Security checklist for configuring the Balabit's Privileged Session Management

June 19, 2018

Abstract
Security checklist for Balabit's Privileged Session Management (PSM)

Table of Contents

1. Security checklist for configuring PSM

The following checklist is a set of recommendations and configuration best practices to ensure that your PSM is configured securely.

Encryption-related settings

- One Identity recommends using 2048-bit RSA keys (or stronger).
- Use strong passwords: at least 8 characters that include numbers, letters, special characters, and capital letters. For local PSM users, require the use of strong passwords (set **AAA > Settings > Minimal password strength** to `strong`). For details, see *Procedure 5.2, Setting password policies for local users* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- When exporting the configuration of PSM, or creating configuration backups, always use encryption. Handle the exported data with care, as it contains sensitive information, including credentials. For details on encrypting the configuration, see *Procedure 4.7.6, Encrypting configuration backups with GPG* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Use every keypair or certificate only for one purpose. Do not reuse cryptographic keys or certificates, for example, do not use the certificate of the PSM webserver to encrypt audit trails, or do not use the same keypair for signing and encrypting data.
- Do not use the CBC block cipher mode, or the `diffie-hellman-group1-sha1` key exchange algorithm. For details, see *Section 11.6, Supported encryption algorithms* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Always encrypt your audit trails to protect sensitive data. For details, see *Procedure 7.10.1, Encrypting audit trails* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

Connection policies

- When configuring connection policies, always limit the source of the connection to the client network that requires access to the connection.
- Always use gateway authentication to authenticate clients. Do not trust the source IP address of a connection, or the result of server authentication.
- To prevent Denial of Service (DoS) attacks against PSM, set the **Connection rate limit** option of your connection policies. For details, see *Procedure 7.1, Configuring connections* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Configure your RDP connection policies to use strong encryption. To enable SSL-encryption for the RDP protocol, see *Procedure 10.5, Enabling TLS-encryption for RDP connections* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- In RDP connections, if the client uses the Windows login screen to authenticate on the server, the password of the client is visible in the audit trail. To avoid displaying the password when replaying the audit trail, you are recommended to encrypt the upstream traffic in the audit trail using a separate

All questions, comments or inquiries should be directed to `<info@balabit.com>` or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*

certificate from the downstream traffic. For details, see *Procedure 7.10.1, Encrypting audit trails* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

- Ensure that host key verification is enabled in SSH connection policies. That is, the **Server side hostkey settings > Allow plain host keys** and **Server side hostkey settings > Allow X.509 host certificates** options do not have the **No check required** option selected. For details, see *Procedure 11.1, Setting the SSH host keys and certificates of the connection* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

Appliance access

- Accessing the PSM host directly using SSH is not recommended or supported, except for troubleshooting purposes. In such case, the One Identity Support Team will give you exact instructions on what to do to solve the problem.
  For security reasons, disable SSH access to PSM when it is not needed. For details, see *Procedure 6.6.2, Enabling SSH access to the PSM host* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

- Permit administrative access to PSM only from trusted networks. If possible, monitored connections and administrative access to the PSM web interface should originate from separate networks.
- Configure PSM to send an alert if a user fails to login to PSM. For details, see the **Login failed** alert in *Section 4.6.4, System related traps* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Configure **Disk space fill up prevention**, and configure PSM to send an alert if the free space on the disks of PSM is low. For details, see *Procedure 4.6.3, Preventing disk space fill up* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

Networking considerations

- PSM stores sensitive data. Use a firewall and other appropriate controls to ensure that unauthorized connections cannot access it.
- If possible, enable management access to PSM only from trusted networks.
- Make sure that the HA interface of PSM is connected to a trusted network.