

How to deploy Balabit's Privileged Session Management from the Azure Marketplace

Publication date June 19, 2018

Abstract

Azure Installation Guide for Balabit's Privileged Session Management (PSM, formerly called SCB)



Copyright © 1996-2018 One Identity LLC

Copyright © 2018 One Identity LLC. All rights reserved. This document is protected by copyright and is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of One Identity.

This documentation and the product it describes are considered protected by copyright according to the applicable laws.

The Balabit™ name and the Balabit™ logo are registered trademarks of Balabit SA.

The Balabit Shell Control Box™ name and the Balabit Shell Control Box™ logo are registered trademarks of Balabit.

Citrix®, ICA® and XenApp™ are trademarks or registered trademarks of Citrix Systems, Inc.

Linux™ is a registered trademark of Linus Torvalds.

Sun™, Sun Microsystems™, the Sun logo, Sun Fire 4140™, Sun Fire 2100™, Sun Fire 2200™, Sun Fire 4540™, and Sun StorageTek™ are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the U.S. and other countries.

The syslog-ng™ name and the syslog-ng™ logo are registered trademarks of Balabit.

VMware™, VMware ESX™ and VMware View™ are trademarks or registered trademarks of VMware, Inc. and/or its affiliates.

Windows™ 95, 98, ME, 2000, XP, Server 2003, Vista, Server 2008, 7, 8, and Server 2012 are registered trademarks of Microsoft Corporation.

The Zorp™ name and the Zorp™ logo are registered trademarks of BalaSys IT Ltd.

All other product names mentioned herein are the trademarks of their respective owners.

DISCLAIMER. One Identity is not responsible for any third-party websites mentioned in this document. One Identity does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. One Identity will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<https://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes open source software components. For details on the licenses and availability of these software components, see [Appendix E, Open source licenses](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

Table of Contents

Preface	iv
1. Deploying Balabit's Privileged Session Management from the Azure Marketplace	1
1.1. Prerequisites	1
1.2. Limitations	1
1.3. Deploy Balabit's Privileged Session Management from the Microsoft Azure Marketplace	3
1.4. High Availability and redundancy in Microsoft Azure	5

Preface

This document describes how to deploy Balabit's Privileged Session Management (PSM, formerly called SCB) as a Virtual Machine from the Azure Marketplace.

Chapter 1. Deploying Balabit's Privileged Session Management from the Azure Marketplace

This guide provides detailed descriptions for deploying Balabit's Privileged Session Management (PSM) from the Microsoft Azure Marketplace.

Before you start:

Before you start evaluating PSM, make sure you understand what PSM is and how it works. This information can greatly help you get PSM operational. Read the following:

- [Chapter 1, Introduction](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*
- [Chapter 2, The concepts of PSM](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*

1.1. Prerequisites

The following prerequisites must be met to deploy PSM in Microsoft Azure:

- You have a valid Balabit's Privileged Session Management license. When deployed from the Microsoft Azure Marketplace, the Balabit's Privileged Session Management uses the "Bring your own license" model. Note that to deploy two active PSM nodes as an availability set, you must purchase two standalone PSM licenses. To purchase a license, contact One Identity at <sales@balabit.com>.
- Microsoft recommends to use the *Azure Resource Manager (ARM) deployment model*. When you install PSM from the Azure Marketplace, PSM supports only this deployment method. If you need to deploy PSM into an infrastructure that uses the Classic deployment model, contact your One Identity sales representative.
- You have a Microsoft Azure account.

1.2. Limitations

The following limitations apply to PSM when you deploy it from the Microsoft Azure Marketplace.



Warning

Do not export or import configuration between a physical PSM deployment and a virtual one. Because of the differences and limitations between physical and virtual appliances, configure the virtual appliance from scratch to ensure proper functionality. When you migrate a virtual PSM to another one, you can export and import the configuration.

- Root login is not available on the console.
- SSH access is only available after you have completed the Welcome Wizard.
- Currently, the data that is entered during the provisioning phase (for example username, IP address) of creating the virtual machine in Azure is not transferred to PSM. Therefore, only the data entered in the Welcome Wizard will be used.

- By default, you can only use Physical interface 1 (eth0) of PSM, with a single IP address. Aside from changing the IP address of PSM, do not modify other interface-related settings (additional logical interfaces, IP forwarding, and so on) on the **Basic Settings > Network** page of PSM. The number of interfaces you can use depends on the size of your Azure VM. If your VM allows you to use multiple interfaces, you can configure multiple interfaces in PSM. For details, see [*VM with multiple NICs*](#).
- The **Seal the box** functionality is not available.
- The High Availability support of PSM was designed to work between two physical PSM appliances. This feature is not available in Azure environments. For further details, see [*Section 1.4, High Availability and redundancy in Microsoft Azure \(p. 5\)*](#).
- Due to Azure requirements, an additional 5-minute delay has been added to the boot process. This ensures that the root device appears in the system.
- The size of the hard disk in Azure is 100 Gb. You cannot extend this virtual disk size later, nor can you write to Samba or other disks. In case you run out of disk space, either configure a **Backup policy** and an **Archive policy** if you have a server for this purpose, or configure a **Cleanup policy** that deletes the audit trails at certain time intervals. For details, see [*Section 4.7, Data and configuration backups*](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide* and [*Section 4.8, Archiving and cleanup*](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.
- PSM currently cannot receive its IP address using DHCP. Make sure that:
 - The IP address you have configured in Azure and the IP address that you configure for PSM for the **Physical interface 1** on the Networking settings part of the Welcome Wizard are the same. Otherwise, you will not be able to access PSM.
 - You set the internal IP static on the Network Interfaces tab of the Virtual Machine.
 - Do not assign a public IP address to PSM, use PSM as a component of your internal infrastructure. If you absolutely must configure Welcome Wizard from a publicly accessible IP address, note that PSM will be publicly accessible. If you assign a public IP to the web management interface, consider the following:
 - Select a complex passphrase.
 - Limit access to the management interface based on the source IP address, and make sure that brute-force protection for the administrator web login is enabled (they are enabled by default). For details, see [*Procedure 4.3.1, Configuring user and administrator login addresses*](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.
 - Configure an email alert or SNMP trap for administrator logon events. For details, see [*Procedure 4.5.2, Configuring e-mail alerts*](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide* and [*Procedure 4.5.3, Configuring SNMP alerts*](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.
 - Forward the logs of PSM to a log server (for example, to a [*syslog-ng server, or an syslog-ng Store Box appliance*](#)) so that if the local logs are compromised, you still have an authentic copy of the original logs.
 - For security reasons, disable SSH access to PSM when it is not needed. Accessing the PSM host directly using SSH is not recommended or supported, except for troubleshooting purposes.

If you enable SSH access, restrict the clients that can access PSM based on their source IP address, and make sure that brute-force protection is enabled (they are enabled by default). For details, see [Procedure 6.5.2, Enabling SSH access to the PSM host](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

- To prevent unauthorized access to the audit trail files recorded on PSM, configure proper access control rules for the user groups and encrypt every audit trail. If you use encryption, store your keys in the personal or in the temporary key store. For details, see [Procedure 7.10.1, Encrypting audit trails](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*,
- Upgrading PSM in Azure is the same as upgrading a physical appliance: you have to upload the firmware on the PSM web interface. For detailed instructions, see [How to upgrade to Balabit's Privileged Session Management 5 LTS](#).

1.3. Procedure – Deploy Balabit's Privileged Session Management from the Microsoft Azure Marketplace

Purpose: To have a Balabit's Privileged Session Management running in Microsoft Azure, complete the following steps.

Steps:

Step 1. **Deploy Balabit's Privileged Session Management from the Microsoft Azure Marketplace.** Create and configure a Balabit's Privileged Session Management virtual machine (VM) in the Azure portal. For details, see the [Microsoft Azure documentation](#), here we just describe the PSM-specific settings.

Step a. [Login to the Azure portal](#), select **Shell Control Box** from the Azure Marketplace, then click **Create**.

Step b. Fill the required fields of the **Basics** blade. Note that you must fill the **User name** and **Authentication Password/SSH public key** fields, but PSM will not actually use these settings (PSM will use the parameters you configure in the PSM Welcome Wizard).

Step c. Choose a size for the VM. If you want to use this machine in production and need help about sizing or architecture design, contact your One Identity sales representative. The number of interfaces you can use depends on the size of your Azure VM. If your VM allows you to use multiple interfaces, you can configure multiple interfaces in PSM. For details, see [VM with multiple NICs](#).

Step d. On the **Settings** blade, disable monitoring.

Step e. When the deployment is finished, navigate to the network settings of the new VM in the Azure portal. Change the IP address of the PSM network interface to Static, and note down the IP address and the hostname (you will need it in the PSM Welcome Wizard).

Step f. If you want to backup or archive data from PSM into Azure, [create an Azure File Share](#). Note down the following information of the file share, because you will need it to configure PSM backups and archiving: URL, Username, Password.

**Warning**

If you have multiple PSM VMs, make sure to use a separate file share for each PSM.

Step 2. Complete the PSM Welcome Wizard. Complete the PSM Welcome Wizard (for details, see [Procedure 3.2, Configuring PSM with the Welcome Wizard](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*). Note the following points specific for Azure deployments. When configuring the network settings of PSM note the following points.

**Warning**

Do not export or import configuration between a physical PSM deployment and a virtual one. Because of the differences and limitations between physical and virtual appliances, configure the virtual appliance from scratch to ensure proper functionality. When you migrate a virtual PSM to another one, you can export and import the configuration.

Step a. Into the **Physical interface EXT or 1 — IP address** field, enter the static IP address of the PSM VM that you set on the Azure portal.

Step b. Default GW: The default gateway is usually the first address in a subnet (for example, if your subnet is 10.7.0.0/24, then the gateway will be 10.7.0.1).

Step c. Hostname: Use the hostname you have configured for the PSM VM on the Azure portal.

Step d. DNS server: You can use any DNS server that the PSM VM can access, even public ones.

Step 3. Configure PSM. Login to PSM and configure it.

Step a. Configure backups for PSM. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see [Section 4.7, Data and configuration backups](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

Step b. Configure archiving for PSM. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see [Section 4.8, Archiving and cleanup](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*. Configuring Archiving policy is highly recommended: because if the disk of the VM fills up, PSM stops working.

Step c. Configure a server: set up a host that is on the same subnet as PSM, and enable Remote Desktop (RDP) or Secure Shell (SSH) access to it.

Step d. Configure a connection on PSM to forward the incoming RDP or Secure Shell (SSH) connection to the host and establish a connection to the host. See [Procedure 3.3, Logging in to PSM and configuring the first connection](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide* for details.

Step e. Replay your session in the browser. See [Procedure 16.1.2, Replaying audit trails in your browser](#) in *The Balabit's Privileged Session Management 5 LTS Administrator Guide* for details.

In case you have questions about PSM, or need assistance, contact your One Identity representative.

1.4. High Availability and redundancy in Microsoft Azure

In a Microsoft Azure deployment, the high-availability and redundancy of the PSM appliance is provided by the Microsoft Azure infrastructure, according to the [Azure Storage SLA](#).

Redundancy

The data in your Microsoft Azure storage account is always replicated to ensure durability and high availability, meeting the Azure Storage SLA. The exact type of replication depends on your storage account settings, but every disk is stored in 3 copies.

For details, see [Locally redundant storage](#) in the *Azure Storage replication* document, and [Service Healing - Auto-recovery of Virtual Machines](#).

High Availability

If a hardware failure occurs, Azure moves the Virtual Machine to another location and restarts it in 5-15 minutes. In case you require higher SLA, you are recommended to deploy two standalone PSM nodes into an availability set. Note that to deploy two active PSM nodes as an availability set, you must purchase two standalone PSM licenses.

For details, see [Locally redundant storage](#) in the *Azure Storage replication* document, and [Service Healing - Auto-recovery of Virtual Machines](#).