CYBERARK®
The Identity Security Company™

PAM Administration

Troubleshooting

Agenda

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

1. Describe the basic flow for troubleshooting issues in the CyberArk environment

2. Describe, locate, and manage the log files generated by the Vault and various components

3. Describe, configure and use the xRay agent

Troubleshooting Flow

Overview

The basic troubleshooting methodology for the PAM solution requires a thorough understanding of:

1. Your system implementation
2. How components communicate with each other in your environment
3. What is the current behavior compared to the expected behavior?

This methodology is designed to provide guidance and might not apply to every scenario

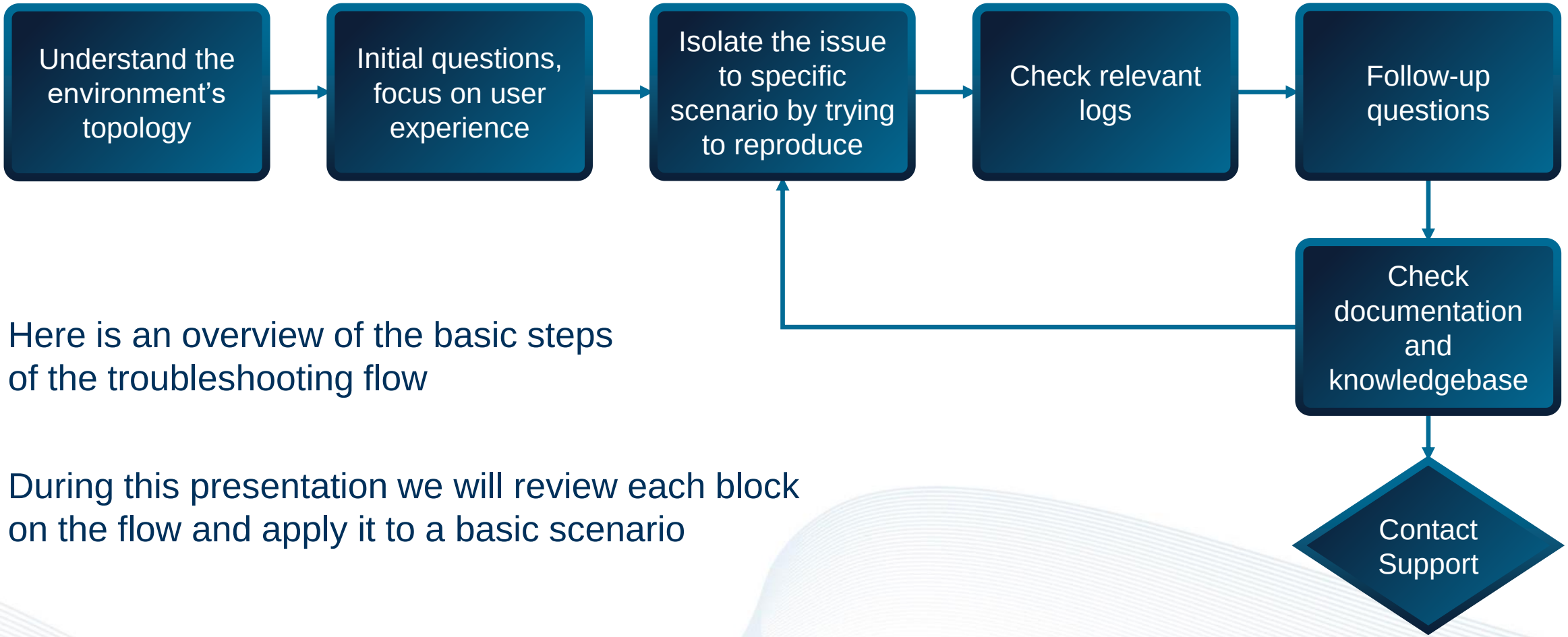
It is important to write down any information gathered during this process and any tests performed, as all of this information will be required when opening a case with **CyberArk** support

Prerequisites

1. Knowledge of the environment layout
2. Access to the different servers
3. Access to CyberArk Knowledgebase (Customer Community)
4. Access to CyberArk documentation (publicly available online)

The latest version of the documentation will contain the most recent enhancements and notes.

Troubleshooting Flow

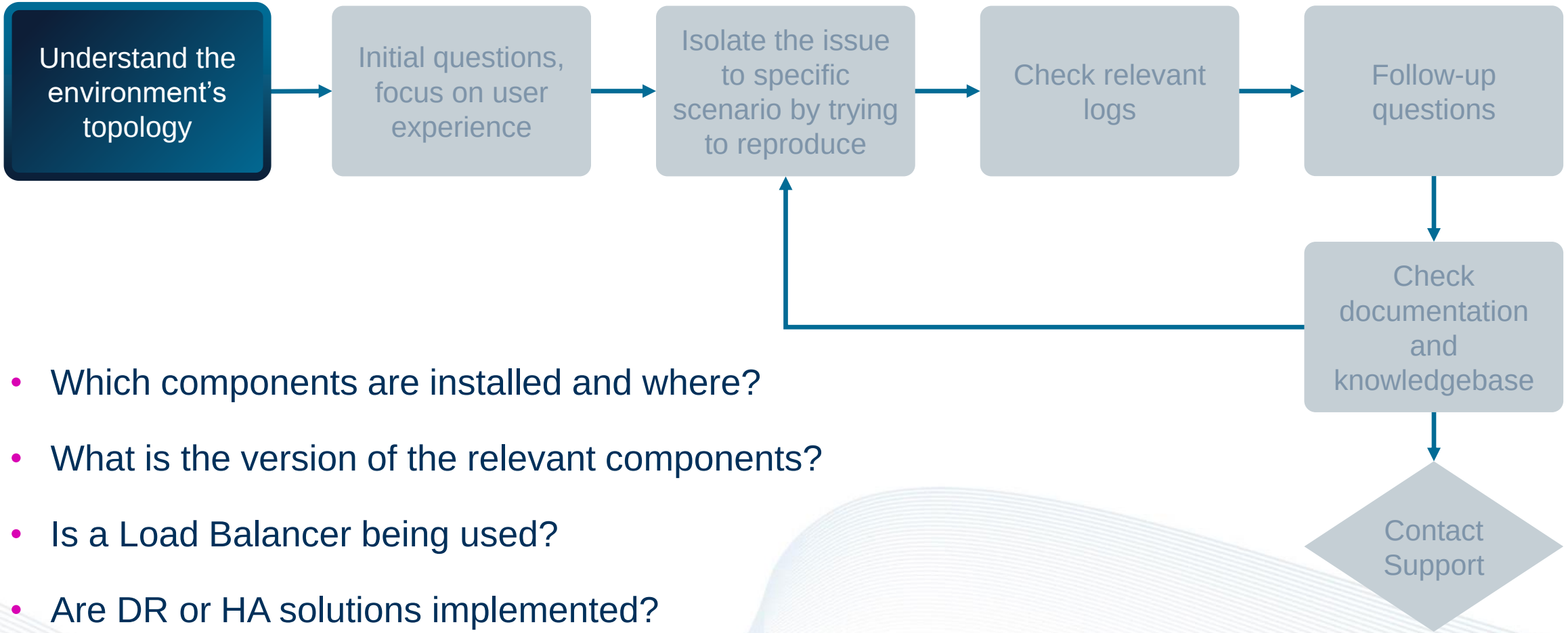


Here is an overview of the basic steps of the troubleshooting flow

During this presentation we will review each block on the flow and apply it to a basic scenario

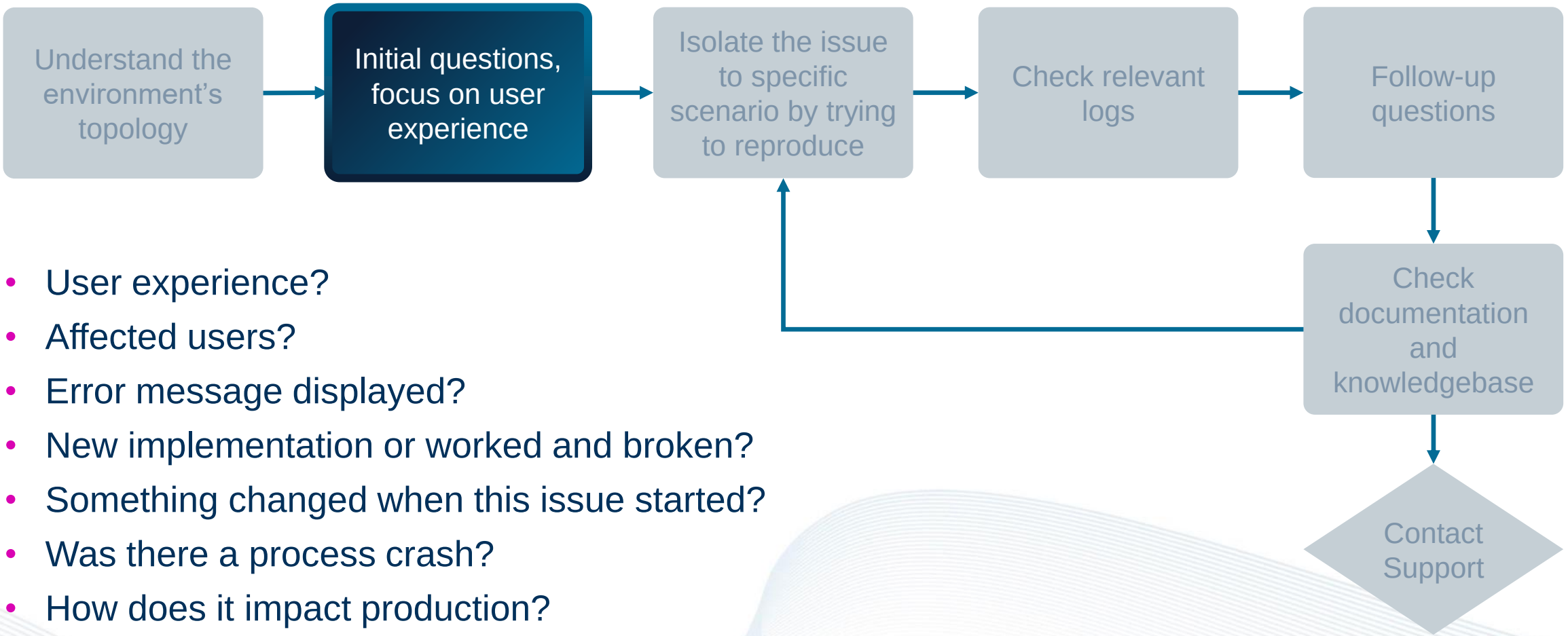
CYBERARK®

Understanding the Environment



- Which components are installed and where?
- What is the version of the relevant components?
- Is a Load Balancer being used?
- Are DR or HA solutions implemented?

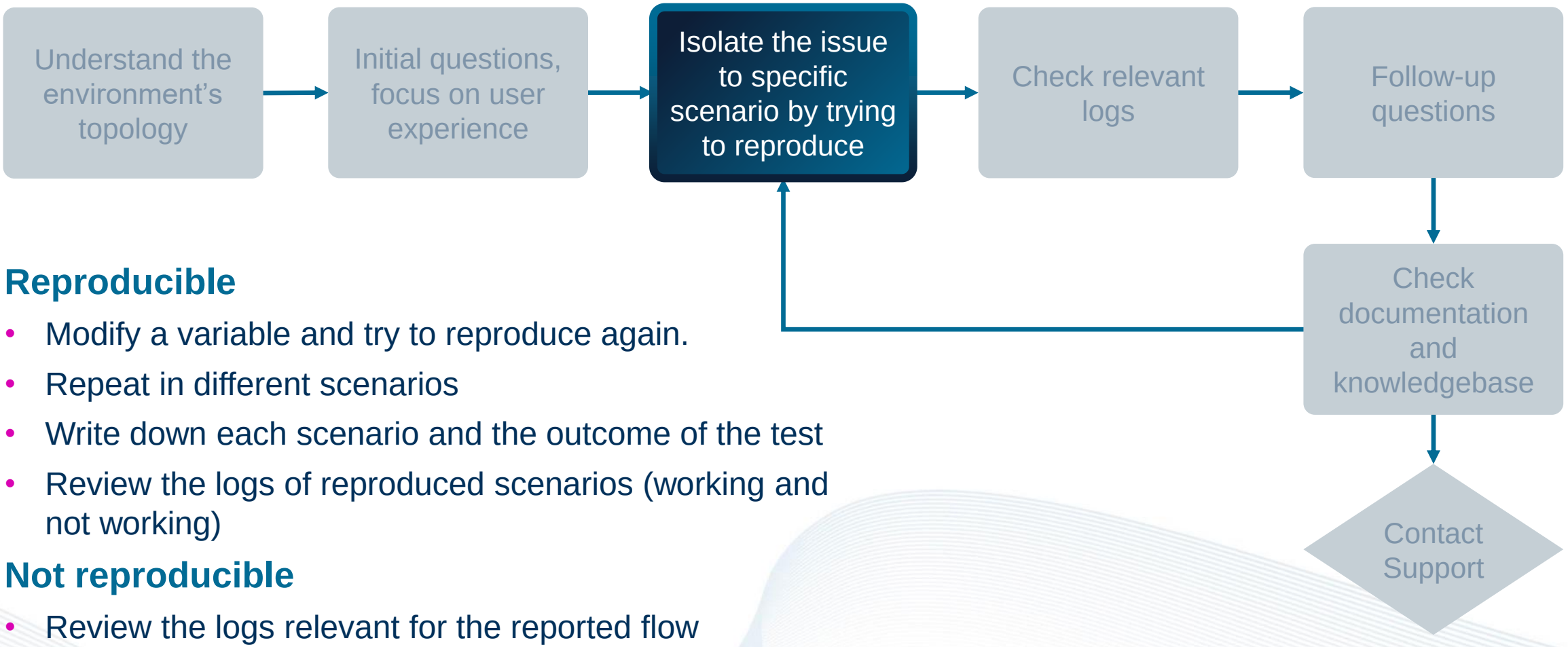
Initial Questions



- User experience?
- Affected users?
- Error message displayed?
- New implementation or worked and broken?
- Something changed when this issue started?
- Was there a process crash?
- How does it impact production?
- Reproducible?

CYBERARK®

Isolation and Reproduction



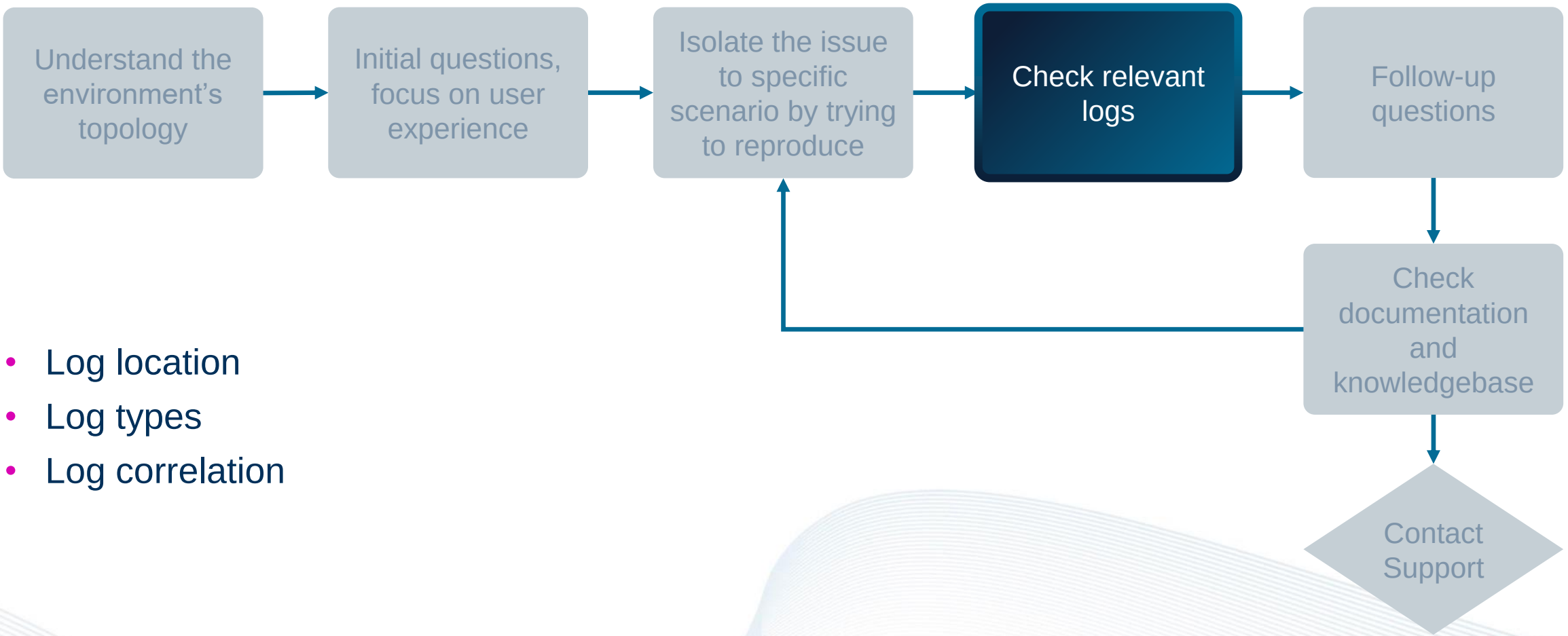
Reproducible

- Modify a variable and try to reproduce again.
- Repeat in different scenarios
- Write down each scenario and the outcome of the test
- Review the logs of reproduced scenarios (working and not working)

Not reproducible

- Review the logs relevant for the reported flow

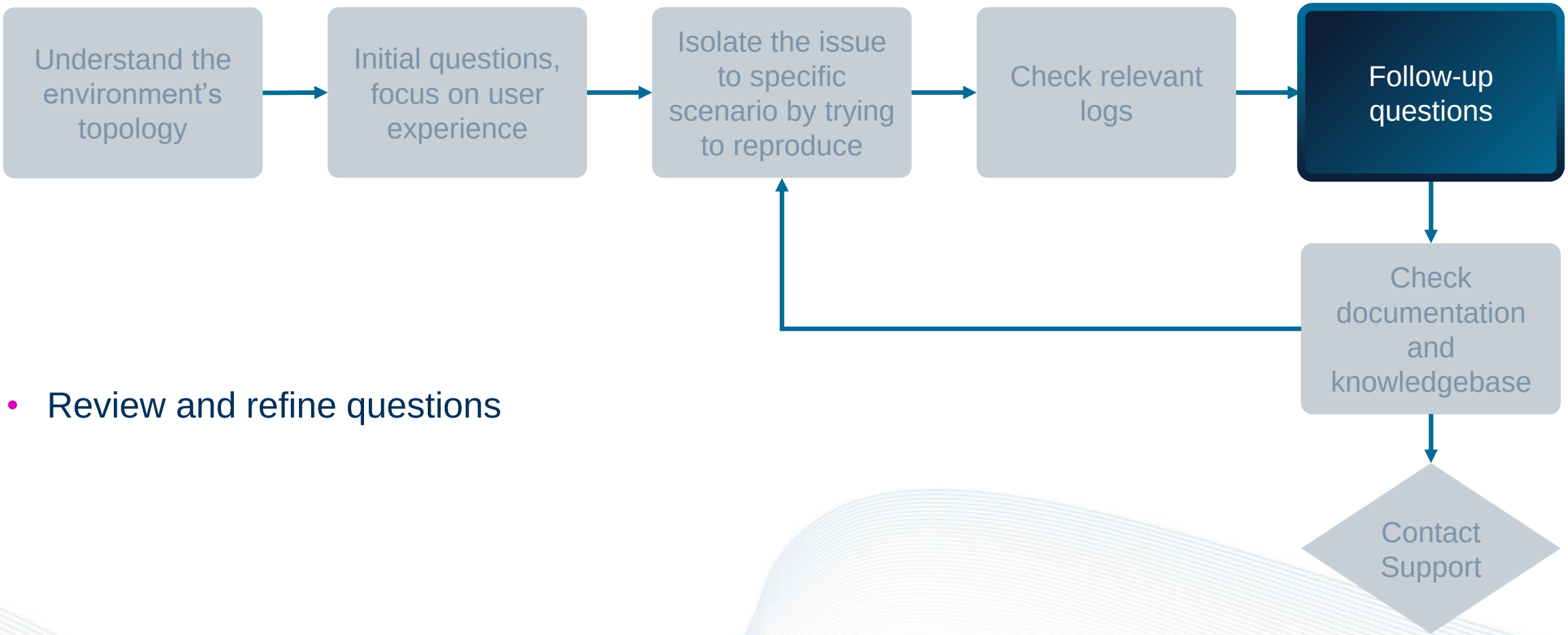
Checking the Logs



- Log location
- Log types
- Log correlation

CYBERARK®

Follow-Up Questions



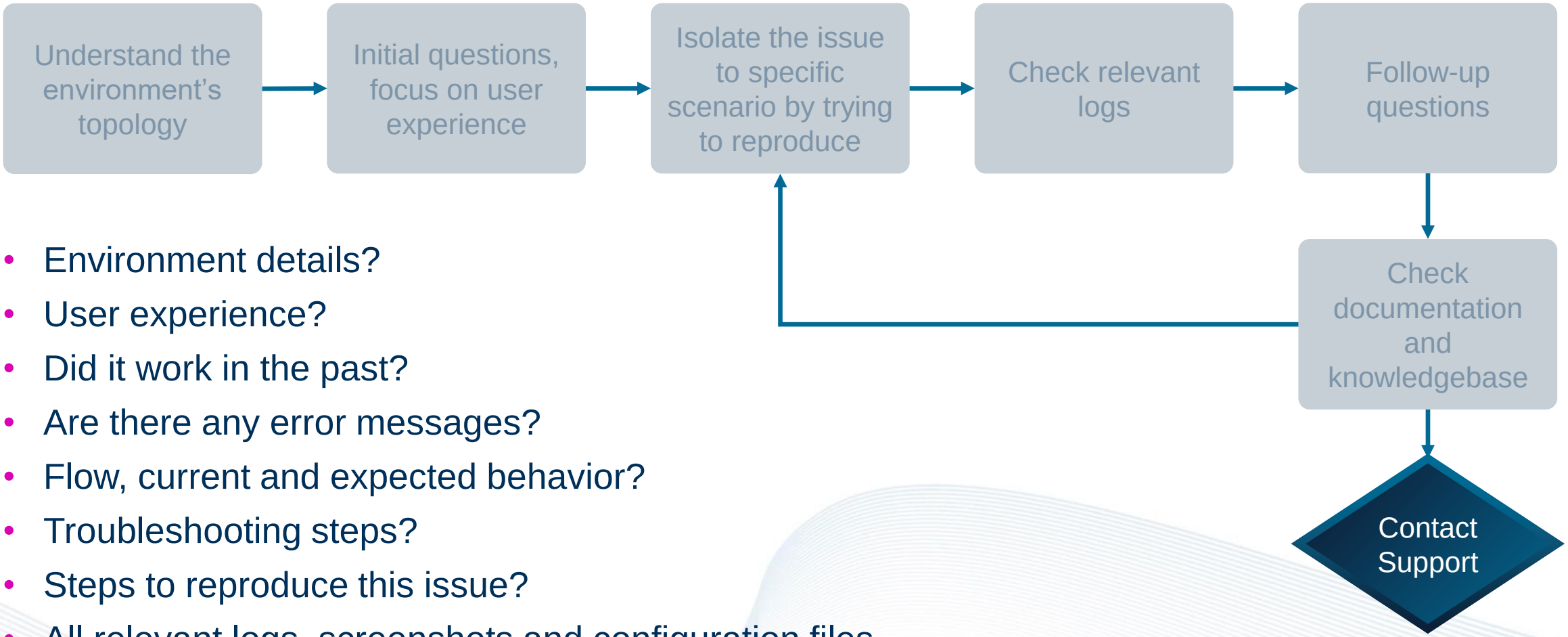
- Review and refine questions

Documentations and Knowledge Base

- Colleagues and end users
- Knowledge base
- Messages and Responses document; Installation and implementation documents
- Re-run scenarios

CYBERARK

Contacting CyberArk Support



- Environment details?
- User experience?
- Did it work in the past?
- Are there any error messages?
- Flow, current and expected behavior?
- Troubleshooting steps?
- Steps to reproduce this issue?
- All relevant logs, screenshots and configuration files

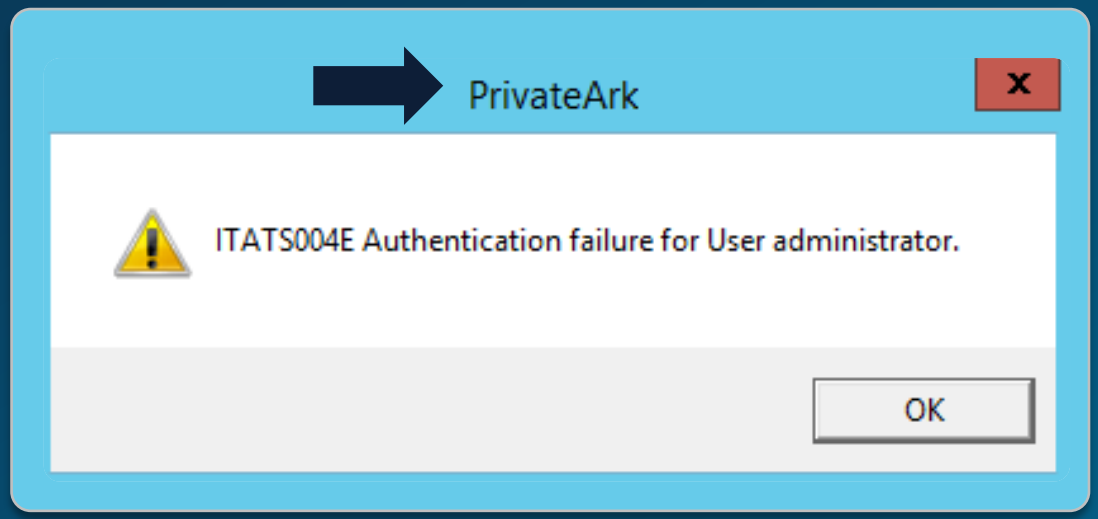
CYBERARK®

Troubleshooting Flow: Example

User Unable to Login

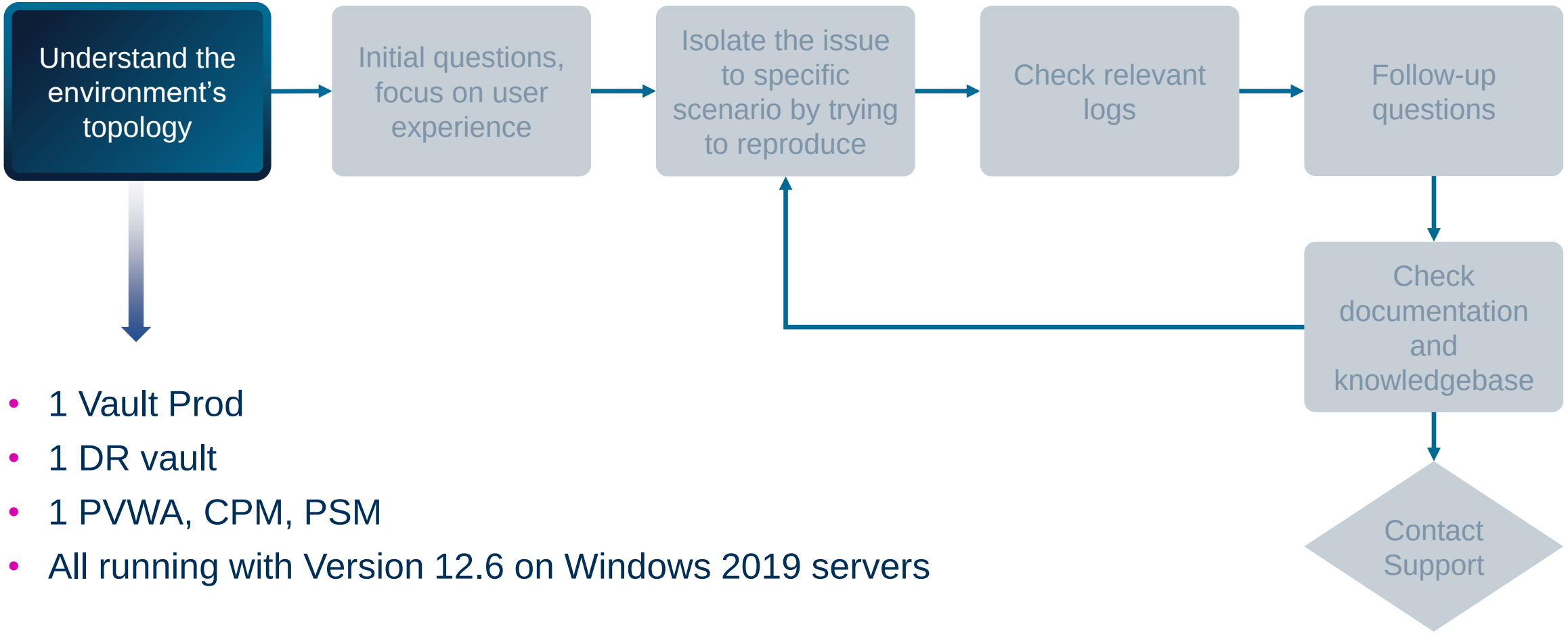
A user is unable to login to the PrivateArk client using the administrator user.

They see the following message.



User Unable to Login

Understand the Environment

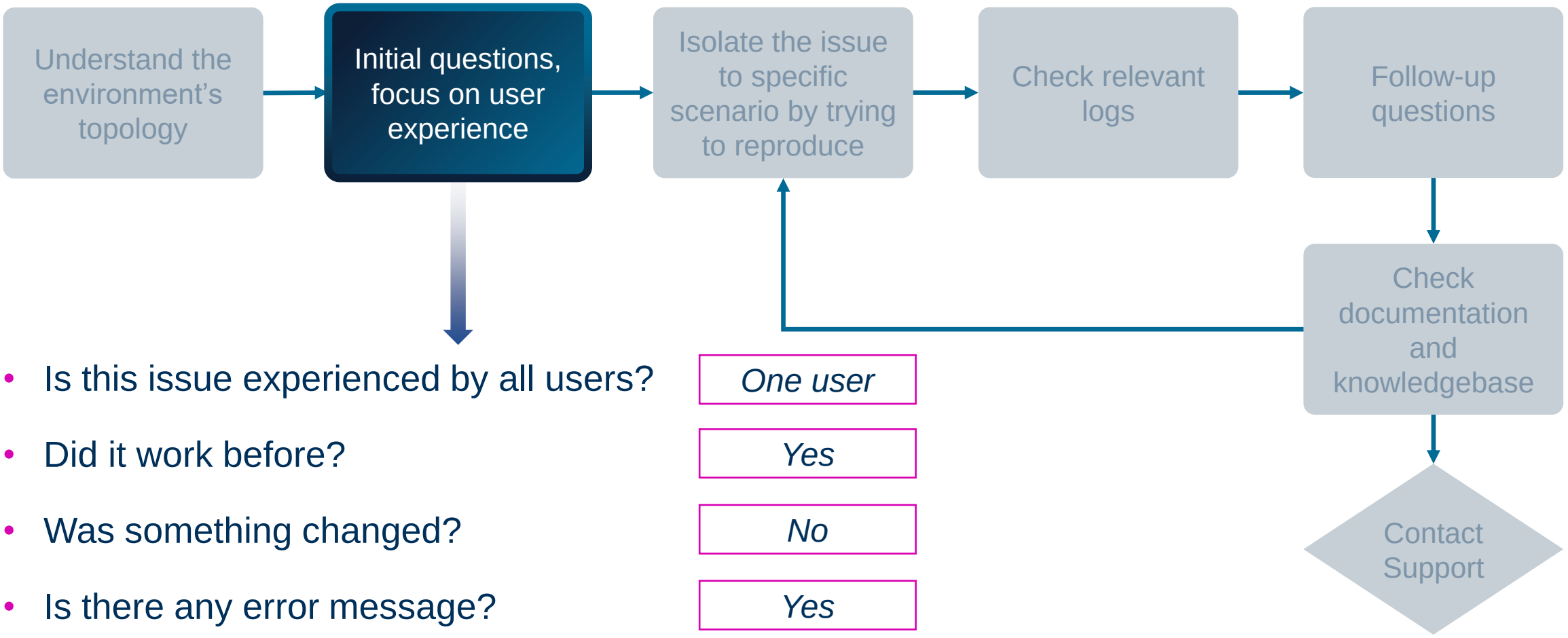


- 1 Vault Prod
- 1 DR vault
- 1 PVWA, CPM, PSM
- All running with Version 12.6 on Windows 2019 servers

CYBERARK®

User Unable to Login

Initial Questions

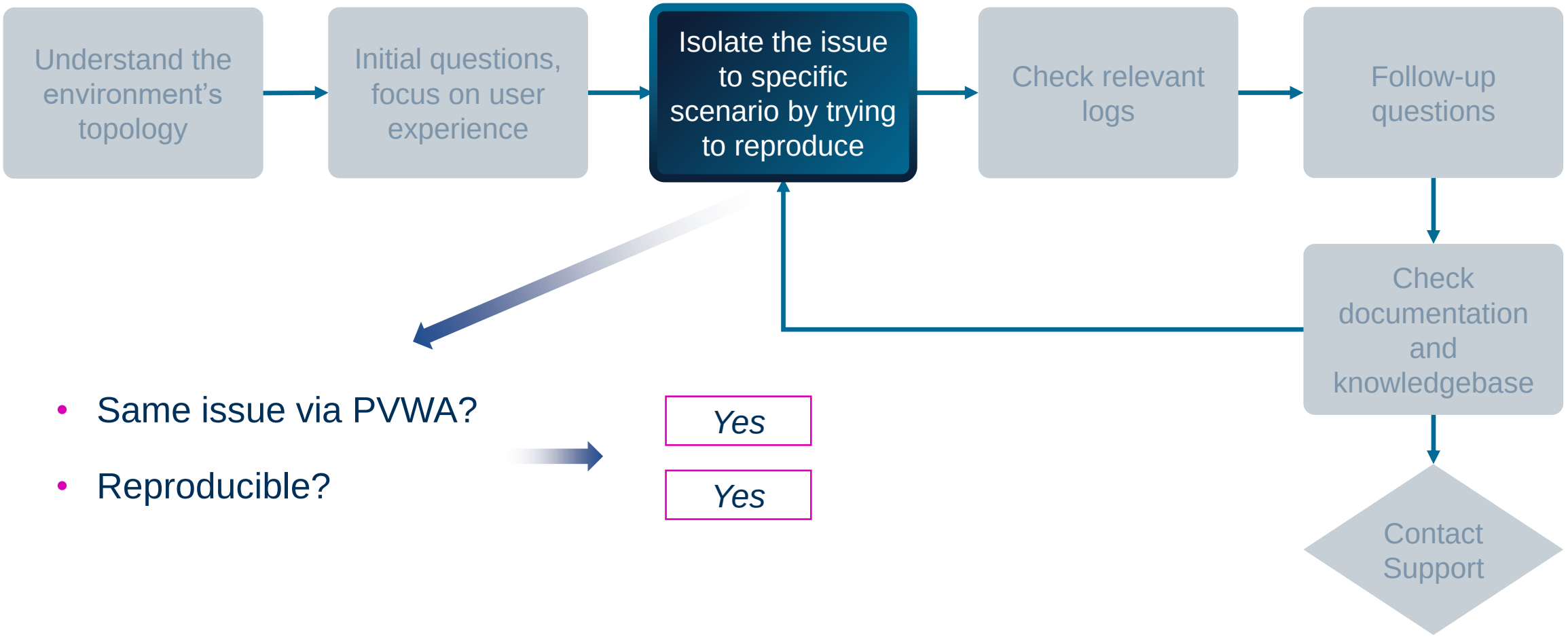


- Is this issue experienced by all users? *One user*
- Did it work before? *Yes*
- Was something changed? *No*
- Is there any error message? *Yes*

CYBERARK®

User Unable to Login

Isolation and Reproduction

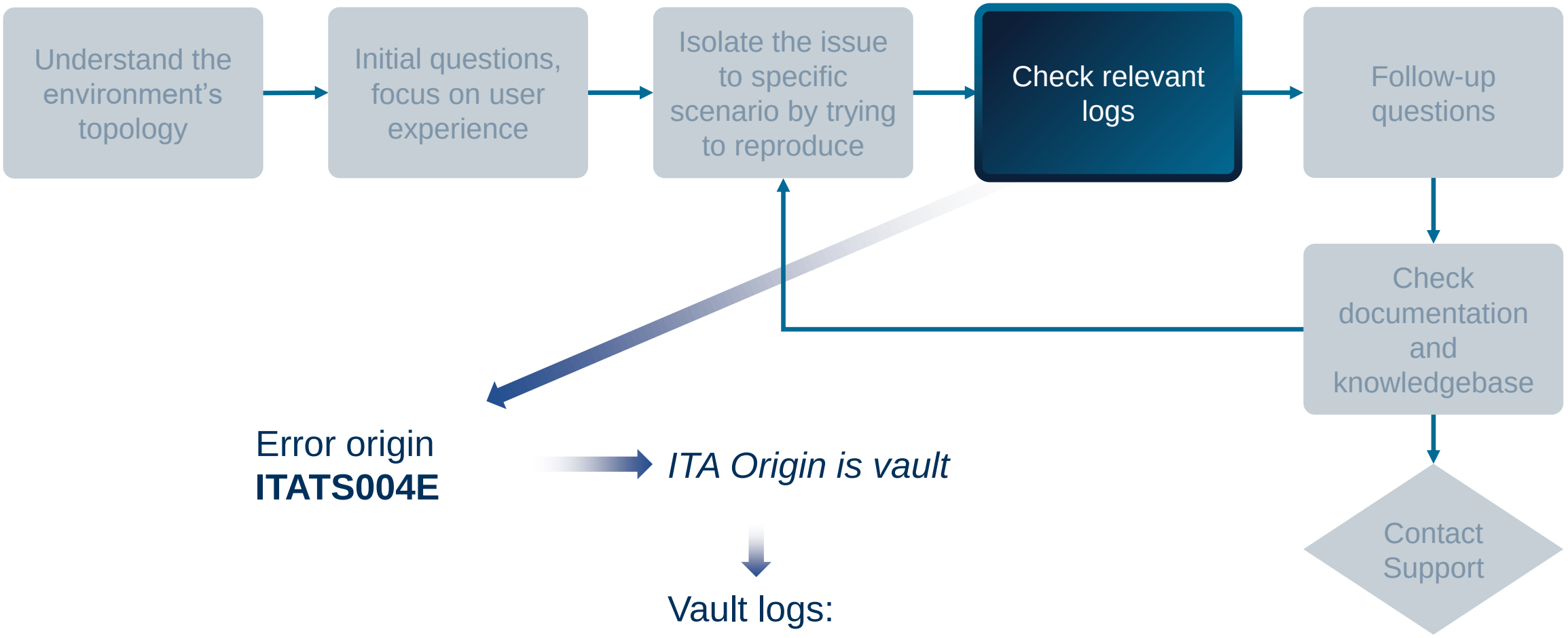


- Same issue via PVWA? → *Yes*
- Reproducible? → *Yes*

CYBERARK®

User Unable to Login

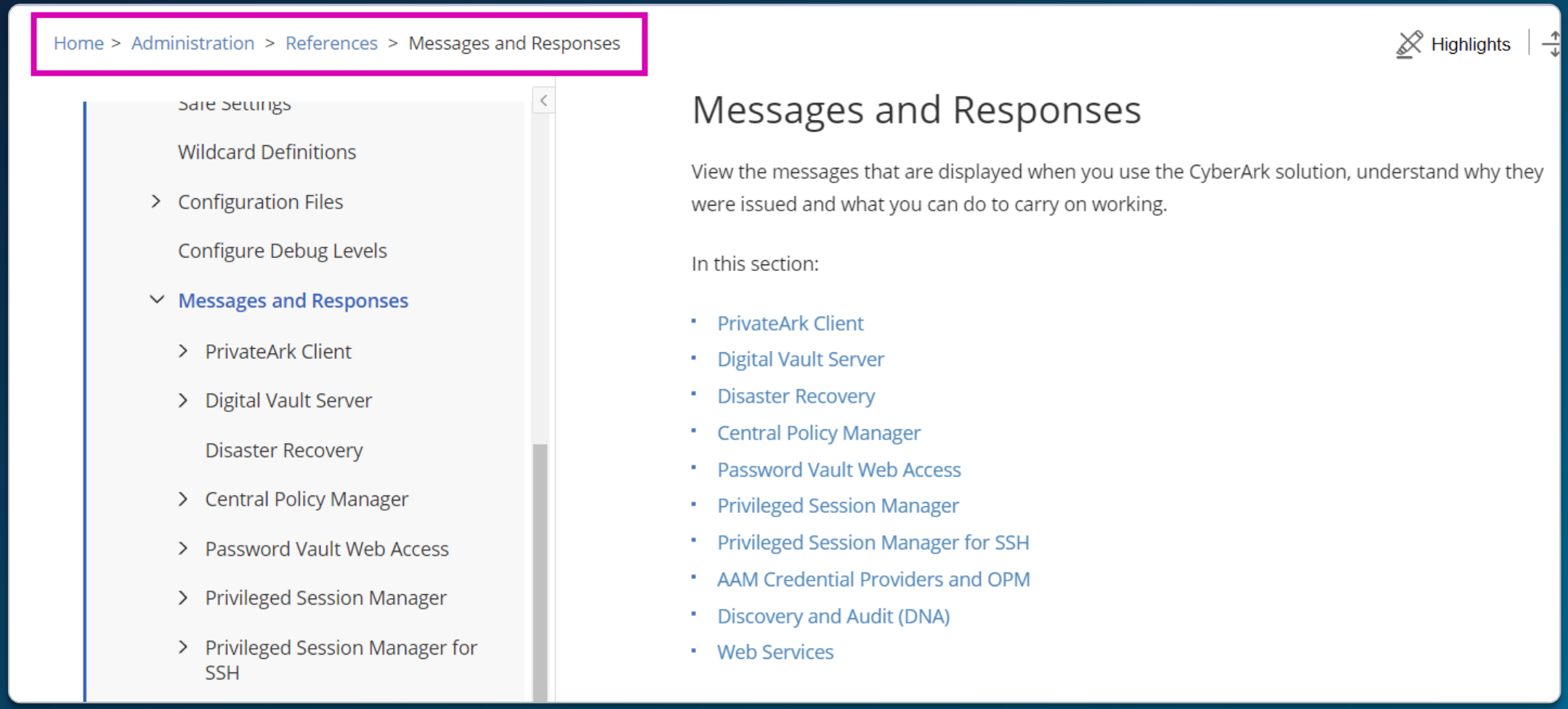
Checking the Logs



CYBERARK®

Check Messages and Responses

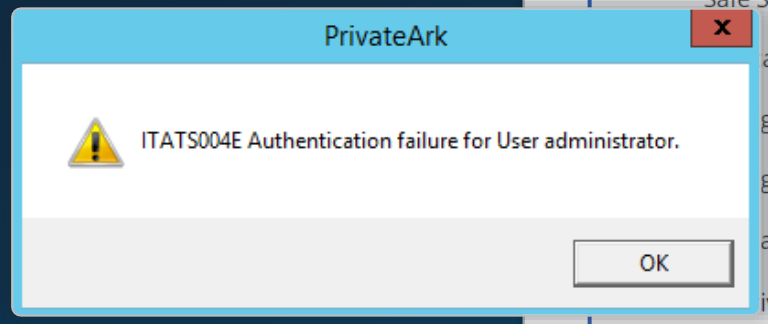
Try to identify the problem by searching in the **Messages and Responses** page in on the online documentation



CYBERARK®

Check Messages and Responses

Messages displayed to end users are intentionally generic, listing many possible causes.



Home > Administration > References > Messages and Responses > Digital Vault Server > Application

Highlights

- References
  - Configure the system through PVWA
  - Vault Specifications
  - Vault Audit Action Codes
  - Safe Settings
  - ard Definitions
  - guration Files
  - gure Debug Levels
  - ages and Responses
  - ivateArk Client
  - Digital Vault Server
    - Application
    - Global
    - Storage Manager

ITATS004E Authentication failure for User <username>

Recommended Action:

If an authentication failure occurs, the administrator can refer to the Vault log (either the Console log or the ITAlog) for a detailed error description.

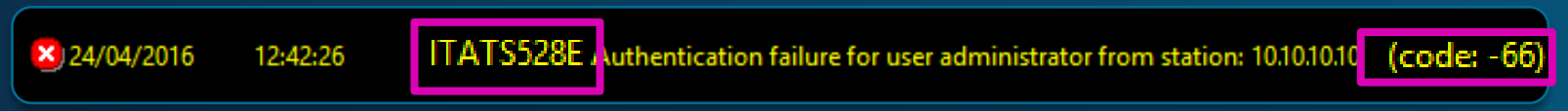
Possible Cause	Recommended Action
The user name and/or password are incorrect.	Make sure the correct user credentials were used or that the administrator can reset the user's password.
The user is not allowed to access the station.	To grant access to the station, include the station IP address in the accessible network area list.
The PKI certificate is wrong, invalid, expired or revoked.	Make sure the user has a valid and correct PKI certificate.
The user attempted to logon with an authentication method not defined for the user, including: PKI CyberArk Authentication RADIUS LDAP Provider	Ensure that the user is using the correct authentication method, or modify his details to match the authentication method he is using.
An error was returned while querying the LDAP for user object information.	Make sure the LDAP server is operating and communicating normally. Make sure LDAP parameters, including BindUserName and BindPassword, are set correctly.

CYBERARK®

Check Messages and Responses

Because the error message starts with ITA, we know that the Vault server originated this error.

- At this point we will go to the Vault server and inspect the ITA log.
- There may be multiple log entries for the same problem.
- Try to find the first entry related to this problem
- When looking at the ITA log, we see an error message **ITATS528E** with a code of **66**
- When we search for that error, we see the exact cause of the problem and the solution.



ITATS528E **Authentication failure for User <username> from station <station> (Code: <code>).**

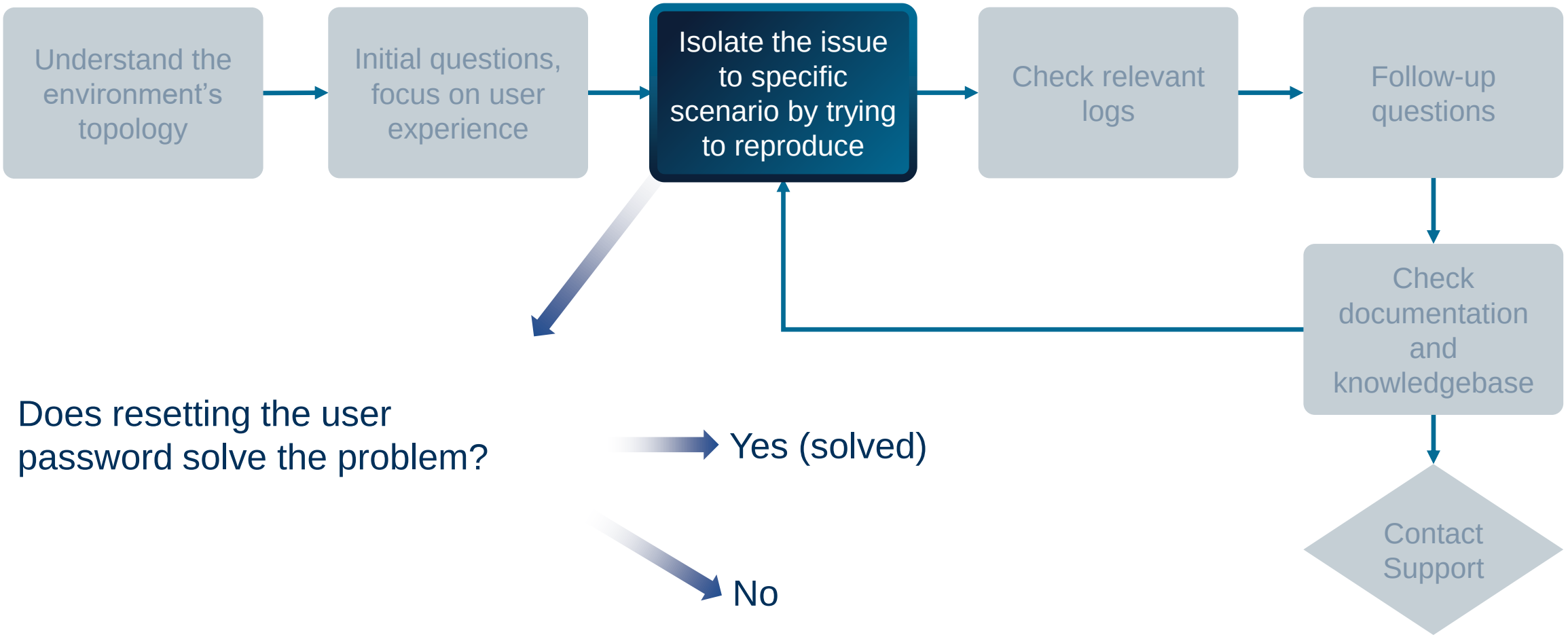
Recommended Action:

This authentication failure could be due to one of several reasons, depending on the code that is displayed:

- Code 66 – The specified password is incorrect. Specify the correct password or change it using the Change Password option.
- Code 76 – The server tried to send data to the client, but failed.
- Code 77 – The server requires specific data from the client, but did not receive it.
- Code 84 – The NT Authentication ticket that was used to authenticate has expired. Verify that the times set on the Vault and the NT Authentication Agent machines are synchronized.
- Code108 – LDAP connection failed due to either the wrong user or password. Specify the correct credentials, then try to authenticate again.
- Code 109 – The user's DN LDAP directory does not exist in the Vault. Verify that the directory is configured in the Vault server and has authentication usage.
- Code 110 – The user was not found in the LDAP directory. Verify that the user exists in the directory under the directory base context that was configured in the directory configuration file.

CYBERARK®

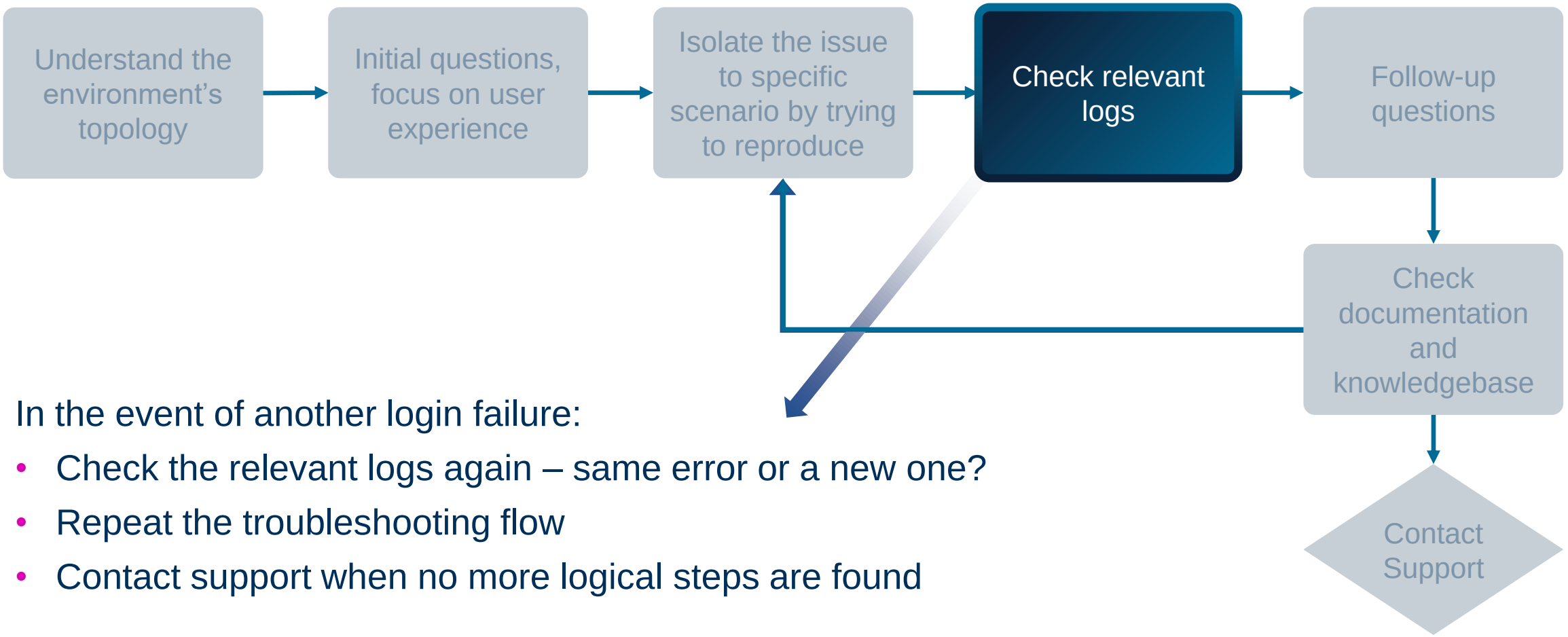
User Unable to Login
Solution



CYBERARK®

User Unable to Login

Problem Not Resolved



In the event of another login failure:

- Check the relevant logs again – same error or a new one?
- Repeat the troubleshooting flow
- Contact support when no more logical steps are found

CYBERARK®

Logs

In this section we will discuss the logs generated by the various system components, how to set the debug mode, and the logs location

Overview

CYBERARK®

Types of Logs

Log files are divided into several types:

Console Log

Provides component-level entries such as service up or down

Error Log

Exists in some components, and will include only error entries

Trace Log

Provides detailed entries of workflows related to that component

Debug Log

Those logs may come in different types, sometimes they will be the trace files, with additional information and sometimes they will come at a form of separate files depending on the component.

For the full list of log locations, please see the implementation guide

Understanding CyberArk Logs

The log message code is built from four segments

for example:

ITA FW 001 I

Firewall is open for client communication

ITA – The source component of the message is the **Vault** server

FW – The module with the message is the **Vault** FW

001 – Message number

I – The message category

Log messages are separated into four major categories:

Informational:
ITAFW001I *Firewall is open for client communication*

Warning:
ITATS319W *Firewall contains external rules*

Error:
ITATS691E *LDAP synchronization error*

System:
ITADB367S *Server unable to communicate with firewall*

See **CyberArk Messages and Responses** for additional information

CYBERARK®

Reviewing the Logs

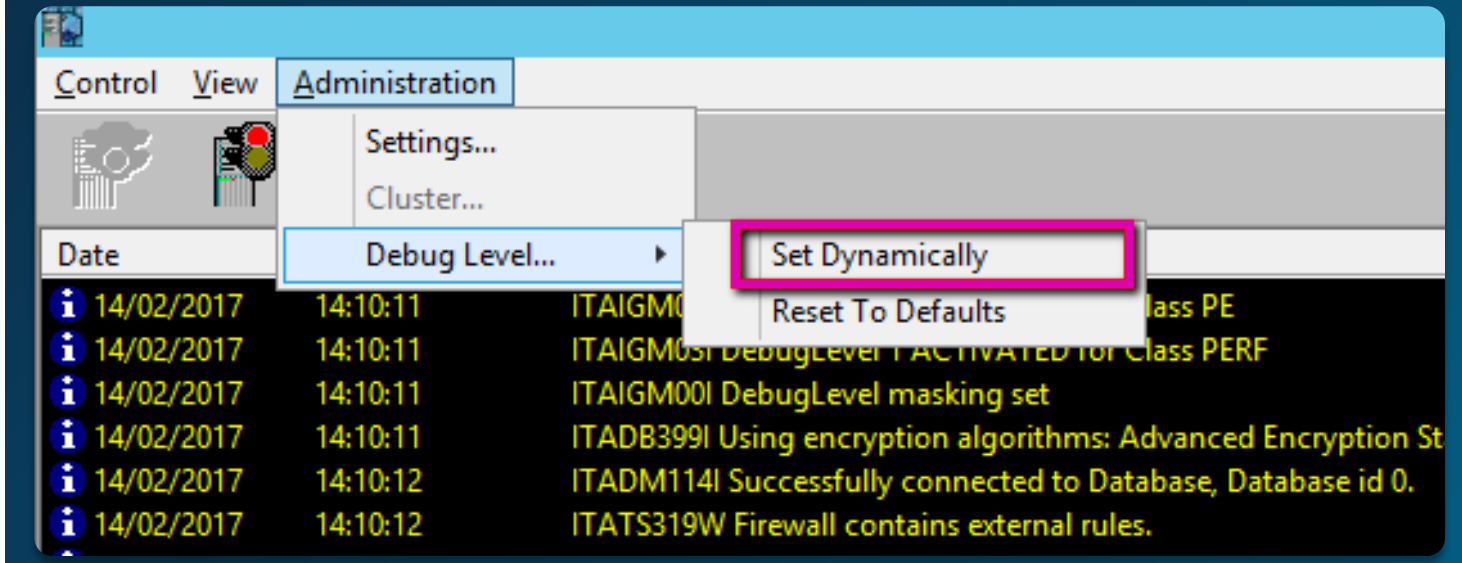
Once we get to a point where we need to go over log files, there are a number of questions to ask:

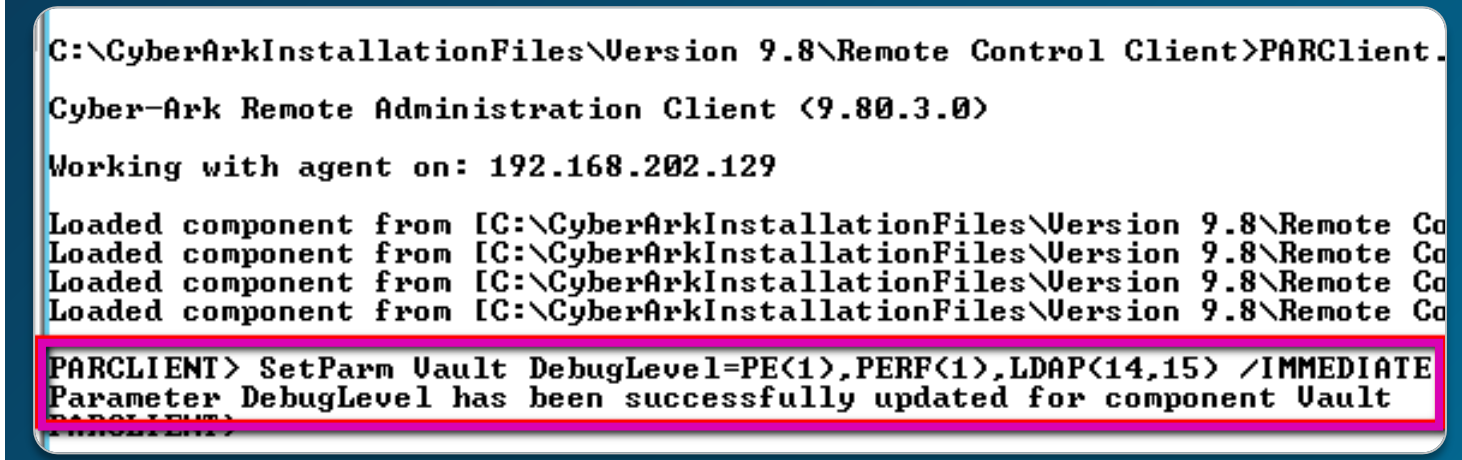
- Which log file do we need to review?
- What do we search for?
  - Keywords (Error, Failed, Failure…)
  - Timestamps
  - User name
  - Object name (Account name, safe name)
- Are there correlated entries in other logs?
  - Log events and time of the issue
  - Different components
  - CyberArk logs and OS logs

Debug Mode and Log Location

Set the Debug Mode for the Vault ITAlog

- The Vault debug levels can be changed in the ***dbparmi.ini*** file (requires a restart)
- The Vault debug levels can be changed without a restart using the **PARclient** or **Central Administration Station**

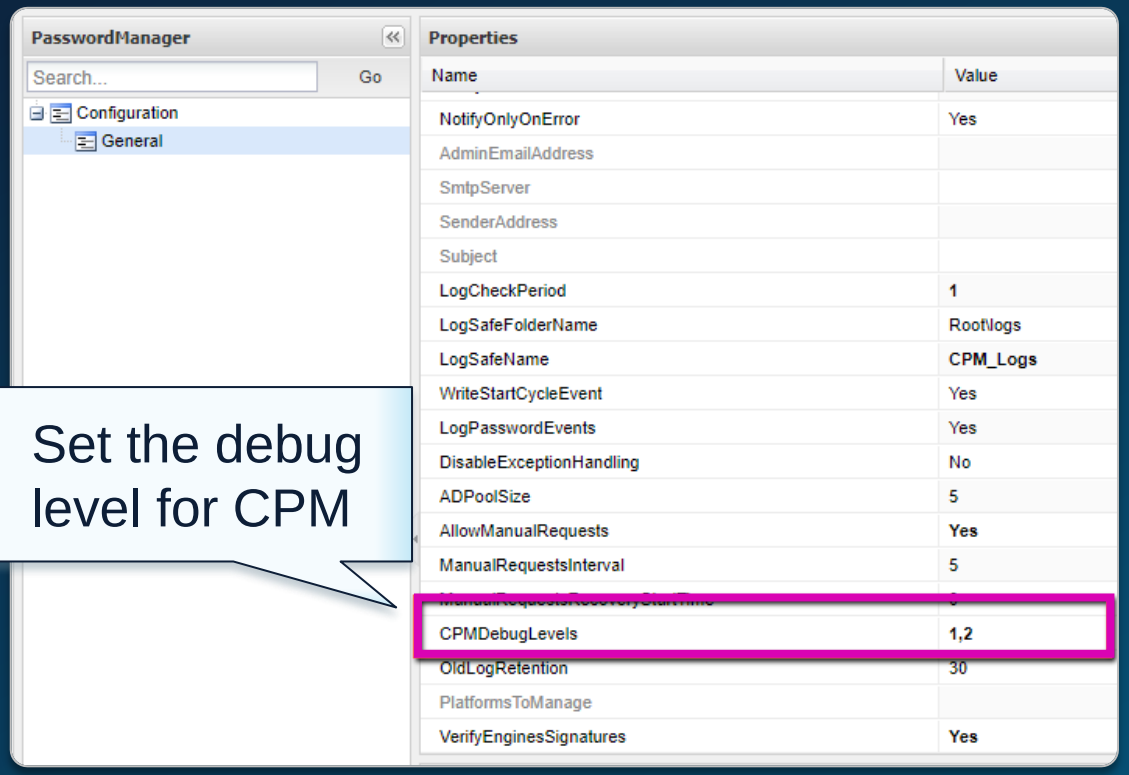


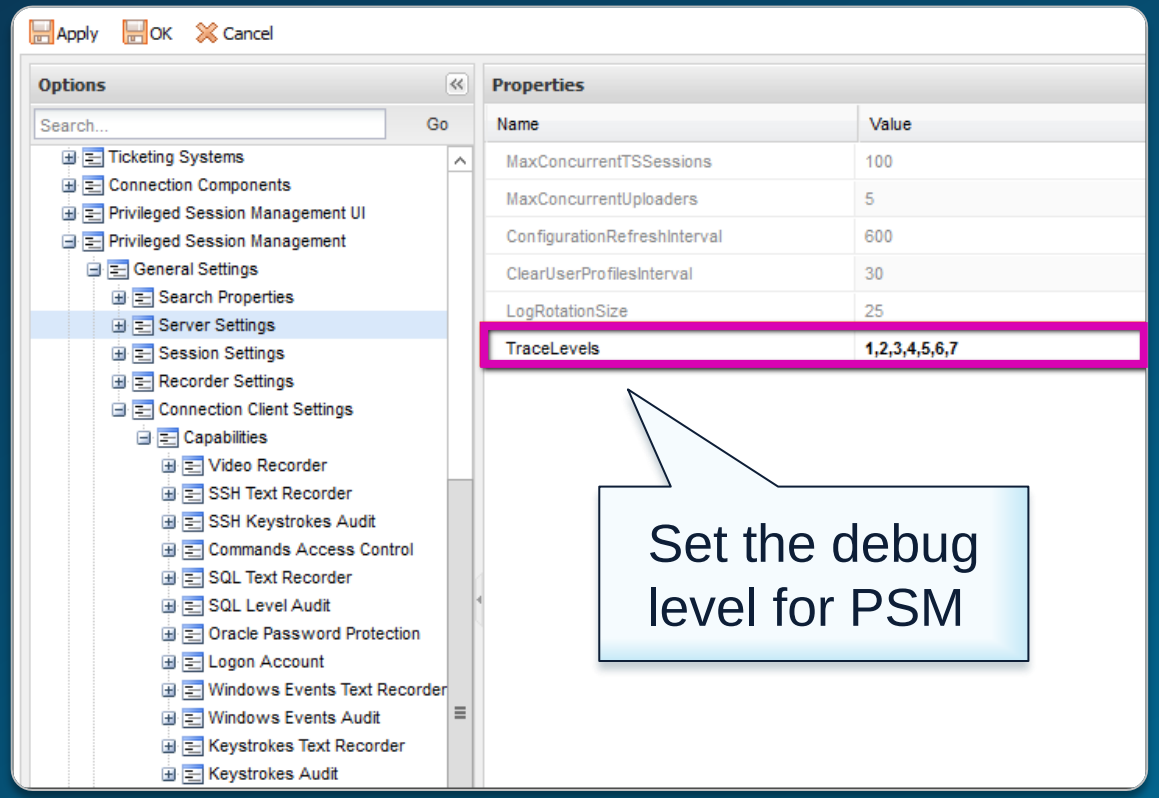


CYBERARK

Set the Debug Mode for the Components

Debug mode for components can be set in the configuration files stored on the **Vault** or via the **PVWA** Web UI

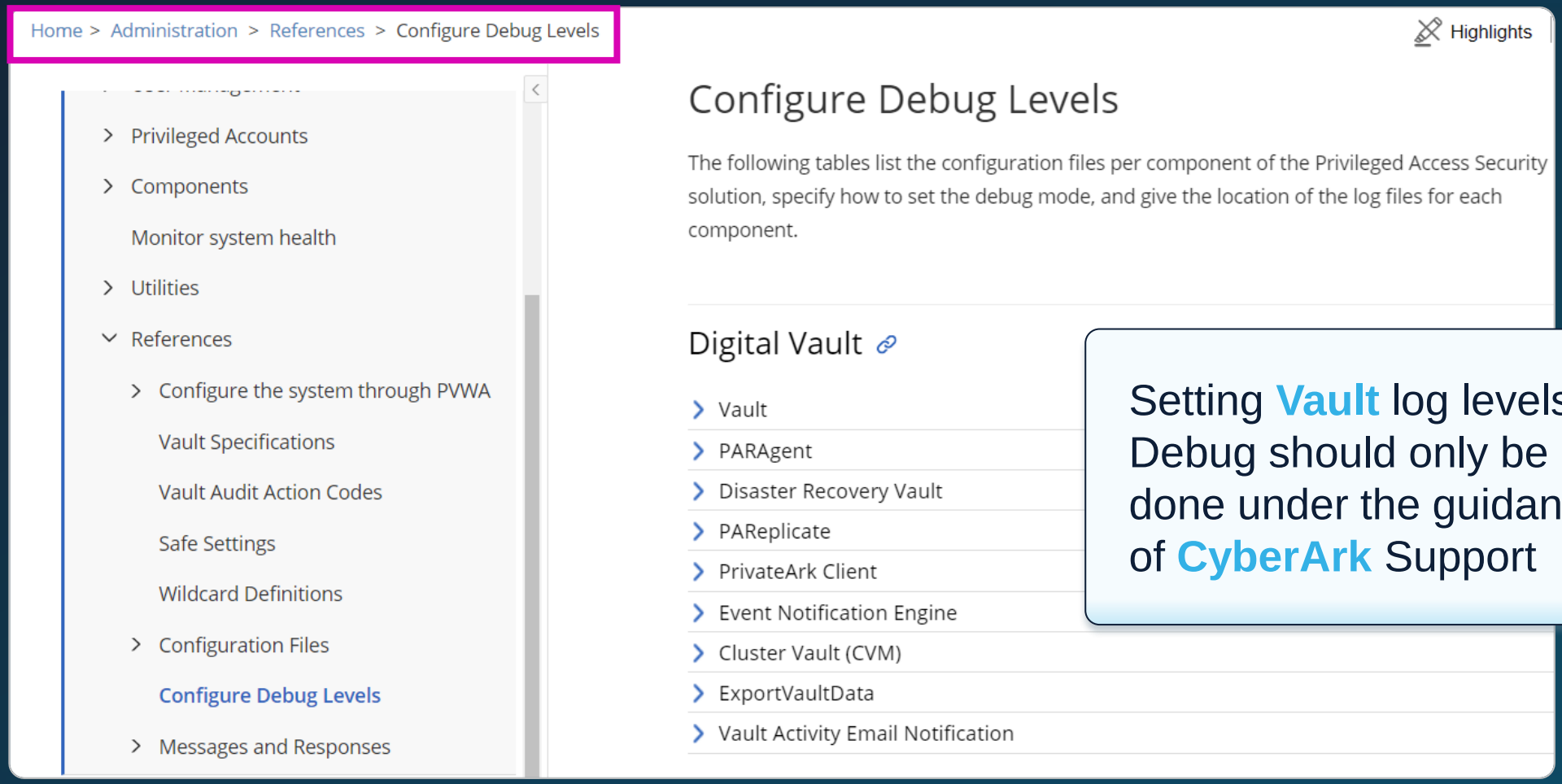




CYBERARK®

Log Locations and Configuring the Debug Levels

Detailed information about setting debug level for different components and location of the log files can be found in the online documentation



Setting **Vault** log levels to Debug should only be done under the guidance of **CyberArk** Support

CYBERARK®

Cheat Sheet – Vault and Related Components

Vault	Changes Require a Vault Restart
Configuration File	DBParm.ini
	…\Database\my.ini. - Database Configuration File
Debug	DebugLevel=PE(1),PERF(1) - Detailed Vault services debug
	LDAP(14,15) - Detailed LDAP debug
Logs	Italog.log
	Trace.dX (X is a number from 0 to 4)
	…\Database\VaultDB.log - Database log

Disaster Recovery	
Configuration File	PADR.ini
Debug	EnableTrace=yes
Logs	PADR.log

Ene	Event Notification Engine
Configuration File	\Program Files\PrivateArk\Server\Event Notification Engine\ENEConf.ini
	Vault ➔Safe:"Notification Engine"➔root\EventNotificationEngine.ini
Debug	EventNotificationEngine.ini
	[Debug] • ControllerDebugLevel=1,2,3,4 • CollectorDebugLevel=1,2 • ParserDebugLevel=1,2 • SMTPSenderDebugLevel=1,2 • ConfigurationManagerDebugLevel=1,2
Logs	ProgramFiles\PrivateArk\Server\EventNotification Engine\Logs\ENEConsole.log
	ProgramFiles\PrivateArk\Server\EventNotification Engine\Logs\ENETrace.log

Logic Container	
File Name	LogicContainer.Log
Logs	C:\ProgramFiles (x86)\PrivateArk\Server\LogicContainer\LogicContainer.log

PAReplicate	Backup and Restore
Debug	In the PAReplicate.exe command executed, add the following flag: /EnableTrace
Logs	PAReplicate.log

Client	Run –PAInfo.exe
Debug	In the Client:
	Tools ➔ Options ➔ Advanced ➔ Log Configuration
Logs (Win XP and Win 2003	\Documents and Settings\<user>\Application Data\CyberArk\PrivateArk\PALog.txt
Logs (Win7 and Win 2008	\Users\<user>\AppData\Roaming\CyberArk\PrivateArk

CLICK "NEXT" TO CONTINUE

CYBERARK®

Cheat Sheet – Components

CPM	Central Password Manager
Configuration File	Vault ➔ Safe “Password Manager”➔ root\policies\<policy>.ini
Debug	PVWA ➔ Administration Tab ➔ CPM settings
	CPMDebugLevels=2 (default) 0 – No messages will be written to the trace log. 1 – CPM exceptions will be written to the trace log (Default Level) 2 – CPM trace messages will be written to the trace log. 3 – CPM CASOS activities will be written to the trace log. 4 – CPM CASOS debug activities will be written to the trace log. 5 – CPM CASOS errors will be written to the trace log. 6 – All CPM CASOS activities and errors will be written to the trace log.
Logs – CPM	\Program Files\CyberArk\PasswordManager\Logs\pm.log \Program Files\CyberArk\PasswordManager\Logs\pm-error.log\Program Files\CyberArk\PasswordManager\Logs\PMConsole.log\Program Files\CyberArk\PasswordManager\Logs\PMTrace.log
Logs –Plug-ins	\Program Files\CyberArk\passwordManager\Logs\ThirdParty*.log

PSM	Privileged Session Manager
Configuration File	\Program Files\CyberArk\PSM\Basic_psm.ini
	PVWA ➔ Administration Tab ➔ Options ➔ Privileged Session Management
Debug	PVWA ➔ System tab ➔ Options ➔ Privileged Session Management ➔ General Settings
	Server Settings ➔ TraceLevels=1,2,3,4,5,6,7 Recorder settings ➔ TraceLevels=1,2 Connection Client Settings ➔ TraceLevels=1,2
Logs	<installation folder>\Logs (and subfolders) or according to parameter “LogsFolder” (located in Basic_psm.ini file)

PVWA	Password Vault Web Access
Configuration File	\wwwroot\PasswordVault\web.config
	Vault ➔ Safe “PVWAConfig” ➔ root\PVConfiguration.xml
	Vault ➔ Safe “PVWAConfig” ➔ root\Policies.xml
Debug	PVWA ➔ Administration Tab ➔Options ➔ Logging
	DebugLevel=High (options are None/High/Low/Profiling)
	InformationLevel=High (options are None/High/Low/Profiling)
Logs	%windir%\temp\
	CyberArk.Webapplication.log
	CyberArk.WebConsole.log
	CyberArk.WebSession.<Sessionid>.log

CLICK “NEXT” TO CONTINUE

CYBERARK®

xRay Agent

In this section we will discuss the **CyberArk xRay** utility, which can be used to collect log and configuration files from the **CyberArk** components and share them with **CyberArk** or partner support

Overview

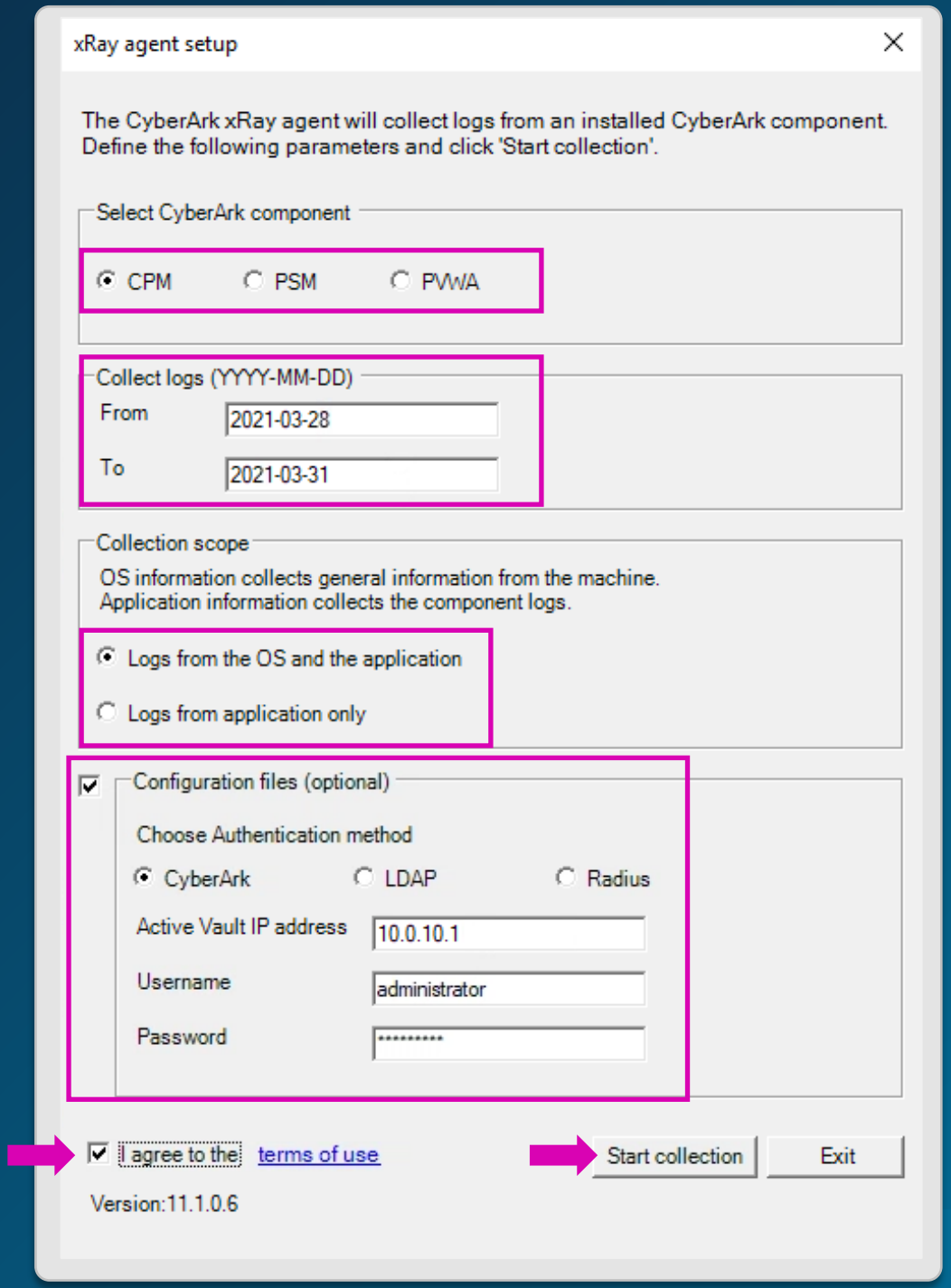
CyberArk xRay collects logs and configuration files from **PAM** components in a simple, single-step process

- The utility can be run from a remote machine or on any of the **CyberArk** servers
- All data files are encrypted during collection, regardless of whether they are collected locally or remotely, and then transferred back to the **xRay** machine
- You can share the collected data with your partner or **CyberArk**, knowing that it is safely encrypted during transfer
- When sharing with **CyberArk**, shared data is linked to a case to allow Enterprise Support easy and secure access to the collected data

The utility can be downloaded from the **CyberArk Marketplace**

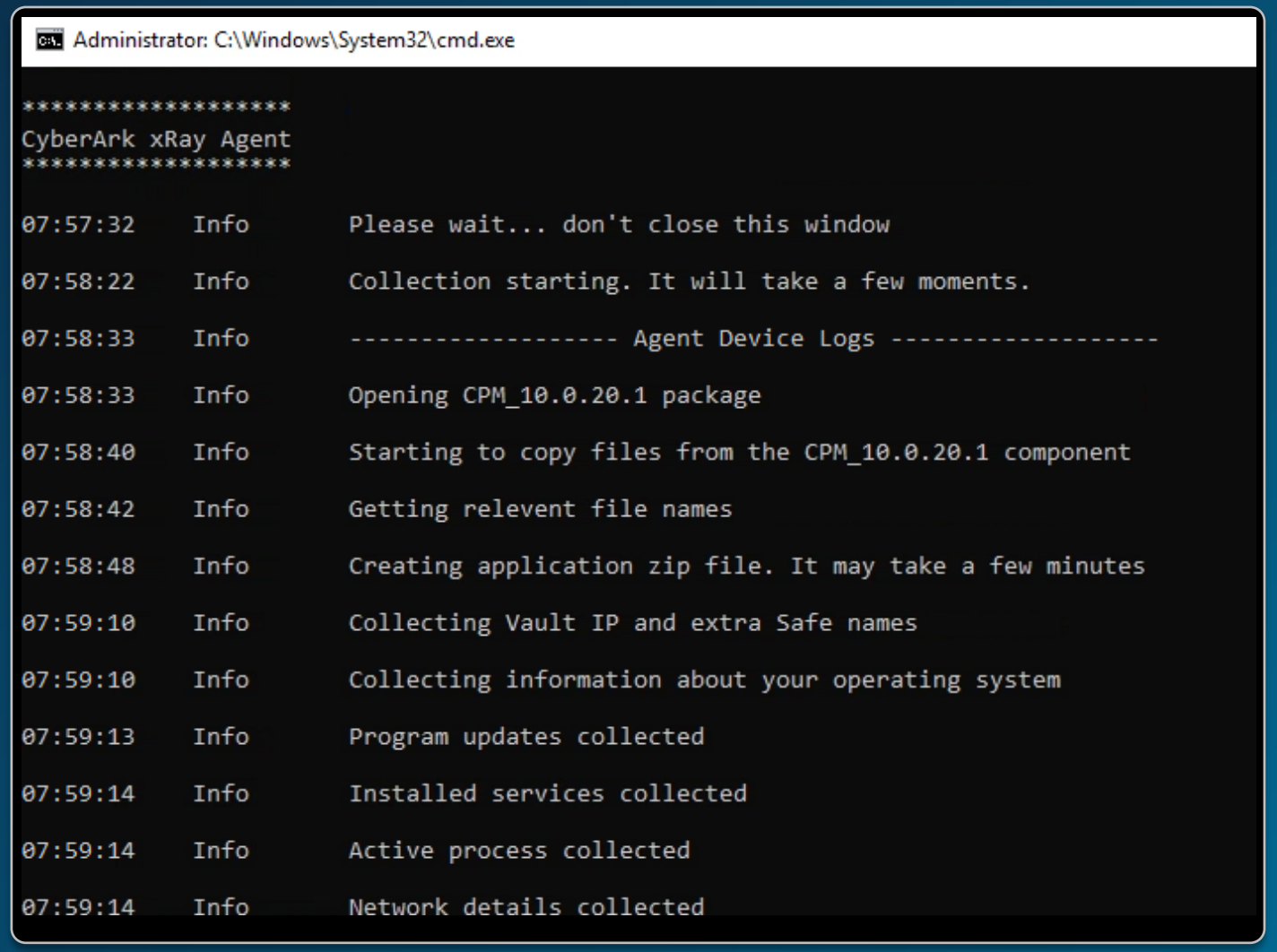
Agent Setup

- Select the component
- Select time frame for the collection and collection level.
- Select Collection scope
  - Logs from OS and the application
  - Logs from application only
- Optionally, enable and provide the Active Vault IP address and Administrative user credentials for configuration files collection
- Agree to the Terms of Use and click *Start Collection*



Monitor Collection Process

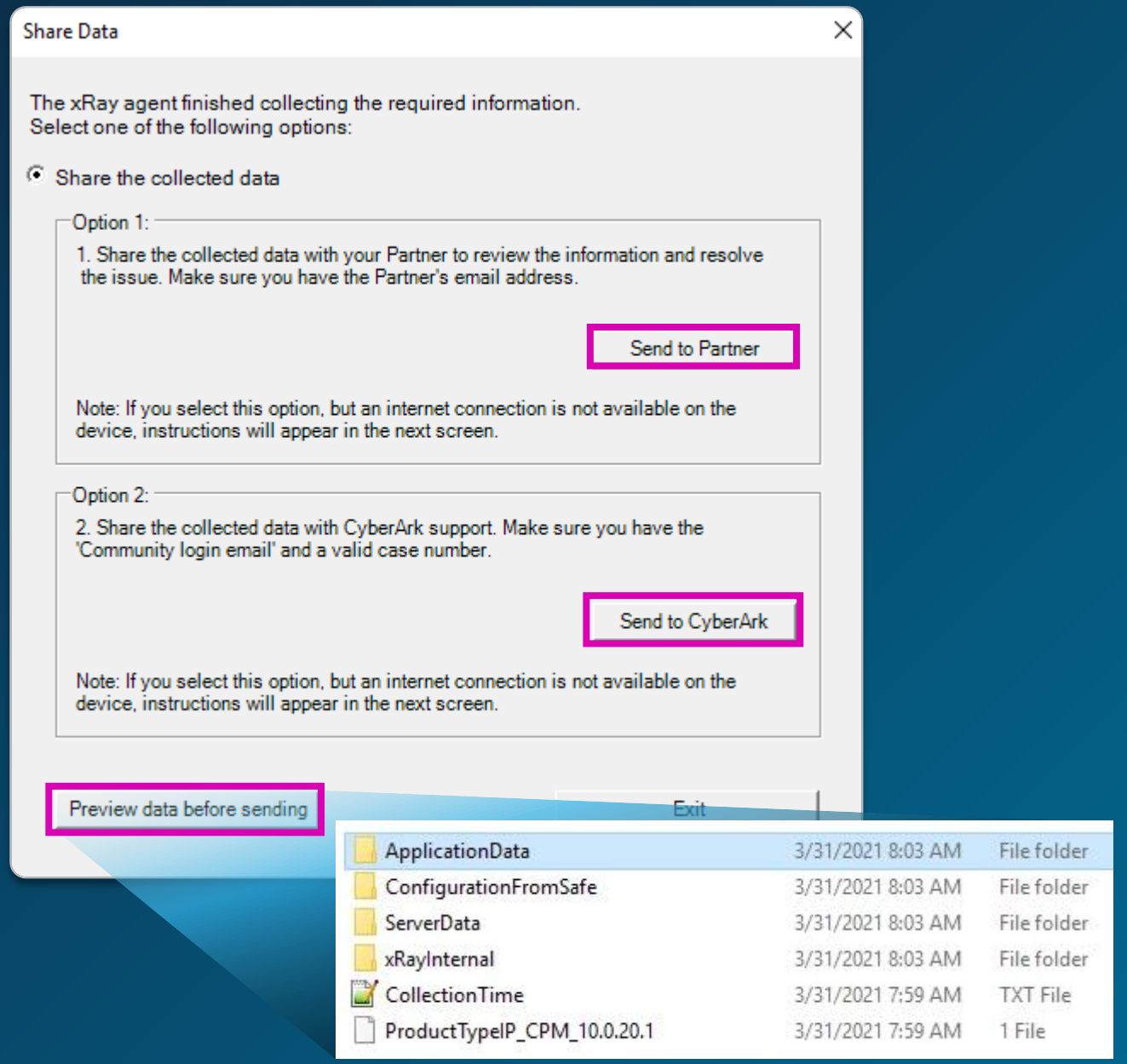
You can monitor the collection process as it collects the component files



CYBERARK®

Share the Collected Data

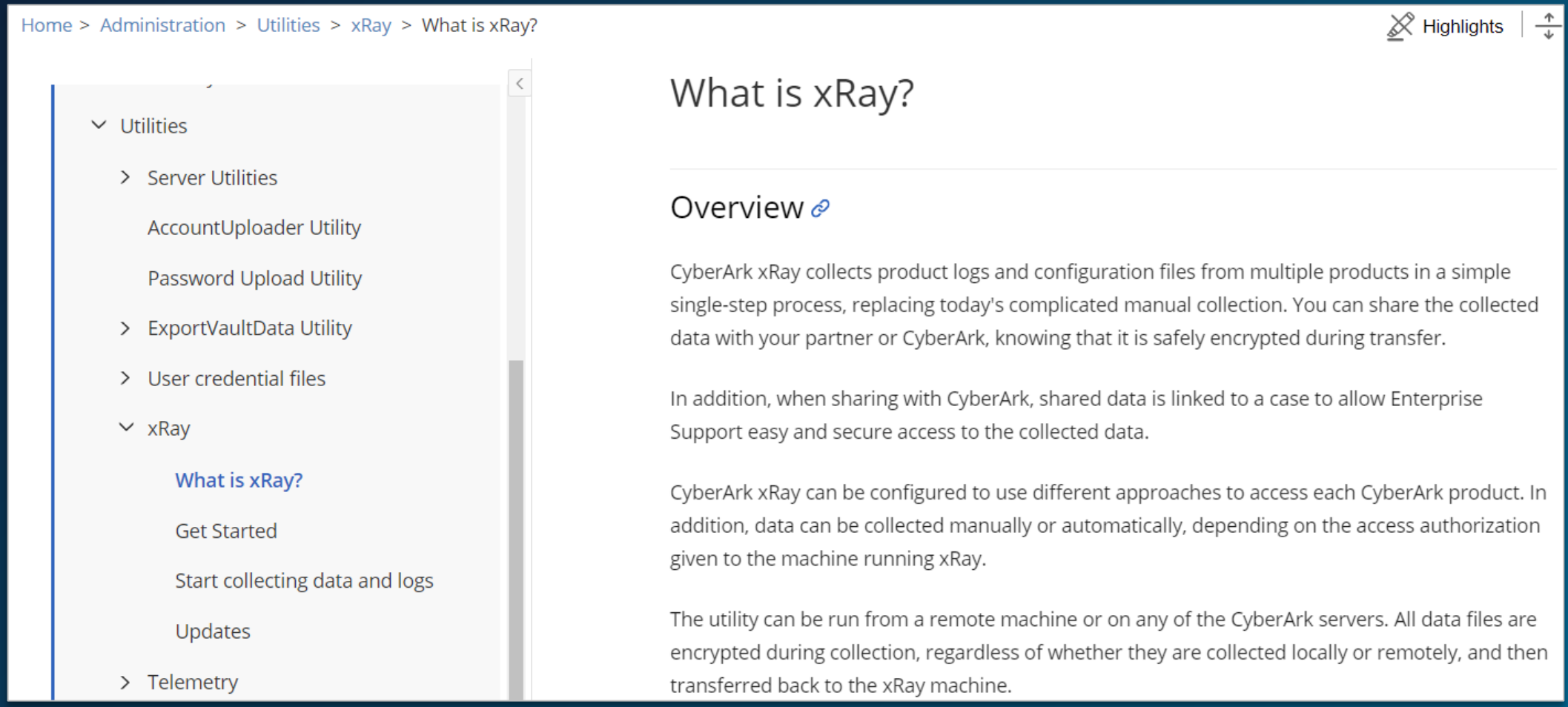
- Once the process is complete, you can select whether to:
  - Share the collected data with your Partner
  - Share the collected data with CyberArk
- You can also preview the data before sending
- When sharing information with CyberArk, make sure you have:
  - A Technical Community account
  - Case number



CYBERARK®

Documentation

Additional information can be found in the [CyberArk documentation]



CYBERARK

Summary

Summary

In this session we covered:

- The basic flow for troubleshooting issues in the CyberArk environment
- How locate and manage the log files generated by the Vault and various components
- How to configure and use the xRay agent

Additional Resources

Utilities

xRay (login required)

Community Resources

CyberArk Customer Community (login required)

CyberArk Subreddit

Note: The CyberArk subreddit is not hosted or moderated by CyberArk.

Online Training

Working with CyberArk Support

CYBERARK®