



CYBERARK®
The Identity Security Company™

PAM Administration

System Monitoring and Common
Administrative Tasks



Agenda

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

- Monitor the system health via various methods:
 - REST
 - Email
 - SIEM
 - SNMP
- Monitor replications and DR status
- Perform common administrative tasks related to system maintenance

System Monitoring

- Monitoring components via REST and the System Health pane
- Monitoring components via email notifications
- Monitoring components via SIEM
- Monitoring components via SNMP
- Monitoring replications and DR

Monitoring System Health via REST

System Health

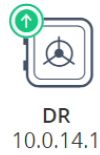
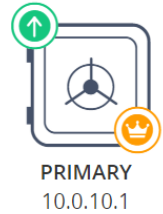
The **System Health** page provides information on:

You can export consolidated information about the system health using the **REST API**

System Health

Last sign in

Vaults



Connectivity status for **PVWA**, **CPM**, **PSM** and **PTA**

Accounts managed by **CPM**

Web Portal

App User Instances (1)



Active Users

3

CPM and Accounts Discovery

App User Instances (1)



Managed Accounts

41

PSM and PTA for SSH

App User Instances (2)



Concurrent Sessions

2

PTA

App User Instances (1)



Monitored Targets

4
Activate Windows
Go to Settings to activate Windows.

The health of the **Primary** and **DR Vaults**

PSM concurrent sessions

System Health - Components

The following information is provided for each component:

- **IP Address**
- **Version**
- **Component User**
- **Connectivity Status:**
 - Connected
 - Disconnected
- **Last Log On Date:**
 - The date when this component user last logged on to the Vault

[< Back To System Health](#)

PSM and PSM for SSH

IP Address	Version	Component User	Connectivity Status ↓	Last Log On Date
10.0.30.1	12.2	PSMApp_psm-ssh-...	✓ Connected	Feb 23, 2022 6:46 AM
10.0.20.1	12.2	PSMApp_COMPONE...	✓ Connected	Feb 23, 2022 6:47 AM



Monitoring via Email Notifications

Best Practice – Monitoring Components

- After installing the components, you can configure email notifications to be sent out if the components' user or users become disconnected.
- This should be done for all component users you wish to monitor.
- Examples include:
 - **PVWAApUser**
 - **PasswordManager**
 - **DR**
 - **Backup**

Notification: PasswordManager on IP: 10.0.20.1 is inactive

Message 1 of 16

From **VaultAdmins** 
To **vaultadmin01@cyber-ark-demo.local** 
Date **Today 08:43**

CyberArk Enterprise Password Vault

Dear Vincent Applegate,

The system detected that CPM identified by user PasswordManager on address 10.0.20.1 has not been running for 19 minutes.
The last successful Vault access was recorded at 2/5/2019.

Please check the PasswordManager log files.

Best regards,
CyberArk

This mail has been sent to you through the CyberArk PIM Suite Notification Service

Enabling Component Monitoring – 1

There is an email template that you can customize by going to:
Options / Notification Settings / Notification Agent Rules

Locate the rule **Component is inactive** -
Template ID: 206

Properties	
Name	Value
• TemplateID	206
RecipientTO	VaultAdmin
RecipientCC	
RecipientBCC	
• SendMethodID	SMTPCA

Searching for "206" will bring you to the template, where you can edit the **Body** parameter

Apply OK Cancel

Notification Settings

206Go

[CyberArk] Successful file transfer - <CA-FileTransfer>

Notification: CyberArk DR replication is not running

Notification: CyberArk Vault backup is not running

A new <TaskName/> report has been generated

Report <TaskName/> could not be generated

A new <TaskName/> report has been generated

Report <TaskName/> could not be generated

Notification: Vault license is about to expire

Notification: <CA-Component/> on IP: <CA-IpAddress>

ENE Wizard

Password reset request

Password reset request failed

[CyberArk] File content is invalid - <CA-UploadFileN>

[Secure Email] - Please complete your mail recipient

EventNotificationEngine

Properties

Name	Value
• ID	206
• Type	Text
Charset	
• Subject	Notification: <CA-Component/> on IP: <CA-IpAddress/> is inactive
Header	
• Body	Dear <CA-RecipientFirstName/> <CA-RecipientLastName/>, The system ha...
Footer	This mail has been sent to you through the CyberArk PIM Suite Notificatio...

Export

Apply OK Cancel

Enabling Component Monitoring – 2

Use the **PrivateArk Client** to enable monitoring of a specific **CyberArk** component user account:

- Select the user and click **Update**
- In the **General** tab, check the box for: ***Send email notification if component is not connected***

Update User: PasswordManager

Time Limitations | Personal details | Phone/Notes | Business/Internet
General | Authentication | Authorizations | Member Of

General Details

User Name: PasswordManager

User type: CPM Authorized Interfaces...

Location: \ Browse...

☐ Gateway Account

☐ Provide full impersonation

☐ Provide partial impersonation

☐ Provide impersonation with additional Server authentication

☐ Disable User

Quota

☐ Enable Quota

Size: MB Used: 0 MB

Monitoring

☒ Send email notification if component is not connected

Replace Photo...

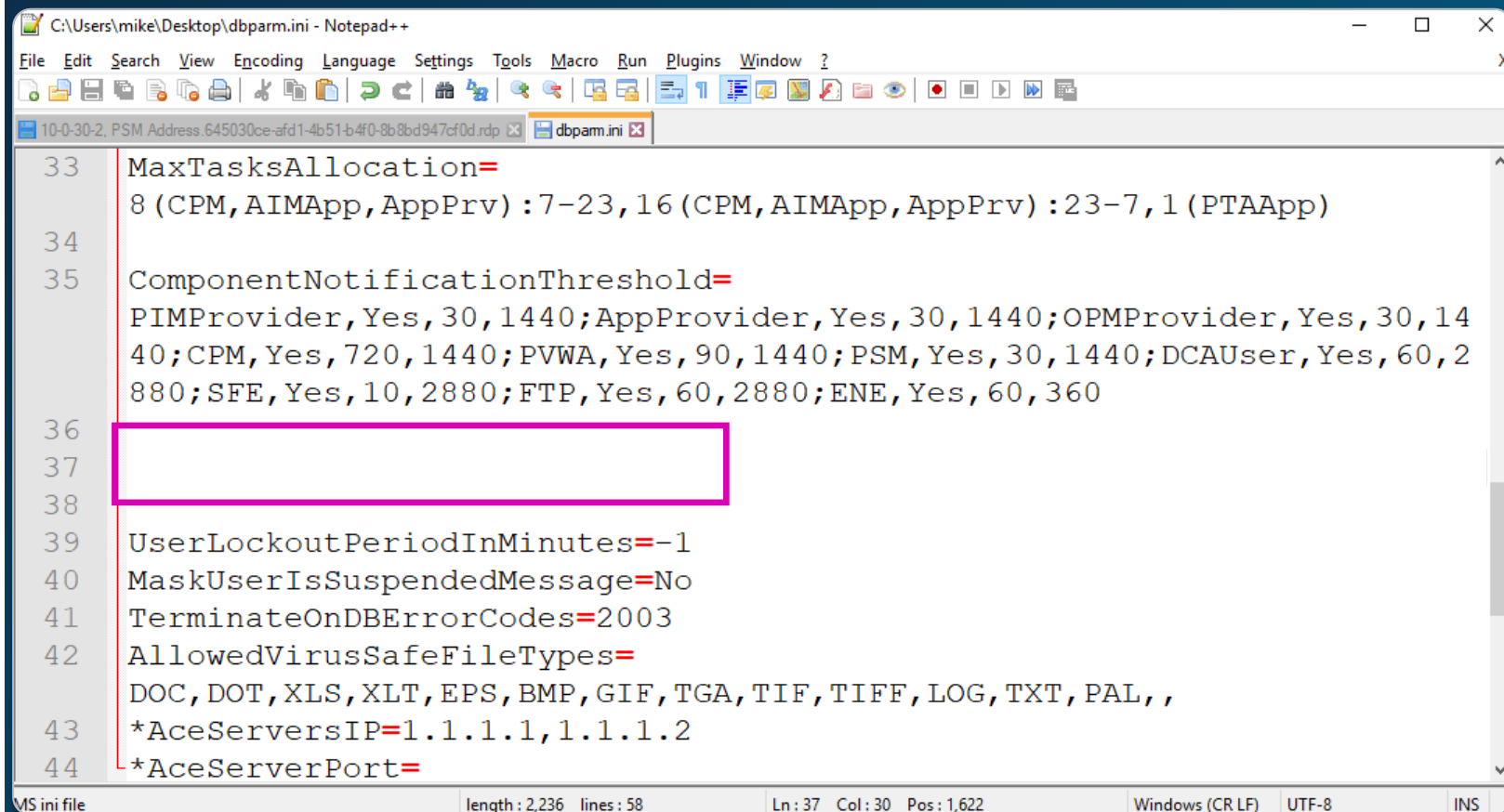
OK Cancel

Enabling Component Monitoring – 3

In **dbparm.ini**, you will need to add the parameter:

ComponentMonitoringInterval

A value of **1** means one minute will pass between checks.



```
C:\Users\mike\Desktop\dbparm.ini - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
10-0-30-2, PSM Address.645030ce-afd1-4b51-b4f0-8b8bd947cf0d.rdp dbparm.ini
33 MaxTasksAllocation=
   8 (CPM, AIMApp, AppPrv) : 7-23, 16 (CPM, AIMApp, AppPrv) : 23-7, 1 (PTAApp)
34
35 ComponentNotificationThreshold=
   PIMProvider, Yes, 30, 1440; AppProvider, Yes, 30, 1440; OPMPProvider, Yes, 30, 14
   40; CPM, Yes, 720, 1440; PVWA, Yes, 90, 1440; PSM, Yes, 30, 1440; DCAUser, Yes, 60, 2
   880; SFE, Yes, 10, 2880; FTP, Yes, 60, 2880; ENE, Yes, 60, 360
36
37
38
39 UserLockoutPeriodInMinutes=-1
40 MaskUserIsSuspendedMessage=No
41 TerminateOnDBErrorCodes=2003
42 AllowedVirusSafeFileTypes=
   DOC, DOT, XLS, XLT, EPS, BMP, GIF, TGA, TIF, TIFF, LOG, TXT, PAL, ,
43 *AceServersIP=1.1.1.1, 1.1.1.2
44 *AceServerPort=
```

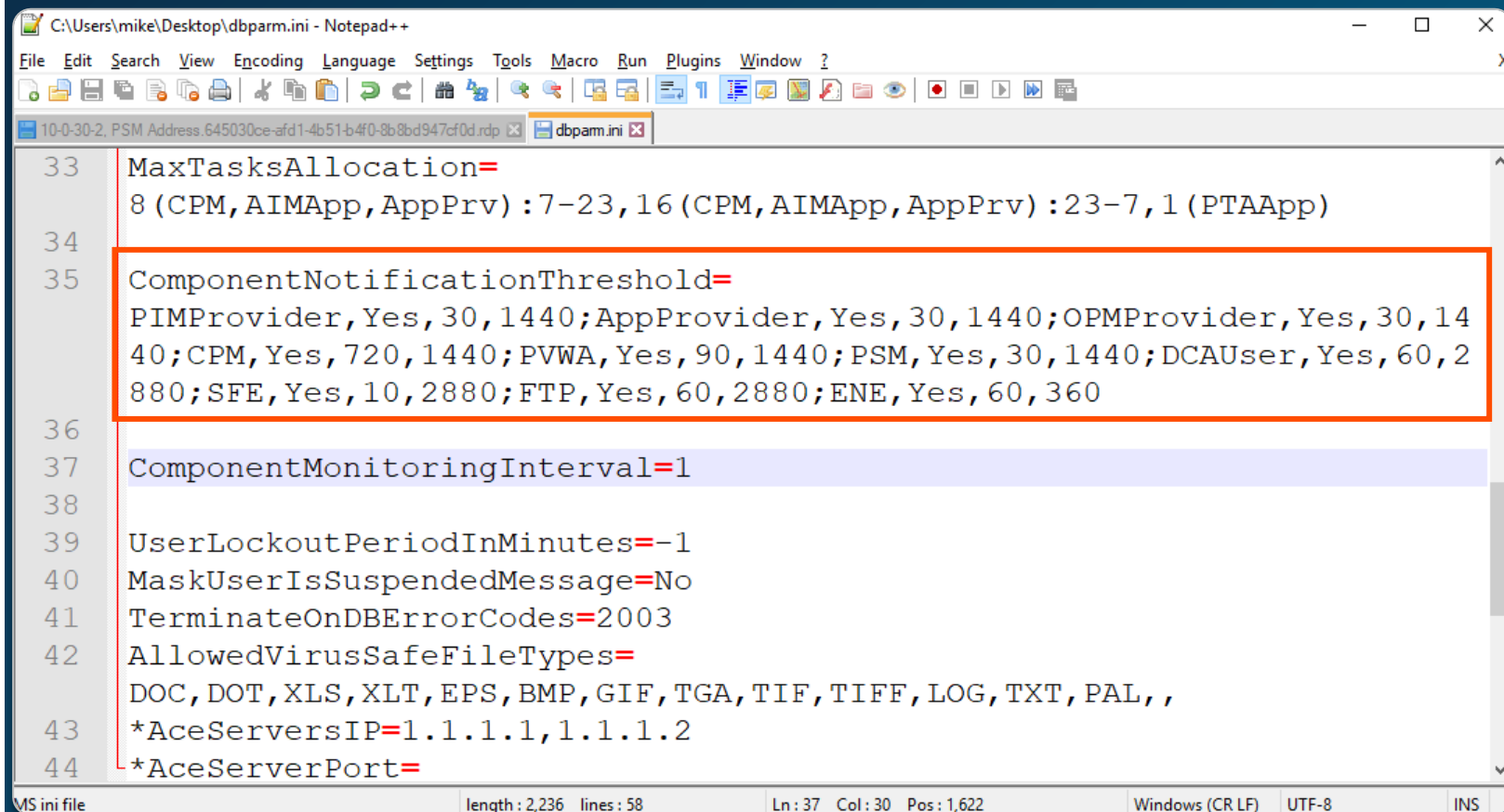
Enabling Component Monitoring – 4

The actions taken when the **Vault** detects that a component is disconnected are defined in the parameter:

ComponentNotificationThreshold

E.g.: **CPM, Yes, 720, 1440**

- **CPM** will be checked.
- Notifications will be sent.
- The first after **720** minutes
- Subsequent notifications sent every **1440** minutes.



```
C:\Users\mike\Desktop\dbparm.ini - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
10-0-30-2, PSM Address.645030ce-afd1-4b51-b4f0-8b8bd947cf0d.rdp dbparm.ini
33 MaxTasksAllocation=
   8 (CPM, AIMApp, AppPrv) : 7-23, 16 (CPM, AIMApp, AppPrv) : 23-7, 1 (PTAApp)
34
35 ComponentNotificationThreshold=
   PIMProvider, Yes, 30, 1440; AppProvider, Yes, 30, 1440; OPMPProvider, Yes, 30, 14
   40; CPM, Yes, 720, 1440; PVWA, Yes, 90, 1440; PSM, Yes, 30, 1440; DCAUser, Yes, 60, 2
   880; SFE, Yes, 10, 2880; FTP, Yes, 60, 2880; ENE, Yes, 60, 360
36
37 ComponentMonitoringInterval=1
38
39 UserLockoutPeriodInMinutes=-1
40 MaskUserIsSuspendedMessage=No
41 TerminateOnDBErrorCodes=2003
42 AllowedVirusSafeFileTypes=
   DOC, DOT, XLS, XLT, EPS, BMP, GIF, TGA, TIF, TIFF, LOG, TXT, PAL, ,
43 *AceServersIP=1.1.1.1, 1.1.1.2
44 *AceServerPort=
```

Enabling Component Monitoring – 5

- In the event of a loss of communication between the component and the **Vault**, there will now be an **ITAllog** error indicating the component's loss of communication
- And because we have enabled email notifications, **Vault Admins** will also get a notification in their in-box.

✖	05/02/2019	08:56:06	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:56:21	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:56:36	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:56:49	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:56:51	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:57:06	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:57:21	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
✖	05/02/2019	08:57:46	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.
i	05/02/2019	08:57:57	ITATS319W Firewall contains external rules.
i	05/02/2019	09:03:58	ITADB487W Component User PasswordManager has not accessed the Vault for 39 minutes.
✖	05/02/2019	09:08:58	ITATS433E IP Address 10.0.20.1 is suspended for User PasswordManager.

Monitor via SNMP With Remote Control Agent

Remote Control

The **CyberArk Vault Remote Control** feature enables users to carry out a number of remote operations on the **Vault**, **DR Vault**, and **ENE** components. It consists of two elements:

Remote Control Agent

- Installed as part of the **Vault**, both the **Primary** and **DR**
- **Windows** service

Remote Control Client

- A utility that runs from a command line interface.
- Executes tasks on a **Vault** component where the **Remote Control Agent** is installed.
- Does not require any other **Vault** components to be installed on the same computer, not even the **PrivateArk Client**.

Remote Monitoring

The **Remote Control Agent** can use **SNMP** to send Vault traps to a remote terminal. This enables users to receive both Operating System and **Vault** information:

Operating System Information

- CPU, memory, and disk usage
- Event log notifications
- Service status

Component-specific Information

- Primary and DR Vault status
- Primary and DR Vault logs



CyberArk provides two **MIB** files (for SNMP v1 and SNMP v2) that describe the SNMP notifications that are sent by the **Vault**. These files can be uploaded and integrated into the enterprise monitoring software.

Remote Monitoring – SNMP Parameters

Parameter	
SNMPCommunity	
Description	The name of location where the SNMP traps originated.
Acceptable Values	String
Default Value	-
MonitoredEventLogNames	
Description	The names of the event logs of activities that have taken place since the Server started, such as Application, Security, and System. In Linux, specify the following files: <code>/var/log/messages</code> and <code>/var/log/kernel</code>
Acceptable Values	String
Default Value	-
SNMPTrapsThresholdCPU	
Description	The interval in seconds between checks for CPU usage and the usage percentage threshold for SNMP traps, and the type of alerts that are written in the log. The threshold, retries, retriesinterval and state-full values are optional.
Acceptable Values	Interval > 0,Threshold >= 0,[Retries > 0,RetriesIntervals>0,State-full – Yes/No]
Default Value	200,90,3,30,NO

Remote Monitoring	
SNMPHostIP	
Description	The IP address of the remote computer where SNMP traps will be sent.
Acceptable Values	IP address (supports multiple entries)
Default Value	-
SNMPTrapPort	
Description	The port through which SNMP traps will be sent to the remote computer. Specify either port 161 or 162.
Acceptable Values	Port
Default Value	162
SNMPTrapInterval	
Description	The number of seconds that pass between notifications.
Acceptable Values	Number
Default Value	30

For a complete list of parameters, refer to the **CyberArk PAM Self Hosted** documentation:

<https://docs.cyberark.com>

Remote Administration

The **Remote Control Agent** allows administrators to do the following from the **Client**:

- Retrieve logs
- Set parameters
- Restart the Vault
- Restart services
- Reboot the Vault server
- Retrieve machine statistics such as memory and processor usage

Vault commands:

Start Vault	Start a Vault on the remote machine.
/Last	Starts the Vault with the last known good configuration files.
Stop Vault	Stop a Vault on the remote machine.
/Normal	Wait for active tasks to complete before stopping the Vault. This is the default.
/Immediate	Force active tasks to complete before stopping the Vault.
/Terminate	Stop the Vault without completing active tasks.
Restart Vault	Restarts a Vault on the remote machine.

ENE commands:

Start ENE	Start the ENE service.
Stop ENE	Stop the ENE service. Before stopping, the ENE service will send out notifications for all the activities that it has already recognized.
Status ENE	Show activity status of the ENE service on the remote machine.
GetLog ENE	Show the ENE log file on the remote machine.
/LogFile Trace/Console	Whether the ENE log file will be ENETrace.log or ENEConsole.log.

DR Vault commands:

Start PADR	Start a DR Vault on the remote machine.
Stop PADR	Stop a DR Vault on the remote machine.
Restart PADR	Restarts a DR Vault on the remote machine.
Status PADR	Show activity status of a DR Vault on the remote machine.
GetLog PADR	Shows the Disaster Recovery Vault log file, PADR.log, on the remote machine.



CYBERARK[®]
The Identity Security Company[™]

Monitor via SIEM

Vault Health Monitoring via SIEM

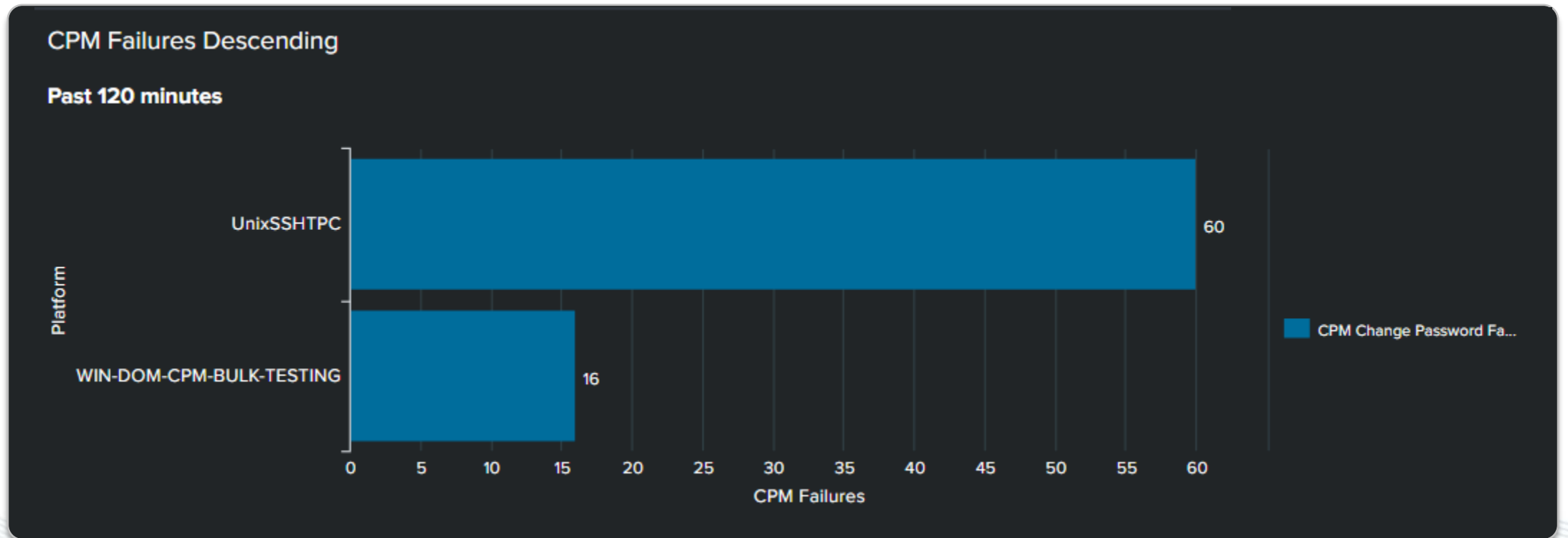


To increase the visibility of CyberArk's solution, measurements can be sent from the **Vault** via the syslog protocol and can be aggregated in a SIEM tool.

- The **Vault** can be configured to send health statistics to SIEM applications such as Splunk and ArcSight. This is done by setting the **SendMonitorMessage** parameter in dbparm.ini to **yes**.
- Statistics include transaction queue/execution time, number of tasks, CPU usage, and more.
- You should create a baseline specific to your environment to identify system trends and thresholds.
- Monitor statistics regularly in order to detect variations from your baseline.

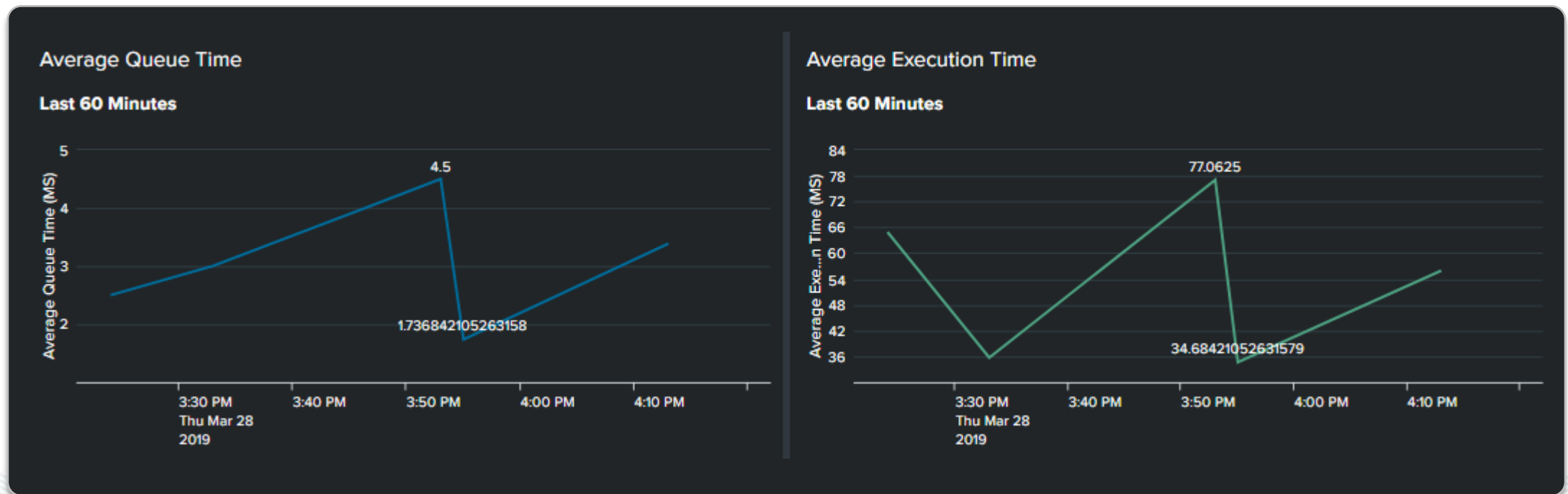
Application Monitoring Sample Dashboards (Splunk)

- Shows systemic issues with specific platforms
- Additional drill-down can show trends for specific error messages
- Platforms at top of list can be prioritized to address most widespread issues first



Application Monitoring Sample Dashboards (Splunk)

- Shows overall Vault activity over time
- Can be customized by time range
- Trends can be stacked to compare current loads to historical loads
- Visualizes impact from various replication cycles and EVD jobs

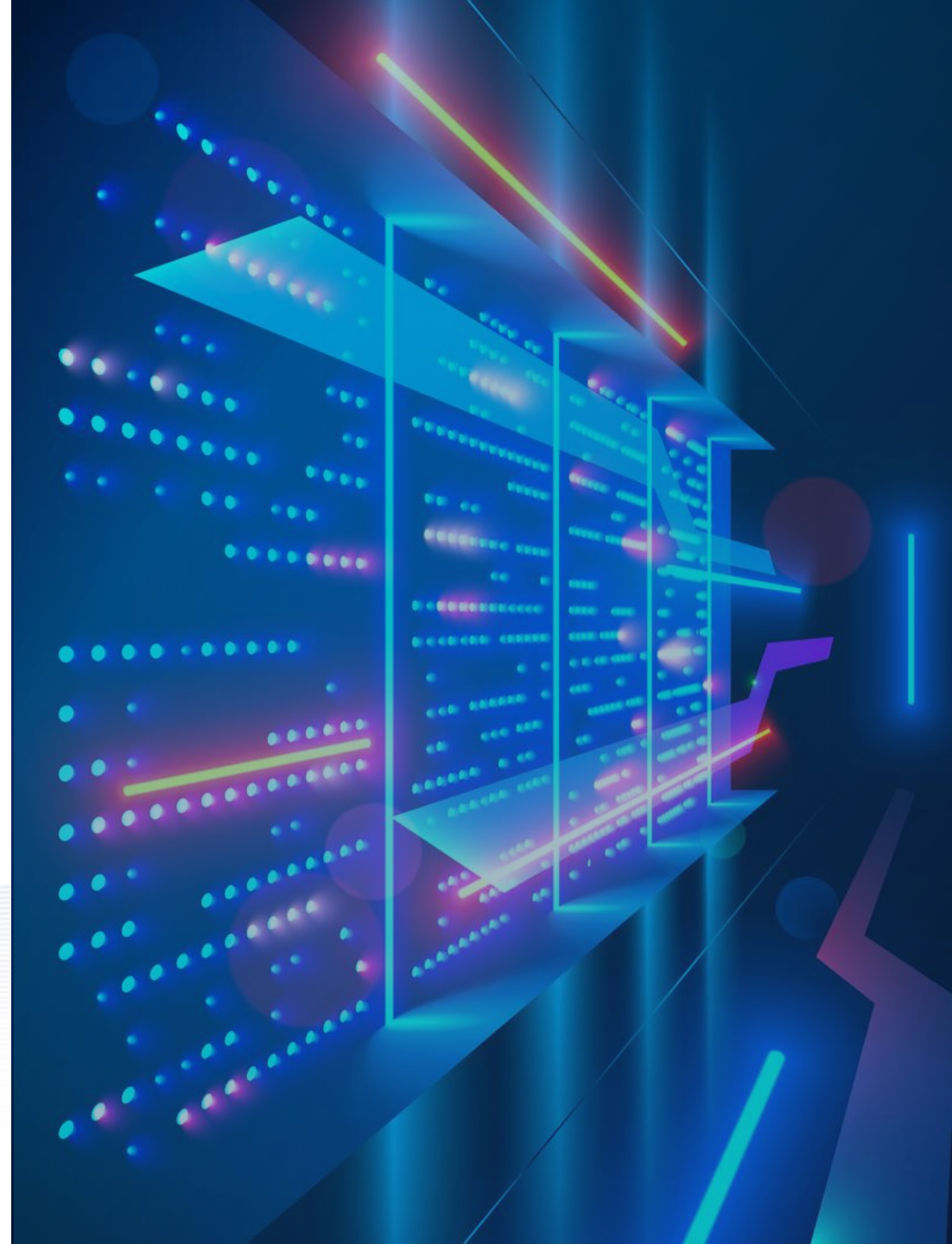


Monitoring Replications

Monitoring Backup and DR Replications

It is critical to be notified ASAP when Backup and DR are not operating.

- The **Vault** can be configured to send email notifications when the **Backup** and **DR** users fail to connect after a specific time period.
- By default, these notifications are sent to the members of the Vault Admins group, although they can be sent to any predefined recipients.
- In addition, a relevant message will be written in **ITALog.log**.



Enabling Backup Monitoring

To activate the Backup Status Notification, you need add the ***BackupNotificationThreshold*** parameter to ***dbparm.ini***

BackupNotificationThreshold=Yes, Yes, 48, 24, 12

Configures the **Vault** to monitor missing replication

Sends notifications whenever a missing replication is detected according to the following timeframes

First notification will be sent 48 hours after the missing procedure is detected

Subsequent notifications will be sent every 24 hours after that

The backup replication status will then be checked every 12 hours

Enabling Monitoring of DR Replications

To activate DR monitoring, you need add the *DRNotificationThreshold* parameter to *dbparm.ini*

DRNotificationThreshold=Yes, Yes, 2, 24, 30m

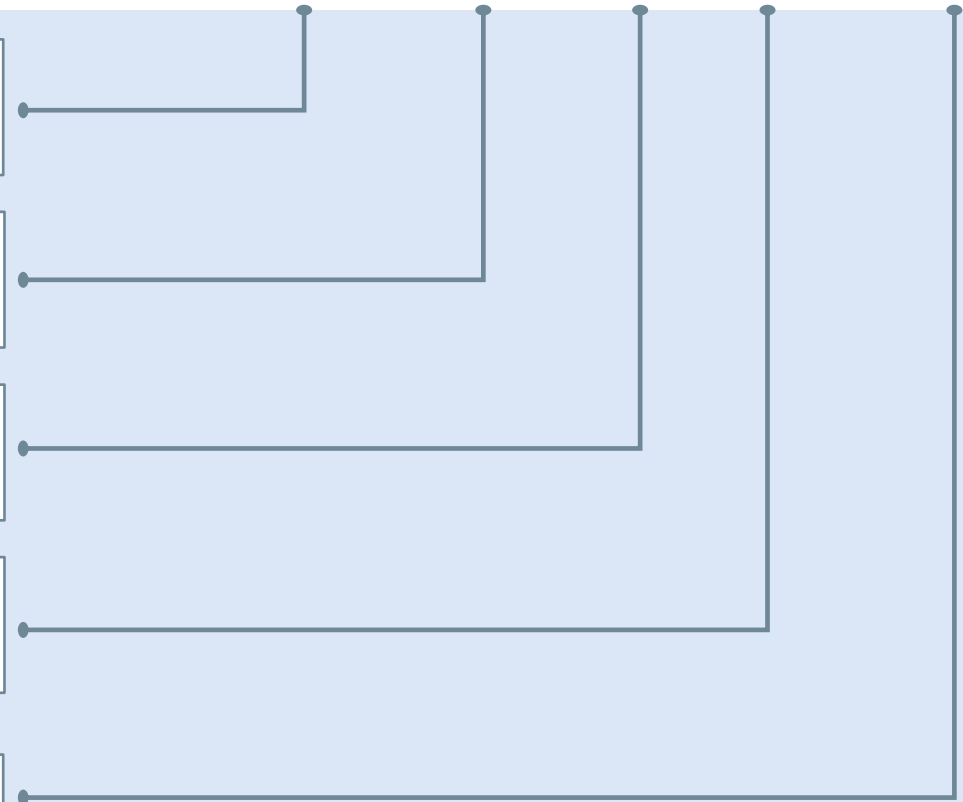
Configures the **Vault** to monitor missing DR User connections

Sends notifications whenever a missing connection is detected according to the following timeframes

First notification will be sent 2 hours after the missing procedure is detected

Subsequent notifications will be sent every 24 hours after that

The DR status will then be checked every 30 minutes



Common Tasks

- Rotate CPM Logs
- Clearing Safe history
- Other common tasks

CPM Log Rotation

During daily **CPM** operations, the log files folder and its subfolder can grow to a huge amount of data.

- Extremely large log files can lead to disk space issues on the **CPM** Server and can make troubleshooting difficult
- All the **CPM** log files can be automatically uploaded to a Safe in the **Vault** on a regular basis, according to a predefined time period.

LogCheckPeriod

► The interval in hours after which the log files will be uploaded to the Vault

It is recommended to upload **CPM** logs to a Safe

LogSafeName

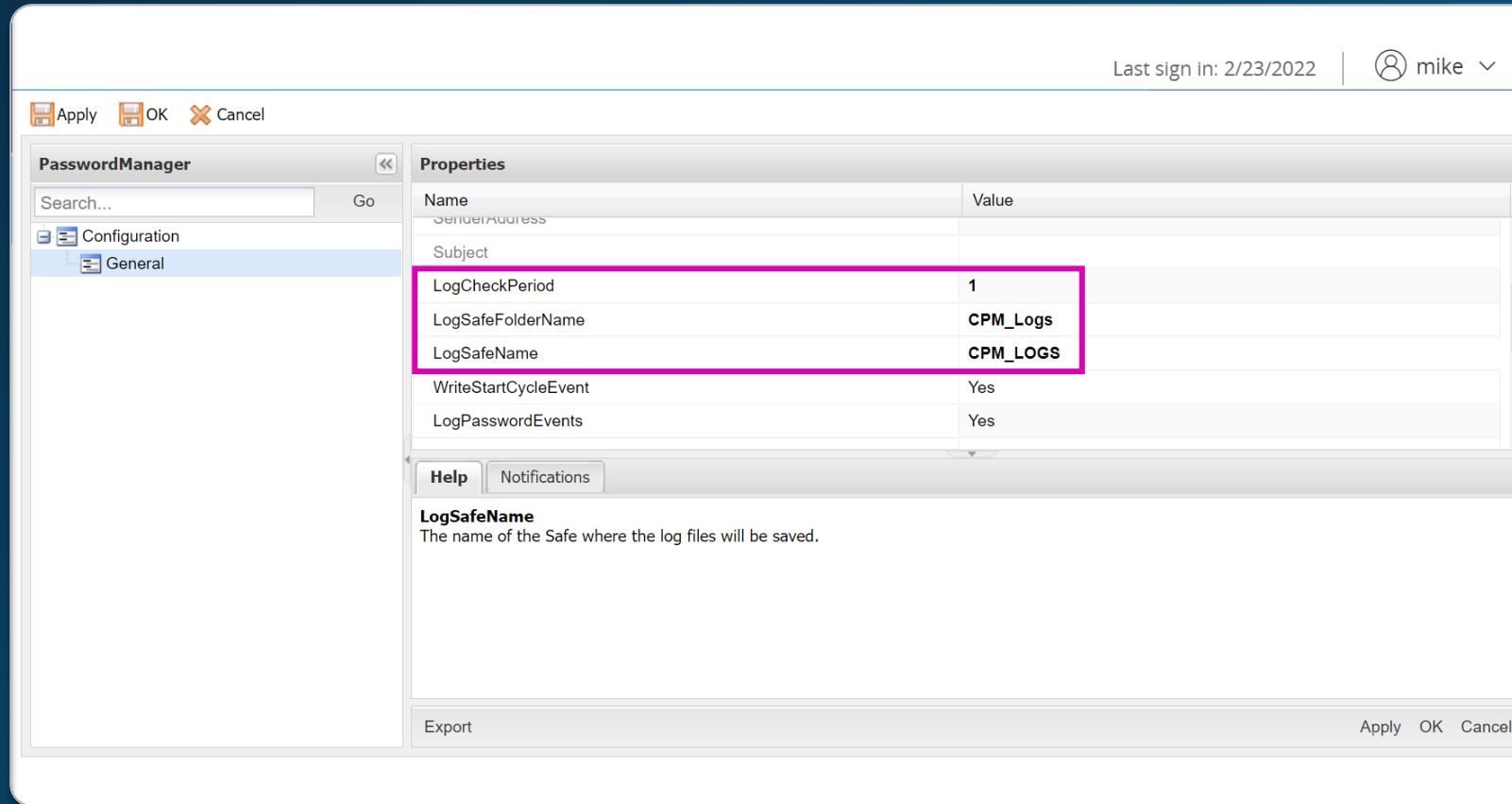
► The name of the safe where the log files will be saved

And then automatically purge old and obsolete logs files

CPM Log Rotation - Configuration

Configure the CPM to archive logs to the **Vault** periodically using the **LogCheckPeriod**, **LogSafeName** and parameters in **CPM Settings**.

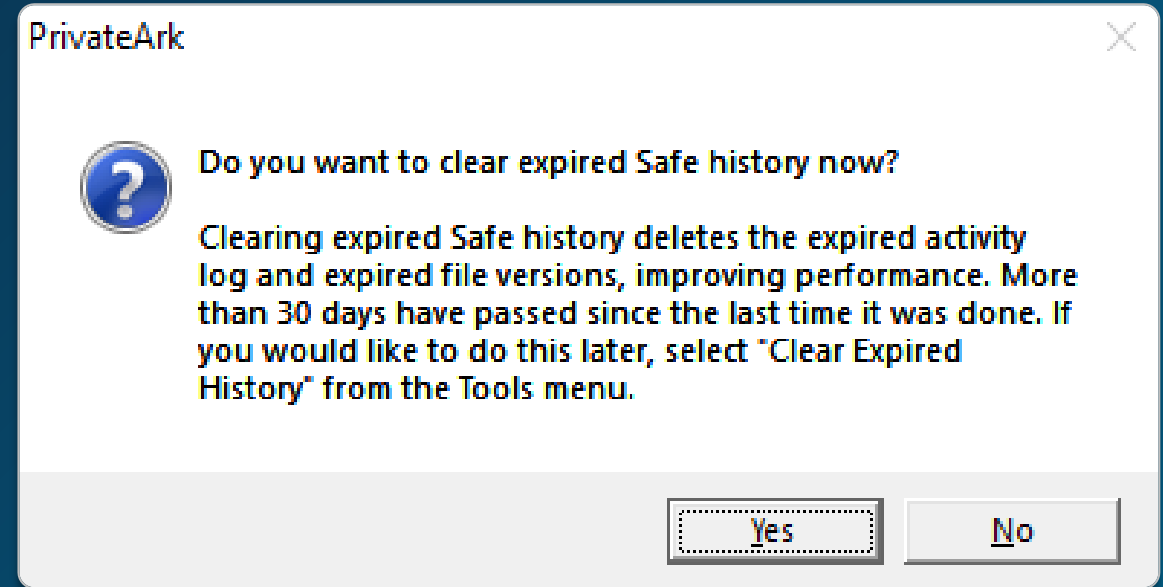
Once the log **Safe** has been defined, an automatic process will periodically remove old log files.



Clearing Safe History

Periodically, you need to clear the **Safe** history

- Only file versions and **Safe** history logs that have been held for longer than the time specified in the **Safe Properties History** window can be deleted
- To clear the **Safe History**, select **Clear Expired History** from the **Tools** menu in the PrivateArk Client, then **Safe**
- When you open a **Safe** via the **PrivateArk Client**, you will be prompted to clear expired Safe history



Recommended Tasks

WEEKLY

Check ITAlog.log once a week for a month.

- If not much noise is found, change interval to every two weeks.
- If you don't know what Normal looks like, it is harder to identify when something Abnormal occurs.

Use [M&R](#) guide and search the Customer Community to understand messages.

Example of noise:

Messages **"ITATS319W Firewall contains external rules."** will appear every 15 min with the default value in the **dbparm.ini: MonitorFWRulesInterval**

QUARTERLY

Check license capacity to make sure you are not approaching license limits.

Check free space to make sure systems have adequate capacity.

- If space is limited, check monthly or every other month.

Recommended Tasks

QUARTERLY

- Review, manage, test directory mappings.
- Periodically (quarterly, annually) test Master account and password login procedure.
- Periodically (quarterly, annually) test DR/BC failover procedures, including password reset disk for the Vault host administrator.

ANNUALLY

- Schedule a formal **CyberArk Security Services Health Check** annually / periodically.

Recommended Tasks

- Use the built-in capabilities of Syslog and SIEM to monitor your environment.
- Use Remote Control Agent for monitoring via SNMP.
- Know where the logs are.
- **Diagram your environment with server names, IPs, and server function, and current CyberArk version.**
- Make sure archive logs setting is adequate for the amount of time traces and LC (Logic Container) logs that need to be archived.
 - Ideally having 24 hours of archived traces would be preferred from a support perspective.
 - Vault traces and LC logs are located in the same archive folder.
 - Make sure you provide Support with the correct log when requested.
- Have a tool like LogExpert to read logs and search logs for troubleshooting.



Check the Visio/PowerPoint Stencils here:

<https://cyberark-customers.force.com/s/article/Official-Visio-and-PowerPoint-CyberArk-icons>

Recommended Tasks



Make sure the CPMs are configured to auto-rotate logs.



Configure the ***Send Email Notification if Component is not Connected*** option.



Summary

Summary

In this session we covered:

- Monitoring various CyberArk components
- Common Administrative Tasks

Additional Resources



Documentation

[CyberArk Technical Community](#)

[Support Vault](#)