The Privileged Appliance and Modules (TPAM) 1.0

Diagnostics and Troubleshooting Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

TPAM Diagnostics and Troubleshooting Guide
Updated - November 2017
Version - 1.0

Contents

Diagnostics and Troubleshooting

Introduction

This purpose of this guide is to:

- explain the TPAM product use case
- teach how to troubleshoot common issues
- teach how to gather all the necessary information that Support requires to diagnose an issue in the event that a support ticket needs to be opened

TPAM functional overview

Total Privileged Access Management (TPAM) is a robust collection of integrated modular technologies designed specifically to meet the complex and growing compliance and security requirements associated with privileged identity management and privileged access control.

TPAM is comprised of two modules:

- Privileged Password Manager (PPM)
- Privileged Session Manager (PSM)

Privileged Password Manager (PPM) automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. Privileged Password Manager ensures that when administrators require elevated access, that access is granted according to established policy, with appropriate approvals, that all actions are fully audited and tracked and that the password is changed immediately upon its return.

Privileged Session Manager (PSM) provides session control, proxy, audit, recording and replay of high-risk users, including administrators, remote vendors and others. It provides a single point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, alert if connections exceed pre-set time limits and terminate connections.

The appliance runs on a hardened Windows Web Server. An internal firewall is active on the device, protecting against network threats and OS vulnerabilities. The front end provides the administrative interface, the automation routines, and the gateway to the encrypted passwords for the release mechanism. There is no direct access to the OS of the appliance. All configurations occur via the configuration or administrative interfaces.

In addition to storing sensitive data (such as passwords) in encrypted form, the hard disk of the appliance is fully encrypted. This prevents exposure of data should the disk be lost or stolen.

The connections to remote managed systems are accomplished utilizing the most secure standard methods available. In most cases, this will be SSH. A setup guide is provided to accomplish the necessary configuration on the remote system. In most cases, this will include the definition of a functional userID with password change capability.

If a system is managed by PPM then the appliance also makes connections to these managed systems to ensure that the stored password is valid on the managed system. Any 'out of sync'conditions are reported, and based on the configuration settings, automatically corrected.

Methods of access

The TPAM appliance has several methods of access:

- Configuration interface (HTTPS via direct connection, with network option)
- Administrative interface (HTTPS via network access)
- User interface (HTTPS via network access)
- System Administrator CLI (SSH via network access)
- User CLI (SSH via network access)
- User API (SSH client application via network access)

Deployment scenarios

High availability clustering is an option for customers to support TPAM with a minimum of down time and eliminate a single point of failure. Each appliance is configured with a cluster role. The cluster role choices are:

- Primary -Acts as the information source for the cluster. Only one primary allowed per cluster.
- Replica -redundant appliance that is kept in synch with the primary. Can be configured to automatically fail over if it loses contact with the primary.
- Standalone -this role only applies to DPAs enrolled in the cluster and cannot be changed.

Common issues

For solutions to common issues please go to https://support.oneidentity.com/tpam-appliance and click on the Knowledge Base link on the left side of the page. Solutions to many issues found by customers are posted here.

Examples of some common issues are:

- PSM Session Connection issues-Issues establishing remote sessions to managed systems, including unavailable ports and java issues, etc.
- Connection failures between PPM and managed systems-Incorrect functional account password, unavailable ports, etc.
- Restoring HA Clusters, replication issues-Failover due to communication between appliances, etc.
- Hardware failures, RMAs (hardware replacement)
- Web Interface Login / Availability issues
- Downloading and applying hotfixes, patches etc.-downloads are available from https://support.oneidentity.com

Common setup issues

- When replacement appliances are received, there is a specific process for restoring the appliance from backup.
- Configuring network settings on new or replaced appliances The appliance(s) must be accessed using the config port to update the network settings for the appropriate subnet, etc.

Troubleshooting checklist

Troubleshooting TPAM issues begins with collecting all relevant information. With version 2.5 of TPAM the **Support Bundle** was created to allow Technical Support to collect a data file that includes vital information about the TPAM appliance. The information in this file will be used for troubleshooting issues when calling in to open a service request.

The **Support Bundle** is an un-encrypted file but does not contain any sensitive customer data such as passwords, only information about the appliance itself.

To create a support bundle:

1. Select **System Status/Settings | System Status** from the menu.

2. Click the **Support Bundle** tab.
3. Based on your conversation with technical support, select/clear the check boxes in the **Optional Items** section. Enter a **Start Date** and **End Date** to narrow the results.
4. Click the **Create Support Bundle** button. Once the bundle is complete it is displayed in the Bundle list.
5. Select the bundle name from the list that you want to download.
6. Click the **Download Bundle** button.
7. Click the **OK** button to save the file offline. Now the zip file can be emailed to Technical Support.

CLI IDs

It is recommended that customers create a Sys-Admin CLI user ID and that they download and store the key outside of the appliance. A CLI Sys-Admin user ID is a special user account used to access TPAM remotely via the CLI (command line interface). When accessing TPAM through the CLI they can only execute specific commands supported by the TPAM CLI. A Sys-Admin CLI user ID can access the TPAM appliance when the web interface becomes unavailable and thus perform various troubleshooting steps.

Steps to add a Sys-Admin CLI user ID are included in the System Administrator Guide.

Logs

Logs are located in the tpam /admin interface. Logs included here are the Sys-Admin Activity Log, Security Log, Firewall Log, Database Log and Alerts Log. However, there are other logs that can be gathered such as the Primary and Replica logs for HA issues, Mail Agent log, Backup log, Patch log and so on. Particular logs will be requested from the technical support team, dependent on the issue being investigated.

System status

The System Status page is a requirement at all times in order to confirm the version and appliance serial number. To navigate to the System Status page int the /admin interface select **System Status/Settings |System Status** from the menu. On the System Status page scroll down in the embedded text box so the "Appliance Info" is visible in the screen shot. A screen shot of the System Status is a requirement for the escalation team when opening a Collaboration Request.

Network tools

To assist the TPAM System Administrator with troubleshooting common network related problems, TPAM contains network tools that are accessible from the /config and /admin interface. In addition, some specialized configurations can be made to add or manage static routes.

From the /tpam interface navigate to **Management |Network Tools**. From the /config interface the Network Tools is located in the main menu.

Ping utility

The ping utility can be used to verify connectivity to remote hosts and determine latency. Many of the optional parameters for the ping command are available. The available command options are listed along with the short description of each.

To use the ping utility:

1. Select **Net Tools | Ping** from the menu.
2. Enter the IP or Hostname.
3. Select the options desired.
4. Click the **Ping** button. The results will be displayed.

Nslookup utility

Nslookup is a common TCP/IP tool used to test DNS settings and perform similar information gathering using DNS resolution. The TPAM utility for nslookup will use the DNS server(s) configured to TPAM only. The option to specify a server is not provided. TPAM System Administrators can benefit from the ability to use nslookup to resolve hostnames to IP addresses and vice versa.

To use Nslookup:

1. Select **Net Tools | Nslookup** from the menu.
2. Enter the IP address or Hostname to look up.
3. Click the **Lookup** button.

TraceRoute utility

The tracerouteutility is available for examining network routing and connectivity from TPAM to a remote IP address or hostname. The use of traceroute is often disallowed by firewalls, routers, and other network security infrastructure, but if allowed, it can be a valuable diagnostic tool.

To use traceroute:

1. Select **Net Tools | TraceRoute** from the menu.
2. Enter the IP or Hostname to trace.
3. Select the **-d** check box. (Optional)
4. Change the default number of hops and timeout wait. (Optional)
5. Click the **Trace** button.

Telnet Test utility

The Telnet test utility lets a test be performed from the appliance to another system over a specific port. The tool will test the defined port using telnet functionality to verify the port, whether a connection can be made, and then immediately close the connection.

To use the Telnet Test utility:

1. Select **Net Tools | Telnet Test** from the menu.
2. Enter the network address, port and timeout period.
3. Click the **Trace** button.

Performance diagnostics

The system status graphs provide a visual presentation of key statistics for system administrators and technical support. To view the graphs select **System Status/Settings | System Status** from the menu. Click the **Graphs** tab. See the System Administrator Guide for more details.

Prerequisites for contacting support

Technical support is available to customers who have a trial version of a TPAM product or who have purchased a TPAM product and have a valid maintenance contract.

•Submitting the Support Bundle, with a clear description of the issue being reported, is recommended.

•Additional logs/information may be required, and a member of the Support team can determine this based on the issue.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product