# Pexip Infinity and Microsoft Azure

# Deployment Guide

**Software Version 28**

**Document Version 28.a**

**May 2022**

]pexip[

# Contents

# 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.

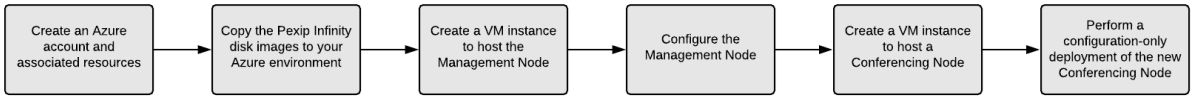
Azure enables you to scale up or down to handle changes in requirements or spikes in conferencing requirements. You can also use the Azure APIs and the Pexip Infinity management API to monitor usage and bring up / tear down Conferencing Nodes as required to meet conferencing demand, or allow Pexip Infinity to handle this automatically for you via its dynamic bursting capabilities.

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.

# 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

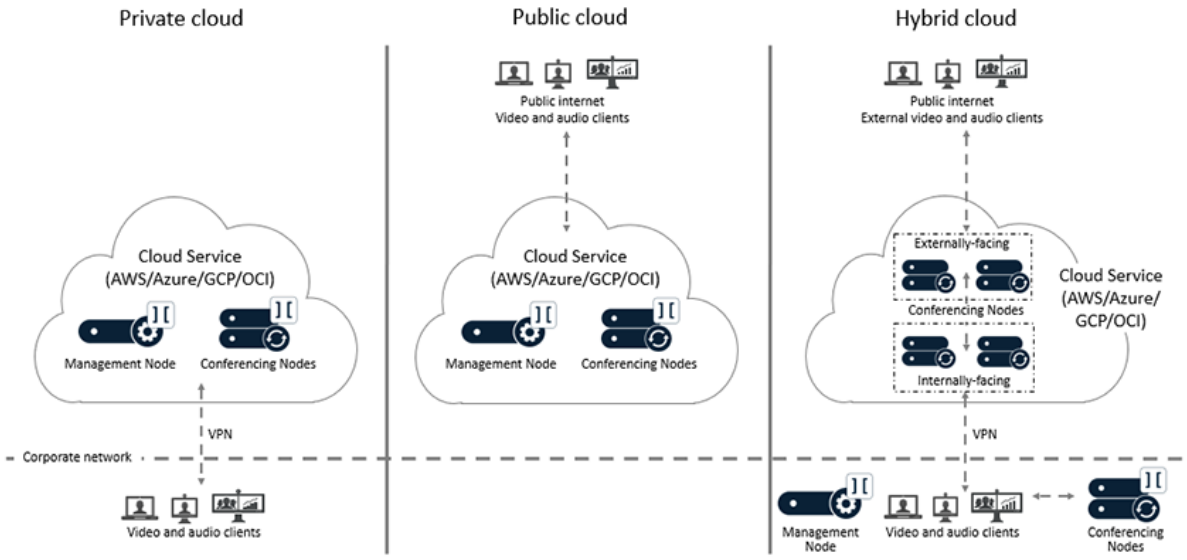
Azure has two deployment models: Classic and Resource Manager.

**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 between the corporate network and 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, you must ensure that your local network allows such routing.
- **Hybrid cloud**: the Management Node, and optionally some Conferencing Nodes, are deployed in the corporate network. A VPN tunnel is created between the corporate network and 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). You may also want to consider dynamic bursting, where the Azure-hosted Conferencing Nodes are only started up and used when you have reached capacity on your on-premises nodes.



All of the Pexip nodes that you deploy in the cloud are completely dedicated to running the Pexip Infinity platform— you maintain full data ownership and control of those 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://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows for more information about using SSH on Azure.
- We do not support Azure deployments in China.

## 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. Our Server design recommendations also apply to cloud-based deployments.

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

- **Management Node**: an **F4s v2** instance.
- **Transcoding Conferencing Nodes**: either an **F8s v2** instance for smaller deployments, or an **F16s v2** or **F32s v2** instance for larger deployments.
- **Proxying Edge Nodes**: an **F4s v2** instance.

An **F8s v2** instance should provide capacity for approximately 15 HD / 37 SD / 270 audio-only calls per Transcoding Conferencing Node. An **F16s v2** instance should provide capacity for approximately 30 HD / 70 SD / 450 audio-only calls, and an **F16s v2** instance provides approximately 56 HD / 112 SD / 880 audio-only calls.

If the Fsv2 series is not available in your region you can use an F-series for your nodes.

## Capacity planning

By default, Azure Resource Manager virtual machine cores have a regional total limit **and** a regional per series (F, Fsv2, etc.) limit, that are enforced per subscription. Typically, for each subscription, the default quota allows up to 10-20 CPU cores per region and 10-20 cores per series. An F8s v2 instance uses 8 CPU cores. Thus, with the default limits in place, only two F8s v2 instances may be deployed (as only 4 CPU cores will remain in either quota pool, which is insufficient for another F8s 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 example, if 10 Transcoding Conferencing Nodes are required, then the quota must be increased to 8 cores x 10 F8s v2 instances = 80 CPU cores of type F8s v2. It may take a number of days for the quota increase request to be processed. For more information see https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits.

## IP addressing

Within a Virtual Network, an instance's private IP addresses can initially be allocated dynamically (using DHCP) or statically. However, after the private IP address has been assigned to the instance it remains fixed and 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 be 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, as it is used for all internal communication between nodes. To associate an instance's public IP address with the node, configure that public IP address as the node's **Static NAT address** (via **Platform > Conferencing Nodes**).

## Assumptions and prerequisites

The Pexip Infinity 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 region/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 region (see Preparing your Azure environment)
- (if necessary) configured a VPN tunnel from the corporate/management network to the Azure Virtual Network
- set your subscription's Microsoft partner ID to Pexip (see Configuring your Azure subscription)
- 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://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview.

## Multiple Virtual Networks

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 Configuring Azure Network Security Groups for port requirements when using multiple VNets.

- From version 21 of Pexip Infinity, you can deploy your Conferencing Nodes in Azure across peered regions (Global VNet Peering). See https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview for more information about virtual network peering. Note that if you are upgrading to version 21 or later, you must not delete the VPN gateway until after you have upgraded. You can then delete the gateway and enable VNet peering.
- For version 20 or earlier, you must use a VNet-to-VNet VPN gateway connection; do not use VNet peering. 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 Azure VNets.

# Configuring your Azure subscription

We recommend setting up a separate subscription for your Pexip deployment.

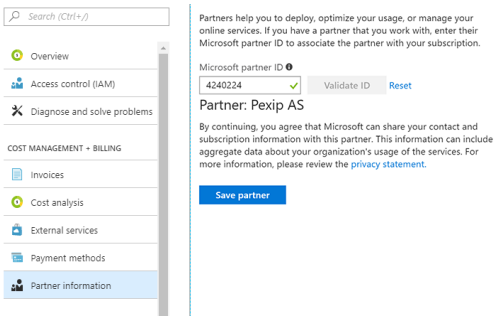
We recommend using a separate subscription because Azure Resource Manager enforces a per hour limit on the number of requests it transacts, hence it's possible for hard limits to be reached if you have other applications that are also transacting with Resource Manager within the same subscription. This applies mainly if you intend to use dynamic bursting into Azure.

If you have an Enterprise Agreement (EA) or Pay-As-You-Go subscription, and you are using this subscription primarily for your Pexip platform, you can link Pexip to this subscription — assigning Pexip as the Microsoft partner provides telemetry to Microsoft that Pexip is associated with the resources consumed by this subscription. This does not apply if you are in the Azure Cloud Solution Provider (CSP) program.

To set your subscription's Microsoft partner ID to Pexip:

1. From the Azure portal, select **Subscriptions**.
2. Select the subscription you are using for your Pexip deployment.
3. Select **Partner Information**.
4. In the **Microsoft partner ID** field , enter **4240224** (Pexip's reference ID) and select **Validate ID**.

   **Partner: Pexip AS** should be displayed.

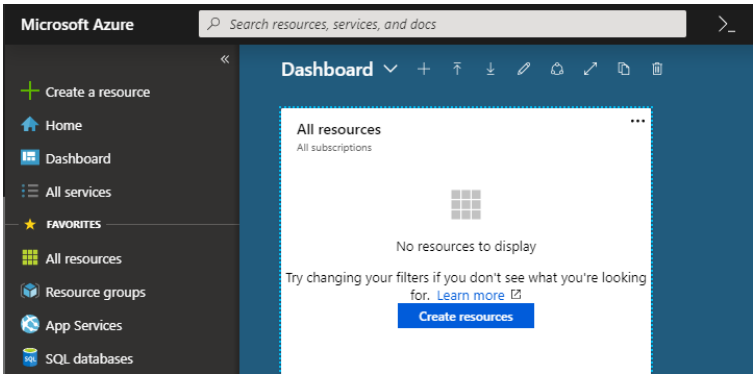



5. Select **Save partner**.

# Preparing your Azure environment

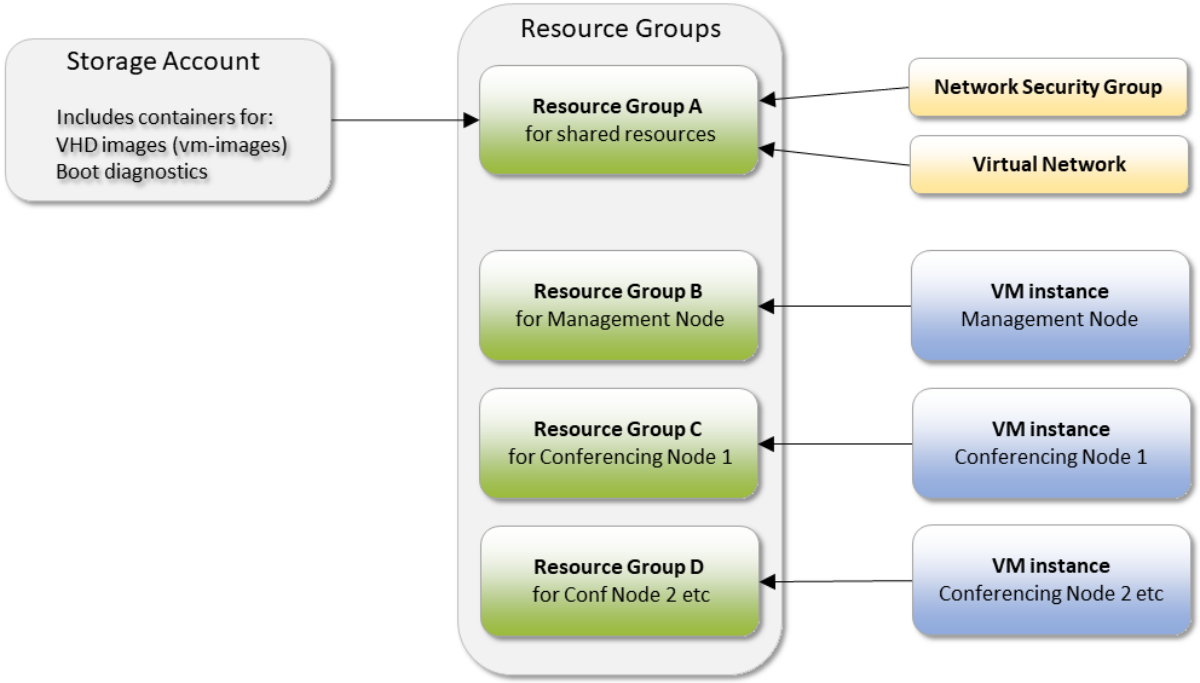
This topic explains how to prepare your Azure environment before installing Pexip Infinity. It describes how to set up your Resource Group, Virtual Network and Storage Account in your chosen Azure region, and to prepare an SSH key if you intend to use key-based authentication.

This guide assumes you are starting with a fresh Azure portal.




Note that the images shown in this guide depict an example deployment. Unless explicitly stated, you should use your own resource names and address spaces etc. as appropriate for your own environment. Also, as the Azure portal is regularly updated, some images and labels shown here may not directly match the currently available options.

The diagram below shows how the various resource elements that you need to create within the Azure environment are related to each other. This topic explains how to create the shared Resource Group, Virtual Network and Storage Account. Subsequent topics in this guide explain how the prepared disk image is created, and how the Resource Groups are created for your VM instances for each Pexip node.




### Using the Azure portal or PowerShell

This guide provides examples of how to complete the tasks using either the Azure portal, or via PowerShell.

When using PowerShell commands you must first sign in to your Azure subscription with the `Connect-AzAccount` command and follow the on-screen directions to authenticate.

If necessary you can change the subscription context with the command:

```
Set-AzContext -SubscriptionId "xxxx-xxxx-xxxx-xxxx"
```

where **xxxx-xxxx-xxxx-xxxx** is the ID of the subscription you want to use.

See Running the script via your Windows client for more information about running PowerShell scripts and Azure Resource Manager.

# Creating a Resource Group

Resource Groups are logical containers for a collection of resources used for your Pexip deployment.

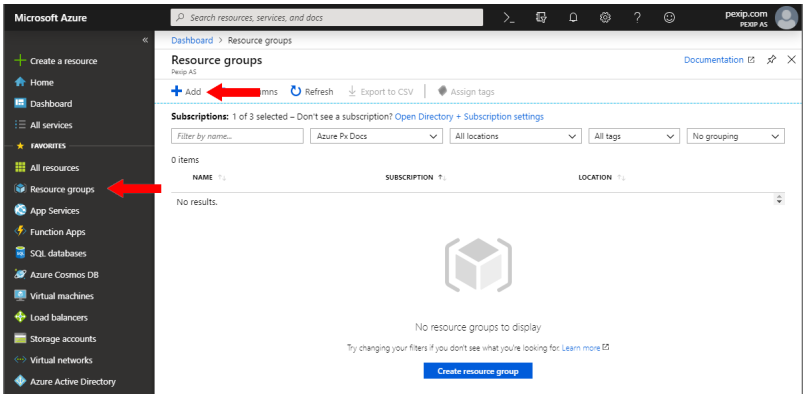
We recommend that all of your shared resources use the same Resource Group. The shared resources that you should place in this Resource Group include:

- Network Security Group
- Virtual Network
- Storage Account
- Prepared disk images (these are used to create the individual VM instances for your Conferencing Nodes and Management Node)

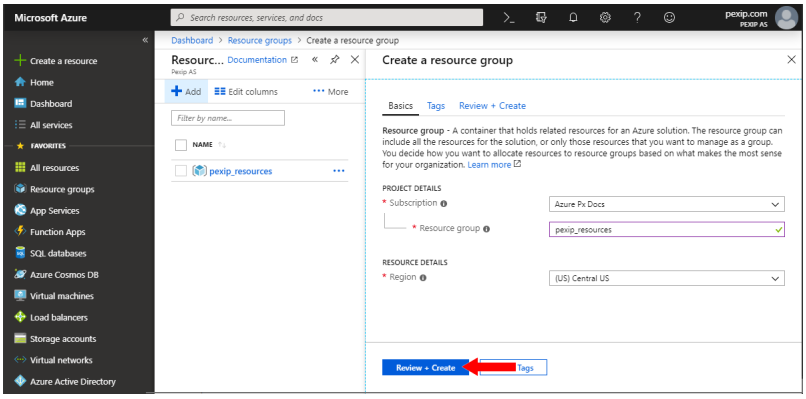
When you deploy your Pexip Infinity nodes, we recommend that each VM instance that you create for your Conferencing Nodes or Management Node is deployed in its own Resource Group. This is not a mandatory requirement but it does allow you to subsequently manage each of your VM instance's resources more easily.

## Azure portal

1. Decide in which region you are going to deploy your Pexip system. You can see the regions and their physical geographic locations at https://azure.microsoft.com/en-gb/global-infrastructure/regions/.
2. Configure a Resource Group for your shared resources.
   a. To create a new Resource Group, from the Azure portal select **Resource Groups** and select **+ Add**.




   b. Select your **Subscription**, enter your **Resource group** name, select your **Region**, and then select **Review + Create**.




   c. On the **Summary** page, select **Create**.

## Powershell

Use the `New-AzResourceGroup` command:

```
New-AzResourceGroup -Name <resource group name> -Location <region name>
```

For example:

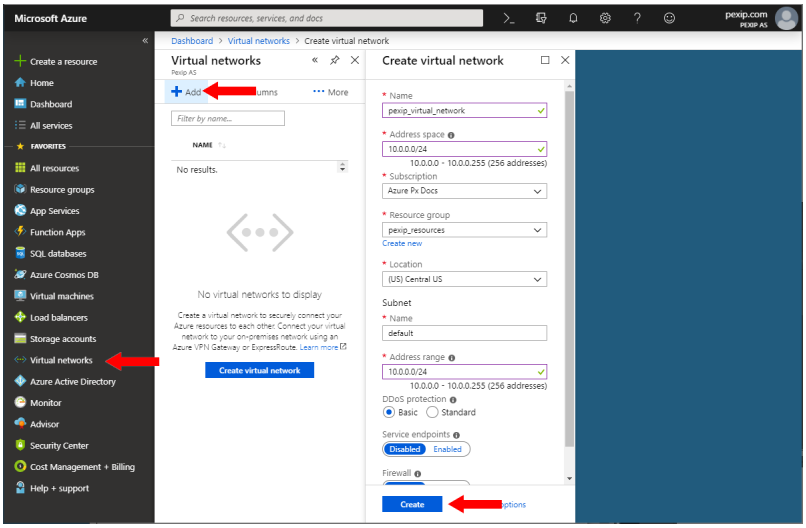
```
New-AzResourceGroup -Name pexip_resources -Location centralus
```

# Creating a Virtual Network

A Virtual Network allows Azure resources to securely communicate with each other, and is where your VM instances will be deployed. See https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview for more information.

**Azure portal**

1. From the Azure portal, select **Virtual Networks**, and select **+ Add**.
2. Configure the Virtual Network's properties:
   a. Give it a **Name**, enter the IP range (**Address space**, **Subnet name** and **Address range**) and then ensure you select your **Subscription**, **Resource group** and your **Location**.
   b. Select **Create**.




**Powershell**

1. Create the virtual network:

```
$virtualNetwork = New-AzVirtualNetwork
-ResourceGroupName <resource group
name> -Location <region name> -Name
<virtual network name> -AddressPrefix
<address range>
```

2. Add a subnet:

```
$subnetConfig = Add-
AzVirtualNetworkSubnetConfig -Name
default -AddressPrefix <subnet range>
-VirtualNetwork $virtualNetwork
```

3. Associate the subnet to the virtual network:

```
$virtualNetwork | Set-AzVirtualNetwork
```

For example:

```
$virtualNetwork = New-AzVirtualNetwork -
ResourceGroupName pexip_resources -
Location centralus -Name pexip_virtual_
network -AddressPrefix 10.0.0.0/24
```

```
$subnetConfig = Add-
AzVirtualNetworkSubnetConfig -Name default
-AddressPrefix 10.0.0.0/24 -VirtualNetwork
$virtualNetwork
```

```
$virtualNetwork | Set-AzVirtualNetwork
```

# Creating a Storage Account

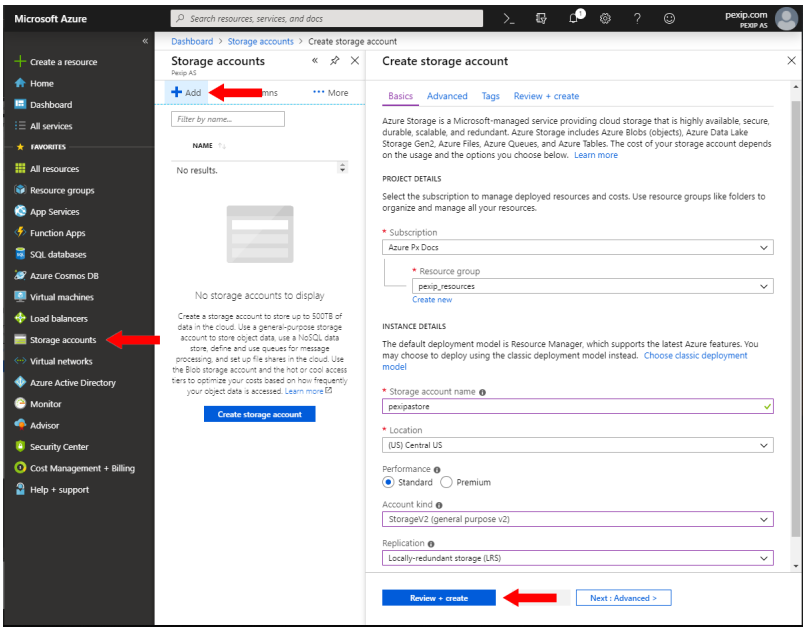
A general-purpose storage account provides access to all of the Azure storage services, and is used for storing the prepared Pexip Infinity VHD images and VM boot diagnostics. (We recommend that the Azure VMs use managed disks, and thus the VMs are not associated with a storage account.)

Note that a storage account cannot use Premium storage if it is used for VM boot diagnostics.

For more information on Azure disk types see https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types.

**Azure portal**

1. From the Azure portal, select **Storage Accounts**, and select **+ Add**.
2. Configure the Storage Account's Basic properties:
   a. Select your **Subscription** and **Resource group**.
   b. Leave the deployment model as ***Resource Manager***.
   c. Give it a **Storage account name**.
   d. Select your **Location**.
   e. Set **Performance** to ***Standard***.
   f. Select an **Account kind** of ***StorageV2***.
   g. Set **Replication** to ***Locally redundant storage (LRS)***.
   h. Select **Review + create**.
   i. Review your inputs and select **Create**.




**Powershell**

Use the `New-AzStorageAccount` command:

```
New-AzStorageAccount -ResourceGroupName
<resource group name> -Name <storage
account name> -Location <region name> -
SkuName Standard_LRS -Kind StorageV2
```

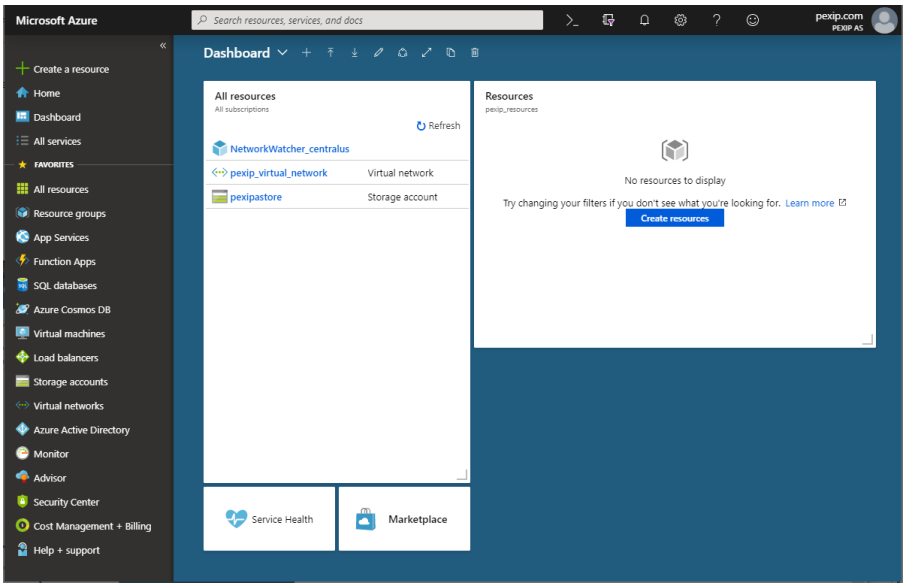
For example:

```
New-AzStorageAccount -ResourceGroupName
pexip_resources -Name pexipastore -
Location centralus -SkuName Standard_LRS -
Kind StorageV2
```

## SSH keys

If you intend to use an SSH key-based template for deploying your VM instances, you should prepare your SSH keys in advance, and optionally store them in Azure, prior to using the template. (This is because using the ***Generate new key pair*** option for the Admin Credential field in the template will generate an error).

You now have a Resource Group, Storage Account and Virtual Network for your Pexip deployment.


Microsoft Azure
Search resources, services, and docs
pexip.com
PEXIP AS
Dashboard
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
All resources
All subscriptions
Refresh
NetworkWatcher_centralus
pexip_virtual_network
Virtual network
pexipastore
Storage account
Resources
pexip_resources
No resources to display
Try changing your filters if you don't see what you're looking for. Learn more
Create resources
Service Health
Marketplace

# 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 is described below and is defined within the Azure Resource Manager (ARM) templates that we provide.

## Inbound security rules

These rules allow administrative/management access to the Management Node and Conferencing Nodes, and allow call signaling and media to Conferencing Nodes:

| 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 Azure 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.

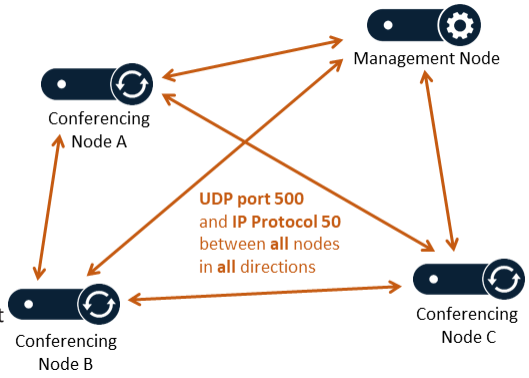
Remember that the Management Node and all Conferencing Nodes must be able to communicate with each other. If your instances only have private addresses, ensure that the necessary external systems such as NTP and DNS servers are routable from those nodes.

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

## Deployment scenarios and inter-node communication requirements for multiple Virtual Networks

In a basic deployment, your Pexip Infinity platform will be deployed within a single Azure Virtual Network (VNet).

In larger deployments you may choose to deploy your Conferencing Nodes across multiple VNets — in which case there must be a directly routable path (no NAT) between all nodes that allows **UDP port 500 (IKE)**, and **IP Protocol 50 (IPsec ESP)** to pass between all nodes in both directions.




These routing requirements and their influence on the various deployment models is as follows:

- **Public/private cloud on a single Azure virtual network**: the Management Node and Conferencing Nodes are all within the same virtual network and communicate with each other within the network over IPsec which is allowed by default within the VNet.
- **Hybrid cloud on a single Azure virtual network**: as for public/private cloud above, except that your VPN tunnel must allow the IPsec traffic between your on-premises nodes and your cloud-hosted nodes.
- **Conferencing Nodes spread over multiple Azure virtual networks**: you should use Global VNet Peering — this means that all network traffic between the peered virtual networks, including the IPsec traffic between nodes, is private and travels over the Azure backbone. (Do not set up a VNet-to-VNet VPN gateway between each virtual network.)

Note that in all cases the Azure Network Security Group templates that we provide allow call signaling and media connectivity into the Pexip Infinity platform.

## 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 (see below).

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/20220330/security-group.json<br>(launch in Azure Portal) | Network security group |
| security-group-with-sip-udp | Enabled | https://pexipas.blob.core.windows.net/templates/20220330/security-group-with-sip-udp.json<br>(launch in Azure Portal) | Network security group |

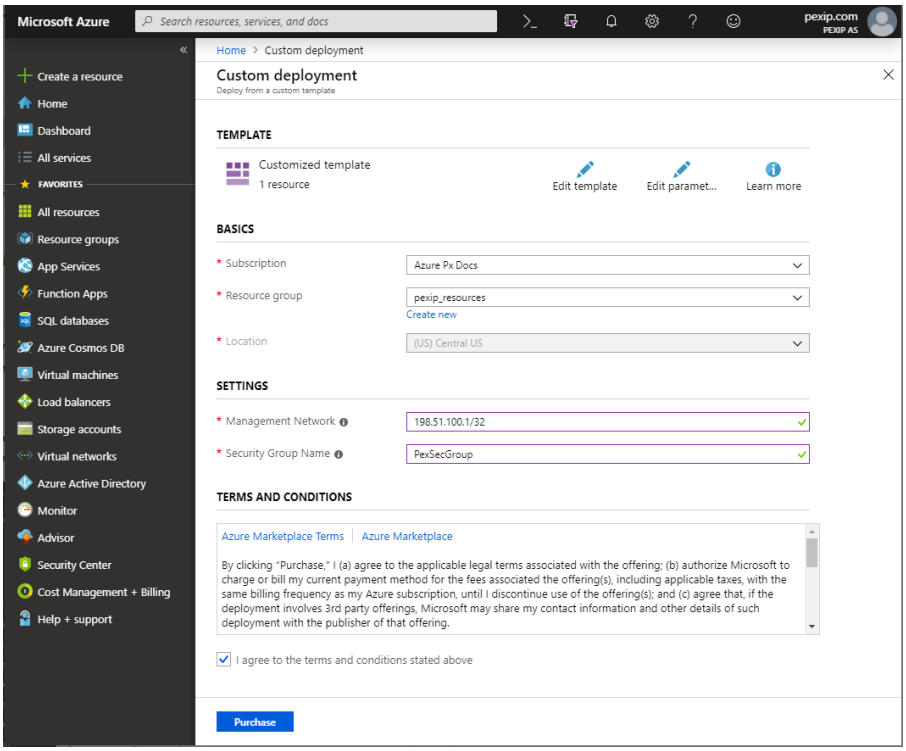
Both templates contain the following parameters:

| Name | Description |
|---|---|
| managementNetwork | Network from which to permit management traffic (CIDR notation e.g. 198.51.100.1/32). |
| securityGroupName | Name of the security group to create. |

## Creating a Network Security Group via the Azure portal

To set up a Network Security Group via the Azure portal:

1. Select the appropriate ARM Template URL link from the table above and sign in to the Azure portal if required.
2. Select your **Subscription** and **Resource group**.
3. Supply the template parameters (Settings):
   - The **Management Network** from which to permit management traffic (CIDR notation e.g. 198.51.100.1/32).
   - The **Security Group Name**.
4. Agree to the legal terms.
5. Select **Purchase**.



# Obtaining and preparing disk images for Azure deployments

Pexip publishes Azure-optimized disk images for the Management Node and for Conferencing Nodes. This topic includes a PowerShell script that copies and prepares your disk images, and instructions for running the script via a Windows client.

## Preparing disk images for use

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

The following PowerShell script copies both of the published VHDs (for a Management Node and for a Conferencing Node) to your storage account (into a storage container called **vm-images**) and then creates an image from those VHDs so that they may be used to deploy VM instances. Note that these images can be stored in your shared resource group (whereas we recommend that each VM instance created from these images is deployed in its own resource group).

You **must** edit the variables in the script to provide the name of the:

- Azure subscription (`$subscriptionName`)
- region (location) to use (`$regionName`)
- resource group (`$resourceGroupName`)
- storage account (`$storageAccountName`)
- Pexip Infinity version-build number to use (`$version` — currently 28-0-0-67306-0-0 for v28 software). If you are running an older version of Pexip Infinity software, see Version information for previous Pexip Infinity releases.

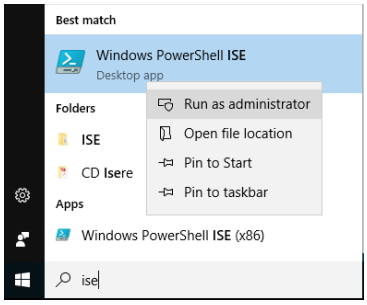
```
# Name of your Azure subscription
$subscriptionName = ""
# Name of the Azure region (location) to use
$regionName = ""
# Name of the resource group to use
$resourceGroupName = ""
# Name of the storage account to copy the disk images into
$storageAccountName = ""
# Name of the container within the storage account to copy the disk images into
$containerName = "vm-images"
# Version of Pexip Infinity to copy
$version = "28-0-0-67306-0-0"

# Add your Azure account to the PowerShell environment
Import-Module Az -MinimumVersion 5.1.0
Connect-AzAccount

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

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

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

# Create the container
New-AzStorageContainer -Name $containerName -Context $ctx

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

# Start copying the Conferencing Node image
```

```
$cnfc = Start-AzStorageBlobCopy -AbsoluteUri "https://pexipas.blob.core.windows.net/infinity/$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-AzStorageBlobCopyState -Blob $mgmt.Name -Container $containerName -Context $ctx
While($status.Status -eq "Pending") {
    $status
    $status = Get-AzStorageBlobCopyState -Blob $mgmt.Name -Container $containerName -Context $ctx
    Start-Sleep 10
}
$status

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

# Create Azure images from the vhd files
$imageConfigMgmt = New-AzImageConfig -Location $regionName
$osDiskVhdUriMgmt = $mgmt.ICloudBlob.Uri.AbsoluteUri
Set-AzImageOsDisk -Image $imageConfigMgmt -OsType "Linux" -OsState "Generalized" -StorageAccountType "Premium_LRS" -BlobUri $osDiskVhdUriMgmt
$imageMgmt = New-AzImage -Image $imageConfigMgmt -ImageName "pexip-infinity-$version-management-node-image" -ResourceGroupName
$resourceGroupName

$imageConfigCnfc = New-AzImageConfig -Location $regionName
$osDiskVhdUriCnfc = $cnfc.ICloudBlob.Uri.AbsoluteUri
Set-AzImageOsDisk -Image $imageConfigCnfc -OsType "Linux" -OsState "Generalized" -StorageAccountType "Premium_LRS" -BlobUri $osDiskVhdUriCnfc
$imageCnfc = New-AzImage -Image $imageConfigCnfc -ImageName "pexip-infinity-$version-conferencing-node-image" -ResourceGroupName
$resourceGroupName

# Print out the prepared disk image resource IDs for later use
"Management Node disk image resource ID:   " + $imageMgmt.Id
"Conferencing Node disk image resource ID: " + $imageCnfc.Id
```

## Running the script via your Windows client

To run the PowerShell script from your Windows PC, you need to connect your local machine to Azure:

1. From your PC, run PowerShell ISE as Administrator by right-clicking on it and selecting **Run as Administrator**.




2. When in PowerShell run the following two commands:
   a. `Install-Module -Name Az -MinimumVersion 5.1.0 -AllowClobber -Scope AllUsers`

      This installs the Azure Resource Manager modules from the PowerShell Gallery.
   b. `Install-Module Azure`

      This installs the Azure Service Management module from the PowerShell Gallery.

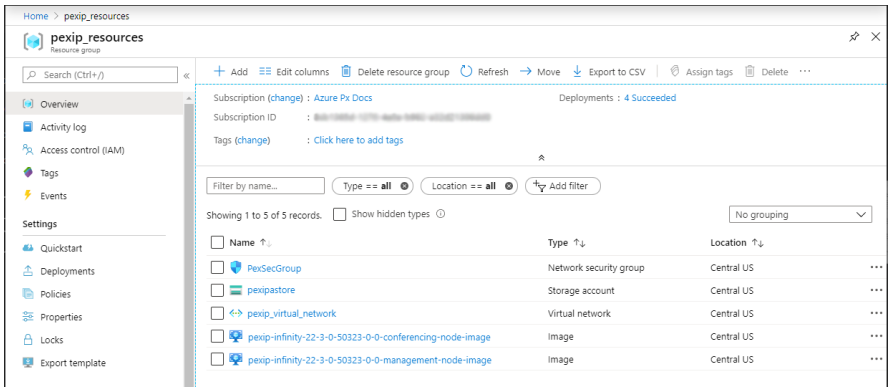
   If you get any prompts while running these commands, select Y for Yes.

   See https://docs.microsoft.com/en-gb/powershell/azure/ for more information about Azure PowerShell.
3. Copy and paste the PowerShell script from above into a text editor and add in your Subscription Name, Region Name, Resource Group Name and Storage Account name (where shown below), and then save the file as a .ps1 file.

```
# Name of your Azure subscription
$subscriptionName = ""
# Name of the Azure region (location) to use
$regionName = ""
# 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
```

4. Run the script:
   a. Close the file, right-click on it and select **Run with PowerShell**.
   b. You are prompted to login, so enter your Azure login credentials.

      If you are using multi-factor authentication, and your credentials are already populated, you may need to manually retype them for the authentication process to complete successfully.
   c. The script will run and copy the images over to your Azure environment. This takes approximately 10 minutes
5. You can use the Azure portal to confirm when the VHD files have been copied across and the images have been created. From the Azure portal go to your Azure dashboard and select your **Resource Group** used for shared resources. You will see the Pexip Management Node and Conferencing Node prepared disk images.




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

## Azure US Government Cloud

If you use Azure US Government Cloud you have to modify the disk images PowerShell script to ensure that you are connected to the correct environment:

- Change `Connect-AzAccount` to `Connect-AzAccount -EnvironmentName AzureUSGovernment`

Note that you will also need to modify the ARM template used to create the VM instances in Azure.

## 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 v21.2 Management Node you must install a v21.2 Conferencing Node rather than a v21 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 (28-0-0-67306-0-0) with the relevant older version as given in the table below:

| Pexip Infinity release | Version number to use in script |
|---|---|
| v27.3 | 27-3-0-65837-0-0 |
| v27.2 | 27-2-0-65796-0-0 |
| v27.1 | 27-1-0-65773-0-0 |
| v27 | 27-0-0-65746-0-0 |
| v26.2 | 26-2-0-62420-0-0 |
| v26.1 | 26-1-0-62381-0-0 |
| v26 | 26-0-0-62340-0-0 |

# Creating VM instances in Azure for your Pexip nodes

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 (either on-premises or in Azure) before deploying any Conferencing Nodes. You must also have prepared your Azure environment.

## Creating a VM instance

You follow the same basic procedure for creating a VM instance in Azure regardless of whether you are creating the Management Node or a Conferencing Node. The main differences are the VM Image Resource ID and VM size that you need to use.

To create the VM instance:

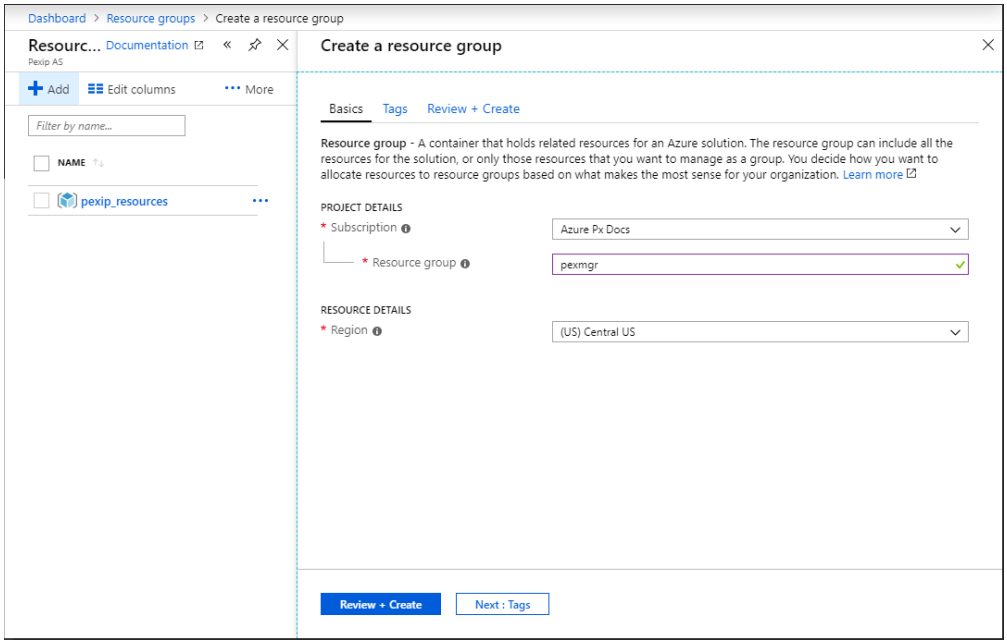
1. Create a new **resource group** to hold the instance.

   We recommend that each VM instance (i.e. the Management Node and each Conferencing Node) is deployed in its own resource group.

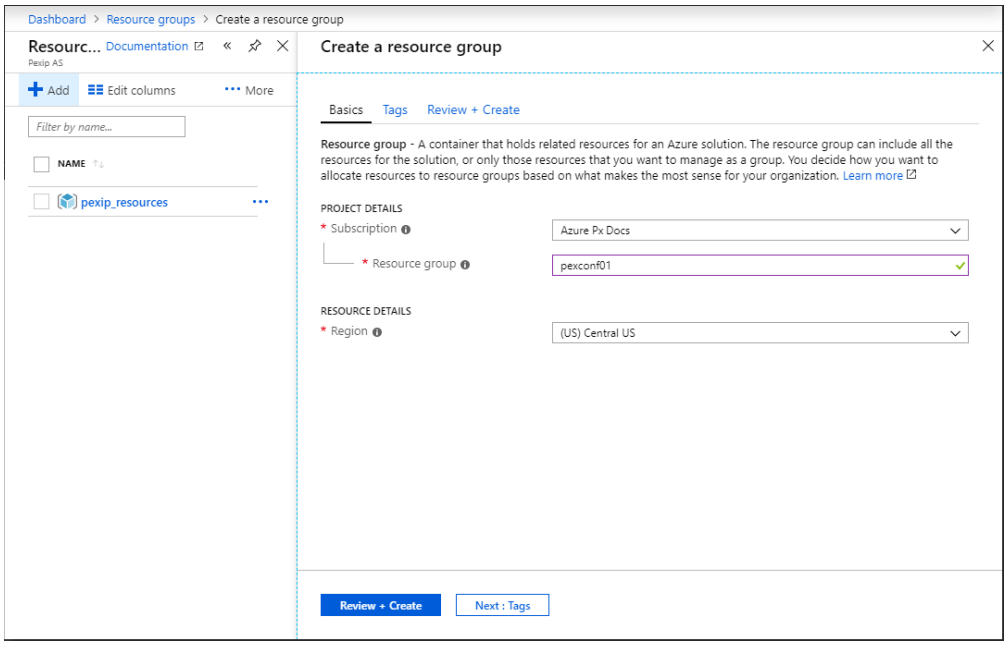
   a. Go to **Resource Groups** and select **+ Add**.

   b. Select your **Subscription** and enter your **Resource group** name, such as pexmgr for the Management Node, or pexconf01, pexconf02 etc. for a Conferencing Node.

   c. Select your **Region**, and then select **Review + Create**.




***Resource Group for the Management Node***




***Resource Group for a Conferencing Node***

d. On the **Summary** page, select **Create**.

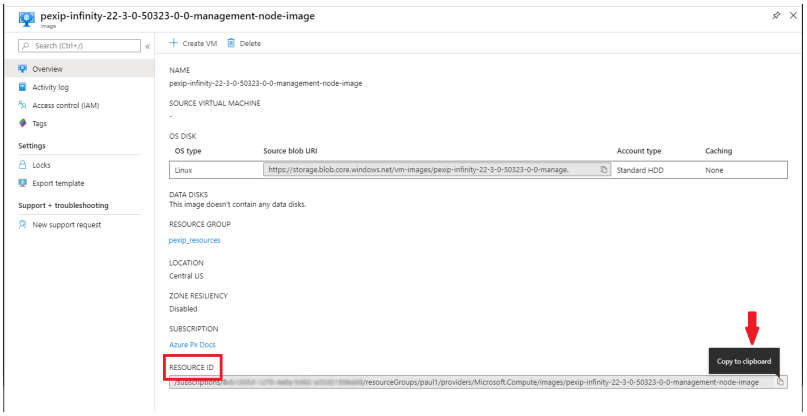
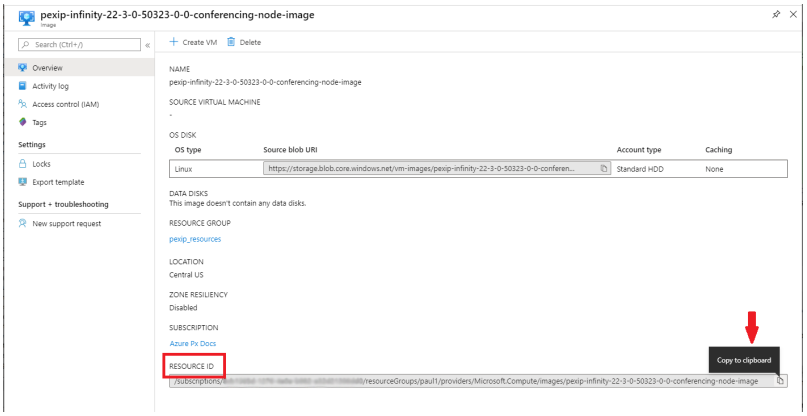
The equivalent example PowerShell commands are:

```
New-AzResourceGroup -Name pexmgr -Location <region name>
New-AzResourceGroup -Name pexconf01 -Location <region name>
```

2. Deploy the instance into the new 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).

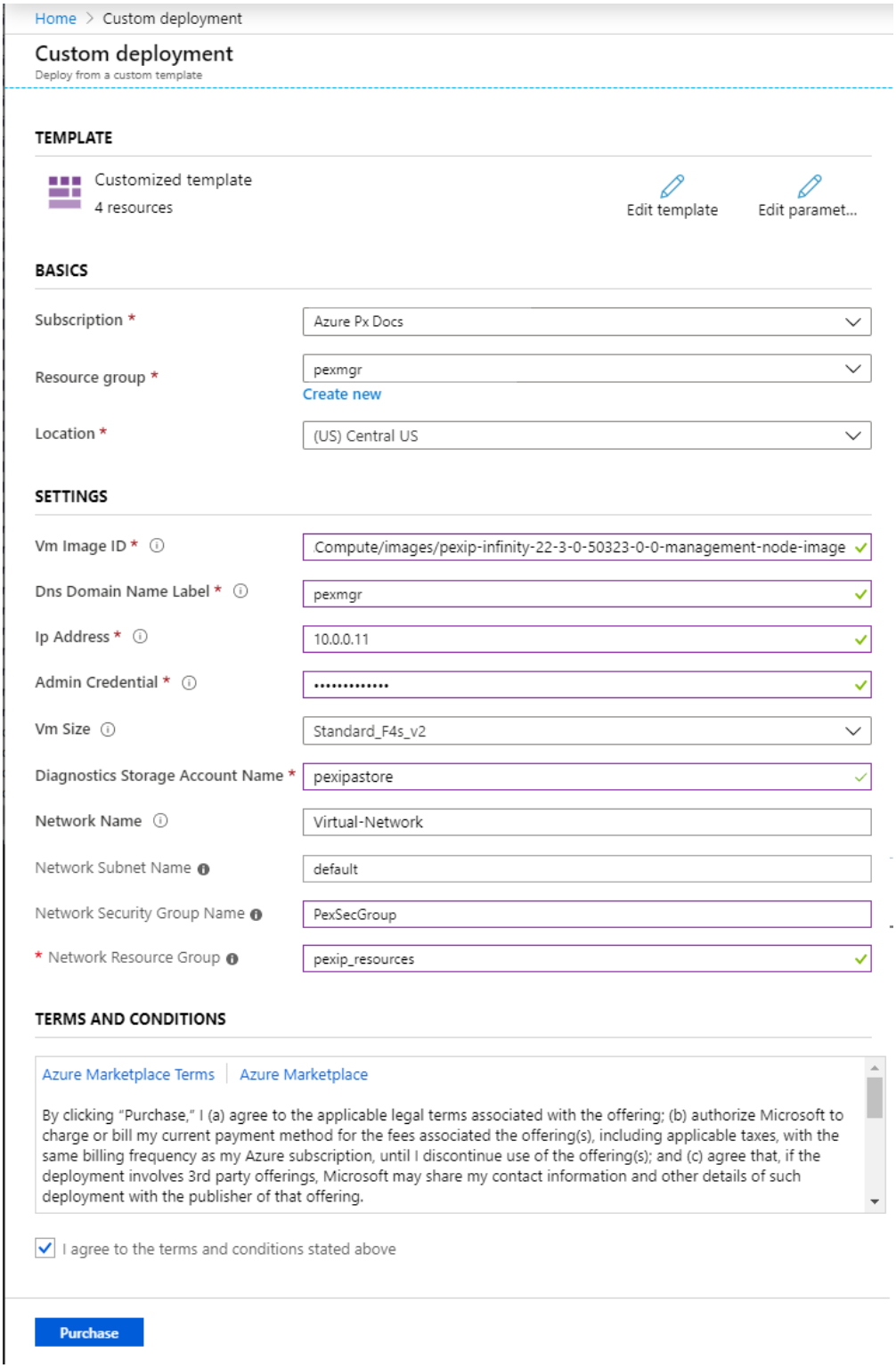
b. Enter the **Basics** by selecting your **Subscription**, **Resource group** and **Location** (region).

c. Complete the **Settings** (these are based on the template's parameters):

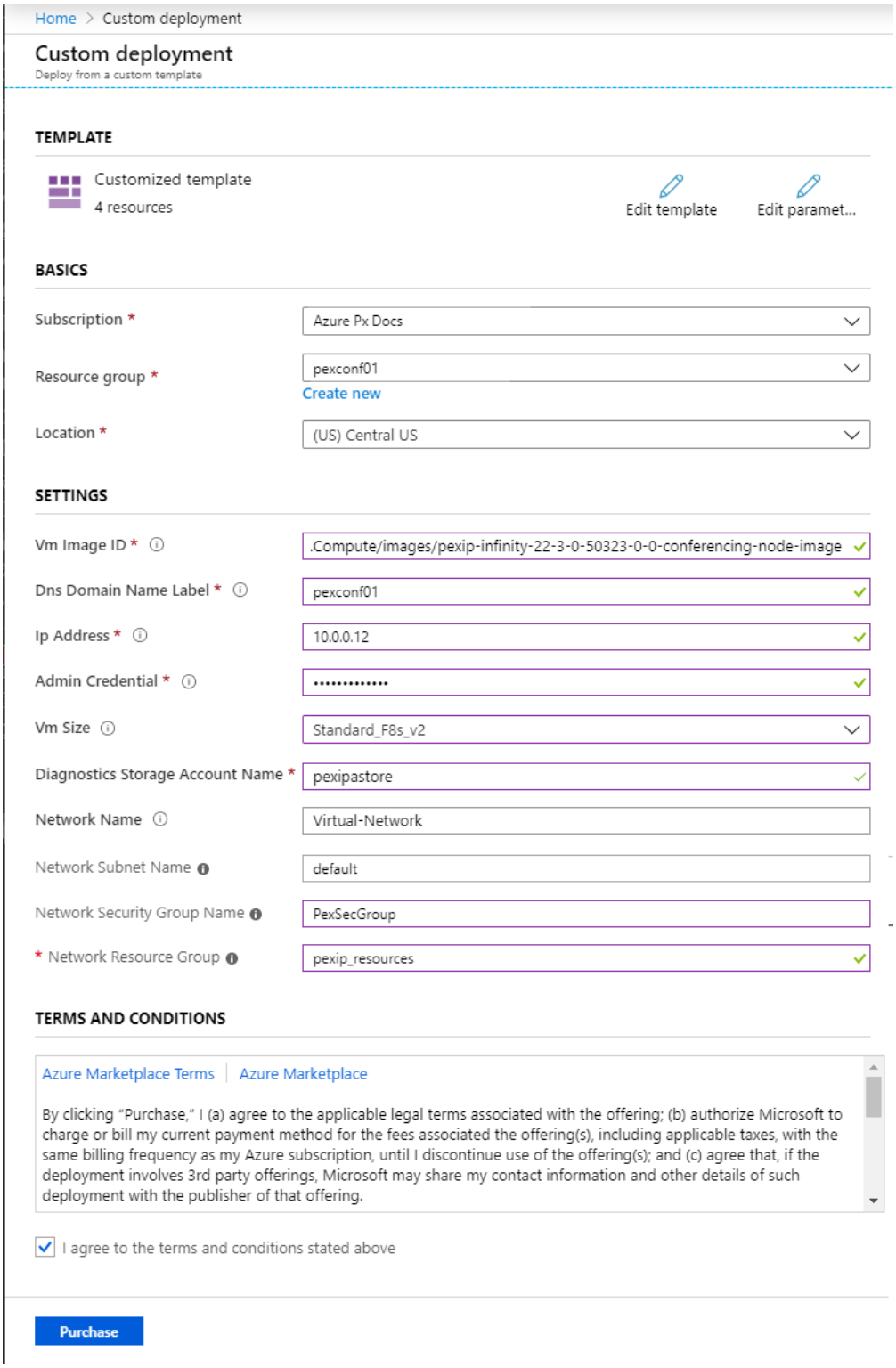
| Name | Description |
|---|---|
| Vm Image ID | The **Resource ID** of the Azure image (which is in the style /subscriptions/mysubscriptionid/resourceGroups/myressourcegroup/providers/Microsoft.Compute/images/myimage).<br><br>This resource ID can be obtained from the Azure portal by selecting your **Resource Group** used for shared resources, and then selecting either your Management Node or Conferencing Node image, and then copying the displayed **Resource ID**.<br><br>  <br><br>***Management Node image resource ID***<br><br>  <br><br>***Conferencing Node image resource ID*** |
| Dns Domain Name Label | The domain name label (i.e. hostname) for the Virtual Machine.<br><br>When deploying an instance with a public IP address, this label must be the host part only — the name must not contain any periods. |
| Ip Address | The statically-assigned private IP address for the Virtual Machine.<br><br>This must be within the IP range of your Virtual Network. Note that the first and last IP addresses of each subnet are reserved for protocol conformance, along with the x.x.x.1-x.x.x.3 addresses of each subnet, which are used for Azure services. |

| Name | Description |
|---|---|
| Admin Credential | 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).<br><br>For SSH key-based templates, this is the public SSH key for logging into the Virtual Machine (e.g. ssh-rsa AAA.... user@host). Do **not** use the ***Generate new key pair*** option (as this will generate an error) but instead use an existing public key or a key already stored in Azure. |
| Vm Size | The size of the Virtual Machine (typically F4s v2 for a Management Node or F8s v2 for a Transcoding Conferencing Node). You can change the **Size** later from within the Azure portal (Virtual Machine settings), if required. See Recommended instance types and call capacity guidelines for more information.<br><br>Azure regularly updates the instance types that can be deployed in each region. Therefore, you may receive a "The requested size for resource <name> is currently not available in location <region> zones" style error when deploying a node. See Troubleshooting instance size errors for help in resolving these errors. |
| Diagnostics Storage Account Name | The name of the storage account to use for boot diagnostics. This can be the same storage account that is used to hold the prepared disk images. Note that this storage account **cannot** use Premium storage. |
| Network Name | The name of the Virtual Network to connect to. |
| Network Subnet Name | The name of the Virtual Network subnet in which to place the Virtual Machine. |
| Network Security Group Name | The name of the Network Security Group to apply to the Virtual Machine. |
| Network Resource Group | The name of the Resource Group containing the Virtual Network and Network Security Group. |

d. Review and confirm the Terms and Conditions.
e. Select **Purchase** to deploy the instance.




***Management Node VM deployment***




***Conferencing Node VM deployment***

3. 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.
4. 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.

To deploy a template via PowerShell commands, follow this model:

```
$Credential=ConvertTo-SecureString <password/key> -asplaintext -force
```

```
New-AzResourceGroupDeployment -ResourceGroupName <resource group name> -TemplateUri <template URL> -vmImageID "<VM disk image Resource ID>" -dnsDomainNameLabel pexmgr -ipAddress "<private IP address>" -adminCredential $Credential -vmSize <VM size> -diagnosticsStorageAccountName <storage account name> -networkName <virtual network name> -networkSubnetName <Virtual Network subnet name> -networkSecurityGroupName <security group name> -networkResourceGroup <resource group name>
```

For example, for a Management Node using the template for password-based authentication and a public IP address:

```
$Credential=ConvertTo-SecureString Abcd_2468 -asplaintext -force
```

```
New-AzResourceGroupDeployment -ResourceGroupName pexmgr -TemplateUri https://pexipas.blob.core.windows.net/templates/20220112/virtual-machine-password-static-public-ip.json -vmImageID "/subscriptions/1bc-etc-9yz/resourceGroups/pexip_resources/providers/Microsoft.Compute/images/pexip-infinity-22-3-0-50323-0-0-management-node-image" -dnsDomainNameLabel pexmgr -ipAddress "10.0.0.5" -adminCredential $Credential -vmSize Standard_F4s_v2 -diagnosticsStorageAccountName pexipastore -networkName pexip_virtual_network -networkSubnetName default -networkSecurityGroupName PexSecGroup -networkResourceGroup pexip_resources
```

## 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 (as described 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 either with or without a public address. Every template enables boot diagnostics for the Virtual Machine instance.

When you deploy this template, Microsoft is able to identify the installation of Pexip software with the Azure resources that are deployed. Microsoft is able to correlate the Azure resources that are used to support the software. Microsoft collects this information to provide the best experiences with their products and to operate their business. The data is collected and governed by Microsoft's privacy policies, which can be found at https://www.microsoft.com/trustcenter. Please contact your Pexip authorized support representative if you do not want to share with Microsoft the telemetry of the VMs that are running Pexip software.

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-static-public-ip | Password based | Yes (static) | https://pexipas.blob.core.windows.net/templates/20220330/virtual-machine-password-static-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/20220330/virtual-machine-password-no-public-ip.json (launch in Azure Portal) | • Network interface • Virtual Machine |
| virtual-machine-sshkey-static-public-ip | SSH key based | Yes (static) | https://pexipas.blob.core.windows.net/templates/20220330/virtual-machine-sshkey-static-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/20220330/virtual-machine-sshkey-no-public-ip.json (launch in Azure Portal) | • Network interface • Virtual Machine |

Prior to 2020, the ARM templates and guidelines provided by Pexip for deploying VM instances used unmanaged disks in a storage account with standard performance. The current ARM templates use managed disks. VMs deployed with a mix of managed and unmanaged disks can co-exist in your Pexip Infinity deployment, however you may want to convert any previously deployed VMs to use managed disks with premium performance. For more information see Converting VM instances to managed disks and to premium performance.

## Azure US Government Cloud

If you use Azure US Government Cloud you have to follow a modified procedure and make some changes to the ARM templates to ensure that you are using the correct environment:

1. Manually download the required ARM template from the template URL shown in the table above (do not use the provided "launch in Azure portal" hyperlink).
2. Modify the ARM template to refer to the correct storage URI for US Government cloud:

   Change `.blob.core.windows.net` to `.blob.core.usgovcloudapi.net`
3. Upload the modified template as a "Custom Template" in your US Government Cloud environment. You can then use this template to create your instances.

## Troubleshooting instance size errors

Azure regularly updates the instance types that can be deployed in each region. Therefore, you may receive a "The requested size for resource <name> is currently not available in location <region> zones" style error when deploying a node.

To resolve these types of errors you can edit the Pexip ARM template to add in a supported instance type for that region:

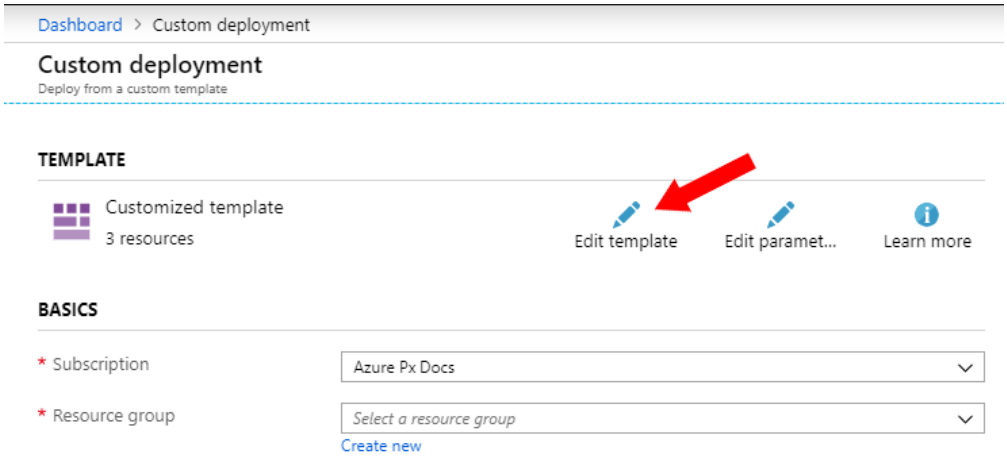
1. Obtain a list of available compute resources for your region:
   a. Run a PowerShell command in the format `Get-AzComputeResourceSku | where {$_.Locations -icontains "<region name>"}`

      For example: `Get-AzComputeResourceSku | where {$_.Locations -icontains "uksouth"}`

      This will output a list of resources, including VirtualMachines, for example:

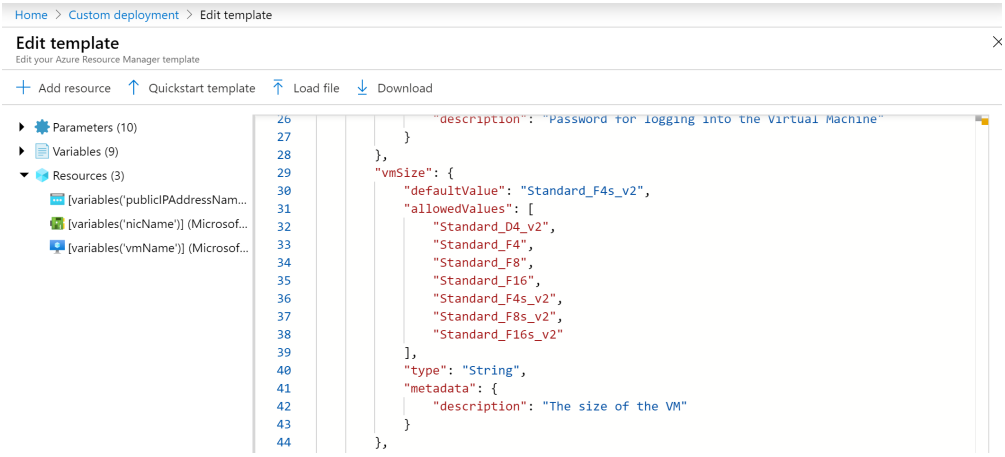
```
virtualMachines        Standard_E32s_v3  uksouth       NotAvailableForSubscription            MaxResourceVolumeMB ...8
virtualMachines     Standard_E64-16s_v3  uksouth       NotAvailableForSubscription            MaxResourceVolumeMB ...6
virtualMachines     Standard_E64-32s_v3  uksouth       NotAvailableForSubscription            MaxResourceVolumeMB ...6
virtualMachines       Standard_E64is_v3  uksouth       NotAvailableForSubscription            MaxResourceVolumeMB ...6
virtualMachines        Standard_E64s_v3  uksouth       NotAvailableForSubscription            MaxResourceVolumeMB ...6
virtualMachines             Standard_H8  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines            Standard_H16  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines            Standard_H8m  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines           Standard_H16m  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines           Standard_H16r  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines          Standard_H16mr  uksouth                                              MaxResourceVolumeMB ...0
virtualMachines         Standard_F2s_v2  uksouth                                              MaxResourceVolumeMB ...4
virtualMachines         Standard_F4s_v2  uksouth                                              MaxResourceVolumeMB ...8
virtualMachines         Standard_F8s_v2  uksouth                                              MaxResourceVolumeMB ...6
```

   b. Identify a resource name that is **not** tagged as "NotAvailableForSubscription" in your region.
2. Edit the Pexip ARM template and add in the resource that you have identified above:
   a. Start to deploy the instance, using the "launch in Azure Portal" link to launch the template as usual.
   b. Select **Edit template**.



c. In the **vmSize** section, add in the name of resource that you have identified above.

Ensure that you maintain the correct style and structure of the list:




d. Select **Save**.

You can now continue to deploy your node.

3. Complete the **Settings** as described above, but for **Vm Size** select the name of the resource you added to the template.

You can change the **Size** later from within the Azure portal (Virtual Machine settings), if required.

# Deploying a Management Node in Azure

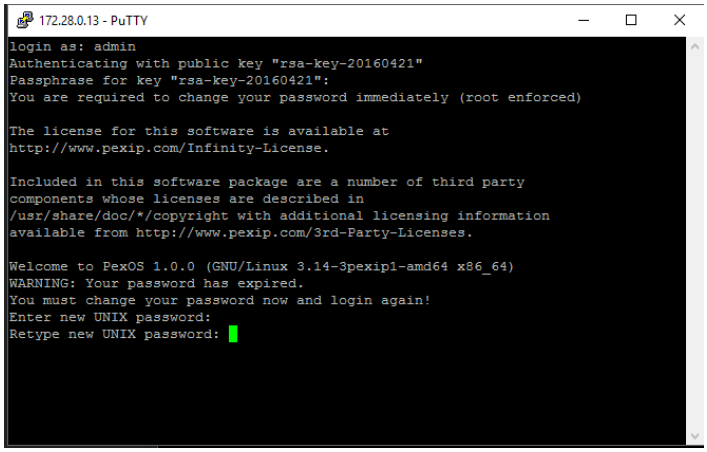
As with all Pexip Infinity deployments, you must first deploy the Management Node before deploying any Conferencing Nodes. In a hybrid cloud deployment the Management Node may be deployed in the corporate network or in Azure. This section describes how to deploy the Management Node in Azure.

To deploy a Management Node in Azure:

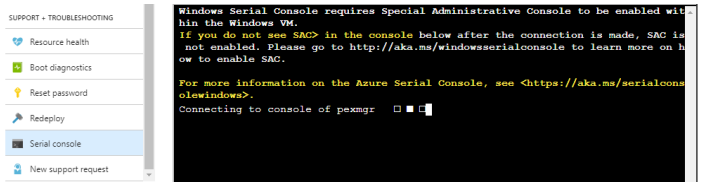
1. Create a VM instance using the prepared Management Node disk image. For more information on this, see:
   - Obtaining and preparing disk images for Azure deployments
   - Creating VM instances in Azure for your Pexip nodes
2. If you are using SSH key-based authentication (instead of password-based 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.

      If you cannot access the Management Node, check that you have allowed the appropriate source addresses in your Network Security Group inbound security rules for management traffic.
   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. Complete the Pexip Infinity installation wizard:
   a. Connect to the Management Node:
      - If using key-based authentication: reconnect over SSH into the Management Node instance by its private IP address.
      - If using password-based authentication: you can connect via the Azure portal's serial console — go to **Virtual Machines**, select your Management Node VM instance, and then select **Serial console**.




   b. 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:

      ```
      [sudo] password for admin:
      ```

c. 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.

d. Complete the installation wizard to apply basic configuration to the Management Node:

| | |
|---|---|
| IP address<br>Network mask<br>Gateway | Accept the defaults for the **IP address**, **Network mask** and **Gateway** settings. |
| Hostname<br>Domain suffix | Enter your required **Hostname** and **Domain suffix** for the Management Node. |
| DNS servers | Configure one or more **DNS servers**. You must override the default values if it is a private deployment. |
| NTP servers | Configure one or more **NTP servers**. You must override the default values if it is a private deployment. |
| Web administration username<br>Password | Set the **Web administration username** and **password**. |
| Enable incident reporting | Select whether or not to **Enable incident reporting**. |
| Send deployment and usage statistics to Pexip | Select whether or not to **Send deployment and usage statistics to Pexip**. |

ℹ 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.

```
[sudo] password for admin:
Running Pexip installation wizard...
Pexip installation wizard
                              IP Address [10.0.0.11]:
                         Network mask [255.255.255.0]:
                                 Gateway [10.0.0.1]:
                                        Hostname: pexmgr
                                   Domain suffix: vc.example.com
                                DNS servers [8.8.8.8]:
NTP servers [0.pexip.pool.ntp.org 1.pexip.pool.ntp.org]:
                  Web administration username [admin]:
                           Web administration password:
                              Re-enter previous value:
                    Enable incident reporting (yes/no): yes
 Send deployment and usage statistics to Pexip (yes/no): yes
Applying configuration...
Attempting to retrieve time from NTPServer="0.pexip.pool.ntp.org" Remaining-tr
ies="4"
Attempting to set system time
System time set correctly

Rebooting.


Broadcast message from admin@pexipmcumgr
        (/dev/ttyS0) at 13:31 ...

The system is going down for reboot NOW!

System going down for reboot
```

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 configure your Pexip Infinity platform licenses, VMRs, aliases, locations etc. as described in Initial platform configuration — Azure before you go on to add Conferencing Nodes.

# Initial platform configuration — Azure

After you have run the installation wizard, you must perform some preliminary configuration of the Pexip Infinity platform before you can deploy a Conferencing Node.

This section lists the configuration required, and provides a summary of each step with a link to further information.

All configuration should be done using the Pexip Infinity Administrator interface.

**No changes** should be made to any Pexip VM via the terminal interface (other than as described when running the initial Pexip installation wizard) unless directed to do so by Pexip support. This includes (but is not limited to) changes to the time zone, changes to IP tables, configuration of Ethernet interfaces, or the installation of any third-party code/applications.

## Accessing the Pexip Infinity Administrator interface

The Pexip Infinity Administrator interface is hosted on the Management Node. To access this:

1. Open a web browser and type in the IP address or DNS name that you assigned to the Management Node using the installation wizard (you may need to wait a minute or so after installation is complete before you can access the Administrator interface).
2. Until you have uploaded appropriate TLS certificates to the Management Node, your browser may present you with a warning that the website's security certificate is not trusted. You should proceed, but upload appropriate TLS certificates to the Management Node (and Conferencing Nodes, when they have been created) as soon as possible.

   The **Pexip Infinity Conferencing Platform** login page will appear.
3. Log in using the web administration username and password you set using the installation wizard.

You are now ready to begin configuring the Pexip Infinity platform and deploying Conferencing Nodes.

As a first step, we strongly recommend that you configure at least 2 additional NTP servers or NTP server pools to ensure that log entries from all nodes are properly synchronized.

It may take some time for any configuration changes to take effect across the Conferencing Nodes. In typical deployments, configuration replication is performed approximately once per minute. However, in very large deployments (more than 60 Conferencing Nodes), configuration replication intervals are extended, and it may take longer for configuration changes to be applied to all Conferencing Nodes (the administrator log shows when each node has been updated).

Brief details of how to perform the initial configuration are given below. For complete information on how to configure your Pexip Infinity solution, see the Pexip Infinity technical documentation website at docs.pexip.com.

## Configuring the Pexip Infinity platform

This table lists the Pexip Infinity platform configuration steps that are required before you can deploy Conferencing Nodes and make calls.

| Configuration step | Purpose |
|---|---|
| **1. Enable DNS**<br>**(System > DNS Servers)** | Pexip Infinity uses DNS to resolve the hostnames of external system components including NTP servers, syslog servers, SNMP servers and web proxies. It is also used for call routing purposes — SIP proxies, gatekeepers, external call control and conferencing systems and so on. The address of at least one DNS server must be added to your system.<br>You will already have configured at least one DNS server when running the install wizard, but you can now change it or add more DNS servers. |

| Configuration step | Purpose |
|---|---|
| **2. Enable NTP**<br>**(System > NTP Servers)** | Pexip Infinity uses NTP servers to obtain accurate system time. This is necessary to ensure correct operation, including configuration replication and log timestamps.<br>We strongly recommend that you configure at least three distinct NTP servers or NTP server pools on all your host servers and the Management Node itself. This ensures that log entries from all nodes are properly synchronized.<br>You will already have configured at least one NTP server when running the install wizard, but you can now change it or add more NTP servers. |
| **3. Add licenses**<br>**(Platform > Licenses)** | You must install a system license with sufficient concurrent call capacity for your environment before you can place calls to Pexip Infinity services. |
| **4. Add a system location**<br>**(Platform > Locations)** | These are labels that allow you to group together Conferencing Nodes that are in the same datacenter. You must have at least one location configured before you can deploy a Conferencing Node. |
| **5. Upload TLS certificates**<br>**(Platform > TLS Certificates)** | You must install TLS certificates on the Management Node and — when you deploy them — each Conferencing Node. TLS certificates are used by these systems to verify their identity to clients connecting to them.<br>All nodes are deployed with self-signed certificates, but we strongly recommend they are replaced with ones signed by either an external CA or a trusted internal CA. |
| **6. Add Virtual Meeting Rooms**<br>**(Services > Virtual Meeting Rooms)** | Conferences take place in Virtual Meeting Rooms and Virtual Auditoriums. VMR configuration includes any PINs required to access the conference. You must deploy at least one Conferencing Node before you can call into a conference. |
| **7. Add an alias for the Virtual Meeting Room**<br>(done while adding the Virtual Meeting Room) | A Virtual Meeting Room or Virtual Auditorium can have more than one alias. Conference participants can access a Virtual Meeting Room or Virtual Auditorium by dialing any one of its aliases. |

## Next step

You are now ready to deploy a Conferencing Node — see Deploying a Conferencing Node in Azure for more information.

# Deploying a Conferencing Node in Azure

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

Creating a new Conferencing Node is a two-step process:

1. Deploying a new VM instance in Azure.
2. Configuring the VM with the details of the specific Conferencing Node being deployed, using a file generated from the Pexip Infinity Management Node.

## Deploying the VM instance in Azure

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 for your Pexip nodes

   We recommend that each Conferencing Node VM instance is deployed in its own resource group.

   Note that if you have upgraded your Pexip Infinity software, you need a Conferencing Node disk image for the software version you are currently running.
2. After the instance has booted, perform a configuration-only deployment on the Management Node to inform it of the new Conferencing Node as described below.

## Generating, downloading and deploying the configuration file

1. From the Pexip Infinity Administrator interface, go to **Platform > Conferencing Nodes** and select **Add Conferencing Node**.
2. You are now asked to provide the network configuration to be applied to the Conferencing Node, by completing the following fields:

| Option | Description |
|---|---|
| Name | Enter the name to use when referring to this Conferencing Node in the Pexip Infinity Administrator interface. |
| Description | An optional field where you can provide more information about the Conferencing Node. |
| Role | This determines the Conferencing Node's role:<br>◦ ***Proxying Edge Node***: a Proxying Edge Node handles all media and signaling connections with an endpoint or external device, but does not host any conferences — instead it forwards the media on to a Transcoding Conferencing Node for processing.<br>◦ ***Transcoding Conferencing Node***: a Transcoding Conferencing Node handles all the media processing, protocol interworking, mixing and so on that is required in hosting Pexip Infinity calls and conferences. When combined with Proxying Edge Nodes, a transcoding node typically only processes the media forwarded on to it by those proxying nodes and has no direct connection with endpoints or external devices. However, a transcoding node can still receive and process the signaling and media directly from an endpoint or external device if required. |
| Hostname<br>Domain | Enter the hostname and domain to assign to this Conferencing Node. Each Conferencing Node and Management Node must have a unique hostname.<br><br>The Hostname and Domain together make up the Conferencing Node's DNS name or FQDN. We recommend that you assign valid DNS names to all your Conferencing Nodes. |

| Option | Description |
|---|---|
| IPv4 address | Enter the IP address to assign to this Conferencing Node when it is created.<br>This should be the Private IP address that you assigned to the VM instance (the ipAddress ARM template parameter). |
| Network mask | Enter the IP network mask to assign to this Conferencing Node.<br>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 IPv4 address | Enter the IP address of the default gateway to assign to this Conferencing Node.<br>This 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). |
| Secondary interface IPv4 address | Leave this option blank as dual network interfaces are not supported on Conferencing Nodes deployed in public cloud services. |
| Secondary interface network mask | Leave this option blank as dual network interfaces are not supported on Conferencing Nodes deployed in public cloud services. |
| System location | Select the physical location of this Conferencing Node. A system location should not contain a mixture of proxying nodes and transcoding nodes.<br>If the system location does not already exist, you can create a new one here by clicking + to the right of the field. This will open up a new window showing the **Add System Location** page. |
| SIP TLS FQDN | A unique identity for this Conferencing Node, used in signaling SIP TLS Contact addresses. |
| TLS certificate | The TLS certificate to use on this node. This must be a certificate that contains the above **SIP TLS FQDN**. Each certificate is shown in the format **<subject name> (<issuer>)**. |
| IPv6 address | The IPv6 address for this Conferencing Node. Each Conferencing Node must have a unique IPv6 address. |
| Gateway IPv6 address | The IPv6 address of the default gateway.<br>If this is left blank, the Conferencing Node listens for IPv6 Router Advertisements to obtain a gateway address. |
| IPv4 static NAT address | Configure the Conferencing Node's static NAT address, if you have a assigned a public/external IP address to the instance.<br>Enter the public address allocated by Azure. |
| Static routes | From the list of **Available Static routes**, select the routes to assign to the node, and then use the right arrow to move the selected routes into the **Chosen Static routes** list. |
| Enable distributed database | This should usually be enabled (checked) for all Conferencing Nodes that are expected to be "always on", and disabled (unchecked) for nodes that are expected to only be powered on some of the time (e.g. nodes that are likely to only be operational during peak times). |
| Enable SSH | Determines whether this node can be accessed over SSH.<br>***Use Global SSH setting***: SSH access to this node is determined by the global **Enable SSH** setting (**Platform > Global Settings > Connectivity > Enable SSH**).<br>***Off***: this node cannot be accessed over SSH, regardless of the global **Enable SSH** setting.<br>***On***: this node can be accessed over SSH, regardless of the global **Enable SSH** setting.<br>Default: ***Use Global SSH setting***. |

3. Select **Save**.

4. You are now asked to complete the following fields:

| Option | Description |
|---|---|
| Deployment type | Select ***Generic (configuration-only)***. |
| SSH password | Enter the password to use when logging in to this Conferencing Node's Linux operating system over SSH. The username is always ***admin***.<br><br>Logging in to the operating system is required when changing passwords or for diagnostic purposes only, and should generally be done under the guidance of your Pexip authorized support representative. In particular, do not change any configuration using SSH — all changes should be made using the Pexip Infinity Administrator interface. |

5. Select **Download**.

   A message appears at the top of the page: "The Conferencing Node image will download shortly or click on the following link".

   After a short while, a zip file with the name **pexip-<hostname>.<domain>.xml** is generated and downloaded.

   Note that the generated file is only available for your current session so you should download it immediately.

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

   If you cannot access the Conferencing Node, check that you have allowed the appropriate source addresses in your security group inbound rules for management traffic. In public deployments and where there is no virtual private network, you need to use the public address of the node.

   The Conferencing Node will apply the configuration and reboot. After rebooting, it will connect to the Management Node in the usual way.

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

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 becomes available, the Management Node reports the status of the Conferencing Node as having a last contacted and last updated date of "Never". "Connectivity lost between nodes" alarms relating to that node may also appear temporarily.

# Configuring dynamic bursting to the Microsoft Azure cloud

Pexip Infinity deployments can burst into the Microsoft Azure cloud when primary conferencing capabilities are reaching their capacity limits, thus providing additional temporary Conferencing Node resources.

This provides the ability to dynamically expand conferencing capacity whenever scheduled or unplanned usage requires it. The Azure cloud Conferencing Nodes instances are only started up when required and are automatically stopped again when capacity demand normalizes, ensuring that Azure costs are minimized.

For complete information about dynamic bursting, see Dynamic bursting to a cloud service.

## Configuring your system for dynamic bursting to Microsoft Azure

These instructions assume that you already have a working Pexip Infinity platform, including one or more primary (always on) Conferencing Nodes in one or more system locations. These existing Conferencing Nodes can be deployed using whichever platform or hypervisor you prefer.

### Firewall addresses/ports required for access to the Azure APIs for cloud bursting

Access to the Microsoft Azure APIs for cloud bursting is only required from the Management Node.

The Management Node always connects to destination port 443 over HTTPS.

DNS is used to resolve the Azure API addresses. Currently, Pexip Infinity uses the following DNS FQDNs (but these may change in the future):

- login.microsoftonline.com
- management.azure.com

### Setting up your bursting nodes in Microsoft Azure and enabling bursting in Pexip Infinity

You must deploy in Azure the Conferencing Nodes that you want to use for dynamic bursting, and then configure the Pexip Infinity location containing those nodes as the overflow destination for the locations that contain your primary (always on) Conferencing Nodes:

1. In Pexip Infinity, configure a new system location for media overflow e.g. "Azure burst", that will contain your bursting Conferencing Nodes.

   (Note that system locations are not explicitly configured as "primary" or "overflow" locations. Pexip Infinity automatically detects the purpose of the location according to whether it contains Conferencing Nodes that may be used for dynamic bursting.)
2. In Azure, set up an Active Directory (AD) application and assign the required permissions to it that will allow the Pexip Infinity Management Node to log in to Azure to start and stop the node instances.

   See Configuring an Active Directory (AD) application and permissions for controlling overflow nodes for more information.
3. Deploy in Azure the Conferencing Nodes that you want to use for dynamic bursting. Deploy these nodes in the same manner as you would for "always on" usage (see Deploying a Conferencing Node in Azure), except:
   a. Apply to each cloud VM node instance to be used for conference bursting a tag with a **Key** of **pexip-cloud** and an associated **Value** set to the **Tag value** that is shown in the **Cloud Bursting** section on the **Platform > Global Settings** page (the **Tag value** is the hostname of your Management Node).

      This tag indicates which VM nodes will be started and shut down dynamically by your Pexip system.
   b. When adding the Conferencing Node within Pexip Infinity:
      i. Assign the Conferencing Node to the overflow system location (e.g. "Azure burst").
      ii. Disable (uncheck) the **Enable distributed database** setting (this setting should be disabled for any nodes that are not expected to always be available).
   c. After the Conferencing Node has successfully deployed, manually stop the node instance on Azure.
4. In Pexip Infinity, go to **Platform > Global Settings > Cloud Bursting**, enable cloud bursting and then configure your bursting threshold, minimum lifetime and other appropriate settings for Azure:

| Option | Description |
|---|---|
| Enable bursting to the cloud | Select this option to instruct Pexip Infinity to monitor the system locations and start up / shut down overflow Conferencing Nodes hosted in your cloud service when in need of extra capacity. |
| Bursting threshold | The bursting threshold controls when your dynamic overflow nodes in your cloud service are automatically started up so that they can provide additional conferencing capacity. When the number of additional HD calls that can still be hosted in a location reaches or drops below the threshold, it triggers Pexip Infinity into starting up an overflow node in the overflow location.<br><br>See Configuring the bursting threshold for more information. |
| Tag name and Tag value | These read-only fields indicate the tag name (always **pexip-cloud**) and associated tag value (the hostname of your Management Node) that you must assign to each of your cloud VM node instances that are to be used for dynamic bursting. |
| Minimum lifetime | An overflow cloud bursting node is automatically stopped when it becomes idle (no longer hosting any conferences). However, you can configure the **Minimum lifetime** for which the bursting node is kept powered on. By default this is set to 50 minutes, which means that a node is never stopped until it has been running for at least 50 minutes. If your service provider charges by the hour, it is more efficient to leave a node running for 50 minutes — even if it is never used — as that capacity can remain on immediate standby for no extra cost. If your service provider charges by the minute you may want to reduce the **Minimum lifetime**. |
| Cloud provider | Select ***Azure***. |
| Azure subscription ID | The ID of your Azure subscription. |
| Azure client ID | The ID used to identify the client (sometimes referred to as Application ID). |
| Azure secret key | The Azure secret key that is associated with the Azure client ID. |
| Azure tenant ID | The Azure tenant ID that is associated with the Azure client ID. |

5. Go to **Platform > Locations** and configure the system locations that contain your "always on" Conferencing Nodes (the nodes/locations that initially receive calls) so that they will overflow to your new "Azure burst" location when necessary.

   When configuring your principal "always on" locations, you should normally set the **Primary overflow location** to point at the bursting location containing your overflow nodes, and the **Secondary overflow location** should normally only point at an always-on location.

   Nodes in a bursting location are only automatically started up if that location is configured as a **Primary overflow location** of an always-on location that has reached its capacity threshold. This means that if a bursting location is configured as a **Secondary overflow location** of an always-on location, then those nodes can only be used as overflow nodes if they are already up and running (i.e. they have already been triggered into starting up by another location that is using them as its **Primary overflow location**, or you have used some other external process to start them up manually).

   We recommend that you do not mix your "always on" Conferencing Nodes and your bursting nodes in the same system location.

## Configuring an Active Directory (AD) application and permissions for controlling overflow nodes

Within Azure you must set up an Active Directory (AD) application and permissions to be used by Pexip Infinity to start up and shut down the Conferencing Node overflow instances. You need to ensure that your Azure account has sufficient permissions to register an application with your Active Directory, and assign the application to a role in your Azure subscription.

A summary description of the tasks involved and the required permissions is given below. Full information of how to check your account permissions, create the application and assign a role is available at https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal.

1. Create an Active Directory application of type ***Web app / API***. Enter a name such as "**pexip**" for example.
   a. Use the assigned **Application ID** as the **Azure client ID** in the Pexip Infinity **Global Settings** page.
   b. Generate a key for the application, copy its value and use it as the **Azure secret key** in the **Global Settings** page.

2. Lookup the Directory ID in the properties of your Azure Active Directory and use it as the **Azure tenant ID** in the **Global Settings** page.
3. Assign the Active Directory application to a role. Typically you will assign a role at the Subscriptions level.

   Select **Access Control (IAM) > Add**, select the role you want to assign, and then search for and select your application e.g. "pexip".

   Azure contains many built-in roles; the most appropriate built-in role to use for dynamic bursting is ***Virtual Machine Contributor*** (https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor).

   If you want to create your own custom role (https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-custom-roles), the permissions required by Pexip Infinity are:

| Actions (permissions) | Allows Pexip Infinity to... |
|---|---|
| Microsoft.Authorization/*/read | Read roles and role assignments. |
| Microsoft.Compute/virtualMachines/*/read | Read the properties of a virtual machine (VM sizes, runtime status, VM extensions, etc). |
| Microsoft.Compute/virtualMachines/deallocate/action | Deallocate virtual machines. |
| Microsoft.Compute/virtualMachines/read | Read the properties of a virtual machine. |
| Microsoft.Compute/virtualMachines/start/action | Start virtual machines. |
| Microsoft.Compute/virtualMachines/powerOff/action | Powers off the virtual machine. |

## Configuring the bursting threshold

When enabling your platform for cloud bursting the most important decision you must make is the level at which to set the bursting threshold:

- The bursting threshold controls when your dynamic overflow nodes in your cloud service are automatically started up so that they can provide additional conferencing capacity. When the number of additional HD calls that can still be hosted in a location reaches or drops below the threshold, it triggers Pexip Infinity into starting up an overflow node in the overflow location.

  For example, setting the threshold to 5 means that when there are 5 or fewer HD connections still available in a location, an overflow node will be started up.
- When an overflow location reaches the bursting threshold i.e. the number of additional HD calls that can still be hosted on the Conferencing Nodes in the overflow location reaches the threshold, another overflow node in that location is started up, and so on.

  Note that the current number of free HD connections in the original location is ignored when deciding if the overflow location needs to overflow further — however, new calls will automatically use any available media resource that has become available within the original principal location.
- The bursting threshold is a global setting — it applies to every system location in your deployment.
- Note that it takes approximately 5 minutes for a dynamic node instance to start up and become available for conference hosting. If your principal deployment reaches full capacity, and the overflow nodes have not completed initiating, any incoming calls during this period will be rejected with "capacity exceeded" messages. You have to balance the need for having standby capacity started up in time to meet the expected demand, against starting up nodes too early and incurring extra unnecessary costs.

## Manually starting an overflow node

If you know that your system will need additional capacity at a specific time due to a predictable or scheduled spike in demand, but do not want to wait for the bursting threshold to be triggered before starting up the overflow nodes, you can manually start up any of your overflow nodes.

Do not manually start an overflow node too early. If you manually start up a node more than the **Minimum lifetime** minutes before the node is needed, it will most probably get automatically stopped again before it is used.

You can start overflow nodes via the management API or via the Administrator interface:

- **Via the management API**: the cloud_node status resource can be used to list all of the available overflow nodes, the cloud_monitored_location and cloud_overflow_location resources retrieve the current load on the primary locations and any currently active overflow locations respectively, and the start_cloudnode resource can be used to manually start up any overflow node. This means that a third-party scheduling system, for example, could be configured to start up the overflow nodes via the management API approximately 10 minutes before a large conference is due to start.

  For example, let's assume that you have:
  - a regular spike in conferencing capacity demand at 9:00am every morning
  - an even usage of about 20% of that spike level during the rest of the day
  - a 30:70 ratio between your "always on" capacity and your overflow cloud capacity

  we would recommend:
  - configuring a low bursting threshold, such as 10-20% of your "always on" capacity (i.e. if your "always on" capacity is 80 HD calls, then set the bursting threshold to 12)
  - getting your scheduling system to call the API to manually start up all of your overflow cloud nodes at 8:50am on weekdays.
- **Via the Pexip Infinity Administrator interface**: go to **Status > Cloud Bursting** and select **Start** for the required nodes (the **Start** option is in the final column of the **Cloud overflow nodes** table).

## Converting between overflow and "always on" Microsoft Azure Conferencing Nodes

If you need to convert an existing "always on" Azure Conferencing Node into an overflow node:

1. In Azure:
   a. Apply to the instance a tag with a **Key** of **pexip-cloud** and an associated **Value** set to the **Tag value** that is shown in the **Cloud bursting** section of the **Platform > Global Settings** page.
   b. Manually stop the node instance on Azure.
2. In Pexip Infinity:
   a. Change the system location of the Conferencing Node to the overflow system location (e.g. "Azure burst").
   b. Disable the node's **Enable distributed database** setting.
      You should avoid frequent toggling of this setting. When changing this setting on multiple Conferencing Nodes, update one node at a time, waiting a few minutes before updating the next node.

If you need to convert an existing Azure overflow Conferencing Node into an "always on" node:

1. In Azure:
   a. Remove the tag with a **Key** of **pexip-cloud** from the Azure instance.
   b. Manually start the node instance on Azure.
2. In Pexip Infinity:
   a. Change the system location of the Conferencing Node to a location other than the overflow system location.
   b. Enable the node's **Enable distributed database** setting.
      You should avoid frequent toggling of this setting. When changing this setting on multiple Conferencing Nodes, update one node at a time, waiting a few minutes before updating the next node.

# Managing Azure instances

This section describes the common maintenance tasks for managing your Azure instances:

- Scheduled maintenance events in Azure
- Temporarily removing (stopping) a Conferencing Node instance
- Reinstating (restarting) a stopped Conferencing Node instance
- Permanently removing a Conferencing Node instance
- Backing up VM instances (guidelines)
- Converting VM instances to managed disks and to premium performance

## Scheduled maintenance events in Azure

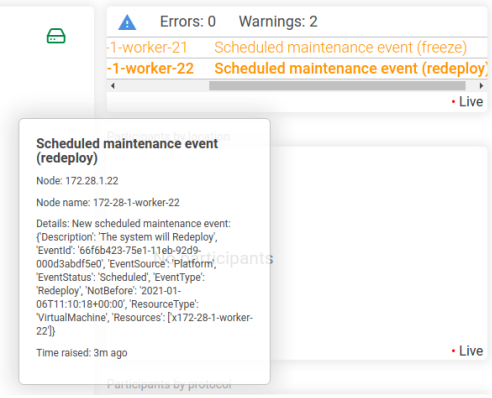
Scheduled Events is an Azure Metadata Service that provides information about upcoming VM maintenance events (for example, a reboot). Pexip Infinity VMs that are deployed in Azure poll for maintenance events automatically. No administrative configuration or action is required within Pexip Infinity or Azure.

When certain events are detected, such as a Freeze event, the Conferencing Node running on that VM is automatically placed into maintenance mode for the duration of the event (it is automatically taken out of maintenance mode when the event is complete).

Placing a Conferencing Node into maintenance mode won't protect any existing calls on that node when the event occurs, but it does mitigate the impact by preventing new calls from being accepted on that node.

The following table shows the types of maintenance events that are detected, the minimum notice period before the event is performed, if the event is acknowledged, if an alarm is raised on Pexip Infinity, and whether the Conferencing Node running on that VM is placed into maintenance mode.

| Event type | Minimum notice period | Acknowledged | Alarm raised | Maintenance mode |
|---|---|---|---|---|
| Freeze | 15 minutes | No | Yes | Yes |
| Reboot | 15 minutes | Yes | No | No |
| Redeploy | 10 minutes | No | Yes | Yes |
| Preempt | 30 seconds | No | Yes | Yes |
| Terminate | User configurable: 5 to 15 minutes | Yes | No | No |




Note that:

- All maintenance events are logged in the support log (modules: **support.pulse** and **support.scheduled_maintenance_events**). Alarms are also logged in the administrator log.

- A node may stay in maintenance mode for several minutes beyond the **NotBefore** timestamp indicated in the "New scheduled maintenance event" log entry.
- The system logs and raises alarms for VMs hosting a Management Node (but there is no maintenance mode for a Management Node),
- Only Pexip Infinity VMs are supported; Teams Connector instances are not supported.

## 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 > Conferencing Nodes**.
   b. Select the Conferencing Node(s).
   c. From the **Action** menu at the top left of the screen, select **Enable maintenance mode** and then select **Go**.
      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 > Live View**.
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 > 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 > 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 > Conferencing Nodes**.
   b. Select the Conferencing Node(s).
   c. From the **Action** menu at the top left of the screen, select **Enable maintenance mode** and then select **Go**.
      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 > Live View**.
2. Delete the Conferencing Node from the Management Node:
   a. Go to **Platform > 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 that 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. If boot diagnostics were enabled on the VM instance, delete the storage container that 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.

# Backing up VM instances (guidelines)

When backing up Azure VMs to a Recovery Services vault, you must shut down the VM before performing the backup.

# Converting VM instances to managed disks and to premium performance

Prior to 2020, the ARM templates and guidelines provided by Pexip for deploying VM instances used unmanaged disks in a storage account with standard performance. The current ARM templates use managed disks. VMs deployed with a mix of managed and unmanaged disks can co-exist in your Pexip Infinity deployment, however you may want to convert any previously deployed VMs to use managed disks with premium performance.

Note that the storage account used for VM boot diagnostics must use standard performance disks.

## Converting unmanaged disks to managed disks

To convert a VM from using unmanaged disks to managed disks via the Azure portal:

1. From the Azure portal, select **Virtual machines** to see a list of all of your instances.
2. Select the VM from the list of virtual machines in the portal.
3. Select **Disks** from the Settings sidepane for the VM.
4. At the top of the Disks pane, select **Migrate to managed disks**.
   If your VM is in an availability set, there will be a warning that you need to convert the availability set first. The warning should have a link you can select to convert the availability set.

5. When the availability set is converted or if your VM is not in an availability set, select **Migrate** to start the process of migrating your disks to managed disks.

The conversion may take 1-2 minutes. The VM will be stopped and restarted after migration is complete.

## Converting managed disks from Standard to Premium

To convert a VM's managed disks from Standard to Premium via the Azure portal:

1. From the Azure portal, select **Virtual machines** to see a list of all of your instances.
2. Select the VM from the list of virtual machines in the portal.
3. If the VM is Running, select **Stop** at the top of VM Overview pane, and wait for the VM to stop.
4. Select **Disks** from the Settings sidepane for the VM.
5. Select the disk that you want to convert.
6. Select **Size + Performance** from the Settings menu.
7. Change the **Account type** from ***Standard HDD*** to ***Premium SSD***.
8. Select **Save**, and close the disk pane.
   The disk type conversion is instantaneous.
9. You can restart your VM after the conversion: return to the VM's Overview pane and select **Start** to restart the VM.