



PAM Administration

Troubleshooting



Agenda

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

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



Troubleshooting Flow



Overview

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

- ▶ Your system implementation
- ▶ How components communicate with each other in your environment
- ▶ 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

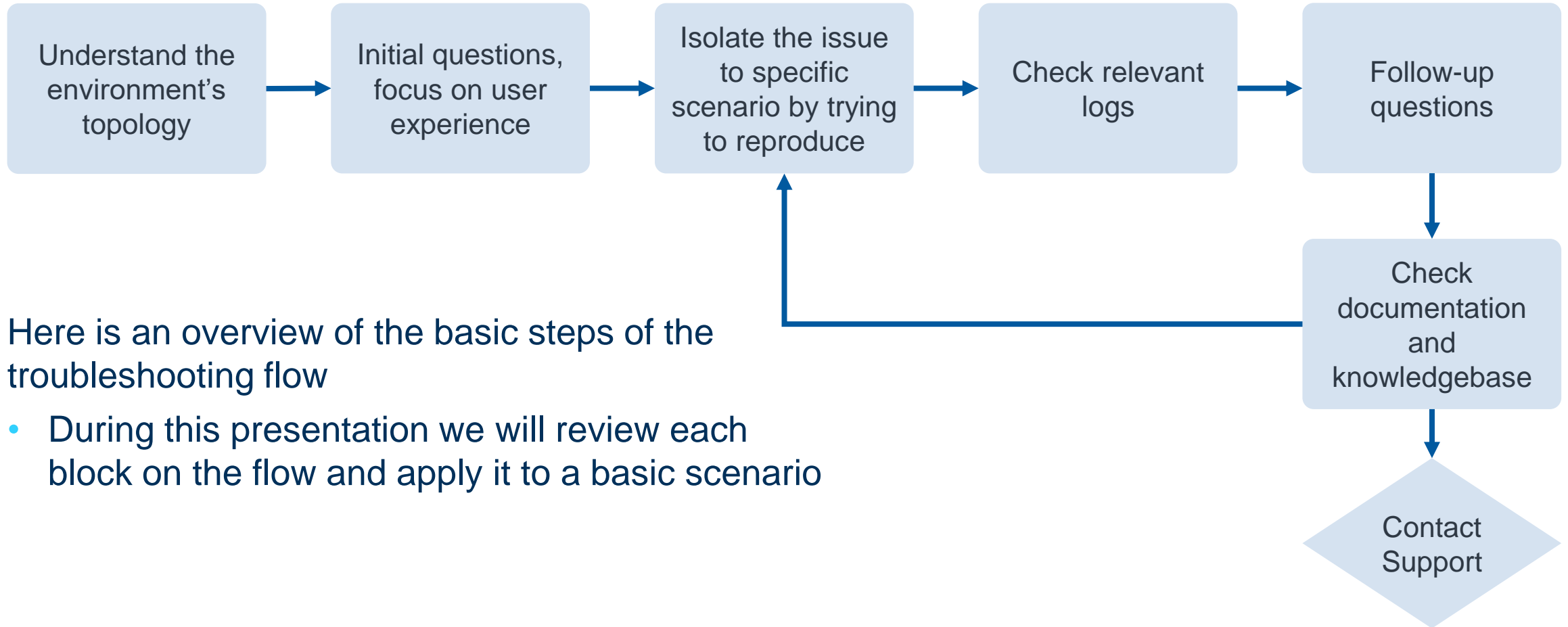
- ▶ Knowledge of the environment layout
- ▶ Access to the different servers
- ▶ Access to **CyberArk** Knowledgebase (Customer Community)
- ▶ Access to **CyberArk** documentation (publicly available online)



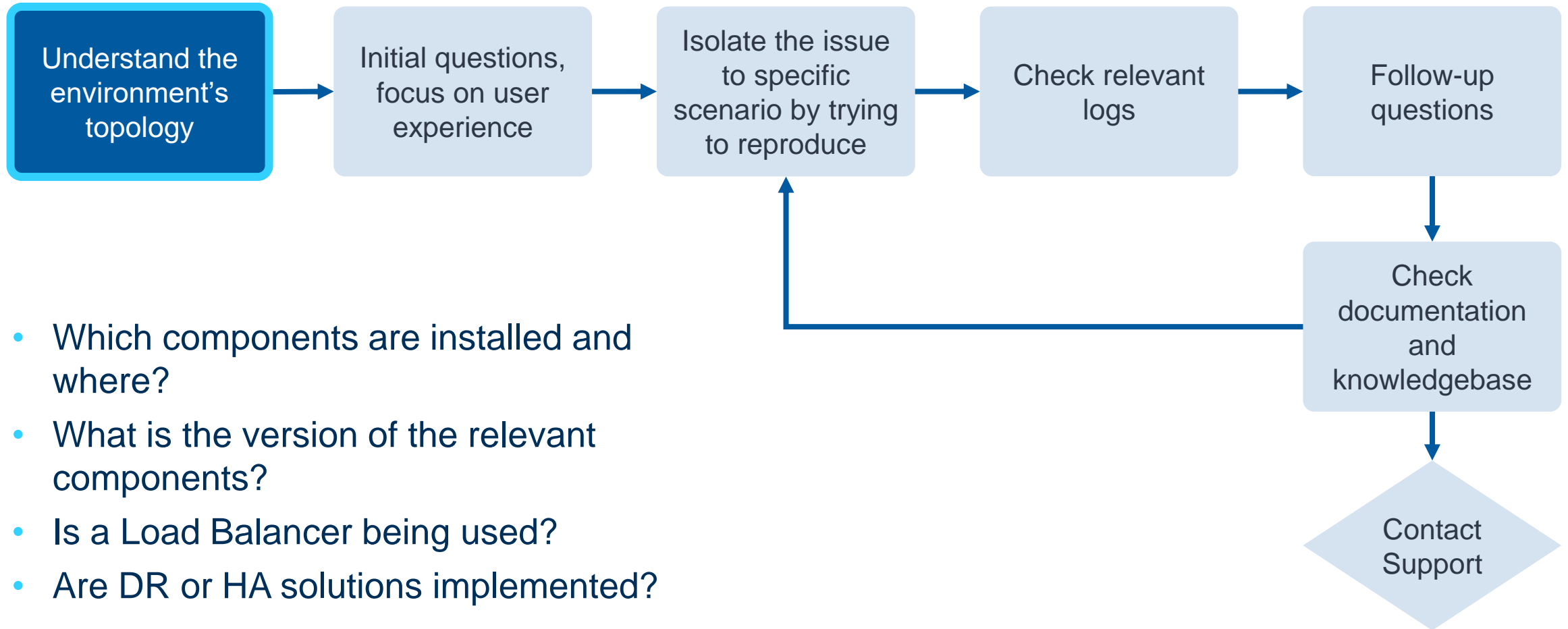
The latest version of the documentation will contain the most recent enhancements and notes.



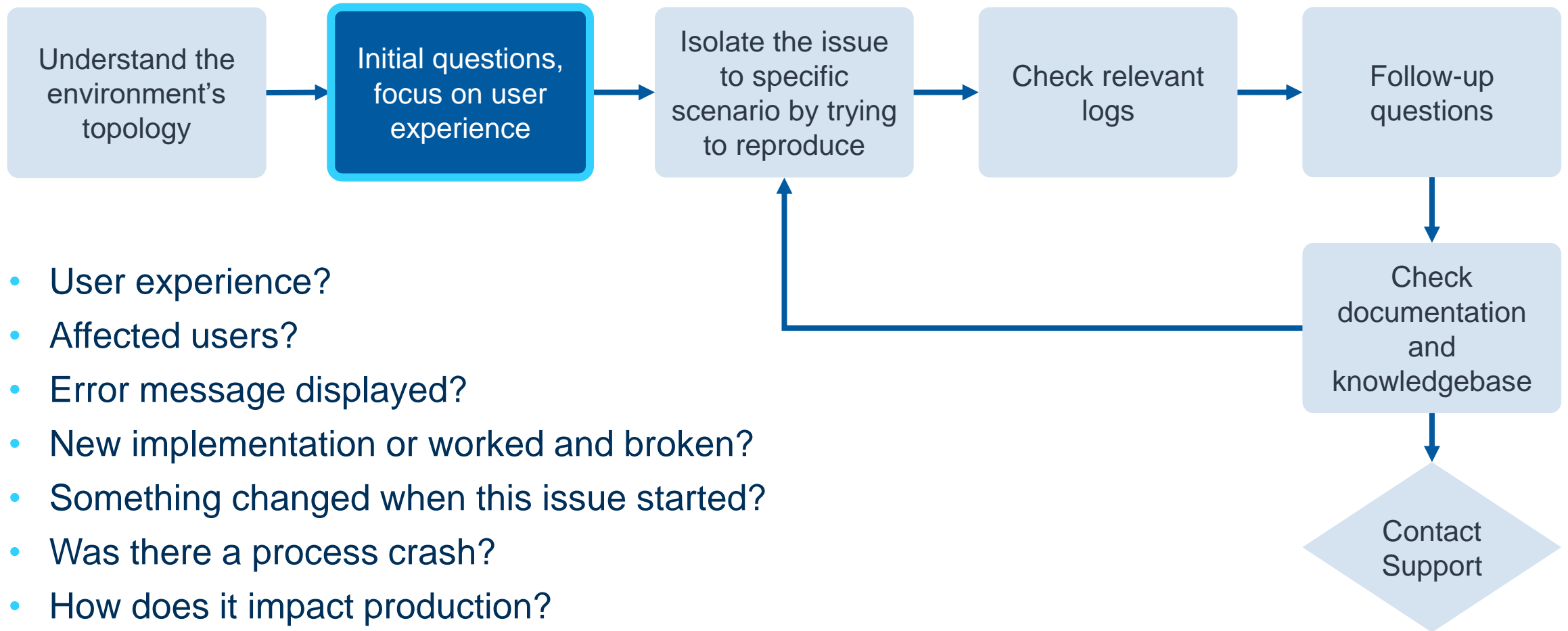
Troubleshooting Flow



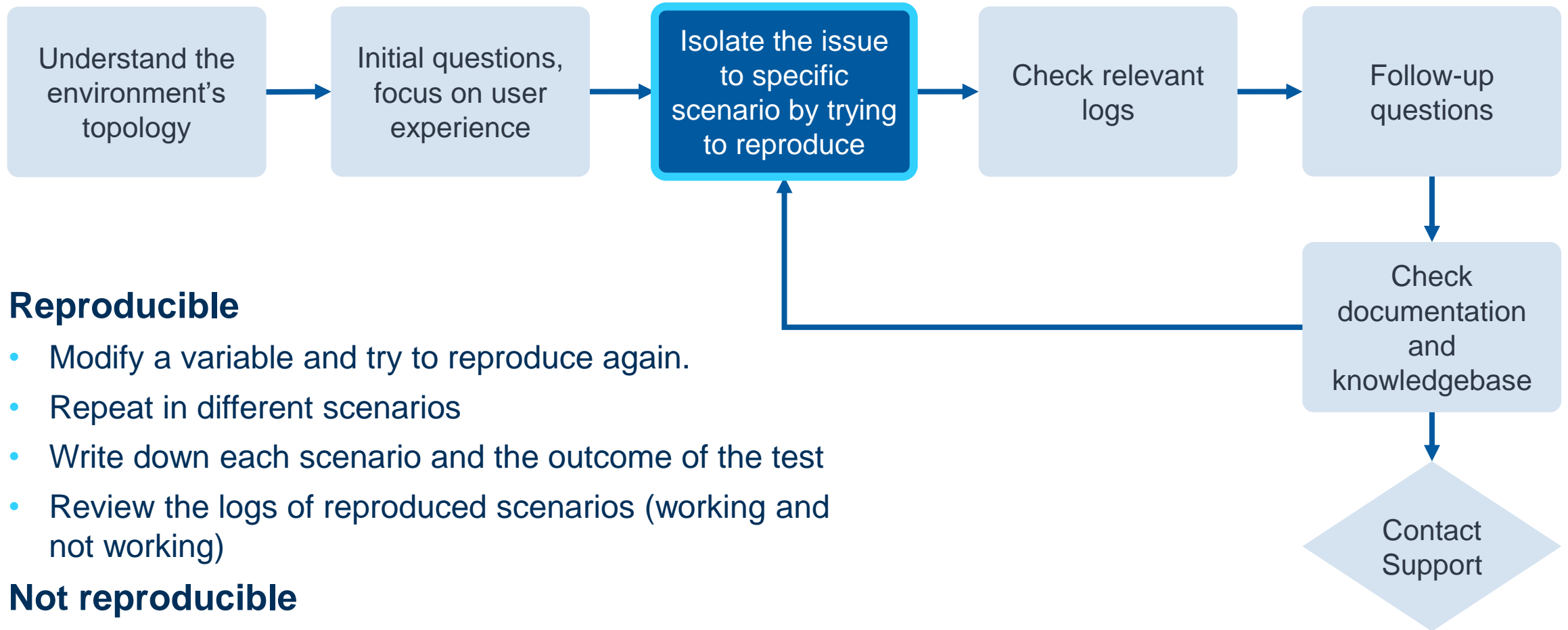
Understanding the Environment



Initial Questions



Isolation and Reproduction



Reproducible

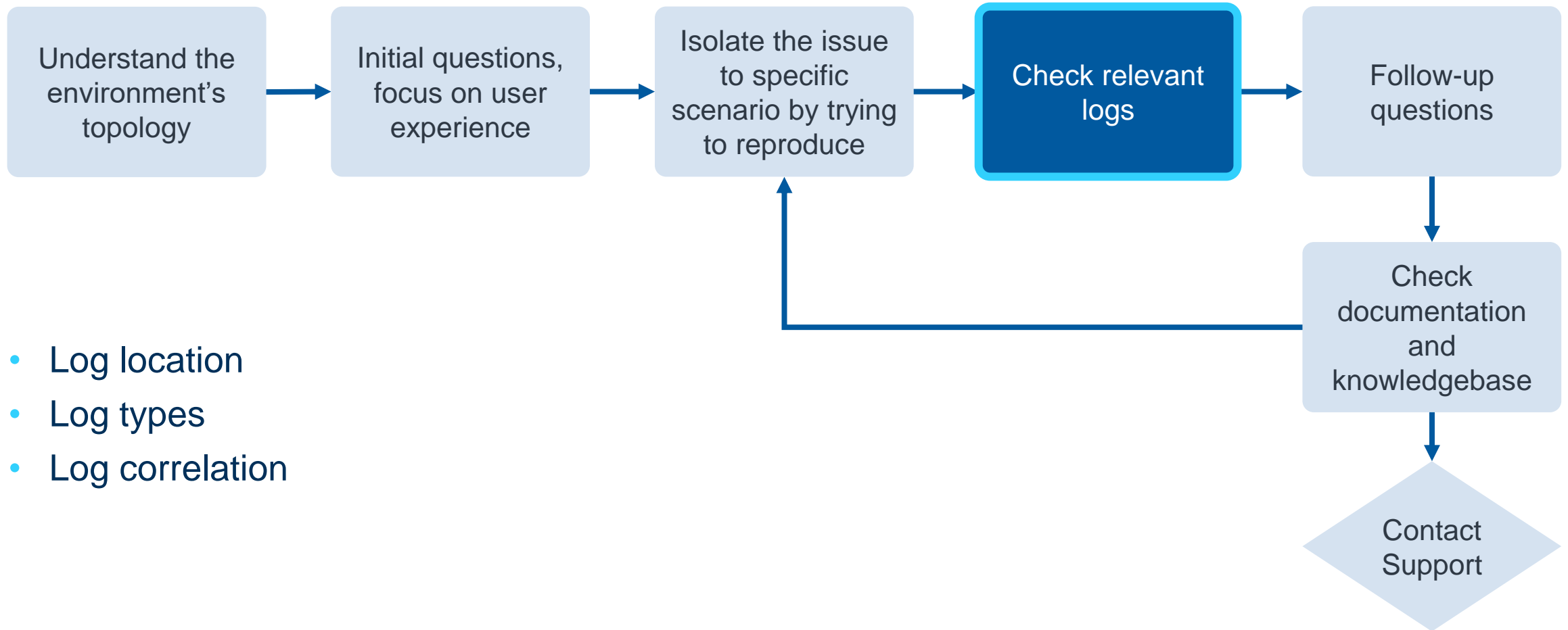
- Modify a variable and try to reproduce again.
- Repeat in different scenarios
- Write down each scenario and the outcome of the test
- Review the logs of reproduced scenarios (working and not working)

Not reproducible

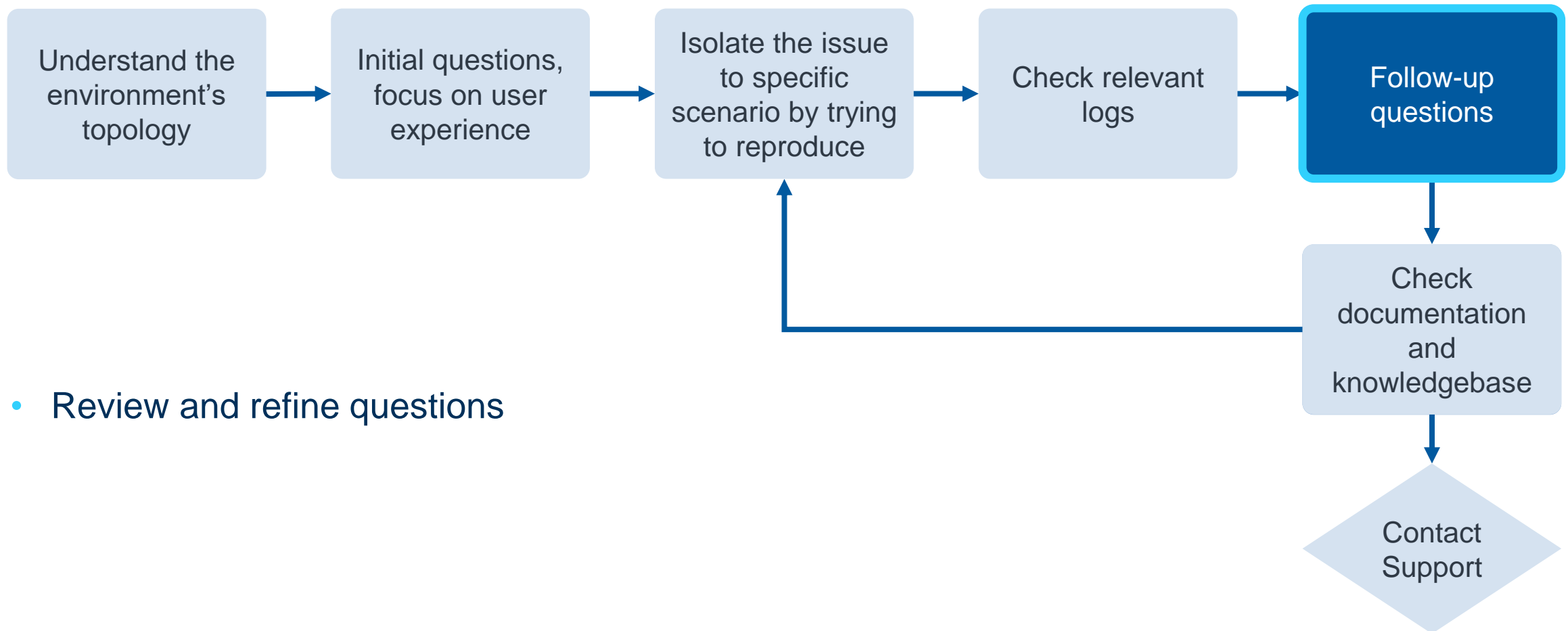
- Review the logs relevant for the reported flow



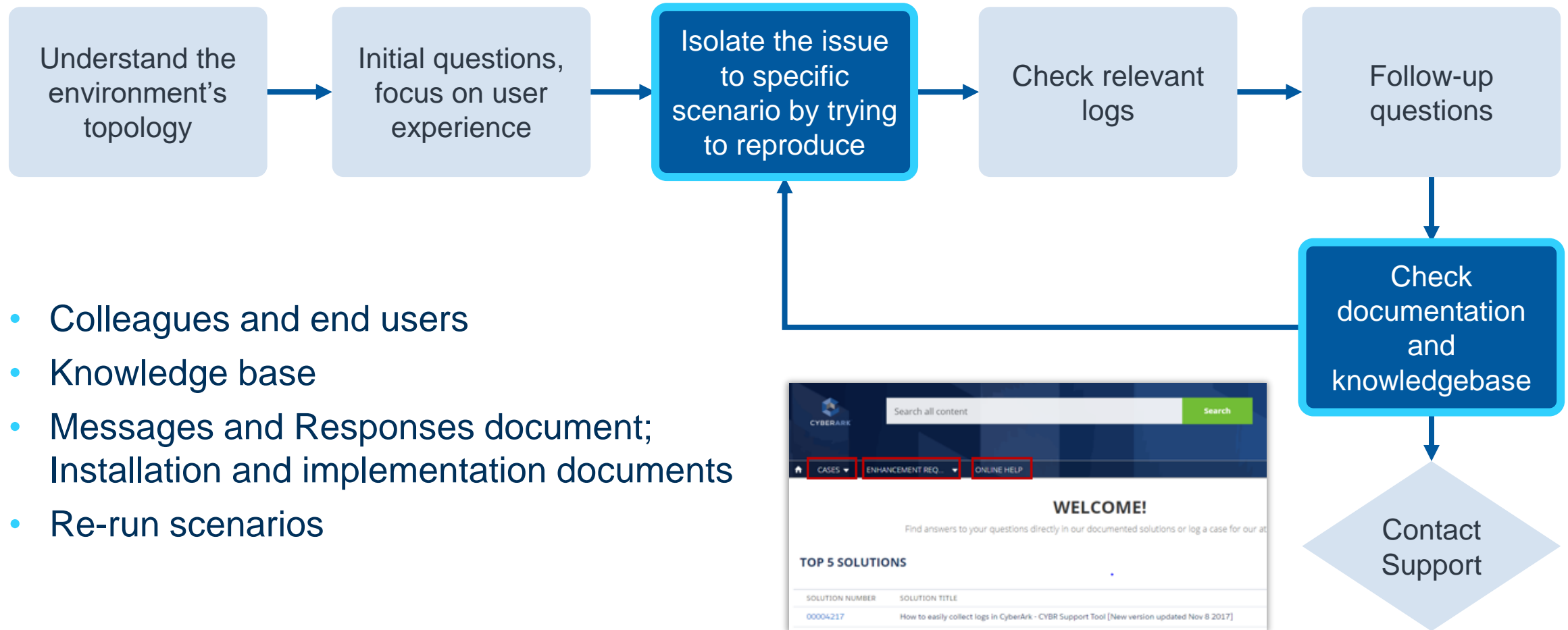
Checking the Logs



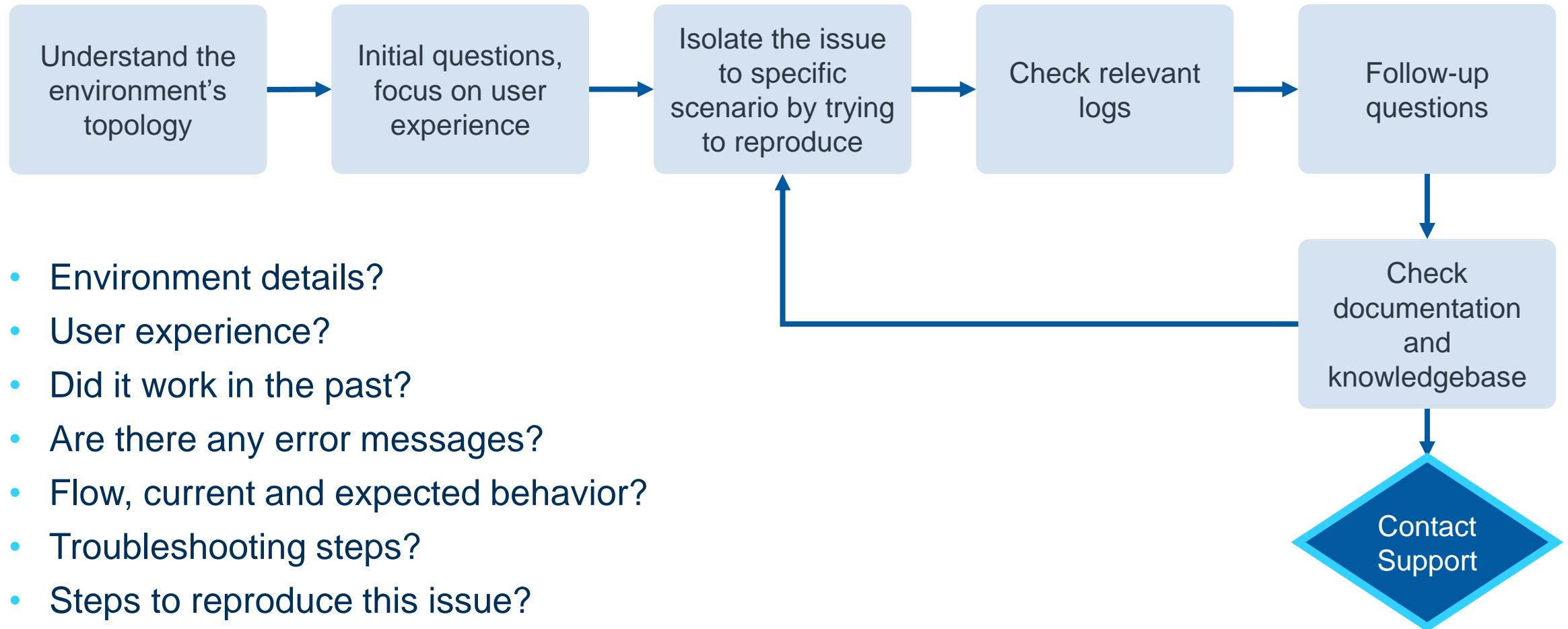
Follow-Up Questions



Documentations and Knowledge Base



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

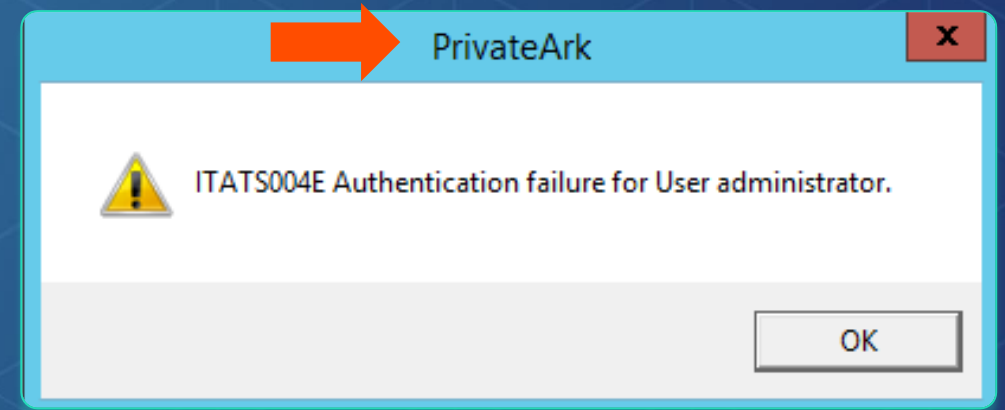


Troubleshooting Flow: Example

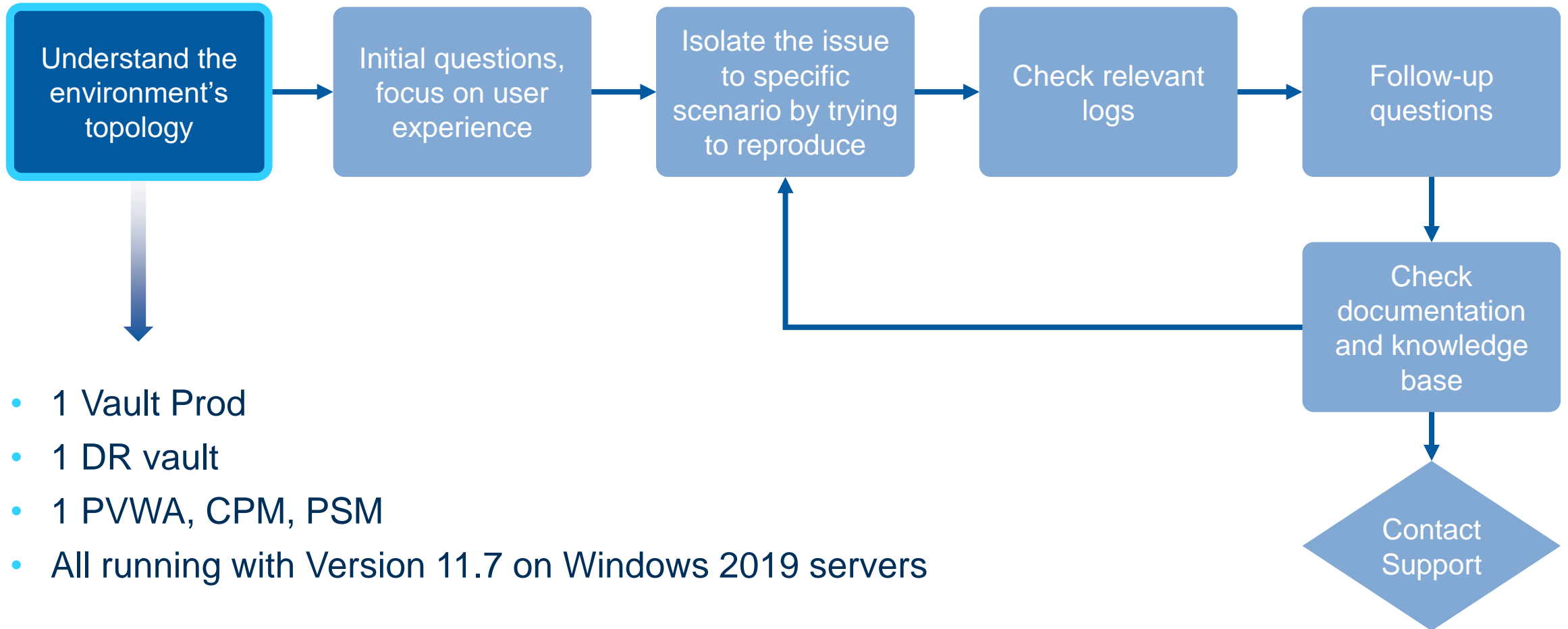


User Unable to Login

- A user is unable to login to the PrivateArk client using the administrator user. They see the following message.

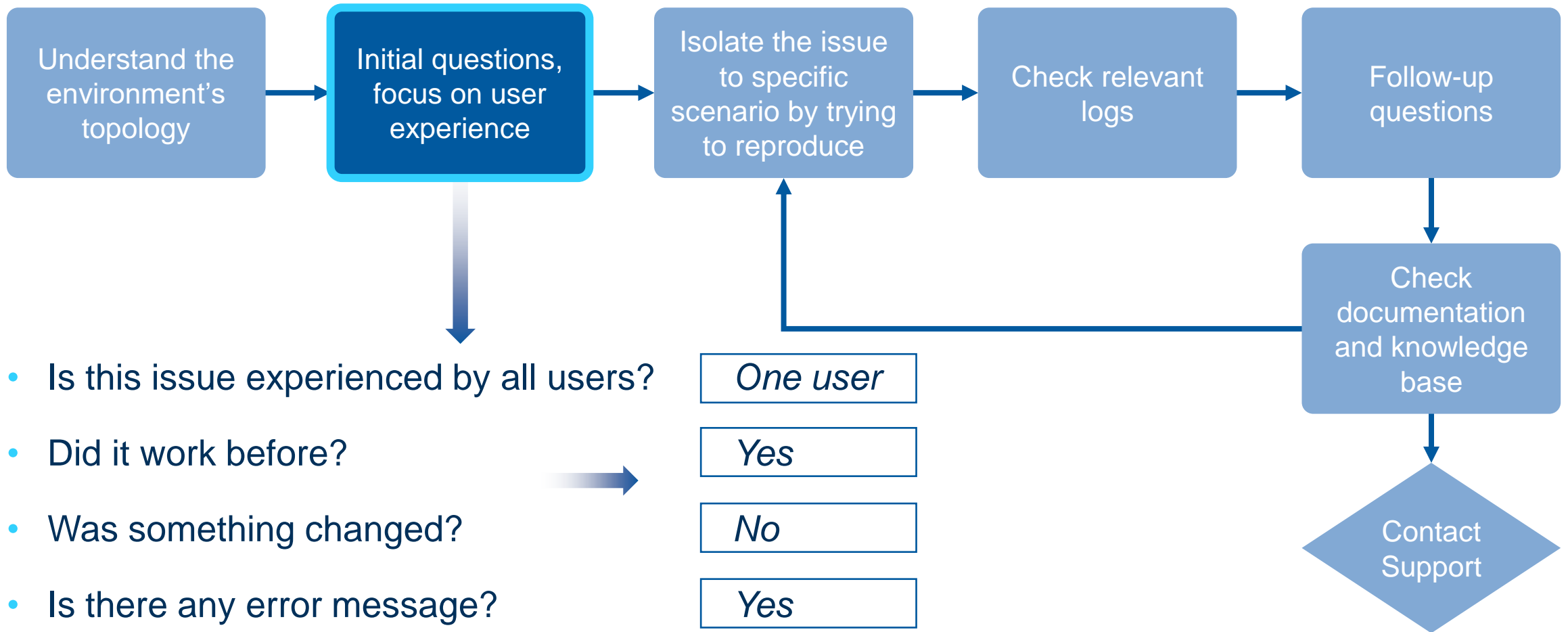


Understand the Environment

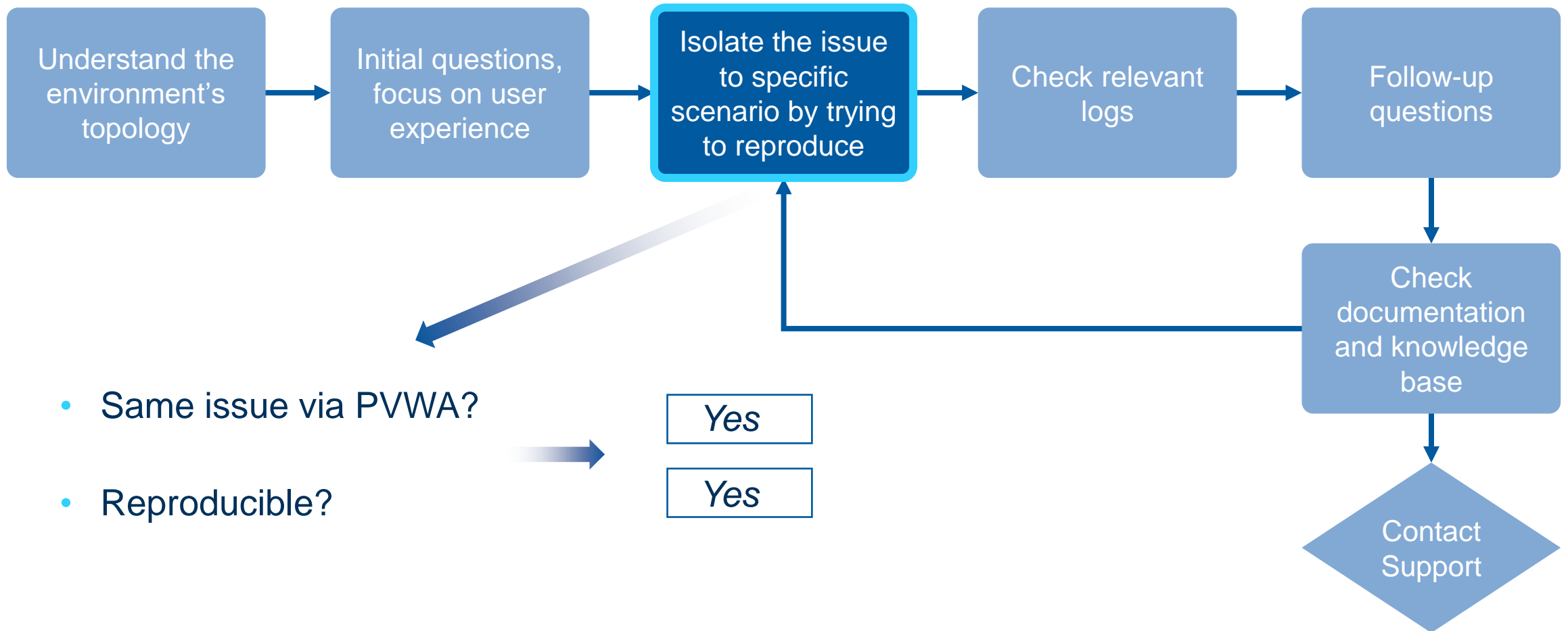


User Unable to Login

Initial Questions

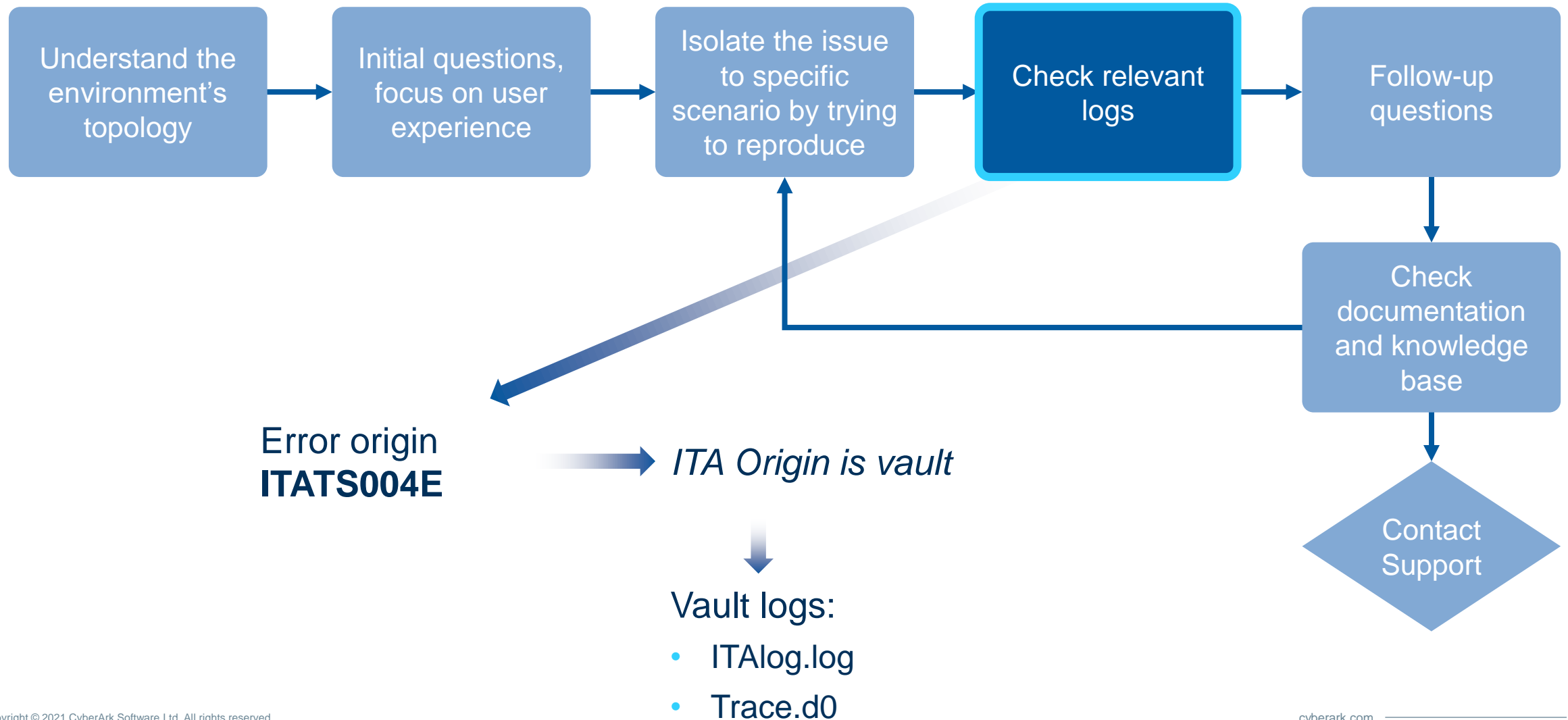


Isolation and Reproduction



User Unable to Login

Checking the Logs



Check Messages and Responses

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

Home > Administration > References > Messages and Responses

Highlights

Messages and Responses

View the messages that are displayed when you use the CyberArk solution, understand why they were issued and what you can do to carry on working.

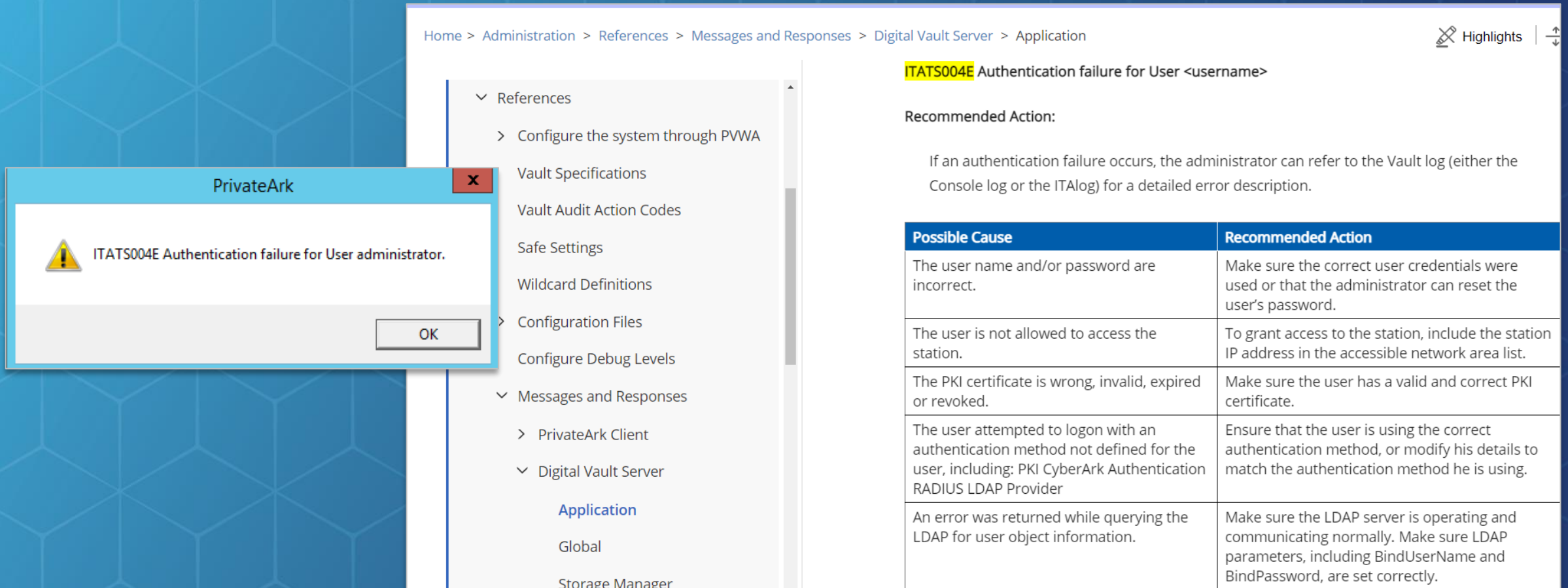
In this section:

- PrivateArk Client
- Digital Vault Server
- Disaster Recovery
- Central Policy Manager
- Password Vault Web Access
- Privileged Session Manager
- Privileged Session Manager for SSH
- AAM Credential Providers and OPM
- Discovery and Audit (DNA)
- Web Services



Check Messages and Responses

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



The screenshot displays the PrivateArk administration console. On the left, a navigation pane shows the hierarchy: Home > Administration > References > Messages and Responses > Digital Vault Server > Application. A modal dialog box titled "PrivateArk" is open, showing a yellow warning icon and the message "ITATS004E Authentication failure for User administrator." with an "OK" button. The main content area shows the "ITATS004E Authentication failure for User <username>" message. Below the message, a "Recommended Action" section states: "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." A table lists possible causes and recommended actions for this error.

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.



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.

✖ 24/04/2016 12:42:26 **ITATS528E** Authentication failure for user administrator from station: 10.10.10.10 (code: -66)

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

Recommended Action:

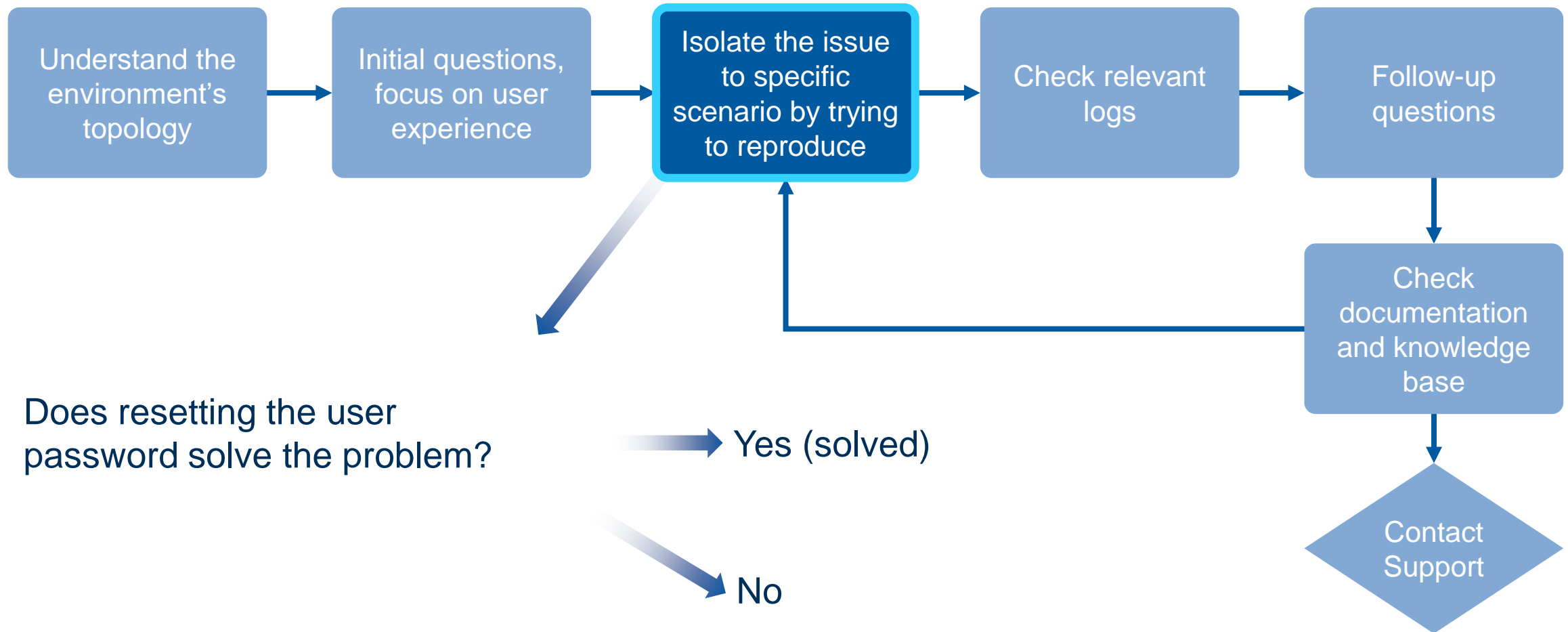
This authentication failure could be due to one of several reasons, depending on the code that is displayed:

- **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.
- Code 108 – 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.



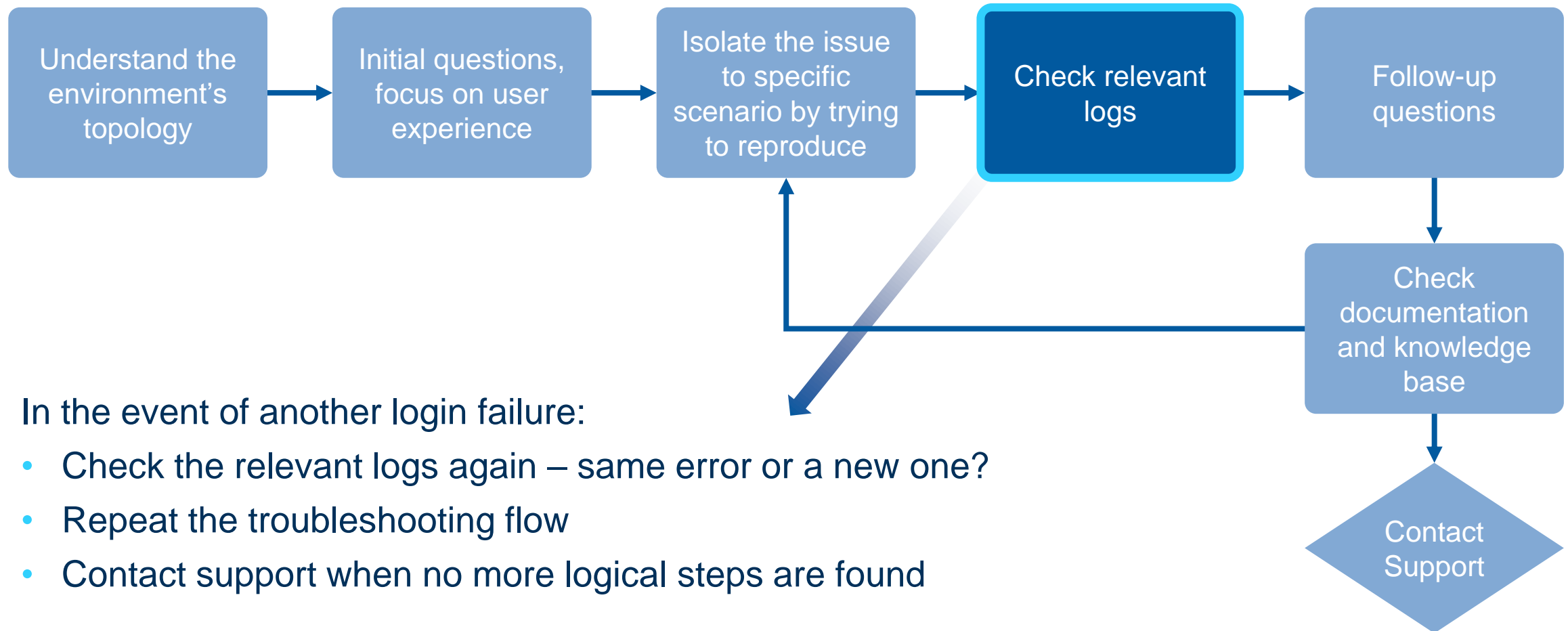
User Unable to Login

Solution



User Unable to Login

Problem Not Resolved



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



Types of Logs

Log files are divided into several types:



Console
Log

Provides component-level entries such as service up or down



Trace
Log

Provides detailed entries of workflows related to that component



Error
Log

Exists in some components, and will include only error entries



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



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:

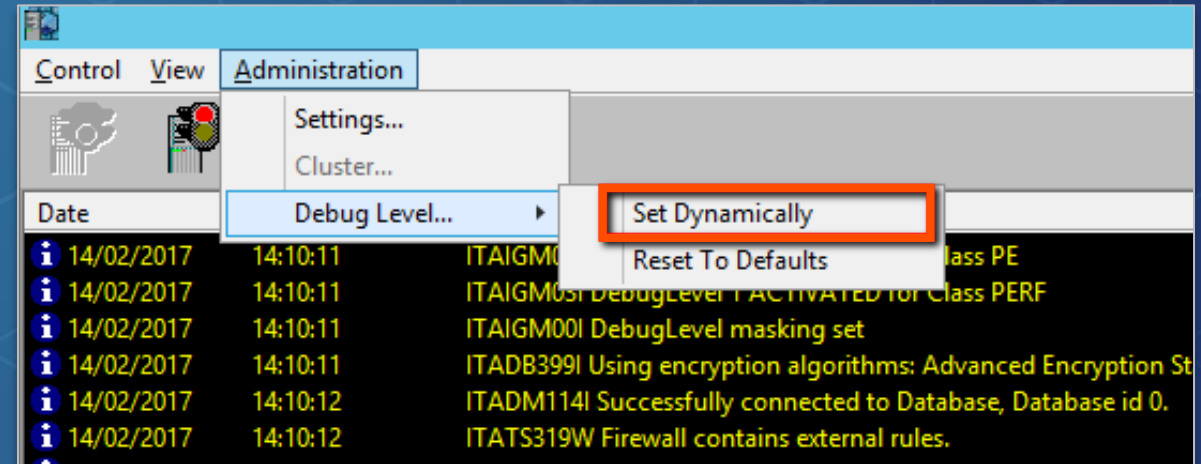
- ▶ Which log file do we need to review?
- ▶ What do we search for?
 - Keywords (Error, Failed, Failure...)
 - Timestamps
 - User name
 - Object name (Account name, safe name)
- ▶ Are there correlated entries in other logs?
 - Log events and time of the issue
 - Different components
 - **CyberArk** logs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

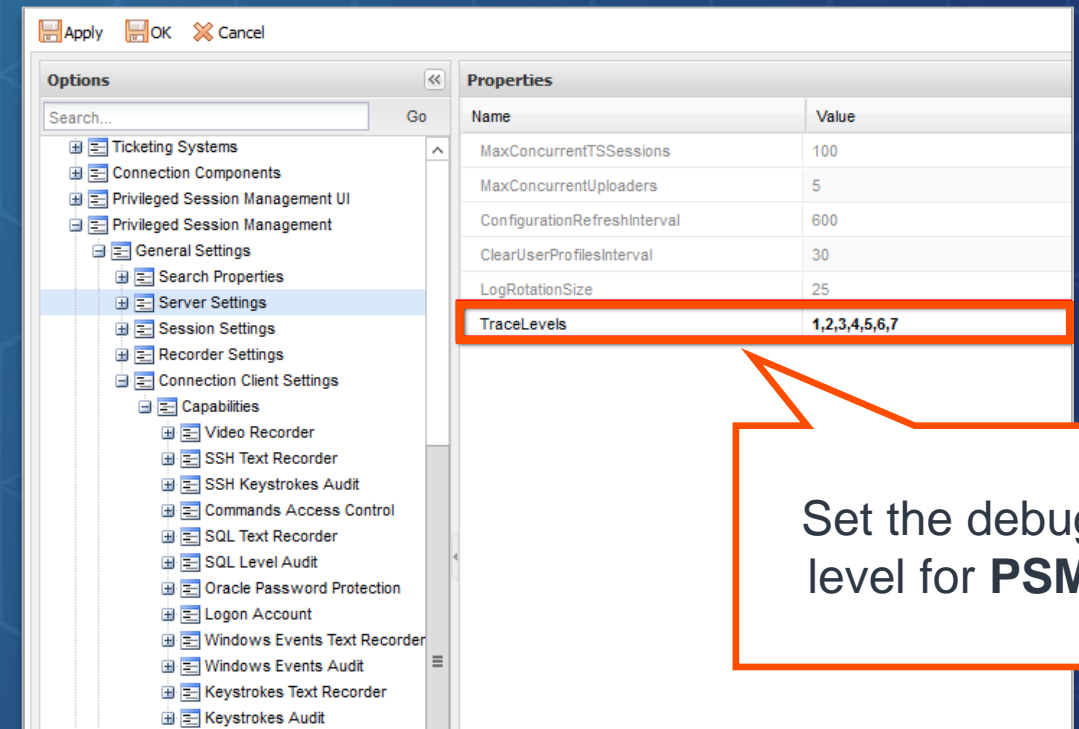
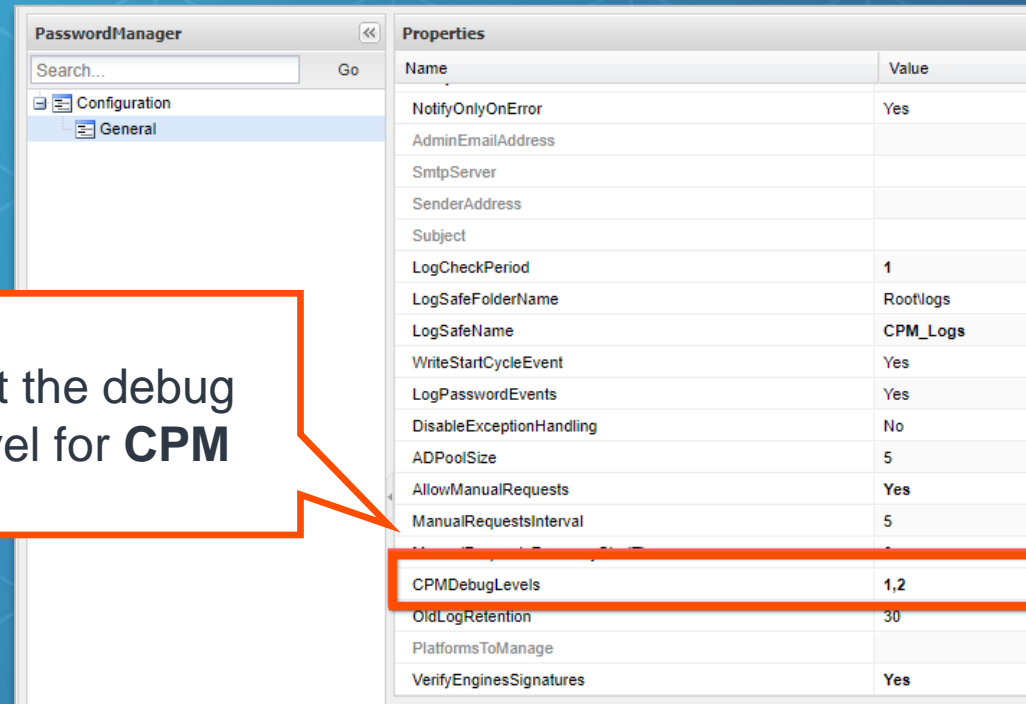


```
C:\CyberArkInstallationFiles\Version 9.8\Remote Control Client>PARClient.  
Cyber-Ark Remote Administration Client (9.80.3.0)  
Working with agent on: 192.168.202.129  
Loaded component from [C:\CyberArkInstallationFiles\Version 9.8\Remote Co  
Loaded component from [C:\CyberArkInstallationFiles\Version 9.8\Remote Co  
Loaded component from [C:\CyberArkInstallationFiles\Version 9.8\Remote Co  
Loaded component from [C:\CyberArkInstallationFiles\Version 9.8\Remote Co  
PARCLIENT> SetParm Vault DebugLevel=PE<1>,PERF<1>,LDAP<14,15> /IMMEDIATE  
Parameter DebugLevel has been successfully updated for component Vault
```



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



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**

The screenshot shows a web page with a navigation breadcrumb at the top: Home > Administration > References > Configure Debug Levels. On the left is a sidebar menu with categories like Privileged Accounts, Components, Utilities, and References. Under References, 'Configure Debug Levels' is highlighted. The main content area is titled 'Configure Debug Levels' and contains an introductory paragraph about configuration files. Below this is a section titled 'Digital Vault' with a list of links to various components: Vault, PARAgent, Disaster Recovery Vault, PAReplicate, PrivateArk Client, Event Notification Engine, Cluster Vault (CVM), ExportVaultData, and Vault Activity Email Notification.

Home > Administration > References > Configure Debug Levels

Configure Debug Levels

The following tables list the configuration files per component of the Privileged Access Security solution, specify how to set the debug mode, and give the location of the log files for each component.

Digital Vault [🔗](#)

- > Vault
- > PARAgent
- > Disaster Recovery Vault
- > PAReplicate
- > PrivateArk Client
- > Event Notification Engine
- > Cluster Vault (CVM)
- > ExportVaultData
- > Vault Activity Email Notification



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] <ul style="list-style-type: none">ControllerDebugLevel=1,2,3,4CollectorDebugLevel=1,2ParserDebugLevel=1,2SMTPSenderDebugLevel=1,2ConfigurationManagerDebugLevel=1,2
	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



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 “PVWACfg” → root\PVConfiguration.xml
	Vault → Safe “PVWACfg” → 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



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*

The screenshot shows the 'xRay agent setup' window. It contains the following sections and highlighted elements:

- Select CyberArk component:** Radio buttons for CPM, PSM, and PVWA. CPM is selected and highlighted with a red box.
- Collect logs (YYYY-MM-DD):** Date range selection. 'From' is 2021-03-28 and 'To' is 2021-03-31. This section is highlighted with a red box.
- Collection scope:** Radio buttons for 'Logs from the OS and the application' and 'Logs from application only'. The first option is selected and highlighted with a red box.
- Configuration files (optional):** A checkbox is checked. Below it, the 'Choose Authentication method' section has radio buttons for CyberArk, LDAP, and Radius. CyberArk is selected. The 'Active Vault IP address' is 10.0.10.1, 'Username' is administrator, and 'Password' is masked. This entire section is highlighted with a red box.
- Agreement:** A checkbox for 'I agree to the terms of use' is checked and highlighted with a red box. A 'Start collection' button is also highlighted with a red box.

Version: 11.1.0.6



Monitor Collection Process

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

```
Administrator: C:\Windows\System32\cmd.exe

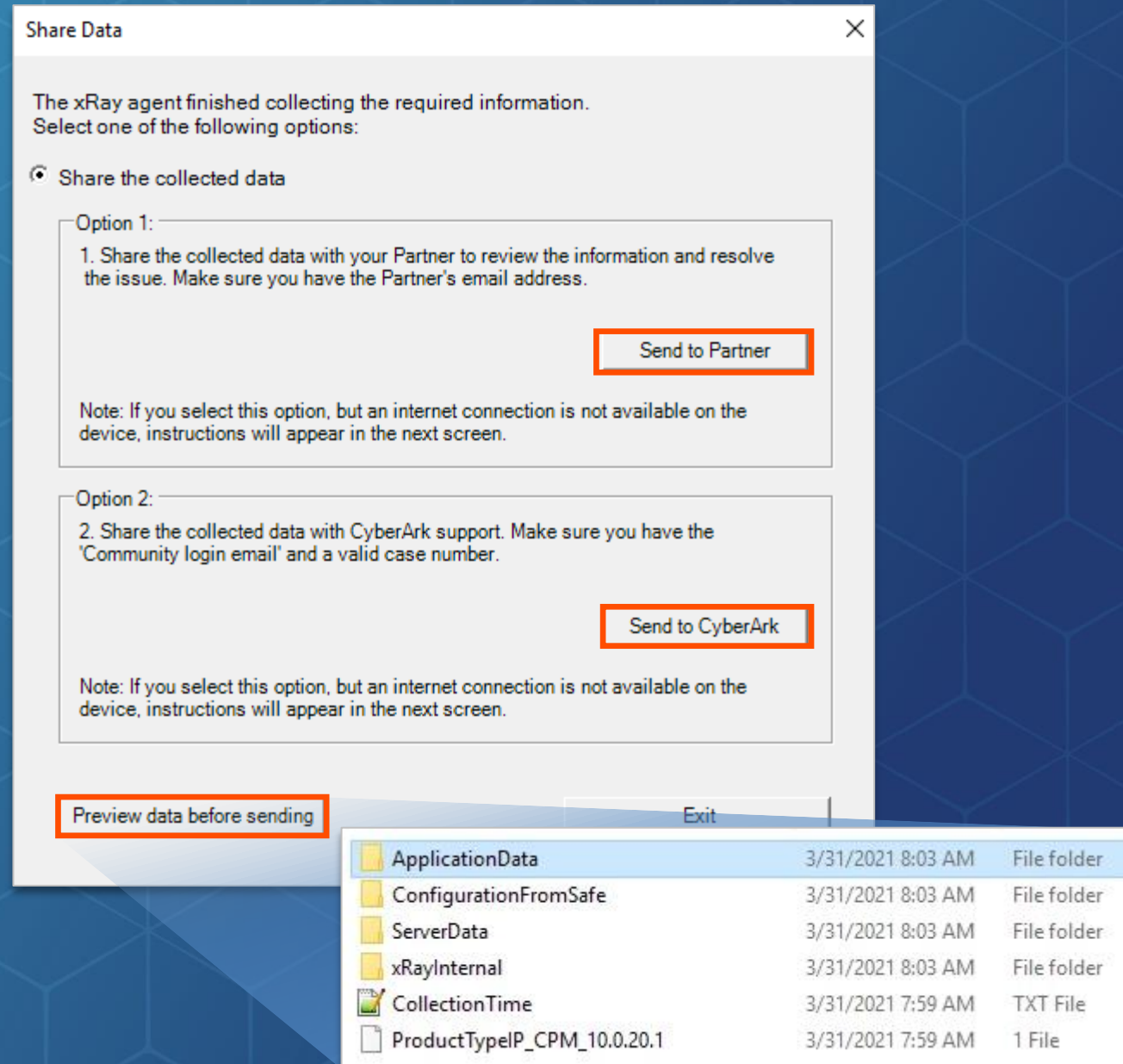
*****
CyberArk xRay Agent
*****

07:57:32      Info      Please wait... don't close this window
07:58:22      Info      Collection starting. It will take a few moments.
07:58:33      Info      ----- Agent Device Logs -----
07:58:33      Info      Opening CPM_10.0.20.1 package
07:58:40      Info      Starting to copy files from the CPM_10.0.20.1 component
07:58:42      Info      Getting relevent file names
07:58:48      Info      Creating application zip file. It may take a few minutes
07:59:10      Info      Collecting Vault IP and extra Safe names
07:59:10      Info      Collecting information about your operating system
07:59:13      Info      Program updates collected
07:59:14      Info      Installed services collected
07:59:14      Info      Active process collected
07:59:14      Info      Network details collected
```



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



Documentation

Additional information can be found in the [CyberArk documentation](#)

The screenshot shows a web page titled 'What is xRay?' within the CyberArk documentation. The breadcrumb trail at the top reads 'Home > Administration > Utilities > xRay > What is xRay?'. On the right side of the header, there is a 'Highlights' icon and a vertical scroll indicator. The left sidebar contains a navigation menu with the following items: 'Utilities' (expanded), 'Server Utilities' (with sub-items 'AccountUploader Utility' and 'Password Upload Utility'), 'ExportVaultData Utility', 'User credential files', 'xRay' (expanded), 'What is xRay?' (selected), 'Get Started', 'Start collecting data and logs', 'Updates', and 'Telemetry'. The main content area has the title 'What is xRay?' followed by an 'Overview' section with a link icon. The overview text states: 'CyberArk xRay collects product logs and configuration files from multiple products in a simple single-step process, replacing today's complicated manual collection. You can share the collected data with your partner or CyberArk, knowing that it is safely encrypted during transfer.' It then adds: 'In addition, when sharing with CyberArk, shared data is linked to a case to allow Enterprise Support easy and secure access to the collected data.' The next paragraph says: 'CyberArk xRay can be configured to use different approaches to access each CyberArk product. In addition, data can be collected manually or automatically, depending on the access authorization given to the machine running xRay.' The final paragraph concludes: '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.'

Home > Administration > Utilities > xRay > What is xRay?

Utilities

- Server Utilities
 - AccountUploader Utility
 - Password Upload Utility
- ExportVaultData Utility
- User credential files
- xRay
 - What is xRay?**
 - Get Started
 - Start collecting data and logs
 - Updates
- Telemetry

What is xRay?

Overview

CyberArk xRay collects product logs and configuration files from multiple products in a simple single-step process, replacing today's complicated manual collection. You can share the collected data with your partner or CyberArk, knowing that it is safely encrypted during transfer.

In addition, when sharing with CyberArk, shared data is linked to a case to allow Enterprise Support easy and secure access to the collected data.

CyberArk xRay can be configured to use different approaches to access each CyberArk product. In addition, data can be collected manually or automatically, depending on the access authorization given to the machine running xRay.

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.



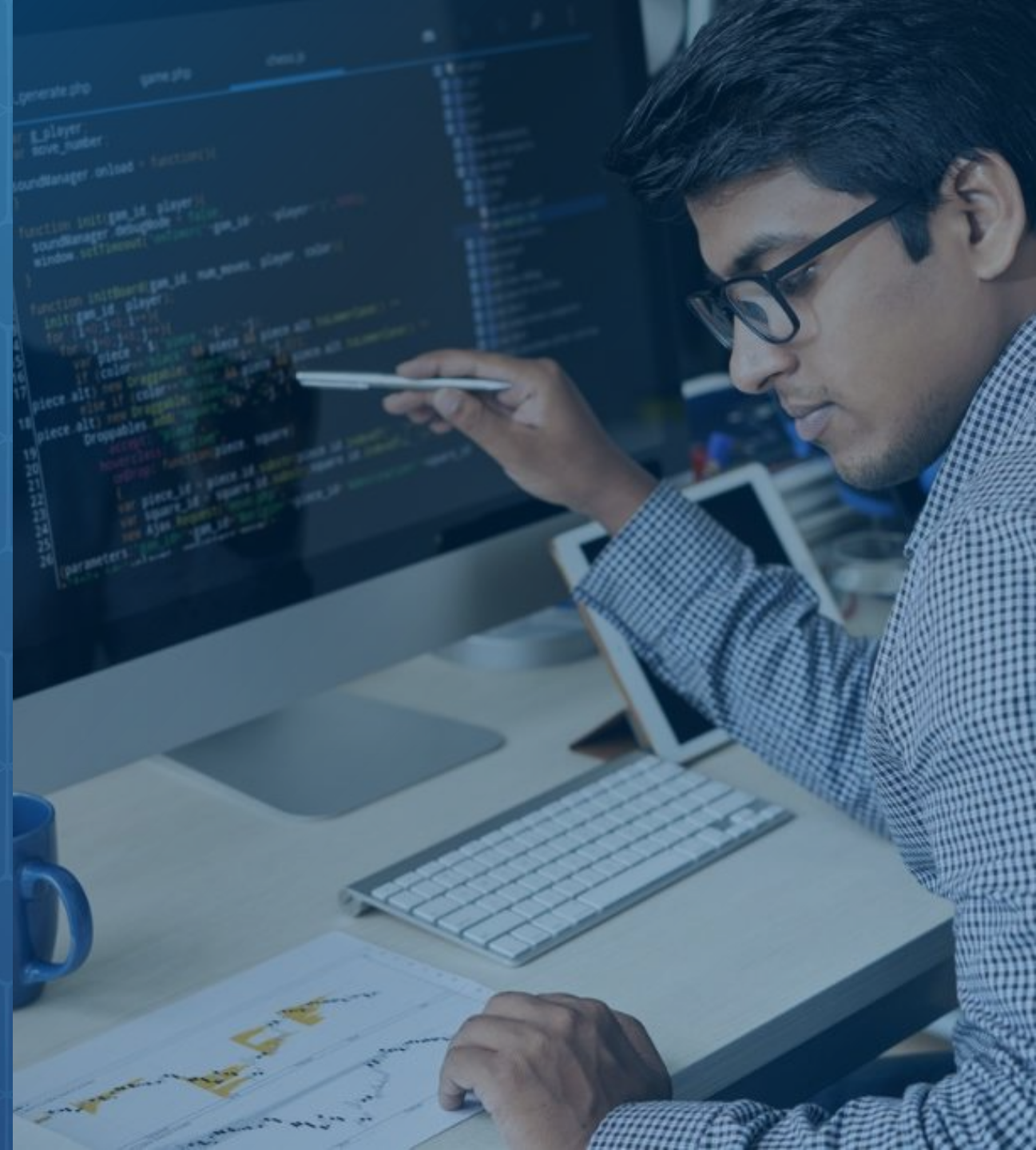
Summary



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*](#)



Online Training:

Working with CyberArk Support:

<https://training.cyberark.com/elearning/working-with-cyberark-support>

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

