Pexip Infinity and Microsoft Azure Deployment Guide

Contents

Introduction 1
Deployment guidelines 2
Configuring Azure Network Security Groups 4
Creating VM instances in Azure 5
Obtaining and preparing disk images for Azure deployments 7
Deploying a Management Node in Azure 10
Deploying a Conferencing Node in Azure 12
Managing Azure instances 14

Introduction

The Microsoft Azure Virtual Machines (VMs) service provides scalable computing capacity in the Microsoft Azure cloud. Using Azure eliminates your need to invest in hardware up front, so you can deploy Pexip Infinity even faster.

You can use Azure to launch as many or as few virtual servers as you need, and use those virtual servers to host a Pexip Infinity Management Node and as many Conferencing Nodes as required for your Pexip Infinity platform.

Azure enables you to scale up or down to handle changes in requirements or spikes in conferencing requirements. You can also use the Azure APIs and the Pexip Infinity management API to monitor usage and bring up / tear down Conferencing Nodes as required to meet conferencing demand.

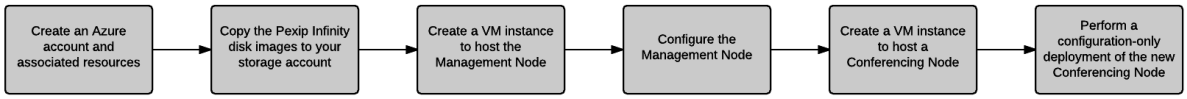
Pexip publishes disk images for the Pexip Infinity Management Node and Conferencing Nodes. These images may be used to launch instances of each node type as required.

© 2016 Pexip AS

Deployment guidelines

This section summarizes the Azure deployment options and limitations, and provides guidance on our recommended Azure instance types, security groups and IP addressing options.

This flowchart provides an overview of the basic steps involved in deploying the Pexip Infinity platform on Azure:



Deployment models

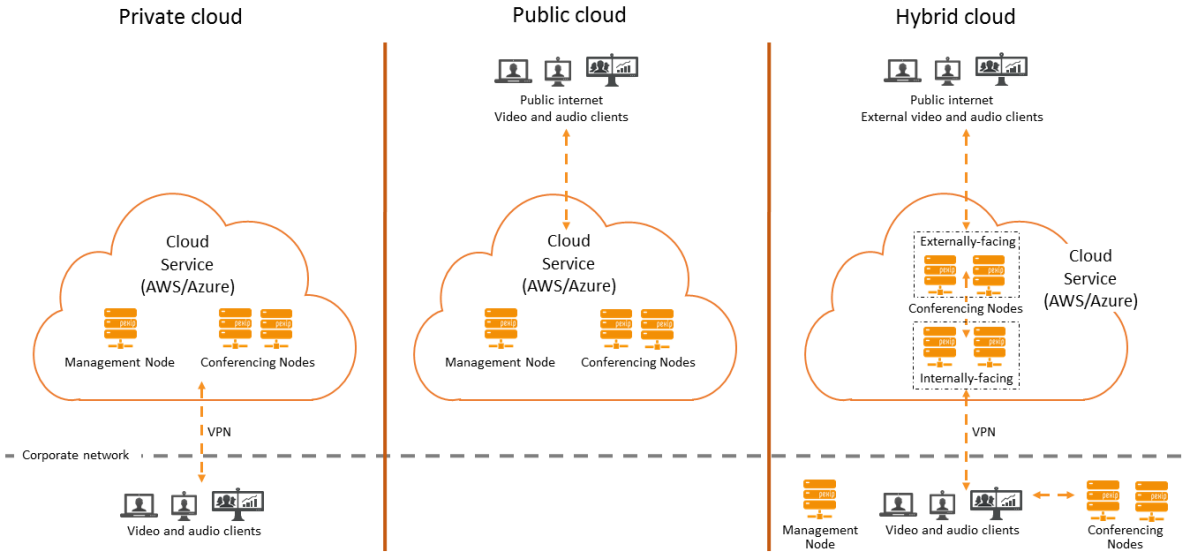
Azure has two deployment models: Classic and Resource Manager.

Resource Manager is the recommended deployment model for new workloads and is the only model supported by Pexip Infinity.

Deployment options

There are three main deployment options for your Pexip Infinity platform when using the Azure cloud:

- **Private cloud**: all nodes are deployed within Azure. Private addressing is used for all nodes and connectivity is achieved by configuring a VPN tunnel from the corporate network to Azure. As all nodes are private, this is equivalent to an on-premises deployment which is only available to users internal to the organization.
- **Public cloud**: all nodes are deployed within Azure. All nodes have a private address but, in addition, public IP addresses are allocated to each node. The node's private addresses are only used for inter-node communications. Each node's public address is then configured on the relevant node as a static NAT address. Access to the nodes is permitted from the public internet, or a restricted subset of networks, as required. Any systems or endpoints that will send signaling and media traffic to those Pexip Infinity nodes must send that traffic to the public address of those nodes. If you have internal systems or endpoints communicating with those nodes then you must ensure that your local network allows this.
- **Hybrid cloud**: the Management Node, and optionally some Conferencing Nodes, are deployed in the corporate network. A VPN tunnel is created from the corporate network to Azure. Additional Conferencing Nodes are deployed in Azure and are managed from the on-premises Management Node. The Azure-hosted Conferencing Nodes can be either internally-facing, privately-addressed (private cloud) nodes; or externally-facing, publicly-addressed (public cloud) nodes; or a combination of private and public nodes (where the private nodes are in a different Pexip Infinity system location to the public nodes).



Limitations

The following limitations currently apply:

- The OS username is always **admin**, regardless of any other username configured through the Azure Portal.
- SSH keys are the preferred authentication mechanism for Pexip Infinity instances hosted in the Azure Cloud. Password-based authentication also works, however, and will use the password provisioned at instance deployment time.

  Note that:
  - Pexip Infinity node instances only support a single SSH key pair.
  - If you are using a Linux or Mac SSH client to access your instance you must use the **chmod** command to make sure that your private key file on your local client (SSH private keys are never uploaded) is not publicly viewable. For example, if the name of your private key file is my-key-pair.pem, use the following command: `chmod 400 /path/my-key-pair.pem`

  See https://azure.microsoft.com/en-gb/documentation/articles/virtual-machines-linux-ssh-from-windows/ for more information about using SSH on Azure.

Recommended instance types and call capacity guidelines

Azure instances come in many different sizes. In general, Pexip Infinity Conferencing Nodes should be considered compute intensive and Management Nodes reflect a more general-purpose workload.

For deployments of up to 20 Conferencing Nodes, we recommend using:

- a **Standard A2** instance for a Management Node
- a **Standard D4 v2** instance for Conferencing Nodes

This should provide capacity for approximately 15 HD / 36 SD / 180 audio-only calls per Conferencing Node.

Capacity planning

By default, Azure Resource Manager limits each location to a maximum of 10 CPU cores per core type. This quota is shared among all instances of that core type in the location. Standard D4 v2 instances use 8 CPU cores of type Dv2. Thus, with the default limits in place, only a single Standard D4 v2 instance may be deployed (as only 2 CPU cores will remain in the quota pool, which is insufficient for another Standard D4 v2 instance).

The allocated quota may be increased by opening a support ticket with Microsoft via the Azure Portal. Ensure that you request a sufficient number of CPU cores for the relevant core type. For example, if 10 Conferencing Nodes are required, then the quota must be increased to 8 cores x 10 Standard D4 v2 instances = 80 CPU cores of type Dv2. It may take a number days for the quota increase request to be processed.

IP addressing

Within a Virtual Network, private IP addresses may be allocated dynamically (using DHCP) or statically, by defining an instance's IP address at launch time. After a private IP address has been assigned to an instance, it will remain associated with that instance until the instance is terminated. The allocated IP address is displayed in the Azure portal.

Public IP addresses may be associated with an instance. Public IPs may dynamic (allocated at launch/start time) or statically configured. Dynamic public IP addresses do not remain associated with an instance if it is stopped — and thus it will receive a new public IP address when it is next started.

Pexip Infinity nodes must always be configured with the private IP address associated with its instance. To associate the instance's public IP address with the node, configure that public IP address as the node's **Static NAT address** (via **Platform Configuration > Conferencing Nodes**).

Assumptions and prerequisites

The deployment instructions assume that within Azure you have already:

- signed up for Azure and created a user account, administrator groups etc.
- decided in which Azure location to deploy your Pexip Infinity platform (one Management Node and one or more associated Conferencing Nodes)
- created a Resource Group, Virtual Network, and Storage Account in the chosen Azure location
- (if necessary) configured a VPN tunnel from the corporate/management network to the Azure Virtual Network
- created a Network Security Group (see Configuring Azure Network Security Groups for port requirements)

For more information on setting up your Azure Virtual Machine environment, see https://azure.microsoft.com/en-gb/documentation/articles/virtual-machines-linux-about/.

Pexip Infinity node instances that are hosted on Azure may be deployed across multiple Azure Virtual Networks (VNets), where each Azure VNet (and the Conferencing Nodes within it) maps onto a Pexip Infinity system location. See https://azure.microsoft.com/en-gb/documentation/articles/vpn-gateway-howto-vnet-vnet-resource-manager-portal/ for information about how to create a connection between VNets in the Resource Manager deployment model by using VPN Gateway and the Azure portal.

To look at a detailed worked example of the steps required to set up your Microsoft Azure environment and deploy Pexip Infinity, see http://www.graham-walsh.com/2016/05/deploying-pexip-azure-part-one/.

Configuring Azure Network Security Groups

Access to Azure instances is restricted by the Azure firewall. This may be configured by associating a subnet or instance with a Network Security Group which specifies the permitted inbound and outbound traffic from the group.

A minimal security group that permits access to a public cloud style Pexip Infinity deployment would look similar to this:

Inbound security rules

Priority	Name	Source	Destination	Service	Action
105	HTTP	Any	Any	TCP/80	Allow
110	HTTPS	Any	Any	TCP/443	Allow
115	H.323 CS	Any	Any	TCP/1720	Allow
120	SIP TCP	Any	Any	TCP/5060	Allow
125	SIP TLS	Any	Any	TCP/5061	Allow
130	TCP call signaling	Any	Any	TCP/33000-39999	Allow
135	TCP call media	Any	Any	TCP/40000-49999	Allow
140	H.323 LS	Any	Any	UDP/1719	Allow
145	SIP UDP *	Any	Any	UDP/5060	Allow
150	UDP call signaling	Any	Any	UDP/33000-39999	Allow
155	UDP call media	Any	Any	UDP/40000-49999	Allow
160	Management traffic	CIDR block: <management station IP address/subnet>	Any	Any/Any	Allow

* only required if you intend to enable SIP over UDP

Where **Any** implies any source/destination and **<management station IP address/subnet>** should be restricted to a single IP address or subnet for management access only.

Outbound security rules

The default network security group rules suffice. These permit outbound traffic to the same Virtual Network, or to the Internet.

A single security group can be applied to the Management Node and all Conferencing Nodes. However, if you want to apply further restrictions to your Management Node (for example, to exclude the TCP/UDP signaling and media ports), then you can configure additional security groups and use them as appropriate for each Azure instance.

Remember that the Management Node and all Conferencing Nodes must be able to communicate with each other. If your instances only have private addresses, ensure that the necessary external systems such as NTP and DNS servers are routable from those nodes.

For further information on the ports and protocols specified here, see Pexip Infinity port usage guide.

Azure Resource Manager (ARM) templates for deploying a security group

Pexip provides two ARM templates — one with, and one without, SIP UDP access enabled — which may be used to deploy a security group containing the above rules. These templates may be used from PowerShell or the Azure CLI. Alternatively, you may use the Azure Portal to deploy a security group using the relevant template.

The details of each template are as follows. You should pick the one most suitable for your needs.

Name	SIP UDP access	Template URL	Resources created
security-group	Disabled	https://pexipas.blob.core.windows.net/templates/20160330/security-group.json (launch in Azure Portal)	Network security group
security-group-with-sip-udp	Enabled	https://pexipas.blob.core.windows.net/templates/20160330/security-group-with-sip-udp.json (launch in Azure Portal)	Network security group

Both templates contain the following parameters:

Name	Description
managementNetwork	Network from which to permit management traffic (CIDR notation e.g. 1.2.3.4/28).
securityGroupName	Name of the security group to create.

Creating VM instances in Azure

To deploy a Pexip Infinity Management Node or a Conferencing Node within Azure you must create an Azure VM instance and then use that instance to host that Pexip node.

This section describes how to create a VM instance from a prepared disk image. You must create a separate VM instance for each Pexip node.

Note that you must deploy the Management Node in your Pexip Infinity platform before deploying any Conferencing Nodes.

Creating a VM instance

To create a VM instance in Azure (for either the Management Node or a Conferencing Node):

1. In the same storage account that contains the prepared disk images, create a new **storage container** to hold the instance disk.
2. Create a new **resource group** to hold the instance.

   Each VM instance (i.e. the Management Node and each Conferencing Node) must be deployed in its own storage container and its own resource group.
3. Deploy the instance into the new storage container and resource group.

   This procedure describes how to do this via the Azure portal using an ARM template provided by Pexip.

   a. Decide which ARM template to use from the table below, and then use the "launch in Azure Portal" link to launch the template (after signing in to Azure if necessary).

   b. Complete the template **Parameters** and select **OK**:

Name	Description
vmImageURI	The URI of the prepared VM disk image (e.g. https://mystorageaccount.blob.core.windows.net/vm-images/my-machine-image.vhd). This should refer to either the Management Node or Conferencing Node prepared disk image, depending on which type of node you want to install.
storageContainerName	The name of the storage container to hold the instance disk.
dnsDomainNameLabel	The domain name label (i.e. hostname) for the Virtual Machine. When deploying an instance with a public IP address, this label must be the host part only — the name must not contain any periods.
ipAddress	The statically-assigned private IP address for the Virtual Machine.
adminCredential	For password-based authentication templates, this is the password for logging into the Virtual Machine. Note that Azure requires a strong password (such as a mix of upper case, lower case and numeric characters). For SSH key-based templates, this is the public SSH key for logging into the Virtual Machine (e.g. ssh-rsa AAA.... user@host).
vmSize	The size of the Virtual Machine (Standard_A2 or Standard_D4_v2).
networkName	The name of the Virtual Network to connect to.
networkSubnetName	The name of the Virtual Network subnet in which to place the Virtual Machine.
networkSecurityGroupName	The name of the Network Security Group to apply to the Virtual Machine.
networkResourceGroup	The name of the Resource Group containing the Virtual Network and Network Security Group.

   c. Select the **Resource group** to hold the instance.

   d. Review and confirm the legal terms.

   e. Select **Create** to deploy the instance.
4. It can sometimes take several minutes for your instance to be created and start running. You can use the Azure portal to monitor the status of your new instance.

   If the instance deployment fails, review the Azure event diagnostics to help identify the problem.
5. You can now complete the deployment of the Pexip node.

   See either Deploying a Management Node in Azure or Deploying a Conferencing Node in Azure as appropriate, depending on the type of node you are deploying (and according to the **vmImageURI** you selected in the ARM template).

Azure Resource Manager (ARM) templates for deploying a VM instance

Pexip provides ARM templates which may be used to deploy a VM instance into a resource group (step 3 above). These templates may be used from PowerShell or the Azure CLI. Alternatively, you can use the templates to deploy an instance via the Azure Portal.

The templates allow you to choose whether to deploy an instance with either password-based or SSH-key based authentication, and with either no public address or a dynamically-allocated public address. Every template enables boot diagnostics for the Virtual Machine instance.

You should pick the template most suitable for your needs. Every template can be used to launch either a Management Node or a Conferencing Node instance.

Name	Authentication	Public IP address	Template URL	Resources created
virtual-machine-password-dynamic-public-ip	Password based	Yes (dynamically allocated)	https://pexipas.blob.core.windows.net/templates/20160330/virtual-machine-password-dynamic-public-ip.json (launch in Azure Portal)	• Public IP address • Network interface • Virtual Machine
virtual-machine-password-no-public-ip	Password based	No	https://pexipas.blob.core.windows.net/templates/20160330/virtual-machine-password-no-public-ip.json (launch in Azure Portal)	• Network interface • Virtual Machine
virtual-machine-sshkey-dynamic-public-ip	SSH key based	Yes (dynamically allocated)	https://pexipas.blob.core.windows.net/templates/20160330/virtual-machine-sshkey-dynamic-public-ip.json (launch in Azure Portal)	• Public IP address • Network interface • Virtual Machine
virtual-machine-sshkey-no-public-ip	SSH key based	No	https://pexipas.blob.core.windows.net/templates/20160330/virtual-machine-sshkey-no-public-ip.json (launch in Azure Portal)	• Network interface • Virtual Machine

Obtaining and preparing disk images for Azure deployments

Pexip publishes Azure-optimized disk images for the Management Node and for Conferencing Nodes.

Preparing disk images for use

Before you can use the published Pexip Infinity disk images, you must copy them to your storage account in Azure. This guide refers to a disk image copied to your storage account as a **prepared disk image**. All deployment operations use prepared disk images.

The following PowerShell script will copy the published disk images for a Management Node and for a Conferencing Node to your storage account so that they may be used to deploy VM instances.

You **must** edit the variables in the script to provide the name of your Azure subscription (`$subscriptionName`), the name of the resource group (`$resourceGroupName`), the name of the storage account (`$storageAccountName`), and the Pexip Infinity version-build number to use (`$version` — currently 13-0-0-32124-0-0 for v13 software). If you are running an older version of Pexip Infinity software, see Version information for previous Pexip Infinity releases.

```
# Name of your Azure subscription
$subscriptionName = ""
```

```
# Name of the resource group to use
$resourceGroupName = ""
# Name of the storage account to copy the disk images into
$storageAccountName = ""
# Name of the container within the storage account to copy the disk images into
$containerName = "vm-images"
# Version of Pexip Infinity to copy
$version = "13-0-0-32124-0-0"

# Add your Azure account to the PowerShell environment
Add-AzureRmAccount

# Set the current subscription
Get-AzureRmSubscription -SubscriptionName $subscriptionName | Select-AzureRmSubscription

# Obtain the access key for the storage account
$storageAccountKey = Get-AzureRmStorageAccountKey -ResourceGroupName $resourceGroupName -Name
$storageAccountName
If($storageAccountKey.GetType().Name -eq "StorageAccountKeys") {
    # AzureRM.Storage < 1.1.0
    $storageAccountKey = $storageAccountKey.Key1
} Else {
    # AzureRm.Storage 1.1.0
    $storageAccountKey = $storageAccountKey[0].Value
}

# Create the storage access context
$ctx = New-AzureStorageContext -StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey

# Ensure that the container exists
New-AzureStorageContainer -Name $containerName -Context $ctx

# Start copying the Management Node image
$mgmt = Start-AzureStorageBlobCopy -AbsoluteUri
"https://pexipas.blob.core.windows.net/infinity/$version/management-node.vhd" -DestContainer
$containerName -DestBlob "pexip-infinity-$version-management-node.vhd" -DestContext $ctx

# Start copying the Conferencing Node image
$cnfc = Start-AzureStorageBlobCopy -AbsoluteUri
"https://pexipas.blob.core.windows.net/infinity/$version/conferencing-node.vhd" -DestContainer
$containerName -DestBlob "pexip-infinity-$version-conferencing-node.vhd" -DestContext $ctx

# Wait for the Management Node image to finish copying
$status = Get-AzureStorageBlobCopyState -Blob $mgmt.Name -Container $containerName -Context $ctx
While($status.Status -eq "Pending") {
    $status
    $status = Get-AzureStorageBlobCopyState -Blob $mgmt.Name -Container $containerName -Context $ctx
    Start-Sleep 10
}
$status

# Wait for the Conferencing Node image to finish copying
$status = Get-AzureStorageBlobCopyState -Blob $cnfc.Name -Container $containerName -Context $ctx
While($status.Status -eq "Pending") {
    $status
    $status = Get-AzureStorageBlobCopyState -Blob $cnfc.Name -Container $containerName -Context $ctx
    Start-Sleep 10
}
$status

# Print out the prepared disk image URLs for later use
```

```
"Prepared Management Node disk image:   " + $mgmt.ICloudBlob.Uri.AbsoluteUri
"Prepared Conferencing Node disk image: " + $cnfc.ICloudBlob.Uri.AbsoluteUri
```

Alternatively, if using the Azure CLI, the following script is equivalent.

You **must** edit the variables in the script to provide the name of your Azure subscription (`subscriptionName`), the name of the resource group (`resourceGroupName`), the name of the storage account (`storageAccountName`) and the Pexip Infinity version number to use (`version` — currently 13-0-0-32124-0-0 for v13 software). If you are running an older version of Pexip Infinity software, see Version information for previous Pexip Infinity releases.

```
#!/bin/sh

set -e

# Name of your Azure subscription
subscriptionName=""
# Name of the resource group to use
resourceGroupName=""
# Name of the storage account to copy the disk images into
storageAccountName=""
# Name of the container within the storage account to copy the disk images into
containerName="vm-images"
# Version of Pexip Infinity to copy
version="13-0-0-32124-0-0"

# Ensure CLI is in ARM mode
azure config mode arm

# Log in to Azure
azure login

# Set the current suscription
azure account set $subscriptionName

# Obtain the access key for the storage account
storageAccountKey=$(azure storage account keys list -g $resourceGroupName $storageAccountName | grep
'Primary' | sed -e 's/^.*Primary: \(.*\)$/\1/')

# Ensure that the container exists
azure storage container create -a $storageAccountName -k $storageAccountKey $containerName || true

# Start copying the Management Node image
azure storage blob copy start --dest-account-name $storageAccountName --dest-account-key
$storageAccountKey --dest-container $containerName --dest-blob "pexip-infinity-$version-management-
node.vhd" "https://pexipas.blob.core.windows.net/infinity/$version/management-node.vhd"

# Start copying the Conferencing Node image
azure storage blob copy start --dest-account-name $storageAccountName --dest-account-key
$storageAccountKey --dest-container $containerName --dest-blob "pexip-infinity-$version-conferencing-
node.vhd" "https://pexipas.blob.core.windows.net/infinity/$version/conferencing-node.vhd"

# Wait for the Management Node image to finish copying
while azure storage blob copy show --json -a $storageAccountName -k $storageAccountKey --container
$containerName --blob "pexip-infinity-$version-management-node.vhd" | grep -q '"copyStatus": "pending"';
do sleep 10; done
azure storage blob copy show --json -a $storageAccountName -k $storageAccountKey --container
$containerName --blob "pexip-infinity-$version-management-node.vhd"

# Wait for the Conferencing Node image to finish copying
while azure storage blob copy show --json -a $storageAccountName -k $storageAccountKey --container
$containerName --blob "pexip-infinity-$version-conferencing-node.vhd" | grep -q '"copyStatus":
"pending"'; do sleep 10; done
azure storage blob copy show --json -a $storageAccountName -k $storageAccountKey --container
```

```
$containerName --blob "pexip-infinity-$version-conferencing-node.vhd"

# Print out the prepared disk image URLs for later use
echo "Prepared Management Node disk image:
https://$storageAccountName.blob.core.windows.net/$containerName/pexip-infinity-$version-management-
node.vhd"
echo "Prepared Conferencing Node disk image:
https://$storageAccountName.blob.core.windows.net/$containerName/pexip-infinity-$version-conferencing-
node.vhd"
```

Now that you have your prepared disk images in your Azure storage account you can use them to create the VM instances in Azure in which you can deploy the Pexip Infinity Management Node and Conferencing Nodes.

Version information for previous Pexip Infinity releases

If you are running an older version of Pexip Infinity software, and you want to deploy a new Conferencing Node, you must use a published Pexip Infinity disk image version that corresponds to the software version running on your Management Node. This includes dot releases — so for example, for a v12.1 Management Node you must install a v12.1 Conferencing Node rather than a v12 Conferencing Node. Similarly, if your system has been upgraded since you first installed the Management Node and some Conferencing Nodes, you will need to obtain and prepare the appropriate Conferencing Node image corresponding to the software version you are currently running.

To obtain the published disk images for older software versions (for both the Management Node and for a Conferencing Node) you need to use the appropriate software version number in the PowerShell scripts supplied above.

You must replace the current version number (13-0-0-32124-0-0) with the relevant older version as given in the table below:

Pexip Infinity release	Version number to use in script
v12	12-0-0-29682-0-0
v12.1	12-1-0-29734-0-0
v12.2	12-2-0-29803-0-0

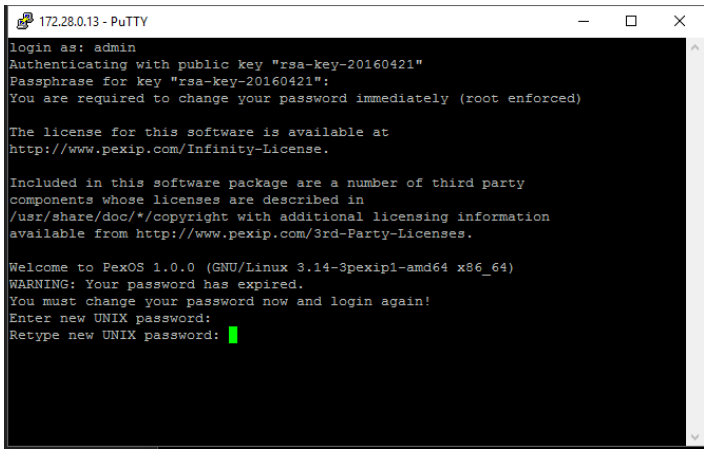
Deploying a Management Node in Azure

As with all Pexip Infinity deployments, you must first deploy the Management Node before deploying any Conferencing Nodes. In a hybrid cloud deployment the Management Node may be deployed in the corporate network or in Azure. This section describes how to deploy the Management Node in Azure.

To deploy a Management Node in Azure:

1. Create a VM instance using the prepared Management Node disk image. For more information on this, see:
   - Obtaining and preparing disk images for Azure deployments
   - Creating VM instances in Azure
2. If using SSH key-based authentication (instead of password-based authentication), after the Management Node instance has booted, you must SSH into the instance to set the operating system password:
   a. Use an SSH client to access the Management Node by its private IP address, supplying your private key file as appropriate.
   b. Follow the login process in the SSH session:
      i. At the login prompt, enter the username ***admin***.
      ii. Supply the key passphrase, if requested.
      iii. At the "Enter new UNIX password:" prompt, enter your desired password, and then when prompted, enter the password again.

This will then log you out and terminate your SSH session.



3. Connect (or reconnect if using key-based authentication) over SSH into the Management Node instance by its private IP address and complete the Pexip Infinity installation wizard as for an on-premises deployment:
   a. Log in as ***admin***, and — if you are using password-based authentication — enter the **password** you supplied when using the ARM template.

      You are presented with another login prompt:

      ```
      Running Pexip installation wizard...
      [sudo] password for admin:
      ```

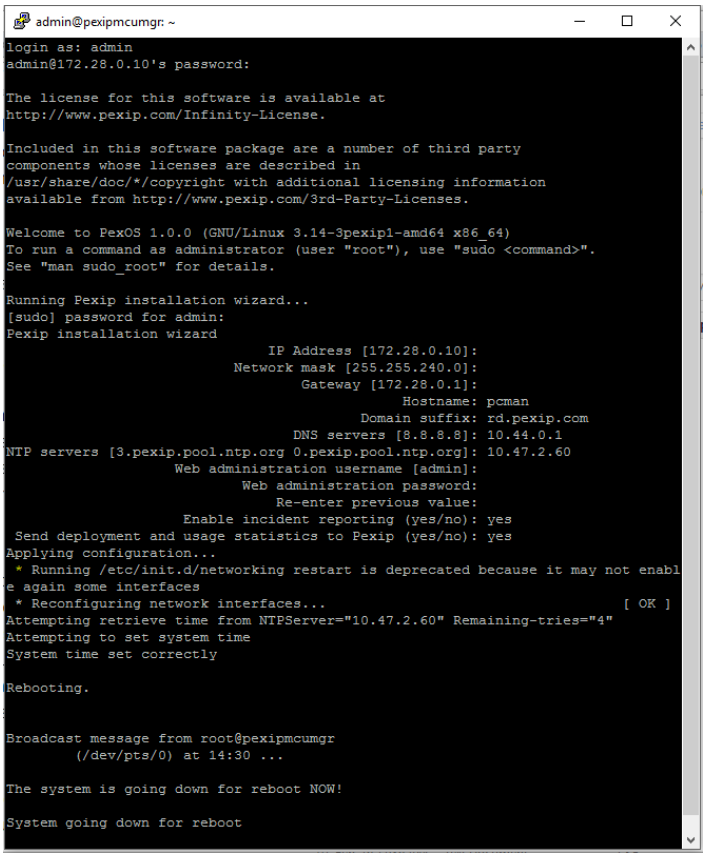
   b. Enter the operating system administrator password (for SSH key-based authentication this is the password you just created in the previous step; for password-based authentication you must enter again the password you supplied when using the ARM template).

      The Pexip installation wizard will begin after a short delay.

   c. Complete the installation wizard to apply basic configuration to the Management Node:
      i. Accept the defaults for the **IP address**, **Network mask** and **Gateway** settings.
      ii. Enter your required **Hostname** and **Domain suffix** for the Management Node.
      iii. Configure one or more **DNS servers** and **NTP servers**. You must override the default values if it is a private deployment.
      iv. Set the **Web administration username** and **password**.
      v. Select whether to **Enable incident reporting** and whether to **Send deployment and usage statistics to Pexip**.

      The DNS and NTP servers at the default addresses are only accessible if your instance has a public IP address. The installation wizard will fail if the NTP server address cannot be resolved and reached.

   After successfully completing the wizard, the SSH connection will be lost as the Management Node reboots.



4. After a few minutes you will be able to use the Pexip Infinity Administrator interface to access and configure the Management Node (remember to use https to connect to the node if you have only configured https access rules in your security group).
   You can now configure your Pexip Infinity platform licenses, VMRs, aliases, locations etc, and add Conferencing Nodes.

Deploying a Conferencing Node in Azure

After deploying the Management Node you can deploy one or more Conferencing Nodes in Azure to provide conferencing capacity.

To deploy a Conferencing Node in Azure:

1. Create a VM instance using the prepared Conferencing Node disk image. For more information on this, see:
   - Obtaining and preparing disk images for Azure deployments
   - Creating VM instances in Azure
2. After the instance has booted, perform a configuration-only deployment on the Management Node to inform it of the new Conferencing Node:
   a. Log in to the Pexip Infinity Administrator interface on the Management Node.
   b. Go to **Platform Configuration > Conferencing Nodes**.
   c. Select **Add Conferencing Node**.
   d. For deployment type, choose ***Generic (configuration-only)***.

e. Enter the details of the new Conferencing Node, including:

IPv4 address	Enter the Private IP address that you assigned to the VM instance (the ipAddress ARM template parameter).
Network mask	Ensure that the mask matches the one defined for the subnet selected for the instance (the networkSubnetName ARM template parameter). For example a subnet with a /20 prefix size has a network mask of 255.255.240.0.
Gateway IP address	The gateway address is the first usable address in the subnet selected for the instance (e.g. 172.31.0.1 for a 172.31.0.0/20 subnet).

f. Select **Finish**.

g. Select **Download Conferencing Node Configuration** and save the XML configuration file.

A zip file with the name **pexip-<hostname>.<domain>.xml** will be downloaded.

3. You must now upload the XML configuration file to the new Conferencing Node:

a. Browse to **https://<conferencing-node-private-ip>:8443/** and use the form provided to upload the XML configuration file to the Conferencing Node VM.

i. Select **Choose File** and select the XML configuration file.

ii. Select **Upload**.

b. The Conferencing Node will apply the configuration and then reboot. When it has rebooted, it will connect to the Management Node.

You can close the browser window used to upload the file.

4. Configure the Conferencing Node's static NAT address, if you have a assigned a public IP address to the instance:

a. Log in to the Pexip Infinity Administrator interface on the Management Node.

b. Go to **Platform Configuration > Conferencing Nodes**) and select the Conferencing Node.

c. Configure the **Static NAT address** as the instance's public IP address (the public address dynamically allocated by Azure).

After deploying a new Conferencing Node, it takes approximately 5 minutes before the node is available for conference hosting and for its status to be updated on the Management Node. (Until it is available, the Management Node will report the status of the Conferencing Node as having a last contacted and last updated date of "Never".)

Managing Azure instances

This section describes the common maintenance tasks for stopping, restarting and permanently removing Conferencing Node Azure instances.

Temporarily removing (stopping) a Conferencing Node instance

At any time you can temporarily remove a Conferencing Node instance from your Pexip Infinity platform if, for example, you do not need all of your current conferencing capacity.

To temporarily remove a Conferencing Node instance:

1. Put the Conferencing Node into maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
   a. Go to **Platform Configuration > Conferencing Nodes**.
   b. Select the Conferencing Node.
   c. Select the **Enable maintenance mode** check box and select **Save**.
      While maintenance mode is enabled, this Conferencing Node will not accept any new conference instances.
   d. Wait until any existing conferences on that Conferencing Node have finished. To check, go to **Status > Conferences**.
2. Stop the Conferencing Node instance on Azure:
   a. From the Azure portal, select **Virtual Machines** to see the status of all of your instances.
   b. Select the instance you want to shut down.
   c. Select **Stop** to shut down the instance.

Reinstating (restarting) a stopped Conferencing Node instance

You can reinstate a Conferencing Node instance that has already been installed but has been temporarily shut down.

To restart a Conferencing Node instance:

1. Restart the Conferencing Node instance on Azure:
   a. From the Azure portal, select **Virtual Machines** to see the status of all of your instances.
   b. Select the instance you want to restart.
   c. Select **Start** to start the instance.
2. Take the Conferencing Node out of maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
   a. Go to **Platform Configuration > Conferencing Nodes**.
   b. Select the Conferencing Node.
   c. Clear the **Enable maintenance mode** check box and select **Save**.
3. Update the Conferencing Node's static NAT address, if appropriate.
   If your Conferencing Node instance was configured with an auto-assigned public IP address, it will be assigned a new public IP address when the instance is restarted.
   a. Go to **Platform Configuration > Conferencing Nodes** and select the Conferencing Node.
   b. Configure the **Static NAT address** as the instance's new public IP address.

After reinstating a Conferencing Node, it takes approximately 5 minutes for the node to reboot and be available for conference hosting, and for its last contacted status to be updated on the Management Node.

Permanently removing a Conferencing Node instance

If you no longer need a Conferencing Node instance, you can permanently delete it from your Pexip Infinity platform.

To remove a Conferencing Node instance:

1. If you have not already done so, put the Conferencing Node into maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
   a. Go to **Platform Configuration > Conferencing Nodes**.
   b. Select the Conferencing Node.
   c. Select the **Enable maintenance mode** check box and select **Save**.
      While maintenance mode is enabled, this Conferencing Node will not accept any new conference instances.
   d. Wait until any existing conferences on that Conferencing Node have finished. To check, go to **Status > Conferences**.
2. Delete the Conferencing Node from the Management Node:
   a. Go to **Platform Configuration > Conferencing Nodes** and select the Conferencing Node.
   b. Select the check box next to the node you want to delete, and then from the **Action** drop-down menu, select **Delete selected Conferencing Nodes** and then select **Go**.
3. Terminate the Conferencing Node instance on Azure:
   a. Delete the resource group which holds the instance:
      i. From the Azure Portal, select **Resource Groups** to see all of your resource groups.
      ii. Select the resource group you want to delete.
      iii. Select **Delete** to delete the resource group.
   b. Delete the storage container which holds the instance disk:
      i. From the Azure Portal, select **All Resources** to see all of your storage accounts.
      ii. Select the storage account that is being used to store the instance disk.
      iii. Under **Services**, select **Blobs** to see all of the storage containers in the storage account.
      iv. Select the storage container you want to delete.
      v. Select **Delete** to delete the storage container.
   c. If boot diagnostics were enabled on the VM instance, delete the storage container which holds the instance boot diagnostics logs:
      i. From the Azure Portal, select **All Resources** to see all of your storage accounts.
      ii. Select the storage account that is being used to store the boot diagnostics logs.
      iii. Under **Services**, select **Blobs** to see all of the storage containers in the storage account.
      iv. Select the storage container you want to delete.
      v. Select **Delete** to delete the storage container.

© 2016 Pexip AS