One Identity Safeguard for Privileged Sessions 5.11

Azure Reference Guide

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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.**

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

SPS Azure Reference Guide
Updated - April 2019
Version - 5.11

Contents

Deploying One Identity Safeguard for Privileged Sessions from the Azure Marketplace

This guide provides detailed descriptions for deploying One Identity Safeguard for Privileged Sessions (SPS) from the Microsoft Azure Marketplace.

Before you start:

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

- "Introduction" in the Administration Guide
- "The concepts of SPS" in the Administration Guide

Prerequisites

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

- You have a valid One Identity Safeguard for Privileged Sessions license. When deployed from the Microsoft Azure Marketplace, the One Identity Safeguard for Privileged Sessions uses the "Bring your own license" model. Note that to deploy two active SPS nodes as an availability set, you must purchase two standalone SPS licenses. To purchase a license, contact our Sales Team.
- Microsoft recommends to use the Azure Resource Manager (ARM) deployment model. When you install SPS from the Azure Marketplace, SPS supports only this deployment method. If you need to deploy SPS into and infrastructure that uses the Classic deployment model, contact your One Identity sales representative.
- You have a Microsoft Azure account.

Limitations

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

⚠ **CAUTION:**

Do not export or import configuration between a physical SPS 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 SPS 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 SPS. Therefore, only the data entered in the Welcome Wizard will be used.
- By default, you can only use Physical interface 1 (eth0) of SPS, with a single IP address. Aside from changing the IP address of SPS, do not modify other interface-related settings (additional logical interfaces, IP forwarding, and so on) on the **Basic Settings > Network** page of SPS.

  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 SPS. For details, see VM with multiple NICs.
- The **Seal the box** functionality is not available.
- The High Availability support of SPS was designed to work between two physical SPS appliances. This feature is not available in Azure environments. For further details, see the High Availability and redundancy in Microsoft Azure.
- 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 "Data and configuration backups" in the Administration Guide and "Archiving and cleanup" in the Administration Guide.
- SPS 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 SPS 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 SPS.
  - You set the internal IP static on the Network Interfaces tab of the Virtual

Machine.

- Do not assign a public IP address to SPS, use SPS as a component of your internal infrastructure. If you absolutely must configure Welcome Wizard from a publicly accessible IP address, note that SPS 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 "Configuring user and administrator login addresses" in the Administration Guide.
    - Configure an email alert or SNMP trap for administrator logon events. For details, see "Configuring e-mail alerts" in the Administration Guide and "Configuring SNMP alerts" in the Administration Guide.
    - Forward the logs of SPS 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 SPS when it is not needed. Accessing the SPS host directly using SSH is not recommended or supported, except for troubleshooting purposes. If you enable SSH access, restrict the clients that can access SPS based on their source IP address, and make sure that brute-force protection is enabled (they are enabled by default). For details, see "Enabling SSH access to the SPS host" in the Administration Guide.
    - To prevent unauthorized access to the audit trail files recorded on SPS, 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 "Encrypting audit trails" in the Administration Guide,

- Upgrading SPS in Azure is the same as upgrading a physical appliance: you have to upload the firmware on the SPS web interface. For detailed instructions, see Upgrade Guide.

Deploy One Identity Safeguard for Privileged Sessions from the Microsoft Azure Marketplace

Purpose:

The following describes how to have a One Identity Safeguard for Privileged Sessions running in Microsoft Azure.

To have a One Identity Safeguard for Privileged Sessions running in Microsoft Azure

1. **Deploy One Identity Safeguard for Privileged Sessions from the Microsoft Azure Marketplace**

   Create and configure a One Identity Safeguard for Privileged Sessions virtual machine (VM) in the Azure portal. For details, see the Microsoft Azure documentation, here we just describe the SPS-specific settings.

   a. Login to the Azure portal, select **One Identity Safeguard for Privileged Sessions** from the Azure Marketplace, then click **Create**.

   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 SPS will not actually use these settings (SPS will use the parameters you configure in the SPS Welcome Wizard).

   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 SPS. For details, see VM with multiple NICs.

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

   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 SPS network interface to Static, and note down the IP address and the hostname (you will need it in the SPS Welcome Wizard).

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

      > ⚠ **CAUTION:**
      >
      > **If you have multiple SPS VMs, make sure to use a separate file share for each SPS.**

2. **Complete the SPS Welcome Wizard**

   Complete the SPS Welcome Wizard (for details, see "Configuring SPS with the Welcome Wizard" in the Administration Guide). Note the following points specific for Azure deployments. When configuring the network settings of SPS note the following points.

> ⚠ **CAUTION:**
>
> **Do not export or import configuration between a physical SPS 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 SPS to another one, you can export and import the configuration.**

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

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`).

c. **Hostname**: Use the hostname you have configured for the SPS VM on the Azure portal.

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

3. Configure SPS

Login to SPS and configure it.

a. Configure backups for SPS. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see "Data and configuration backups" in the Administration Guide.

b. Configure archiving for SPS. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see "Archiving and cleanup" in the Administration Guide. Configuring Archiving policy is highly recommended: because if the disk of the VM fills up, SPS stops working.

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

d. Configure a connection on SPS to forward the incoming RDP or Secure Shell (SSH) connection to the host and establish a connection to the host. See "Logging in to SPS and configuring the first connection" in the Administration Guide for details.

e. Replay your session in the browser. See "Replaying audit trails in your browser in Search (classic)" in the Administration Guide for details.

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

High Availability and redundancy in Microsoft Azure

In a Microsoft Azure deployment, the high-availability and redundancy of the SPS 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 SPS nodes into an availability set. Note that to deploy two active SPS nodes as an availability set, you must purchase two standalone SPS licenses.

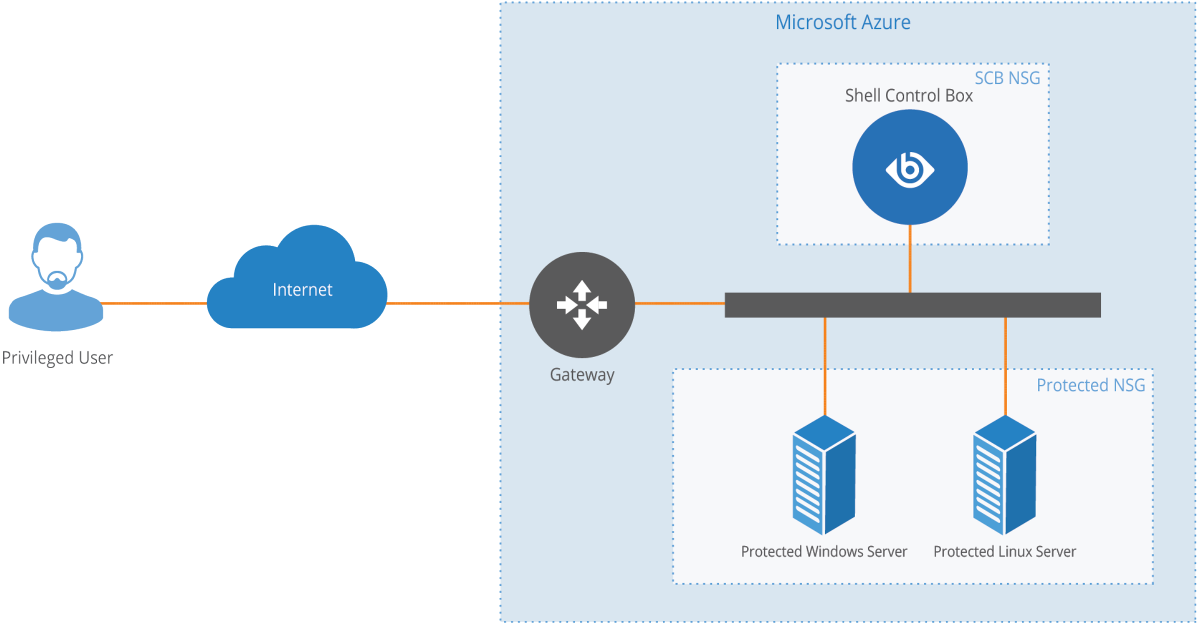
For details, see Locally redundant storage in the *Azure Storage replication* document, and Service Healing - Auto-recovery of Virtual Machines.

Architectural best practices

You can select several configuration options when installing Shell Control Box into Azure. This section will discuss two deployment models: Advanced Resource Manager (ARM) and Classic. Although, SCB can be installed using the ARM model only, you will be able to monitor virtual machines deployed in the Classic model too. The example architectures for both deployment models are described below:

Example architecture for monitoring virtual machines deployed with the ARM deployment model

Figure 1: ARM deployment model



Goal

Protect and audit every remote access connection (RDP and SSH) coming from the Internet and targeting the protected servers, deployed in the ARM model.

Network settings

Public IP addresses:

Every virtual machine has the same public IP address.

Private IP addresses:

Table 1: System related traps

Machine	IP	Subnet
Shell Control Box	10.0.0.10	10.0.0.0/24
Private Windows Server	10.0.0.20	10.0.0.0/24
Private Linux Server	10.0.0.30	10.0.0.0/24

Network Security Group (NSG) rules:

Table 2: SCB NSG

SCB NSG			
From	*Port*	*Verdict*	*Description*
Any	22	Allow	SSH connection to the Protected Linux Server
Any	3389	Allow	RDP connection to the Protected Windows Server
Any	443	Allow	SCB Web GUI
Any	Any	Deny	Any other connection is denied

Table 3: Protected NSG

Protected NSG			
From	*Port*	*Verdict*	*Description*
Any	80	Allow	HTTP service listening on the Protected Linux Server
Any	8080	Allow	HTTP service listening on the Protected Windows Server
10.0.0.10/32	22	Allow	SSH service listening on the Protected Linux Server only allowed from SCB

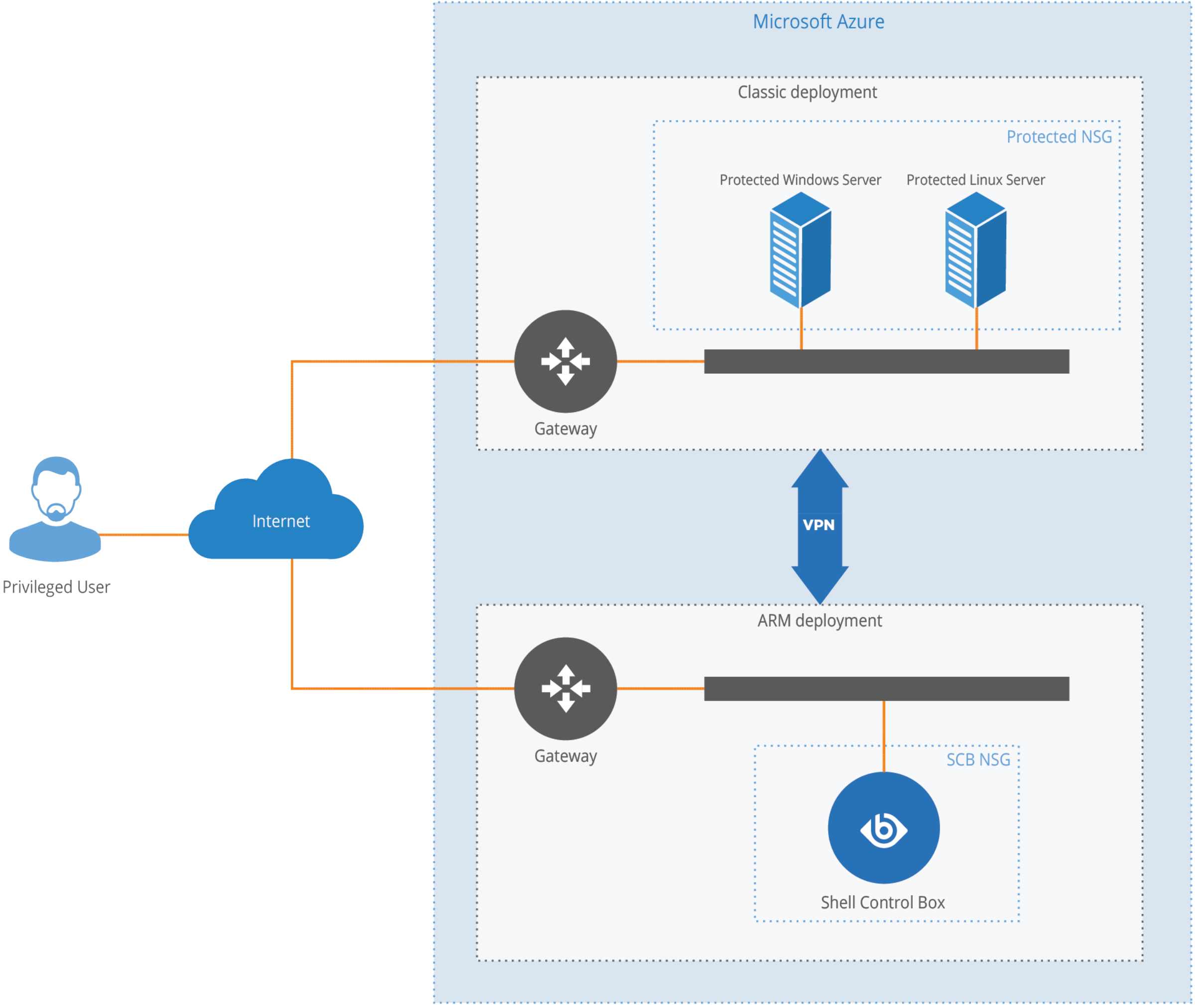
Protected NSG			
10.0.0.10/32	3389	Deny	RDP service listening on the Windows Server only allowed from SCB
Any	Any	Deny	Any other connection is denied

Description

On the two protected servers HTTP services (for example APIs) are running. This example focuses on remote connections, therefore the HTTP services are not audited by SCB. Every incoming RDP and SSH connection will reach SCB, as the NSGs are forcing them. SCB has a configured connection for each protected server. This way, every remote access will be controlled and audited by SCB.

Example architecture for monitoring virtual machines deployed with the Classic deployment model

Figure 2: Classic deployment model



Goal

Protect and audit every remote access connection (RDP and SSH) coming from the Internet and targeting the protected servers, deployed in the Classic model.

Network settings

Public IP addresses:

There is 1 public IP address in every deployment model.

Private IP addresses:

Table 4: System related traps

Machine	IP	Subnet
Shell Control Box	10.0.0.10	10.0.0.0/24
Private Windows Server	10.0.10.20	10.0.10.0/24
Private Linux Server	10.0.10.30	10.0.10.0/24

Network Security Group (NSG) rules:

Table 5: SCB NSG

SCB NSG			
From	*Port*	*Verdict*	*Description*
Any	22	Allow	SSH connection to the Protected Linux Server
Any	3389	Allow	RDP connection to the Protected Windows Server
Any	443	Allow	SCB Web GUI
Any	Any	Deny	Any other connection is denied

Table 6: Protected NSG

Protected NSG			
From	*Port*	*Verdict*	*Description*
Any	80	Allow	HTTP service listening on the Protected Linux Server
Any	8080	Allow	HTTP service listening on the Protected Windows Server
10.0.0.10/32	22	Allow	SSH service listening on the Protected Linux Server only allowed from SCB
10.0.0.10/32	3389	Deny	RDP service listening on the Windows Server only allowed from SCB
Any	Any	Deny	Any other connection is denied

Description

This example architecture is a little bit tricky, because SCB can be deployed in ARM model only, but the two protected servers are operating in a Classic deployment. The only solution for this issue is to connect the two Azure virtual networks (VNets) with a VPN connection. This secure connection will travel across the Microsoft Network only, not the Internet (for a detailed tutorial on how to create it and its limitations, see: Connect virtual networks from different deployment models in the portal). On the two protected servers HTTP services (for example APIs) are running.

This example focuses on remote connections, therefore the HTTP services are not audited by SCB. Every incoming RDP and SSH connection will reach SCB, as the NSGs are forcing them. SPS has a configured connection for each protected server. This way, every remote access will be controlled and audited by SCB.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

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 at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product