Deploying syslog-ng Store Box 5 LTS on Microsoft Azure

June 27, 2018

Table of Contents

1. Introduction

The aim of this guide is to provide detailed, step-by-step instructions on how to set up and install syslog-ng Store Box in a Microsoft Azure virtual environment.

The document comprises the following sections:

- *Section 2, Prerequisites (p. 4)* collects the requirements that you must comply with before deploying SSB on Microsoft Azure.
- *Section 3, Limitations (p. 5)* lists the limitations that apply when installing SSB in a Microsoft Azure virtual environment.
- *Section 4, Deploying SSB on Microsoft Azure (p. 6)* describes how to install SSB in a Microsoft Azure virtual environment.

2. Prerequisites

The following prerequisites must be met before deploying SSB on Microsoft Azure:

- You have a valid Balabit syslog-ng Store Box license.
  syslog-ng Store Box uses the "Bring your own license" model. Note that to deploy two active SSB nodes as an availability set, you must purchase two standalone SSB licenses. To purchase a license, contact Balabit at <sales@balabit.com>.
- You have a Microsoft Azure account.
- You have secure access to your Microsoft Azure Virtual Network resources, for example, through the use of a Virtual Private Network (VPN).
- You have working knowledge of the SSB installation process.
- You are familiar with Microsoft Azure.

3. Limitations

The following limitations apply when deploying SSB on Microsoft Azure:

- SSB High Availability operation mode is not available. If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- Hardware-related alerts and status indicators of SSB may display inaccurate information, for example, display degraded RAID status.
- When running SSB in a virtual environment, it is sufficient to use a single network interface.
- During Microsoft Azure installation, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.
- By default, the disk size of the virtual disk is 10 GiB. If you want to increase the disk size later, see *Chapter 8, Increasing the virtual disk size of SSB under a virtual machine* in *The syslog-ng Store Box 5 LTS Installation Guide*.
- SSB only supports the use of OS disks. It does not support the use of data disks or temporary disks and therefore these cannot be used.

4. Deploying SSB on Microsoft Azure

If you require detailed information about installing the virtual machine, uploading the VHD, or using Microsoft Azure in general consult the following guide: *Create a Linux VM from custom disk with the Azure CLI 2.0* or, check out the How-to guides under the same link.

This guide only focuses on uploading the VHD and installing SSB.

Warning
Hazard of security breach!

During Microsoft Azure installation, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.

4.1. Procedure – Uploading the VHD to Microsoft Azure

Purpose:

To download the `.vhd` file and upload it to Microsoft Azure, complete the following steps.

To use the VHD to create a new Azure VM, you will need to upload the VHD to a storage account and create a managed disk from the VHD.

Steps:

Step 1. Log on to MyBalabit with your credentials.

Step 2. Navigate to **MyBalabit** > **Download** > **syslog-ng Store Box**. Select **Release** `5 LTS`, **Component** `syslog-ng Store Box`, **Revision** `5.0` and download `ssb <full_version_number> compressed VHD disk image`, that is a `.zip` file.
Extract the `.zip` file to the directory of your choice. The extracted file will be `ssb-<full_version_number>.vhd`.

Step 3. Download and install azure-cli from *GitHub - azure-cli*.
You will use the `az` command and its parameters to create all the required prerequisites for uploading the VHD to Microsoft Azure.

Step 4. **Create a resource group:**

```
az group create \
    --name <resource_group_name> \
    --location <resource_group_region>
```

Where:

- `--name`: Name your resource group. For example, `MyResourceGroup`.
- `--location`: The region of the resource group. For example, `westus`.

For details on the command and its parameters, see *az group create*.

Step 5. **Create a storage account:**

```
az storage account create \
    --name <storage_account_name> \
    --resource-group <resource_group_name> \
    --location <storage_account_location> \
    --kind Storage \
    --sku Standard_LRS
```

Where:

- `--name`: Name your storage account. For example, `myStorageAccount`.
- `--resource-group`: The name of the resource group in which you create the storage account. For example, `MyResourceGroup`.
- `--location`: The region of the storage account, but only what is permitted by the resource group. For example, `westus`.
- `--kind`: The type of storage account. You will create a storage, so enter `Storage`, which is the default value.
- `--sku`: The storage account SKU. `Standard_LRS` is a standard, HDD-type storage.

For details on the command and its parameters, see *az storage account create*.

Step 6. **List the storage account keys:**
Save one of these keys for later, because you will need it during the upload process:

```
az storage account keys list \
    --resource-group <resource_group_name> \
    --account-name <storage_account_name>
```

Where:

- `--resource-group`: The name of the resource group in which you have created the storage account. For example, `myResourceGroup`.
- `--account-name`: The name of the storage account. For example, `MyStorageAccount`.

For details on the command and its parameters, see *az storage account keys list*.

Step 7. **Create a storage container inside the storage account:**
You will upload the VHD into this container:

```
az storage container create \
    --name <container_name> \
    --account-name <storage_account_name>
```

Where:

- `--name`: Name your storage container. For example, `MyStorageContainer`.
- `--account-name`: The name of the storage account. For example, `MyStorageAccount`.

For details on the command and its parameters, see *az storage container create*.

Step 8. **Upload the VHD file to the storage container:**

```
az storage blob upload \
    --name <name_of_uploaded_vhd> \
    --account-name <storage_account_name> \
    --account-key <storage_account_key> \
    --container-name <container_name> \
    --type page \
    --file <path_to_local_vhd_file>
```

Where:

- `--name`: Name your blob, that is, the upload VHD. For example, `MyBlob`.
- `--account-name`: The name of the storage account. For example, `MyStorageAccount`.
- `--account-key`: The storage account key that you have saved before.
- `--containername`: The name of the storage container. For example, `MyStorageContainer`.
- `--type`: Defaults to `page` for `.vhd` files.
- `--file`: Path of the file to upload as the blob content. For example, `path/to/ssb-<full_version_number>.vhd`.

For details on the command and its parameters, see *az storage blob upload*.

4.2. Procedure – Creating a Virtual Machine in Microsoft Azure

Step 1. **Create a virtual network with subnet:**

```
az network vnet create
    --name <virtual_network_name> \
    --resource-group <resource_group_name>
```

Where:

- `--name`: Name your virtual network. For example, `MyVnet`.
- `--resource-group`: The name of the resource group in which you have created the storage account. For example, `myResourceGroup`.

For details on the command and its parameters, see *az network vnet create*.

Step 2. *Optional Step:*
Create a network security group:

You can define firewall rules in the network security group.

```
az network nsg create \
    --name <security_group_name> \
    --resource-group <resource_group_name> \
    --location <location>
```

Where:

- `--name`: Name your network security group. For example, `MyNsg`.

- `--resource-group`: The name of the resource group in which you have uploaded the VHD. For example, `MyResourceGroup`.
- `--location`: The region of the storage account, but only what is permitted by the resource group. For example, `westus`.

For details on the command and its parameters, see *az network nsg create*.

Step 3. **Create a network interface:**

Warning
Hazard of security breach!

During Microsoft Azure installation, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.

```
az network nic create \
    --name <network_interface_name> \
    --resource-group <resource_group_name> \
    --location <location> \
    --vnet-name <virtual_network_name> \
    --network-security-group <security_group_name> \
    --subnet <subnet_name> \
```

Where:

- `--name`: Name your network interface. For example, `MyNic`.
- `--resource-group`: The name of the resource group in which you have uploaded the VHD. For example, `MyResourceGroup`.
- `--location`: The region of the storage account, but only what is permitted by the resource group. For example, `westus`.
- `--vnet-name`: The name of the virtual network. For example, `MyVnet`.
- `--network-security-group`: If you have created one, the name of the network security group. For example, `MyNsg`.
- `--subnet`: The name of the subnet. If you have not defined any, the default is `Subnet`.

For details on the command and its parameters, see *az network nic create*.

Step 4. **Create a managed disk:**
This will be the OS disk in the virtual machine.

```
az disk create \
    --name <disk_name> \
    --resource-group <resource_group_name> \
    --source <uri_of_vhd> \
    --sku Standard_LRS \
    --size-gb <disk_size_in_GiB>
```

Where:

- `--name`: Name your managed disk. For example, `MyDisk`.
- `--resource-group`: The name of the resource group in which you have uploaded the VHD. For example, `MyResourceGroup`.
- `--source`: The path to the uploaded VHD on the storage. It will look like the following:
  - The path will have the following structure: `https://<storage_account_name>.blob.core.windows.net/<storage_container_name>/<name_of_uploaded_vhd>`.
  - For example, `https://MyStorageAccount.blob.core.windows.net/MyStorageContainer/MyBlob`.
- `--sku`: The storage account SKU. Select `Standard_LRS` for a standard, HDD-type storage, or `Premium_LRS` for an SSD-type storage. In case of smaller or cheaper virtual machines (for example, Basic A, you can only select `Standard_LRS`).
- `--size-gb`: *Optional*. The size of the disk in GiB. The default value is `10`, the original size of the VHD. You can try SSB with the default disk size, however, for production purposes it is advised to increase the disk size. The maximum value is `4095`.
  If you want to increase the disk size later, see *Chapter 8, Increasing the virtual disk size of SSB under a virtual machine* in *The syslog-ng Store Box 5 LTS Installation Guide*. You cannot decrease the disk size later.

Note
The value you enter cannot be less than the default size of the VHD, which is `10`.

For details on the command and its parameters, see *az disk create*.

Step 5. **Create the virtual machine:**
After preparing all prerequisite resources, you will create the virtual machine:

```
az vm create \
    --name <vm_name> \
    --resource-group <resource_group_name> \
    --nics <network_interface_name> \
    --attach-os-disk <disk_name> \
    --size <size_of_virtual_machine> \
    --os-type Linux
```

Where:

- `--name`: Name your virtual machine. For example, `MyVm`.
- `--resource-group`: The name of the resource group in which you have uploaded the VHD. For example, `MyResourceGroup`.
- `--nics`: The name of the network interface. For example, `MyNic`.
- `--attach-os-disk`: The name of the managed disk. For example, `MyDisk`.
- `--size`: The calculated size of the virtual machine. For example, `Standard_A4_v2`.
  To calculate the size of the virtual machine, consider the following:

- The available virtual machine sizes may vary based on region and your Azure subscription. For details on virtual machine sizing, see *General purpose* or scroll down to **Other sizes** to check the available optimized machines.
- Minimum size: a virtual machine with at least 2 GB memory, for example: `Standard_A1_v2`.
- Recommended size: a virtual machine with at least 8 GB memory, for example: `Standard_A4_v2`.

- `--os-type`: The type of the operating system. Enter `Linux`.

After creating the virtual machine, it will automatically start up, boot, and is available through the private network.

For details on the command and its parameters, see *az vm create*.

Step 6. The Welcome Wizard starts. For details on the initial steps of configuring SSB, see *Chapter 3, The Welcome Wizard and the first login* in *The syslog-ng Store Box 5 LTS Administrator Guide*.

Warning
Hazard of security breach!

During the configuration process of the Welcome Wizard, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.

Note
If you have installed SSB from Azure, the swap column is not available on the system monitor, because in this case, swap memory is not used.