Enable Arc for Azure VMware Solution (AVS)

Overview

This article will help you deploy Arc for Azure VMware Solution. After you have successfully setup the new components needed for this public preview, you will be able to execute operations in Azure VMware Solution vCenter from the Azure portal. Operations are related to Create, Read, Update and Delete (CRUD) Virtual Machines in an Arc-enabled Azure VMware Solution private cloud. Users can also enable guest management and install Azure extensions once the private cloud is Arc-enabled

# Prerequisites

* A jump box Virtual Machine (VM) with network access to the Azure VMware Solution vCenter. From the jump-box VM, ensure you have access to [vCenter and NSX-T portals.](https://docs.microsoft.com/en-us/azure/azure-vmware/tutorial-configure-networking#locate-the-urls-for-vcenter-and-nsx-manager)
* Private cloud should be Internet enabled or should have reachability to Azure end points mentioned in Appendix 1.
* Resource group in the subscription where you have owner/contributor role.
* Have a minimum of 3 free non-overlapping IP addresses.
* Verify that your vCenter Server is 6.7 or above.
* A resource pool with minimum free capacity of 16 GB of RAM, 4 vCPUs. ( We will create a resource pool in case you don’t have one).
* A datastore with a minimum of 100 GB of free disk space that is available through the resource pool.
* On the vCenter Server, allow inbound connections on TCP port 443, so that the Arc resource bridge and VMware cluster extension can communicate with the vCenter server.(For AVS as of today, only the default port of 443 is supported if you use a different port, Appliance VM creation will fail)

> [!NOTE]

> Only the default port of 443 is supported if you use a different port, Appliance VM creation will fail.

At this point, you should have already deployed an Azure VMware Solution private cluster. You need to have a connection from your on-prem environment and/or from your native Azure Virtual Network to the Azure VMware Solution private cloud. We also assume that there will be an isolated NSX-T segment for deploying the Arc for AVS OVA appliance. This segment will be created if not present already.

* For Network planning and setup, use following guide: - [Tutorial - Network planning checklist - Azure VMware Solution | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-vmware/tutorial-network-checklist)

## Registration to Arc for Azure VMware Solution feature Set.

For provider registration using Az CLI, use (this can take some time, 10 minutes);

az provider register --namespace Microsoft.ConnectedVMwarevSphere

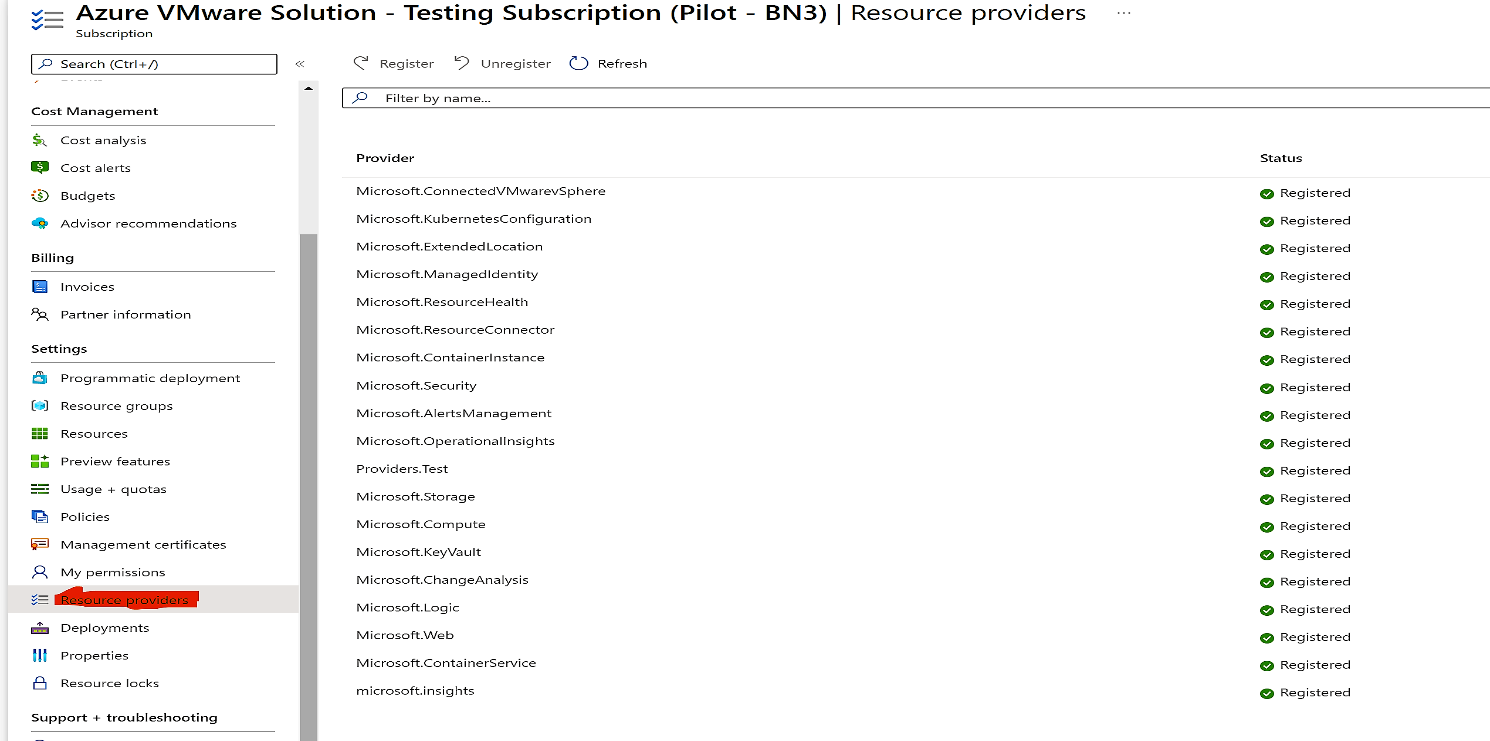
az provider register --namespace Microsoft.ExtendedLocation

az provider register --namespace Microsoft.KubernetesConfiguration

az provider register --namespace Microsoft.ResourceConnector

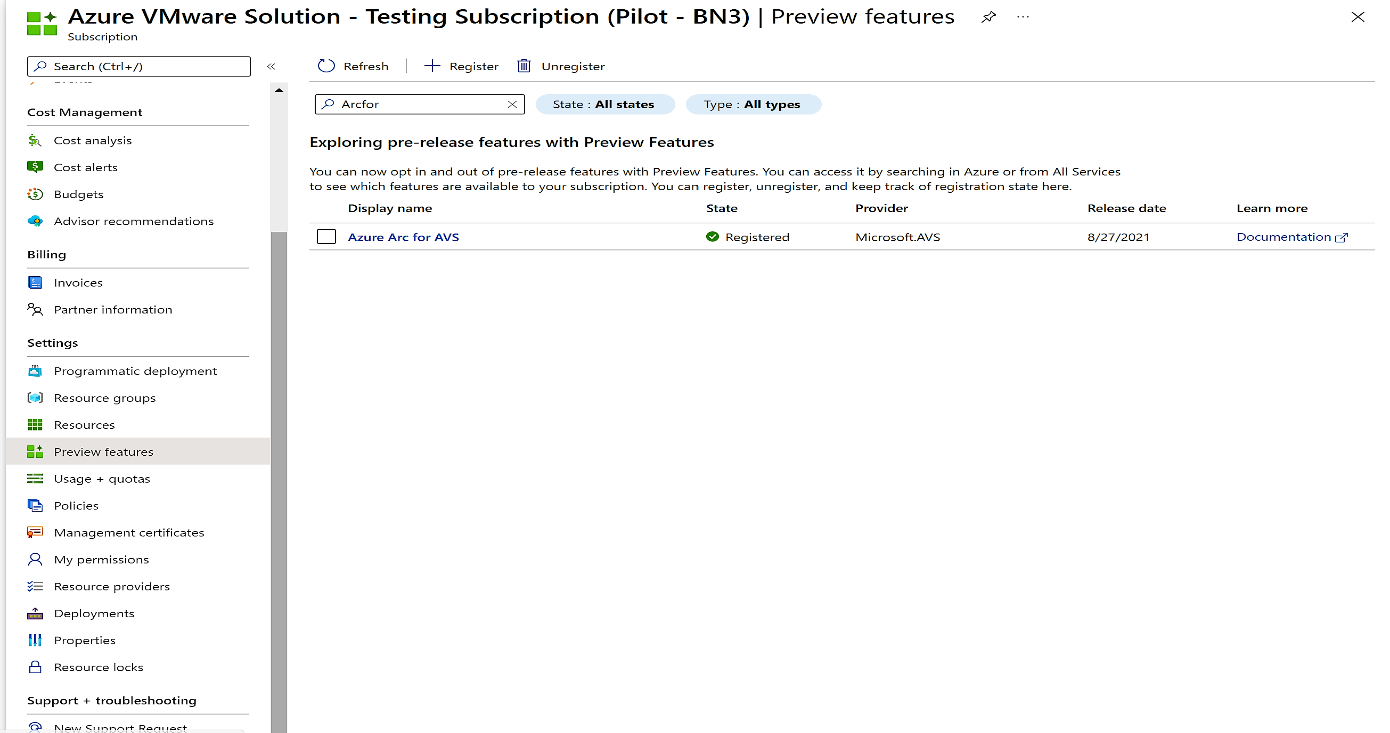
az provider register --namespace Microsoft.AVS

Alternatively, users can login to their Subscription, navigate to the “Resource provider” tab and can register themselves on the resource providers mentioned above.



For feature registration users will have to login to their Subscription and navigate to “preview features” tab and search for “Azure Arc for AVS”. Once registered no other permissions are required for users to access Arc.

Users also need to ensure that they also register themselves to Microsoft.AVS/earlyAccess.



To check if they are registered, use;

az feature show -–name AzureArcForAVS --namespace Microsoft.AVS

# ~~Step by step process to onboard in Arc for AVS preview~~ Onboard process to deploy Azure Arc

1. Log in to the jumpbox VM and extract the contents from the compressed file from the following [location](https://github.com/Azure/ArcOnAVS/releases). The extracted file contains the scripts to install the preview software. Change directory to src\appliance-onboarding-script
2. Open the ‘config\_avs.json’ file and populate all variables.

***Config JSON***

|  |
| --- |
| {  "subscriptionId": "",  "resourceGroup": "",  "applianceControlPlaneIpAddress": "",  "privateCloud": "",  "isStatic": true,  "staticIpNetworkDetails": {  "networkForApplianceVM": "",  "networkCIDRForApplianceVM": "",  "k8sNodeIPPoolStart": "",  "k8sNodeIPPoolEnd": "",  "gatewayIPAddress": ""  }  } |

* subscriptionId, resourceGroup, privateCloud – The subscription ID, Resource Group name and the Private cloud name respectively.
* isStatic are always true.
* networkForApplianceVM – Name for the segment for Arc appliance VM. This will be created if not present.
* networkCIDRForApplianceVM – The IP CIDR of the segment for Arc appliance VM. This should be unique. This should not collide with the address block for private cloud or the existing segments.
* GatewayIPAddress – The gateway for the segment for Arc appliance VM.
* applianceControlPlaneIpAddress – The IP address for the Kubernetes API server. This should be a part of the segment IP CIDR provided but not a part of the k8s node pool IP range.
* k8sNodeIPPoolStart, k8sNodeIPPoolEnd - The starting IP and the ending IP of the pool of IPs to assign to the appliance VM, have to be within the networkCIDRForApplianceVM

***Sample JSON***

|  |
| --- |
| {  "subscriptionId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  "resourceGroup": "test-rg ",  "applianceControlPlaneIpAddress": "10.14.10.10",  "privateCloud": "test-pc",  "isStatic": true,  "staticIpNetworkDetails": {  "networkForApplianceVM": "arc-segment",  "networkCIDRForApplianceVM": "10.14.10.1/24",  "k8sNodeIPPoolStart": "10.14.10.20",  "k8sNodeIPPoolEnd": "10.14.10.30",  "gatewayIPAddress": "10.14.10.1"  } } |

1. You are ready to run the installation scripts. We provide you the option to setup this preview from both a Windows or a Linux based jump box/VM.

Run the following commands to execute the installation script.

|  |  |
| --- | --- |
| **Windows based jump box/VM** | **Linux based jump box/VM** |
| Script is not signed so we need to bypass Execution Policy in PowerShell. Run the following commands.  **Set-ExecutionPolicy -Scope Process -ExecutionPolicy ByPass; .\run.ps1 -Operation onboard -FilePath {config-json-path**} | Add execution permission for the script and run the commands below.  **$ chmod +x run.sh**  **$ sudo bash run.sh onboard {config-json-path}** |

1. You will now see some additional (new) Azure Resources being created in your Resource Group.
   1. Resource bridge
   2. Custom location
   3. VMware vCenter

Please ensure that you are using the same Resource Group as where the Azure VMware Solution private cloud has been created. That is why you also see the Azure VMware Solution Private Cloud ‘type’.

Graphical user interface, text, application

Description automatically generated

## Overview of the Onboarding/~~De-~~Off boarding process

While invoking the script, you will be required to define one of the following ‘Operations’.

**~~Onboard~~** ~~– does the following:~~

1. ~~Download and install required tools to be able to execute preview software from jump box (az cli tools, python etc.), if not present already.~~
2. ~~Create AVS Azure VMware Solution segment as per details if not present already. Create DNS server and zones if not present already. Fetch vCenter credentials.~~
3. ~~Create template for Arc Appliance and take snapshot from template created.~~
4. ~~Deploy the Arc for AVS Azure VMware Solution appliance VM.~~
5. ~~Create an ARM resource for the appliance.~~
6. ~~Create a Kubernetes extension resource for azure VMware.~~
7. ~~Create a custom location.~~
8. ~~Create an Azure representation of the vCenter.~~
9. ~~Link the vCenter resource to the AVS Azure VMware Solution Private Cloud resource.~~

**~~Deboard~~****~~Off board~~** ~~– does the following:~~

1. ~~Download and install required tools to be able to execute preview software from jump box (az cli tools, python etc.), if not present already.~~
2. ~~De-link the vCenter resource from the AVS Private cloud resource.~~
3. ~~Delete the azure representation of the vCenter.~~
4. ~~Delete the Custom Location resource, the Kubernetes extension for Azure VMware operator, the Appliance~~
5. ~~Delete the appliance VM.~~

# Discover and project you VMware infrastructure resources to Azure

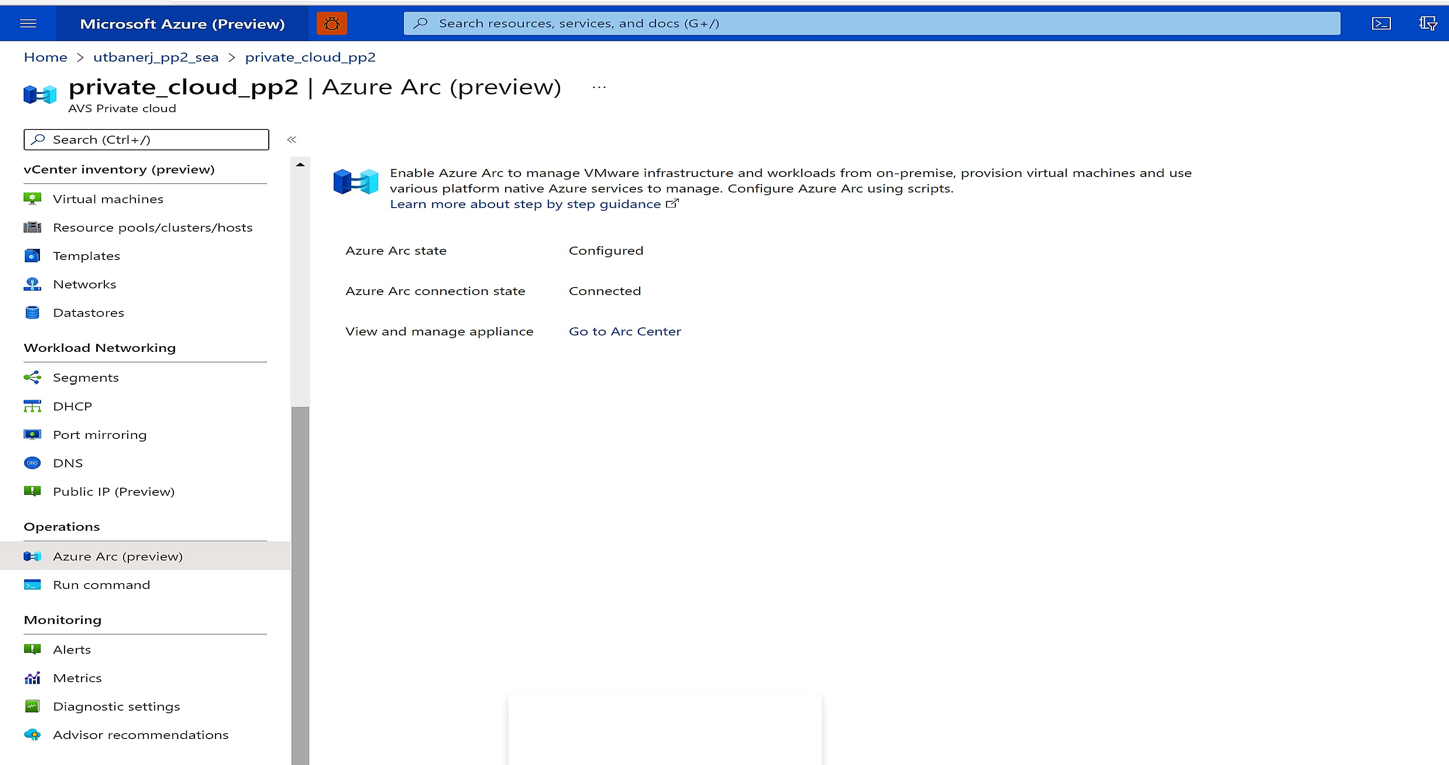
(Discovery & Projection from AVS Private Cloud Blade - section)

1. Once Arc appliance is successfully deployed on customer’s Private cloud, customers can view the status from within Private cloud blade under **“Operations > Arc”**
2. Customer can also view their VMware Infrastructure resources from the private cloud blade under “**Private cloud** then select **“vCenter inventory”.**
3. Customers can discover their VMware Infrastructure resources and then project them to Azure using the same browse experience.  **“Private cloud > vCenter inventory > Virtual Machines.”**
4. **Similar to VMs, customers can enable networks, templates, resource pools and data-stores in Azure.**
5. Once customers enable VMs to be managed from Azure, optionally they can then proceed to install guest management.
6. Enabling guest management will allow customers to install and use extensions.
7. However, to enable guest management customers will be required to use admin credentials as well as VMtools should be running on the VM.
8. AVS vCenter will be available in global search but will NOT be available in the list of vCenters for Arc for VMware.
9. VM extensions available in public preview:
   1. Change tracking,
   2. log analytics,
   3. Update management
   4. and Azure policy guest configuration

**AVS Private Cloud with Azure Arc**

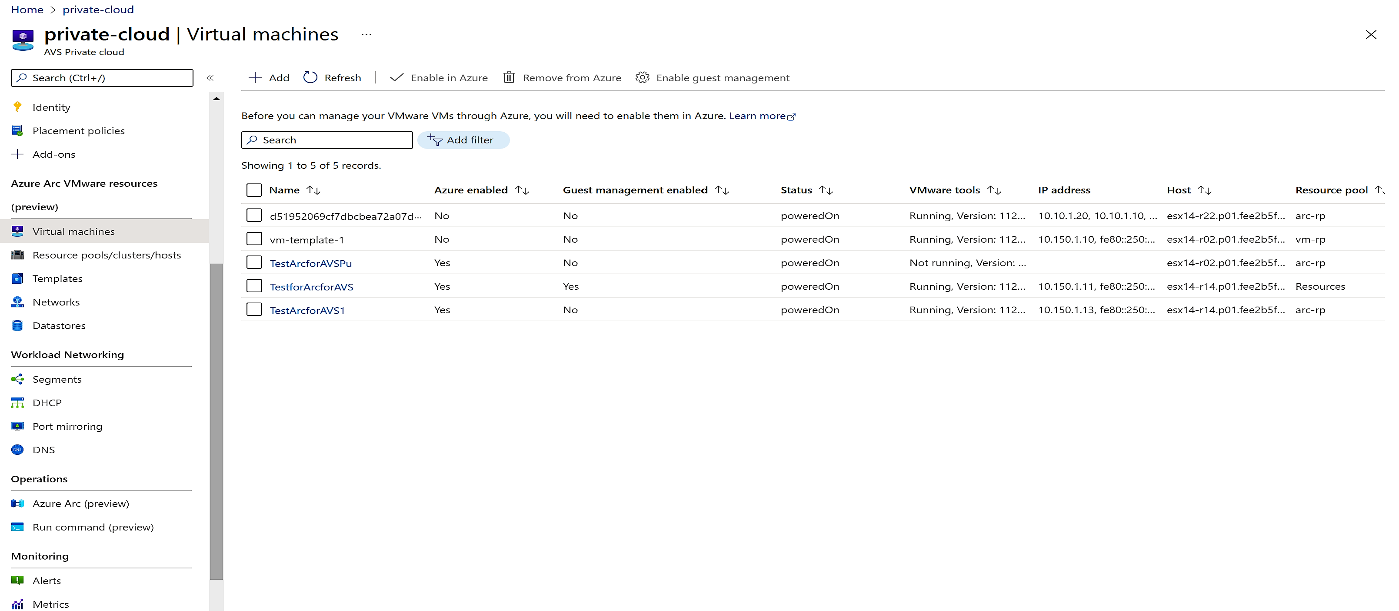
Click on **Operations** > **Azure Arc**. Azure Arc state should show **Configured**.

<crop image below to show the new section>



**Arc enabled VMware resources**

**Once the private cloud is Arc enabled, vCenter resources will appear under “VMware resources”**



# Manage access to VMware resources through Azure Role-Based Access Control

Once your Azure VMware Solution vCenter resources have been enabled for access through Azure, the final step in setting up a self-service experience for your teams is to provide them access to the compute, storage and networking, and other vCenter resources using which they can provision VMs.

This article will describe how to use custom roles to manage granular access to VMware resources through Azure.

## **Arc enabled VMware vSphere Custom Roles**

We provide three custom roles to meet your Role Based Access Controls. These roles can be applied to a whole subscription, resource group or even a single resource.

* Azure Arc VMware Administrator role
* Azure Arc VMware Private Cloud User role
* Azure Arc VMware VM Contributor role

The first role is for Administrator and the last two roles are needed for anyone who needs to deploy/manage a VM.

### **Azure Arc AVS Administrator role**

This custom role provides permissions to perform all operations for the Microsoft.ConnectedVMwarevSphere resource provider. This role should be assigned to users/groups that are administrators that manage Azure Arc enabled Azure VMware Solution ~~(AVS)~~ deployment.

### **Azure Arc AVS Private Cloud User role**

This custom role provides permissions to use the Arc enabled Azure VMware Solution ~~(AVS)~~ vSphere resources that have been made accessible through Azure. This role should be assigned to any users/groups that need to deploy, update or delete VMs.

We recommend assigning this role at the individual resource pool (or host or cluster), virtual network or template that you want the user to deploy VMs with.

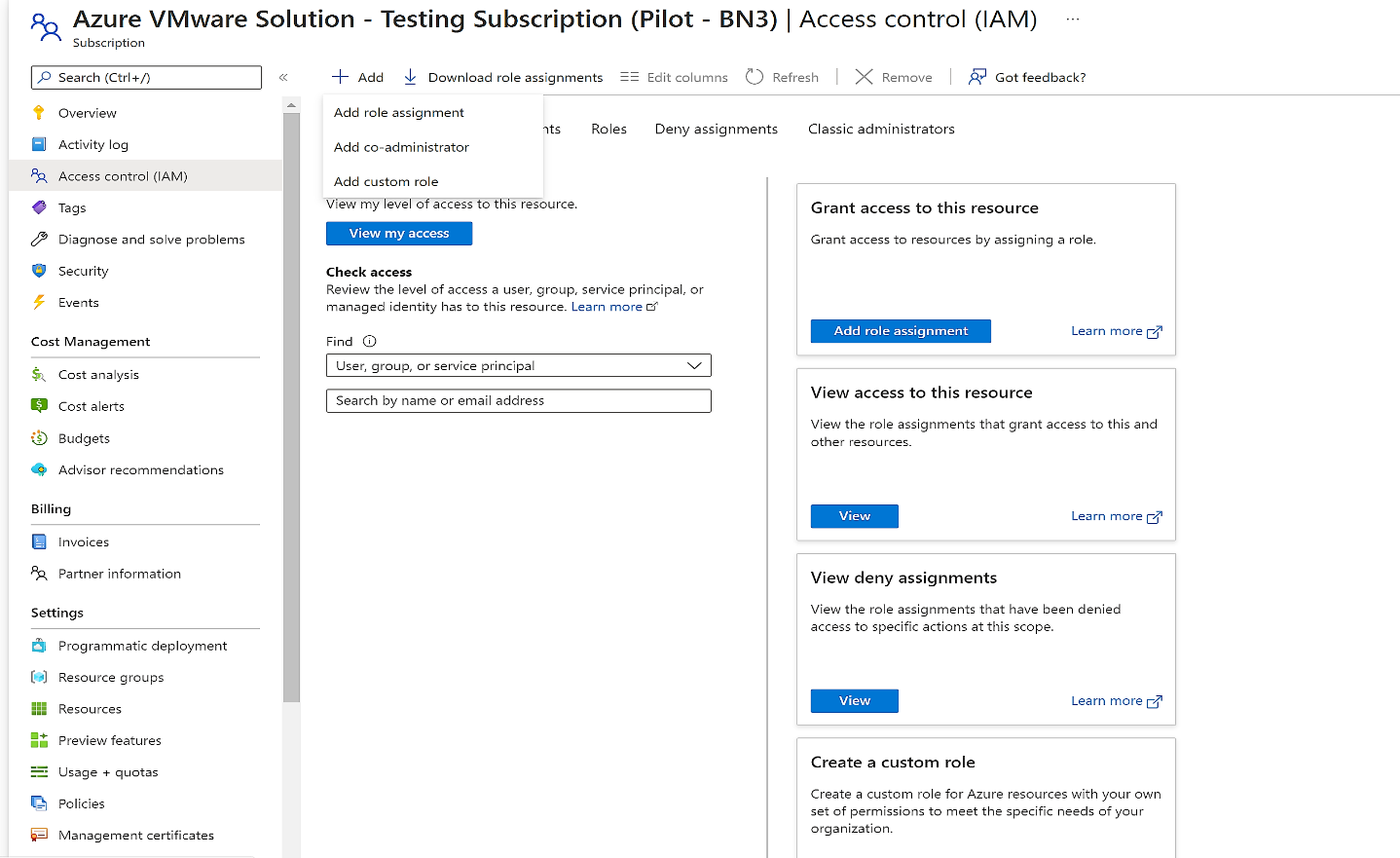
### **Azure Arc AVS VM Contributor**

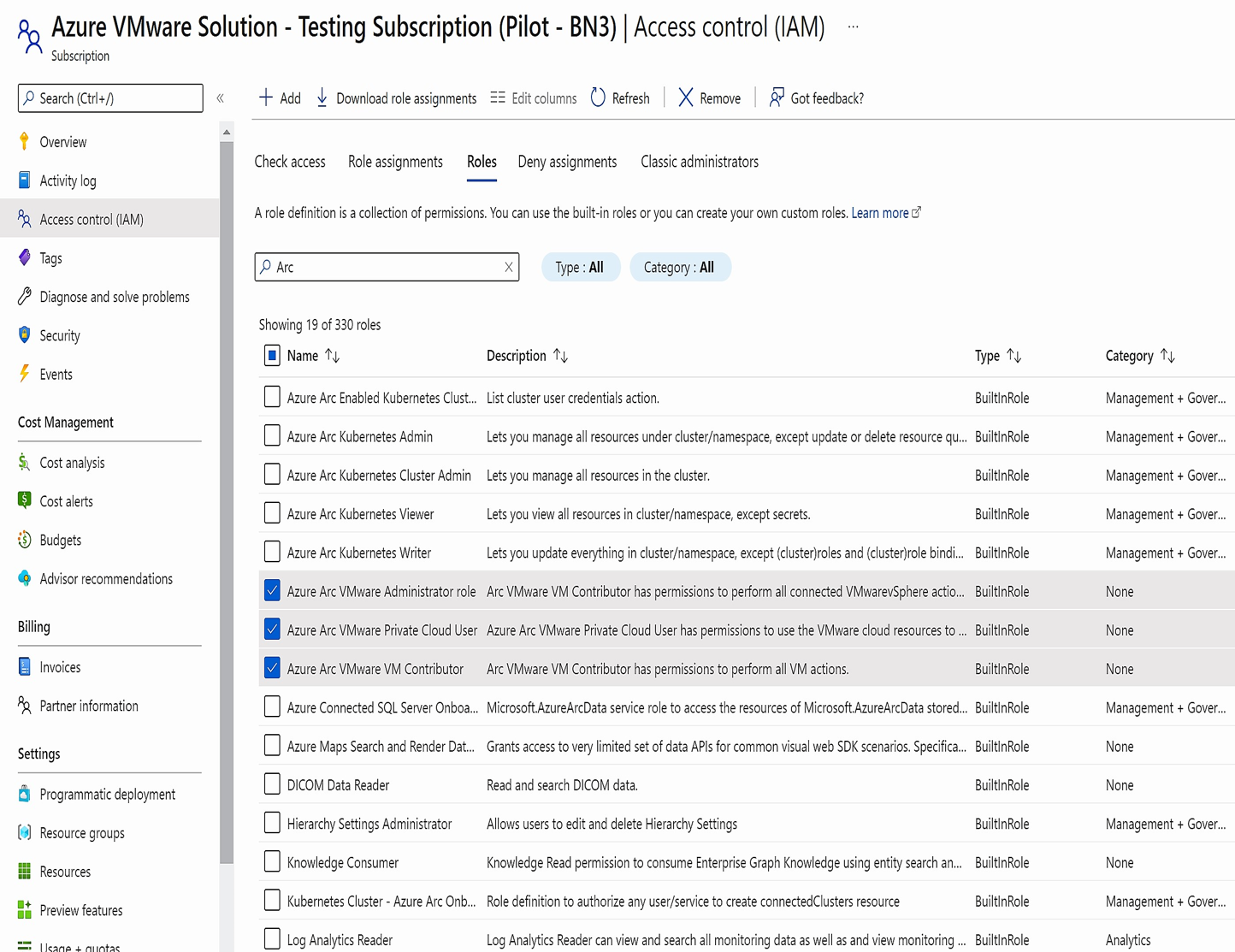
This custom role provides permissions to perform all VMware virtual machine operations. This role should be assigned to any users/groups that need to deploy, update or delete VMs.

We recommend assigning this role at the subscription level or resource group you want the user to deploy VMs with.

## **Assigning the custom roles to users/groups**

1. Go to the [Azure portal](https://aka.ms/ArcVMPublicPreview)
2. Search and navigate to the subscription, resource group or the resource at which scope you want to provide this role.
3. To find the Arc enabled Azure VMware Solution ~~(AVS)~~ vCenter resources,
   1. navigate to the resource group and select the **Show hidden types** checkbox.
   2. search for *" AVS/Azure VMware Solution"*
4. Click on **Access control (IAM)** in the table of contents on the left.
5. Click on **Add role assignments** on the **Grant access to this resource**.
6. Select the custom role you want to assign (one of **Azure Arc AVS Administrator**, **Azure Arc AVS Private Cloud User** or **Azure Arc AVS VM Contributor**)
7. Search for AAD user or group that you want assign this role to
8. Click on the AAD user or group name to select. Repeat this for each user/group you want to provide this permission.
9. Repeat the above steps for each scope and role.





Create Arc enabled Azure VMware Solution Virtual Machine

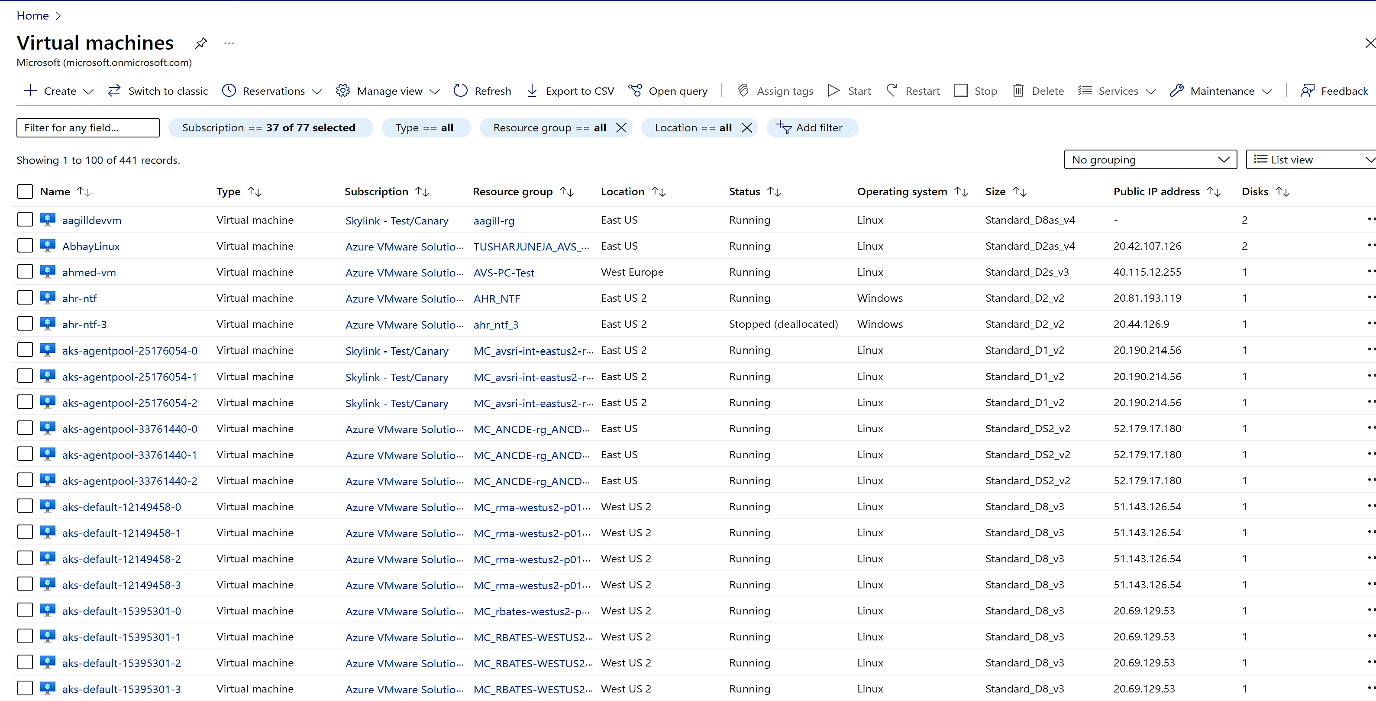
This section will enable users to create a virtual machine on VMware vCenter using Azure Arc.

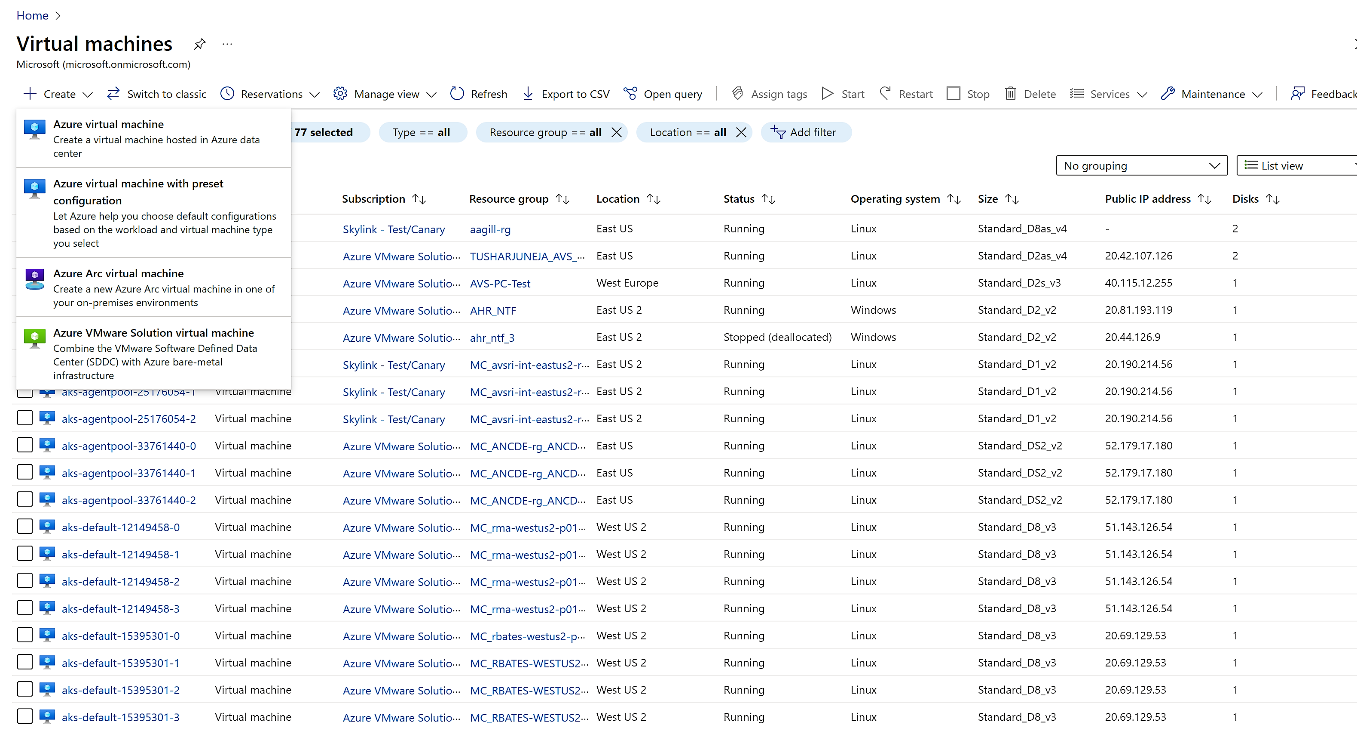
**Pre-requisites to Create Arc enabled AVS VM**

* An Azure subscription and resource group where you have Arc VMware VM contributor role
* A resource pool resource on which you have Arc Private Cloud Resource User Role
* A virtual machine template resource on which on which you have Arc Private Cloud Resource User Role

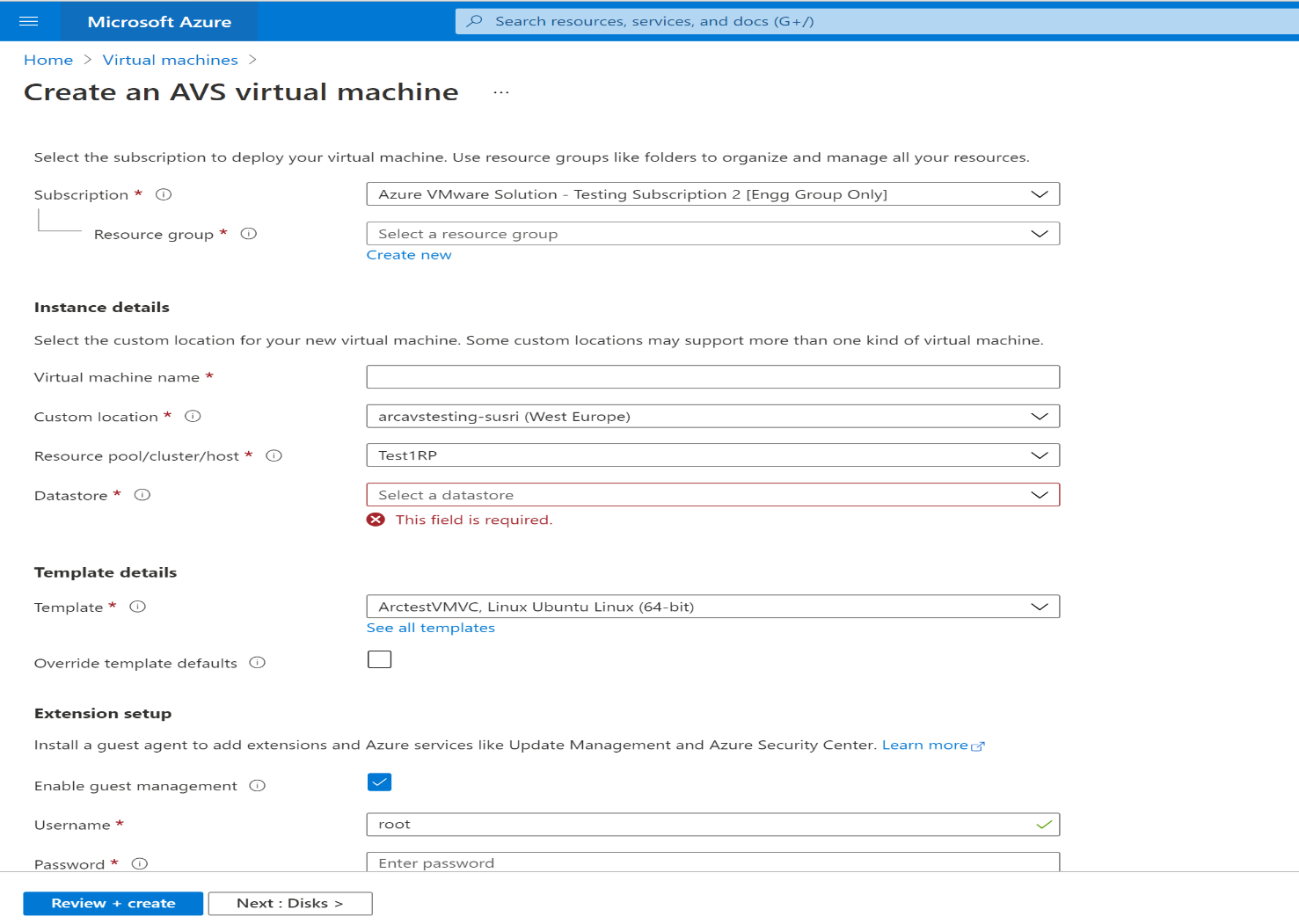
[Optional] A virtual network resource on which on which you have Arc Private Cloud Resource User Role**Create VM flow**

* Open the[**Azure portal**](https://aka.ms/ArcVMPublicPreview)
* Select **+ Create** drop down and select **Azure VMWare Solution Virtual Machine**.





* Select the **Subscription** and **Resource group** where you want to deploy the VM.
* Provide the **Virtual machine name**.
* Select a **Custom location** that your administrator has shared with you.
* Pick the **Resource pool/cluster/host** into which the VM should be deployed.
* Pick the **Template** based on which the VM will be created.
* You can optionally choose to **Override the template defaults** for **CPU Cores** and **Memory**.
* If you choose a Windows template, you can provide a **Username** and **Password** for the **Administrator account**.
* You can optionally change the disks configured in the template. You can add more disks or update existing disks. These disks will be created on the default datastore per the VMWare vCenter storage policies.
* You can optionally change the network interfaces configured in the template. You can add Network interface cards or update existing NICs. You can also change the network that this NIC will be attached to provided you have appropriate permissions to the network resource.
* You can optionally add tags to the VM resource.
* Finally click create after reviewing all the properties.
* The VM should be ~~provisioned~~ created in a few minutes.



Enable Guest Management and Extension Installation:

### **Prerequisite**

The guest management needs to be enabled on the VMware virtual machine before you can install an extension on it. You can enable guest management by following these steps:

1. Go to Azure portal.
2. Find the VMware VM that you want to check for guest management and **install extensions** on. Click on the name of the VM.
3. Click on **Configuration** blade for a VMware VM.
4. If **Enable guest management** is ticked, guest management is enabled. If not, enable guest management by ticking the check box and providing the administrator username and password. On Linux, by using the root account, and on Windows, with an account that is a member of the Local Administrators group. Click on **Apply**.

**Note**: Following are the conditions for enabling guest management on a VM:

1. Your target machine must be running a [supported operating system](https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview#supported-operating-systems).
2. Machine must be able to connects through the firewall to communicate over the Internet, make sure the URLs [listed](https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview#networking-configuration) are not blocked.
3. Machine must not be behind a proxy. It is not supported yet.
4. If you are using a linux VM, the account must not prompt for login on psudo commands. You can do this by following steps:  
    Login to the linux VM
   1. Open terminal and run the following command: sudo visudo
   2. Add the below line at the end of the file. Replace <username> with the appropriate user-name.

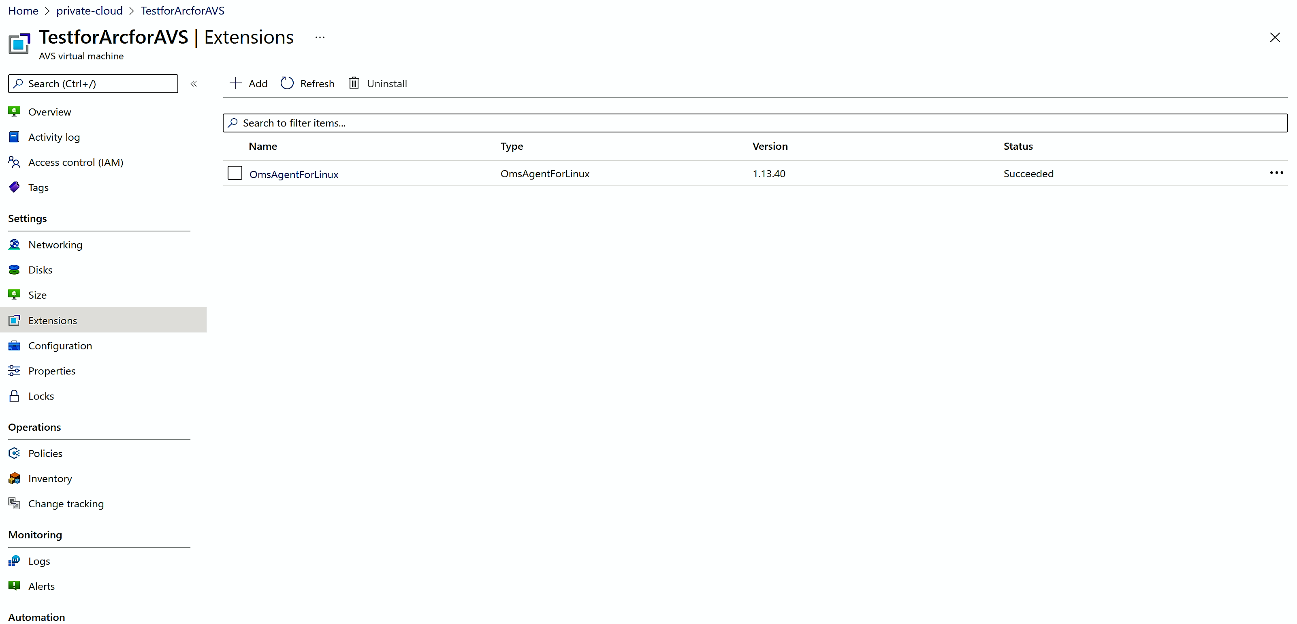
<username> ALL=(ALL) NOPASSWD:ALL

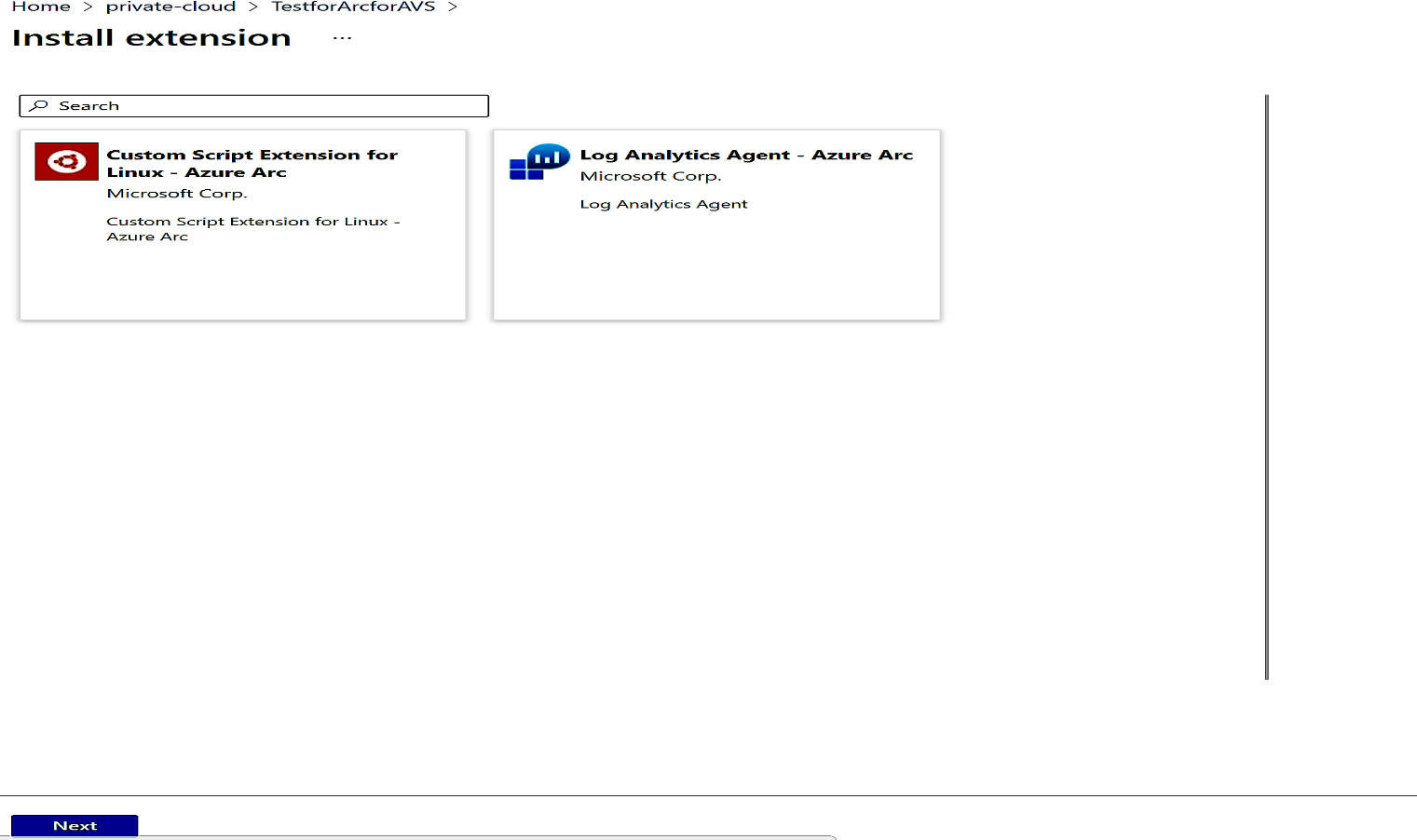
If your VM template has these changes incorporated, you will not need to perform the steps for the VM created from that template.

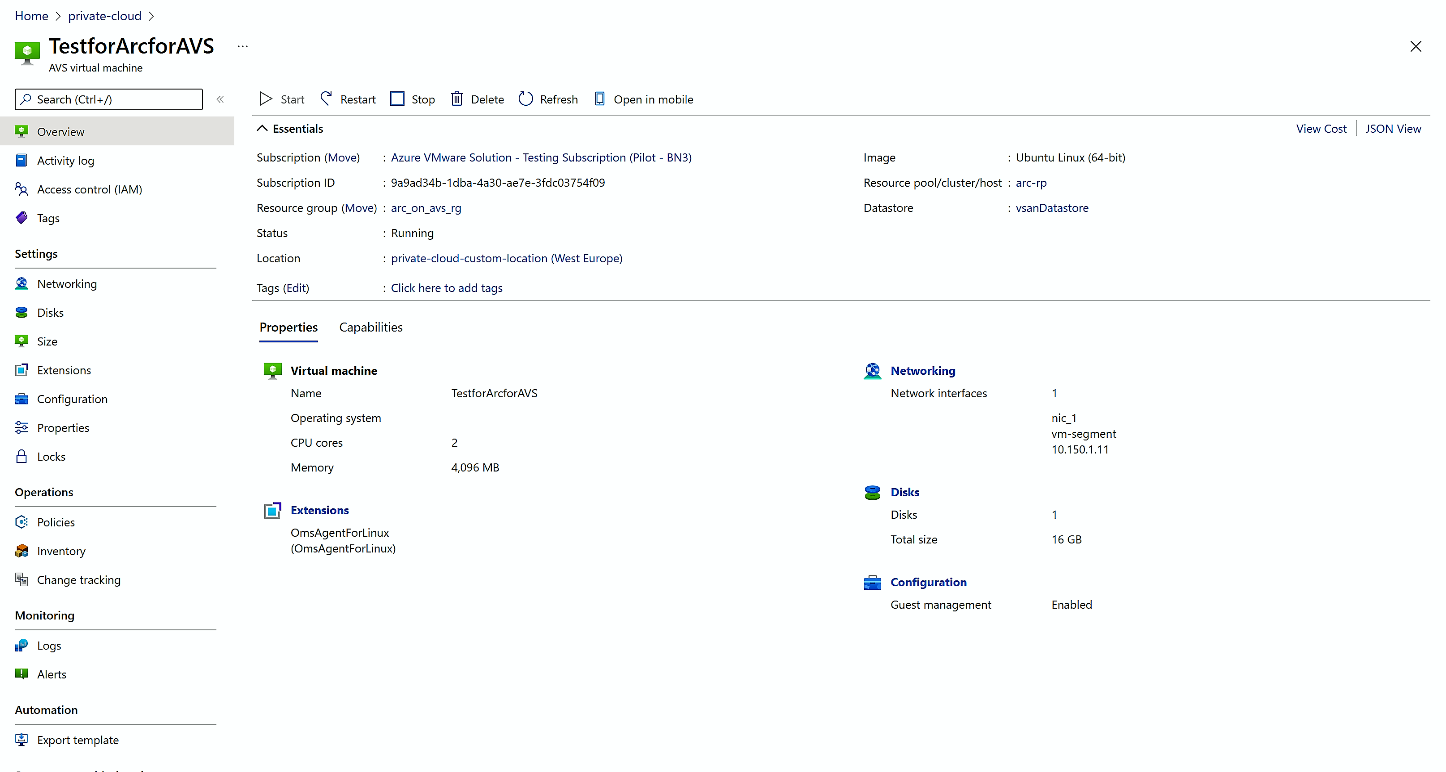
### **Extension Installation steps**

1. Go to Azure portal.
2. Find the Arc enabled AVS VM that you want to install extension on. Click on the name of the VM.
3. Navigate to **Extensions** blade and click on **Add**.
4. Select the extension you want to install.
5. Based on the extension, you will need to provide the details (like workspace Id and key for LogAnalytics extension).
6. Click on **Review + create**.

This will trigger deployment and install the selected extension on the virtual machine.







# Changing Arc appliance credential once you change your SDDC credentials

# ***“Set Credential” :*** command will update the provider credentials for an Appliance resource. Whenever cloudadmin credentials of the private cloud are updated, the following steps should be taken to update the credentials in the appliance resource.

1. Log in to the jumpbox VM from where onboarding was performed. Change directory to the onboarding directory.
2. For windows based jumpbox VM, run the following commands   
   .\.temp\.env\Scripts\activate
3. Run the following command -  
   az arcappliance setcredential vmware --kubeconfig kubeconfig
4. Run the onboard command again. As shown in step 3 in the section above (Step by step process to onboard in Arc for AVS preview)

# Appliance Upgrade (Manual)

Below steps define the workflow to perform manual upgrade of Arc appliance Virtual Machine (VM)

* 1. Login to vCenter
  2. Locate the arc appliance Virtual Machine (VM). This should be in the resource pool which the customer would have configured during onboarding.
     1. Power off the Virtual Machine (VM).
     2. Delete the Virtual Machine (VM)
  3. Delete the downloaded template corresponding to the Virtual Machine.
  4. Get the previous script (Config\_avs) file and add the below configuration item:
     + "register": false
  + Download the latest version of the AVS onboarding script.
  1. Run the new onboarding script with the previous config\_avs.json from the jump box Virtual Machine, without changing any config items.

# Off board from Azure Arc enabled AVS

## Remove your VMware virtual machines from Azure management services

If you have enabled guest management on your Arc enabled AVS VMs and onboarded them to Azure management services by installing VM extensions on them (e.g. you might have installed MMA extension to collect and send logs to an Azure Log Analytics workspace), you will need to uninstall the extensions to prevent continued billing. You will also need to uninstall the Azure Connected Machine agent to avoid any problems installing the agent in future

Following steps can be performed to uninstall extensions from the portal

1. Login to your [Azure VMware Solutions](https://aka.ms/ArcVMPublicPreview) (AVS) private cloud.
2. Click on Virtual machines under “Arc enabled VMware resources” in Private cloud blade.
3. Search and select the virtual machine where you have Guest Management enabled.
4. Click on Extensions.
5. Select the extensions and click Uninstall.
6. Steps 2 to 5 must be performed for all the VMs that have VM extensions installed.
7. To avoid problems onboarding the same VM to guest management, we recommend performing the following steps to cleanly disable guest management capabilities as well.
8. Log in to the virtual machine using administrator or root credentials and run the following command in the shell
   1. azcmagent disconnect --force-local-only
9. Uninstall the ConnectedMachine agent from the machine
10. Set the identity on the virtual machine resource to none.
11. Steps 8 to 10 must be performed for all the VMs that have guest management enabled.

## Remove Arc enabled AVS vSphere resources from Azure

When you enable Arc enabled AVS VMware resources in Azure, a representation is created for them in Azure. Before you can delete the vCenter resource in Azure, you will need to first delete all the Azure resource representations you created for your vSphere resources. To achieve this, perform the following steps:

1. Go to the [Azure portal](https://aka.ms/ArcVMPublicPreview)
2. Click on Virtual machines on Arc enabled VMware resources in the Private Cloud blade.
3. Select all the VMs that have Azure Enabled value as Yes.
4. Click Remove from Azure.
5. This will start deployment and remove these resources from Azure. The resources will continue to remain in your vCenter.
6. Perform the steps 2, 3 and 4 for Resourcespools/clusters/hosts, Tempaltes, Networks, and Datastores
7. Once the deletion is complete, click on Overview.
8. Note the Custom location and the Azure Arc Resource bridge resource in the Essentials section.
9. Click Remove from Azure to remove the vCenter resource from Azure.
10. Go to vCenter resource in Azure and delete.
11. Go to the Custom location resource and click Delete
12. Go to the Azure Arc Resource bridge resource and click Delete
13. At this point, all your Arc-enabled VMware vSphere resources are removed from Azure

## Delete Arc resources from vCenter

During onboarding, to create a connection between your VMware vCenter and Azure, an Azure Arc resource bridge is deployed into your VMware vSphere environment. As the last step, you must delete the resource bridge VM as well the as VM template created during the onboarding.

# Preview FAQ:

* Is the preview available in all regions? – Arc for AVS is currently available in EastUS and West EU, other regions are on the roadmap we will communicate you as and when we open up for other regions.
* How to onboard customer? – Fill in the [customer nomination form](https://forms.office.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR0SUP-7nYapHr1Tk0MFNflVUNEJQNzFONVhVOUlVTVk3V1hNTjJPVDM5WS4u)
* How does support work? –Standard support process for AVS has been enabled to support customers.
* Note this is AVS2.0 only – not available for AVS by Cloudsimple
* Does Arc for AVS supports private end point? Arc for AVS will support private end point at GA however currently it is not supported.
* Is enabling internet the only option to enable Arc for AVS? Yes.
* Is DHCP support available? DHCP support is on the roadmap and will soon be available for customers, for now we are only supporting static IP
* Is proxy Support available? Proxy support is a road map item.

# Debugging tips for known issues (Self-help guide)

* What happens if I face error related to Az CLI?
  + For windows jumpbox, if you have 32-bit Azure CLI installed, verify that your current version of Azure CLI has been uninstalled. This can be done from the Control Panel.
  + To ensure it's uninstalled, try the `az` version to check if it's still installed.
  + If you already installed Azure CLI using MSI, `az` installed by MSI and pip will conflict on PATH. In this case, it's recommended that you uninstall the current Azure CLI version.
  + ~~In windows jumpbox, if you have 32bit Az CLI installed, ensure that your current version of Azure CLI has been uninstalled (can be done form Control Panel). You can ensure it is uninstalled by trying az version to determine if it still exists. If you have already installed Azure CLI using MSI, az installed by MSI and az installed by pip will conflict on PATH. Therefore, it is recommended to uninstall the current Azure CLI version~~
* ~~What happens if In-case my script stopped with the timed-out?~~ My script stopped because it timed-out, what should I do?
  + ~~retry the script for create it will ask a prompt select ‘Y’ and re-run~~ Retry the script for `create`. A prompt will ask you to select `Y` and rerun it.
  + ~~Can be the cluster extension issue which ends up adding the extension in the pending state~~ It could be a cluster extension issue that would result in adding the extension in the pending state.
  + ~~Check for the correct script version~~ Verify you have the correct script version.
  + ~~Check if the vmware pod is correctly running on the system in running state~~ Verify the VMware pod is running correctly on the system in running state.
* Basic trouble-shooting step if the script run was unsuccessful
  + ~~In Custom location name and k8s namespace should contains only alphanumeric characters in lowercase or ‘-‘ and must start and end with alphanumeric characters only~~
  + Ensure feature and Resource providers are registered as per the directions provided in the pre-requisite section.
* What happens if Arc for VMware section shows no data?
  + If the Azure Arc VMware resources in Azure UI shows no data, ensure the said subscription is added in the global default subscription filter.
* I see an error “(ApplianceClusterNotRunning) Appliance Cluster: <resource-bridge-id> expected state to be Succeeded found: Succeeded and expected status to be Running and found: Connected”
  + Execute the script again.
* I am unable to install extensions on my Virtual Machine
  + Check if guest management has been successfully installed.
  + VMtools should be installed on the VM
* I am facing Network related issues during on-boarding
  + Check for the IP conflict. We need IPs with no conflicts or from free pool.
  + Check if the internet is enabled for the network segment.
* Where can I find more information related to Azure Arc resource bridge?
  + For more information follow the link “[Azure Arc resource bridge (preview) overview - Azure Arc | Microsoft Docs”](https://review.docs.microsoft.com/en-us/azure/azure-arc/resource-bridge/overview?branch=pr-en-us-180334)

# Appendixes

## Appendix 1 - Proxy Urls required by the Azure Arc enabled Private Cloud

### Azure Arc services

| **Service** | **URL** |
| --- | --- |
| Microsoft container registry | `https://mcr.microsoft.com` |
| Azure Arc Identity service | `https://\*.his.arc.azure.com` |
| Azure Arc configuration service | `https://\*.dp.kubernetesconfiguration.azure.com` |
| Cluster connect | `https://\*.servicebus.windows.net` |
| Guest Notfication service | `https://guestnotificationservice.azure.com` |
| Resource bridge (appliance) Dataplane service | `https://\*.dp.prod.appliances.azure.com` |
| Resource bridge (appliance) container image download | `https://ecpacr.azurecr.io` |
| Resource bridge (appliance) image download | .blob.core.windows.net \*.dl.delivery.mp.microsoft.com \*.do.dsp.mp.microsoft.com |
| Azure Resource Manger | `https://management.azure.com` |
| Azure Active Directory | https://login.microsoftonline.com |

### Other URLs -

\*.blob.core.windows.net  
[files.pythonhosted.org](http://files.pythonhosted.org/)   
\*.api.cdp.microsoft.com  
[gcr.io](http://gcr.io/)   
[storage.googleapis.com](http://storage.googleapis.com/)   
[registry-1.docker.io](http://registry-1.docker.io/)   
[auth.docker.io](http://auth.docker.io/)   
[production.cloudflare.docker.com](http://production.cloudflare.docker.com/)   
[quay.io](http://quay.io/)

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |