparm.ini
- PrivateArk\Server\Logs
  - Italog.log
  - paragent.log



VAULT CONFIGURATION FILES AND LOGS (PRIVATEARK)

- Many of the **Vault**'s configuration files and logs can also be accessed from remote stations using the PrivateArk Client (located in the ***system*** safe)
  - dbparm.ini
  - Italog.log
  - license.xml
  - paragent.log
  - passparm.ini
  - tsparm.ini

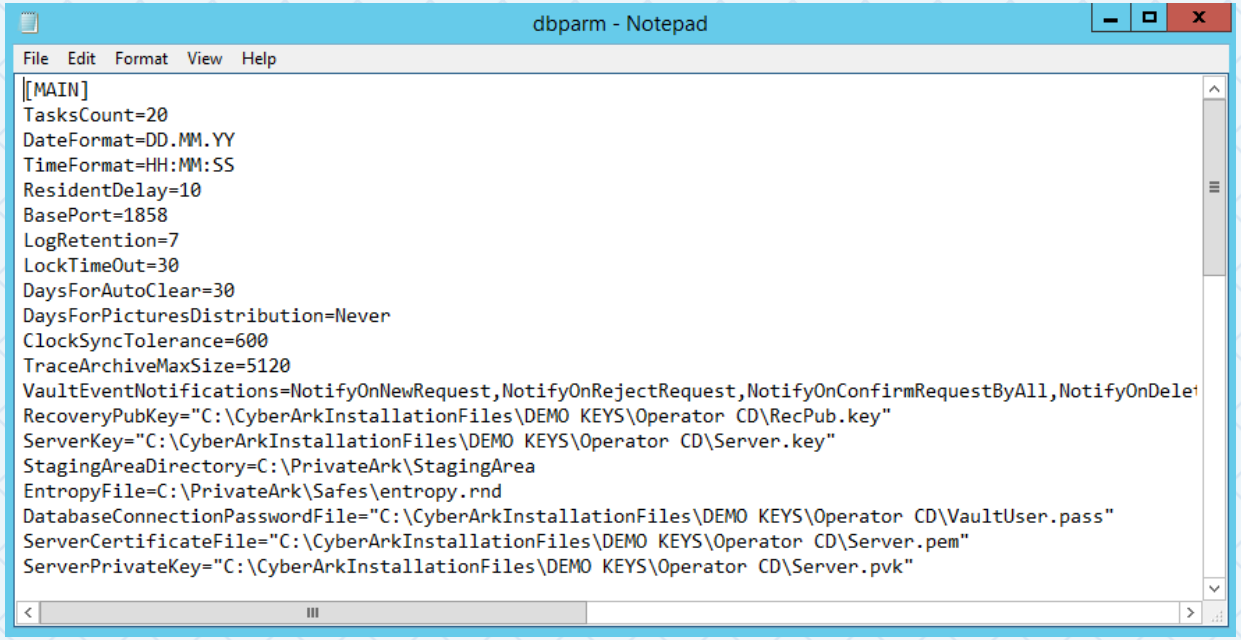


VAULT MAIN CONFIGURATION FILES

dbparm.ini	• Main Configuration file of the Vault • Any change requires a restart of the Vault service
Passparm.ini	• Configure password policy of the Vault
PARagent.ini	• Configure Remote Control Agent in the Vault • SNMP Configuration • PARAgent.log file is copied to the System safe for remote station access
TSParm.ini	• contains the list of directories where the Safe are located.

DBPARM.INI

- **dbparm.ini:** Current Vault configuration file, contains parameters for Log Level, Server Key, Syslog, Timeouts, Recovery Key etc
- **dbparm.sample.ini:** contains all the possible configuration options. Detailed information on the parameters can be found online at [CyberArk Vault Server Parameter Files]
- **dbparm.ini.good:** contains the last known good configuration of the dbparm.ini file, created automatically each time the Vault server successfully starts



VAULT LOG FILES

- The CAVaultManager utility enables you to collect log files from the Vault server to help with troubleshooting, using the “CAVaultManager CollectLogs” command
- This command creates a folder on the Vault server and stores all of the main INI and LOG files on the vault server that can be compressed and uploaded to CyberArk Support when needed
- More information on the “CAVaultManager CollectLogs” command can be found online at “Using the CAVault Manager Commands”

Italog.log	• Main log file of the Vault.
Trace.d (0-4)	• Trace files of the Vault. • It is detailed according to the debug level configured in the dbparm.ini.

VAULT OPTIMIZATIONS

Consult with CyberArk Support before attempting any changes to Vault Performance Parameters!

CPM

HARDWARE SIZING AND HIGH DEMAND CPM ENVIRONMENTS

- One CPM can support up to 100,000 managed passwords IF…
  - The system is optimized with limited use of exclusive passwords and other CPM options
- In environments managing more than 100,000 managed passwords, additional CPMs must be deployed

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
· Quad core processor (Intel compatible) · 8GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Quad core processor (Intel compatible) · 16GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Eight core processors (Intel compatible) · 32GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 4X Eight core processors (Intel compatible) · 64GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM
Software prerequisites			
· Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter) · .NET Framework 4.8 · CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

HARDWARE SIZING AND HIGH DEMAND CPM ENVIRONMENTS

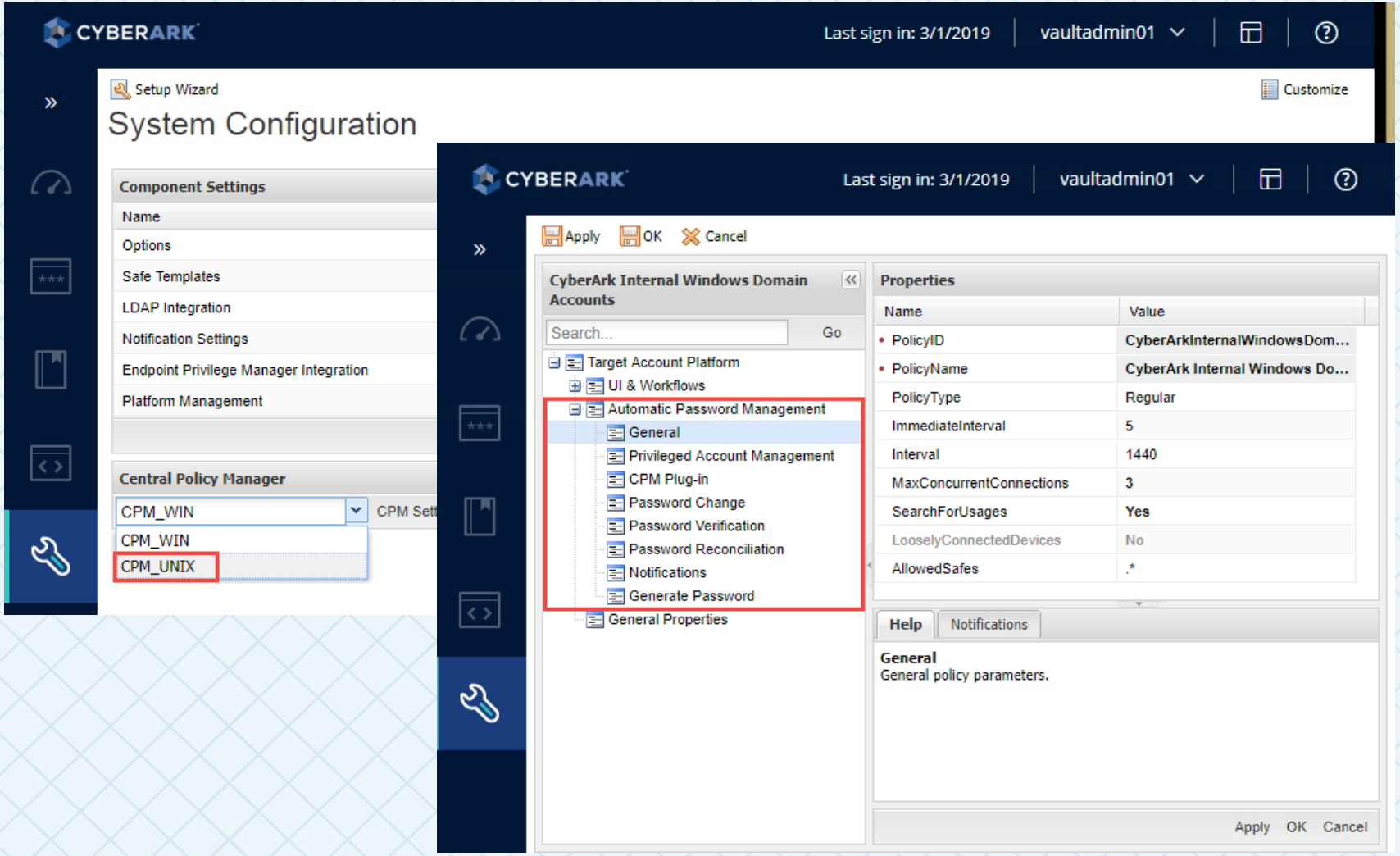
- System Requirements assume a physical machine
- Deploying CPM on virtual machines with equal specifications will not achieve the same level of performance
- It is important to optimize each CPM to achieve maximum efficiency and performance
- A goal of optimization is to reduce workload overhead on the vault caused by the CPM

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
• Quad core processor (Intel compatible) • 8GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Quad core processor (Intel compatible) • 16GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Eight core processors (Intel compatible) • 32GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 4X Eight core processors (Intel compatible) • 64GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM
Software prerequisites			
• Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter) • .NET Framework 4.8 • CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

CONFIGURING THE CPM

- Optimization parameters are configured in the PVWA in 2 ways

1. In Configuration Options > CPM Settings
2. Directly in a Target Platform.



CPM SETTINGS

CPM_UNIX

Search... Go

- Configuration
  - General

Properties

Name	Value
Interval	60
NotifyPeriod	12
NotifyOnlyOnError	Yes
AdminEmailAddress	
SmtpServer	
SenderAddress	
Subject	
LogCheckPeriod	24
LogSafeFolderName	RootNogs
LogSafeName	
WriteStartCycleEvent	Yes
LogPasswordEvents	Yes
CopyPoliciesToCPMInfoSafe	Yes
DisableExceptionHandling	No
ADPoolSize	5
AllowManualRequests	Yes
ManualRequestsInterval	5
ManualRequestsRecoveryStartTime	0
CPMDebugLevels	1
OldLogRetention	7
InitializeTime	0
PlatformsToManage	

Number of minutes after which the Central Password Manager re-reads the list of Password Policy files

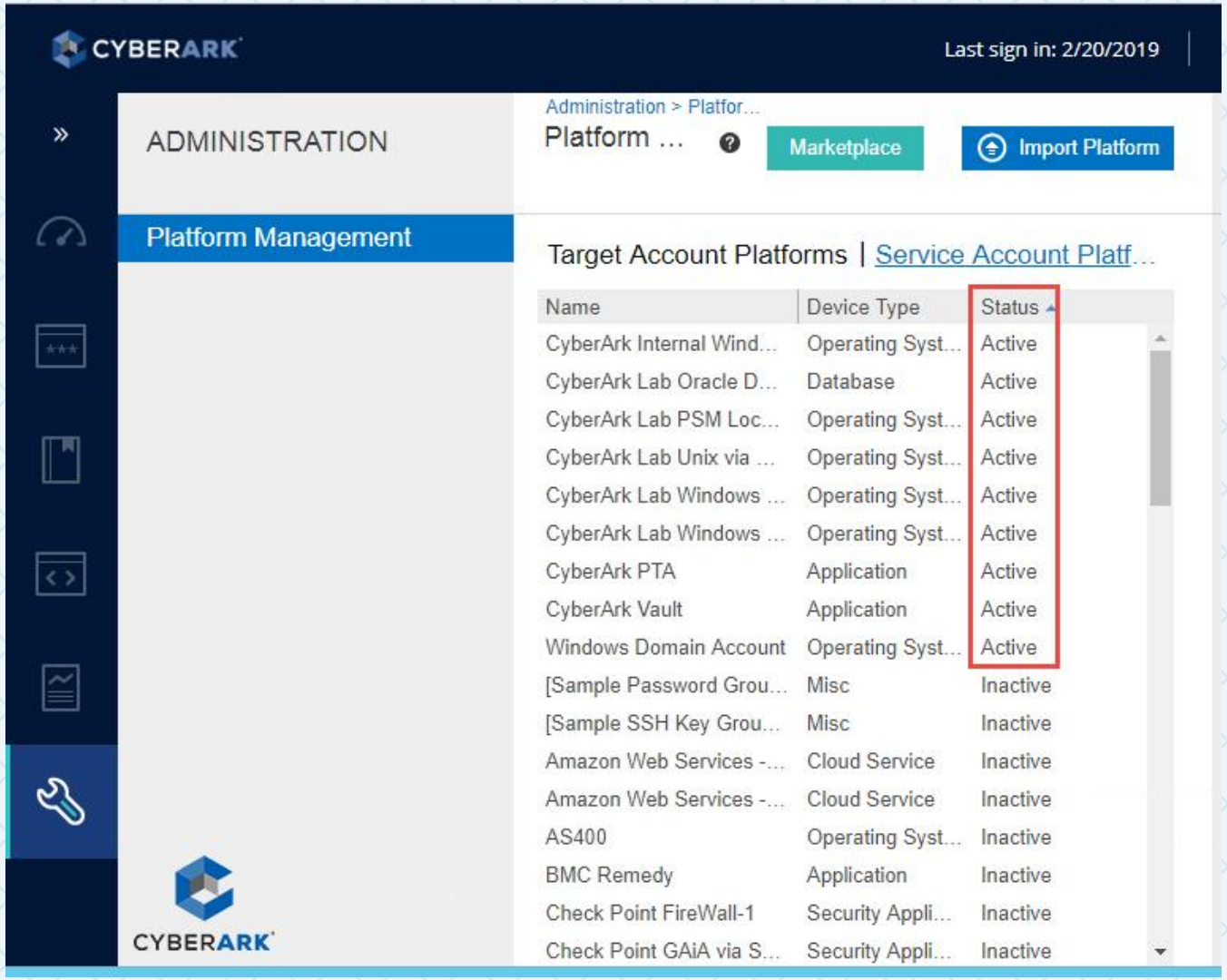
Emails about CPM activity can be sent to a predefined e-mail address

CPM Log Rotation. Each time a log file is uploaded to the Vault, it is copied to the History subfolder of the Log folder, and the Central Password Manager begins writing to a new log file

A new configuration (v9.8) was added to allow a specific CPM server to manage a specific set of platforms

PLATFORM MANAGEMENT

- A CPM will monitor each active platform, and the accounts associated with them
- By default, a number of platforms are active
- Ensure that only platforms with accounts assigned to them, are active



INTERVAL SETTINGS

- Interval settings should remain at the default 1440 minutes or once every 24 hours
- It is recommended to schedule weekly Change Control Windows to perform policy management
- Reserve all but emergency changes during the change window

Properties

Name	Value
PolicyID	Oracle
PolicyName	Oracle Database
PolicyType	Regular
ImmediateInterval	5
Interval	1440
MaxConcurrentConnections	1
SearchForUsages	No
AllowedSafes	.*_ORA_.*

ALLOWED SAFES PARAMETERS

- Optimize CPM queries to the vault by limiting them to safes where passwords are stored
- If applicable, include the safe where the reconcile account is stored
- Consider this as a part of the overall safe design

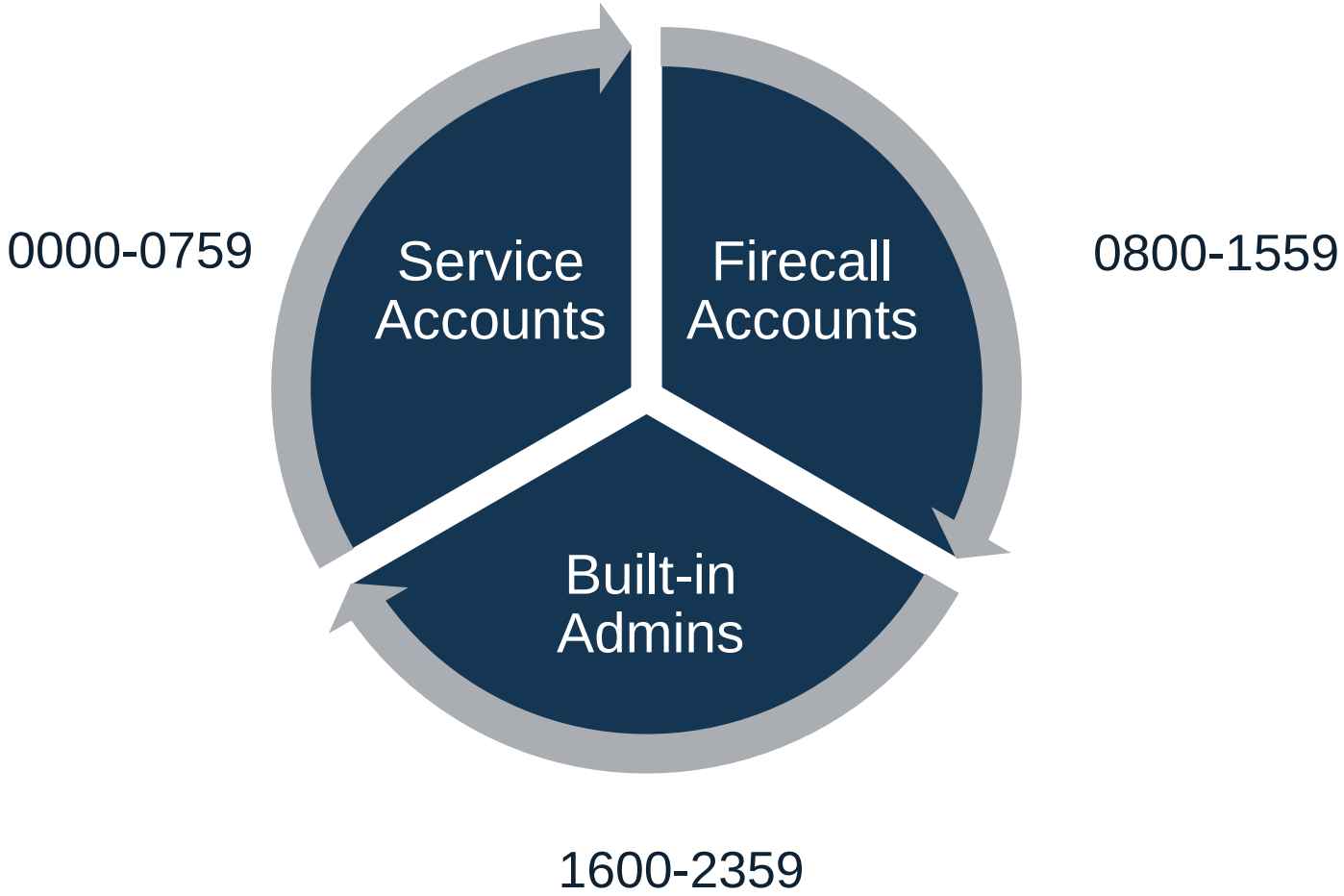
Properties

Name	Value
PolicyID	Oracle
PolicyName	Oracle Database
PolicyType	Regular
ImmediateInterval	5
Interval	1440
MaxConcurrentConnections	1
SearchForUsages	No
AllowedSafes	.*_ORA_.*

FROMHOUR/TOHOUR

Limit the number of CPM actions that can occur at the same time.

Stagger Platforms so that not all of them operate at the same time.



CONCURRENT OPERATIONS

- Limit the number of threads that can be created by the CPM
- Creating a recurring compliance report on accounts associated with a specific Target Account Platform will be useful in this analysis
- Limit the concurrency of each policy until it is demonstrated that more concurrent connections are required

Properties

Name	Value
PolicyID	Oracle
PolicyName	Oracle Database
PolicyType	Regular
ImmediateInterval	5
Interval	1440
MaxConcurrentConnections	1
SearchForUsages	No
AllowedSafes	.*_ORA_.*

RETRY SETTINGS

- MaximumRetries is the number of times the CPM will try to change a password
- When the password change process fails consider increasing the MaximumRetries value
- MinDelayBetweenRetries is the minimum delay in minutes between password management process retries. Increasing this value results in extending the time between retries

Properties

Name	Value
MinValidityPeriod	60
PasswordLevelRequestTimeframe	Yes
ResetOveridesMinValidity	Yes
ResetOveridesTimeFrame	Yes
Timeout	30
UnlockIfFail	No
UnrecoverableErrors	5001,5002,5003,5004,5005,5006,2117
MaximumRetries	10
MinDelayBetweenRetries	360

PVWA

PVWA HARDWARE SIZING

- Size the hardware like you would for a CPM
- CyberArk recommends a dedicated machine for each component

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
· Quad core processor (Intel compatible) · 8GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Quad core processor (Intel compatible) · 16GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Eight core processors (Intel compatible) · 32GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 4X Eight core processors (Intel compatible) · 64GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM
Software prerequisites			
· Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter) · IIS 10.0, 8.5 · .NET Framework 4.8 · Internet Explorer 11.0 · Chrome (any version released in the last six months on Windows and Linux/UNIX) · Firefox (any version released in the last six months on Windows and Linux/UNIX) Not supported for the Monitoring module. · PVWA can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

PVWA REFRESH INTERVAL

- It is recommended to schedule weekly Change Control windows to perform policy management and reserve all but emergency changes to be completed during the change window
- Schedule changes to avoid interference with Password Management operations
- Reduce how often PVWA refreshes its own configuration. The default is 20 minutes. Consider increasing this value to 1440 minutes or once every 24 hours
- An IISRESTART will force a refresh of the PVWA configuration

Properties

Name	Value
PasswordLinkSubject	
AllowOpenFiles	No
DisplayFileOthersColumn	Yes
EnableAddingNewValueToListProperty	Yes
RefreshPeriod	**1440**
FileDownloadTimeout	20
DisplayPolicyNameInList	No

FREQUENTLY/RECENTLY USED ACCOUNT VIEWS

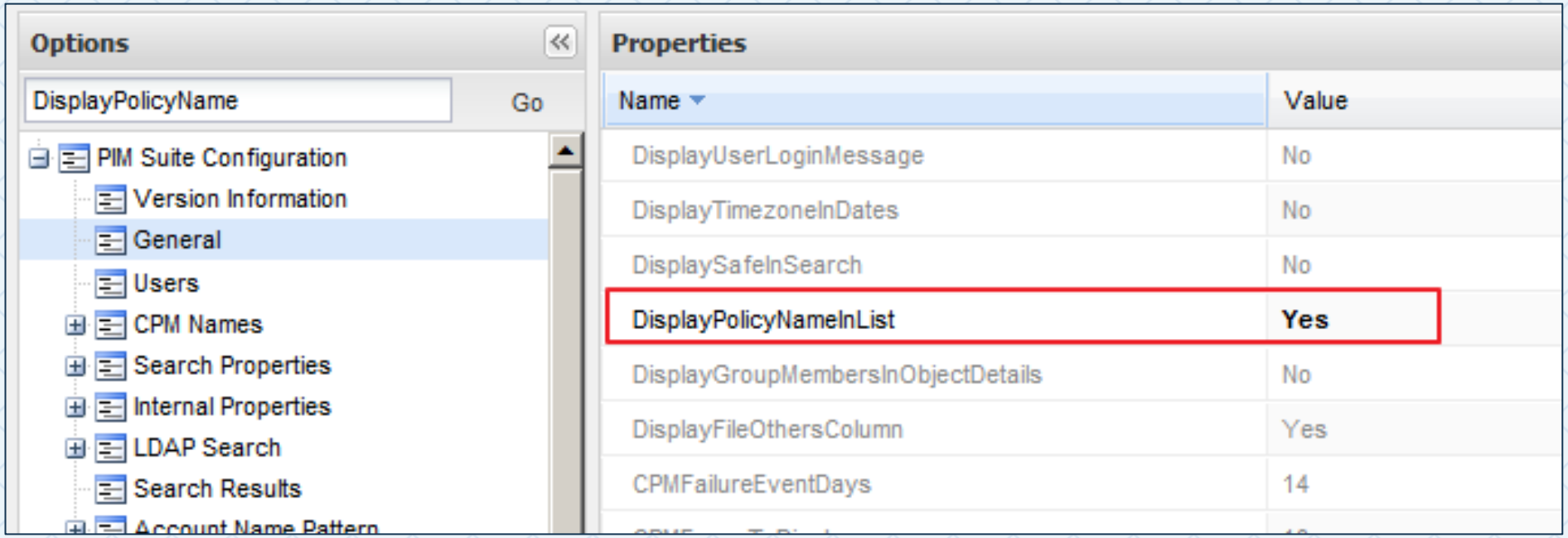
Reduce heavy aggregation calculation by reducing the number of accounts shown in the Frequently/Recently Used Account Views

Properties

Name	Value
RecentlyCount	5
RecentlyDays	3
FrequentlyCount	5
FrequentlyDays	3
MaxRecords	100
ShowDeletedAccountsInFrequentlyRecently	Yes

PLATFORM NAME DISPLAY

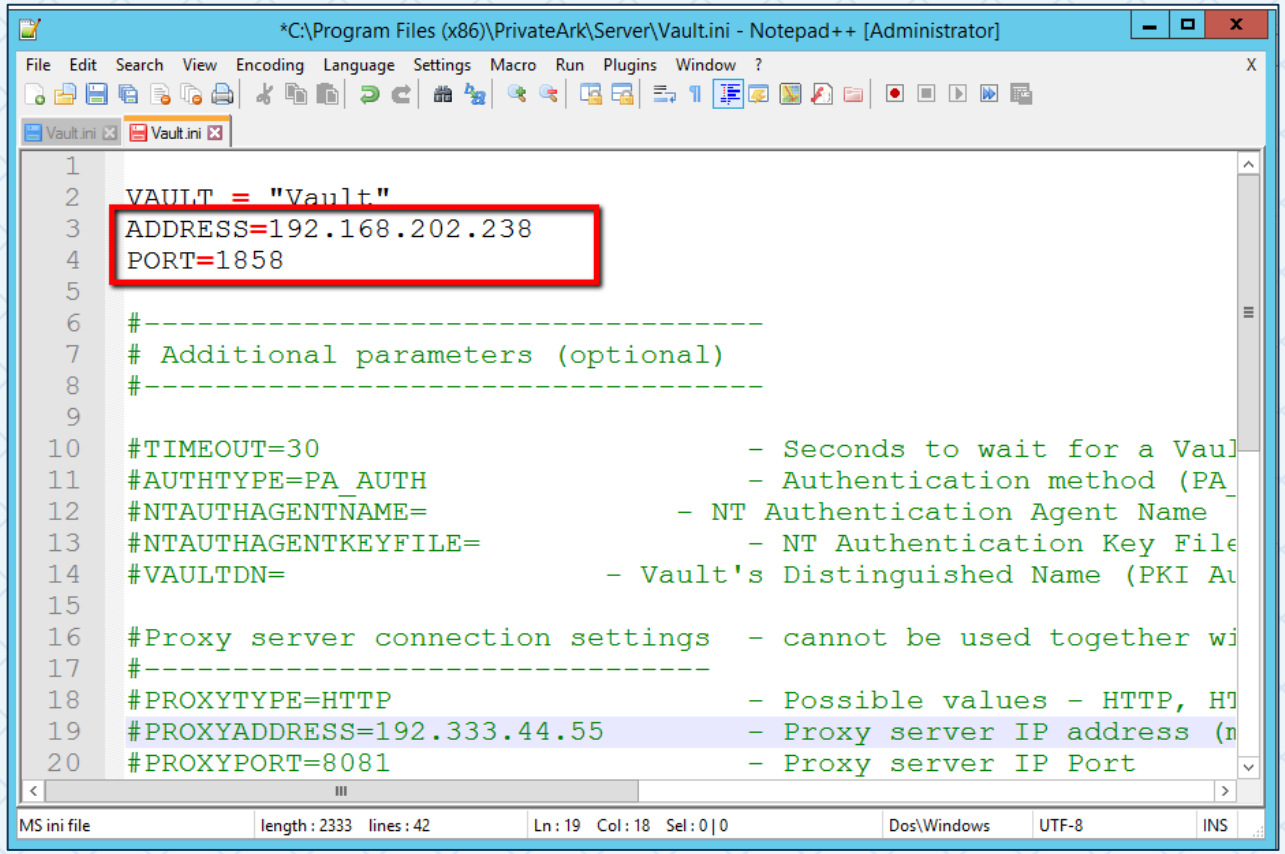
Eliminate translation of PolicyID to Platform Name on Account Details Page



COMMON CONFIGURATION FILES

VAULT.INI FILES

- The Vault.ini file contains the connection details to the Vault (address, port, etc.)



WHERE IS VAULT.INI?

Component	Vault.ini default location
CPM	C:\Program Files (x86)\CyberArk\PasswordManager\Vault
PVWA	C:\CyberArk\Password Vault Web Access\VaultInfo
PSM	C:\Program Files (x86)\CyberArk\PSM\Vault
OPM	/etc/opt/CARKaim/vault
AIM (Windows)	C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Vault
AIM (Unix)	/etc/opt/CARKaim/vault
Replicate	C:\Program Files (x86)\PrivateArk\Replicate
PrivateArk	N/A
ENE	C:\Program Files (x86)\PrivateArk\Server\Event Notification Engine
DR	C:\Program Files (x86)\PrivateArk\PADR\

CREDENTIAL FILES

- The credential files contain the credentials used by various CyberArk components to authenticate to the Vault
- Each component has a configuration file that will inform the administrator where to locate the credential files
- Search CyberArk Docs online for “Create User Credential Files” that will provide detailed instructions on creating credential files and authorization files

Administrator: Command Prompt

```
C:\Program Files (x86)\CyberArk\Password Manager\Vault>CreateCredFile.exe user.i
ni
Vault Username [CPM_NA] ==>
Vault Password (will be encrypted in credential file) ==> *********
Disable wait for DR synchronization before allowing password change (yes/no) [No
] ==>
External Authentication Facility (LDAP/Radius/No) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==>
Use Operating System Protected Storage for credentials file secret (Machine/User
/No) [No] ==>
Command ended successfully

C:\Program Files (x86)\CyberArk\Password Manager\Vault>
```


```
CredFileType=Password
CredFileVersion=2
Username=CPM_NA
VerificationsFlag=16
Password=DA83112ACABA05E99C3CA0D4EEB85A1DF6068F111BA2145CCD810BBC0EFA7A
60C1918D1F2F0105D200B33102193D410D68D30D745B84053EC0A1683F9E7D3FED7464C
1CE0A584B8E26AD988AFBA0284F
ExternalAuthentication=No
AdditionalInformation=AAA12A2AE70B7B9F343034757AFD4610B31606C2
NewPassword=D38949F25BF1D5F28CC6C14257E097E9F49C932789EC730B52754431332
14B9314168136586AA6F028AB55F82A654A3DA6A439ACAE42FE6220280F11F6FD888B32
9093164A04FC856768033E82D5ADA2
```

SUMMARY

In this session we:

- Described Logging and Configurations of Active Components
- Reviewed performance and tuning options for CyberArk Components

THANK YOU