

# Deployment Guide: Microsoft Azure Arc on ThinkAgile MX and VMware vSphere

## Planning / Implementation

Customer IT environments have become very complicated with many applications running on diverse infrastructure spread over on-premises data centers, on the edge, and in multiple clouds. With different tools and frameworks in use and multiple technologies like DevOps and Kubernetes, these IT resources have become hard to view, manage and secure. With the ever-increasing adoption of cloud services, cloud service providers are doing most of their innovation in the cloud today.

Microsoft Azure Arc is a set of technologies that allows customers to view and manage both their on-premises and cloud resources with a single pane of glass self-service portal. Azure Arc allows you to run innovative and advanced Azure services on your on-premises infrastructure - ThinkAgile MX or VMware vSphere as described in this paper. With Azure Arc you can manage both your VMs in Azure and VMs on-premises with a single pane of glass, apply security policies to both and govern them tougher in an easy way.

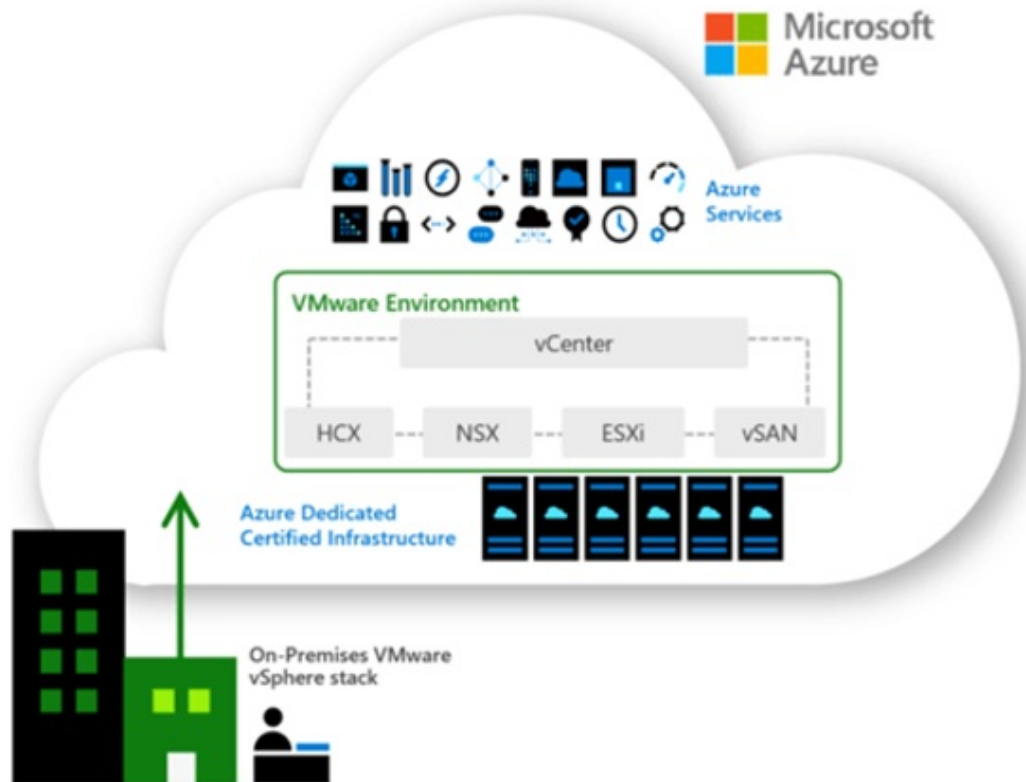


Figure 1. High-level Arc vSphere integration

## Azure Arc Service on VMware vSphere

Azure Arc integration with VMware vSphere offers a hybrid solution that provides customers with the benefits of both Azure and vSphere environments. This integration enables customers to manage their on-premises and multi-cloud infrastructure as well as Azure resources from a single unified control plane, resulting in increased operational efficiency. With Azure Arc integration, customers can leverage the scalability and security features of Azure, while preserving their existing vSphere investment. Additionally, the integration allows customers to use Azure services, such as Azure Kubernetes Service and Azure Policy, on their on-premises and multi-cloud infrastructure, enabling them to modernize their applications and operations. Other benefits include:

- **Centralized management:** Azure Arc allows customers to manage their on-premises, multi-cloud and Azure resources from a single control plane, which simplifies management and increases operational efficiency.
- **Leverage existing investment:** With Azure Arc, customers can leverage their existing vSphere investment while taking advantage of the scalability and security features offered by Azure.
- **Modernize applications:** The integration enables customers to use Azure services, such as Azure Kubernetes Service, on their on-premises and multi-cloud infrastructure, allowing them to modernize their applications and operations.
- **Improved security:** Azure Arc provides security features such as Azure Policy and Azure Security Center, allowing customers to enhance the security of their infrastructure and applications.
- **Compliance and auditing:** Azure Arc provides compliance and auditing capabilities, which makes it easier for customers to meet regulatory requirements and adhere to industry standards.

In summary, Azure Arc integration with vSphere offers a hybrid solution that provides customers with the benefits of both Azure and vSphere environments, enabling them to simplify their infrastructure management, modernize their applications, and enhance their security.

## A single control plane

Overall, a single control plane provides customers with a centralized, unified, and efficient way to manage their infrastructure, improving their operational efficiency and reducing the complexity of managing multiple disparate systems.

- **Simplified management:** By having a single control plane, customers can manage all their on-premises, multi-cloud, and Azure resources from a single console, reducing the complexity of managing multiple disparate systems.
- **Improved efficiency:** With a single control plane, customers can automate and streamline their management processes, reducing the time and effort required to manage their infrastructure.
- **Enhanced visibility:** A single control plane provides customers with a unified view of their infrastructure, allowing them to easily monitor and manage their resources.
- **Consistent policies:** By having a single control plane, customers can enforce consistent policies across their infrastructure, ensuring that their resources are configured and managed in a consistent manner.
- **Better collaboration:** A single control plane makes it easier for teams to collaborate and share information, improving communication and decision-making.

## Before you get started

The following summarizes, at a high-level, what you will need to run Azure Arc.

To use Arc-enabled VMware vSphere, you must deploy an Azure Arc resource bridge (preview) in your VMware vSphere environment. The resource bridge provides an ongoing connection between your VMware vCenter server and Azure. Once you've connected your VMware vCenter server to Azure, components on the resource bridge discover your vCenter inventory. You can enable them in Azure and start performing virtual hardware and guest OS operations on them using Azure Arc.

Requirements:

- An Azure subscription with the appropriate permissions.
- Any system running a vCenter Server versions 6.7 and 7 with ethernet access.
- A vSphere account that can:
  - Read all inventory.
  - Deploy and update VMs to all the resource pools (or clusters), networks, and VM templates that you want to use with Azure Arc.
- For Arc-enabled VMware vSphere, resource bridge has the following minimum virtual hardware requirements:
  - 16 GB of memory
  - 4 vCPUs
  - An external virtual switch that can provide access to the internet directly or through a proxy. If internet access is through a proxy or firewall, ensure these URLs are allow-listed.
- Deploying the Connected Machine agent on a machine requires that you have administrator permissions to install and configure the agent. On Linux this is done by using the root account, and on Windows, with an account that is a member of the Local Administrators group.
- Before you get started, be sure to review the agent prerequisites and verify the following:
  - Your target machine is running a supported operating system.
  - Your account has the required Azure built-in roles.
  - Ensure the machine is in a supported region.
  - Confirm that the Linux hostname or Windows computer name doesn't use a reserved word or trademark.
  - If the machine connects through a firewall or proxy server to communicate over the Internet, make sure the URLs listed are not blocked.

## Step 1: Deploy and Configure VMware ESXi on physical host

1. Download the ESXi ISO image from the VMware website.
2. Burn the ISO image to a CD or USB drive.
3. Insert the CD or USB drive into the physical host and boot from it.
4. Choose the appropriate installation option from the boot menu.
5. Select the target storage device for the ESXi installation.
6. Configure the network settings for the ESXi host, including IP address, subnet mask, and default gateway.
7. Create a password for the root user account.
8. Review and confirm the installation settings.
9. Wait for the installation to complete.
10. Remove the CD or USB drive and restart the physical host.
11. Log in to the ESXi host using the vSphere client or web client, and configure additional settings as needed, such as datastores, virtual switches, and virtual machine

## Step 2: Configure VMware vSphere

1. Download and install the VMware vSphere client on a management system.
2. Connect the vSphere client to the ESXi host and log in as the root user.
3. Create a new datacenter in the vSphere client.
4. Create a new cluster within the datacenter.
5. Add the ESXi host to the cluster.
6. Create and configure virtual switches for network connectivity.
7. Create and configure datastores for storage.
8. Create virtual machines and configure their hardware, operating system, and applications.
9. Configure virtual machine options, such as snapshots, cloning, and resource pools.
10. Monitor the performance of the vSphere environment using the vSphere client or other management tools.

Note: The steps above provide a high-level overview of the process, and actual deployment will depend on the specific requirements of your ESXi & vSphere environment. It's recommended to follow the official VMware documentation for a detailed guide.

## Step 3: Deploy an Arc Resource Bridge Appliance

The next step is to deploy the Azure Resource Bridge Appliance with your VMware vSphere and have it accessible over the network. This should be installed on a Windows 10 or Windows Server machine.

1. Access Azure Portal
2. Go to Azure Arc > Add your infrastructure for free

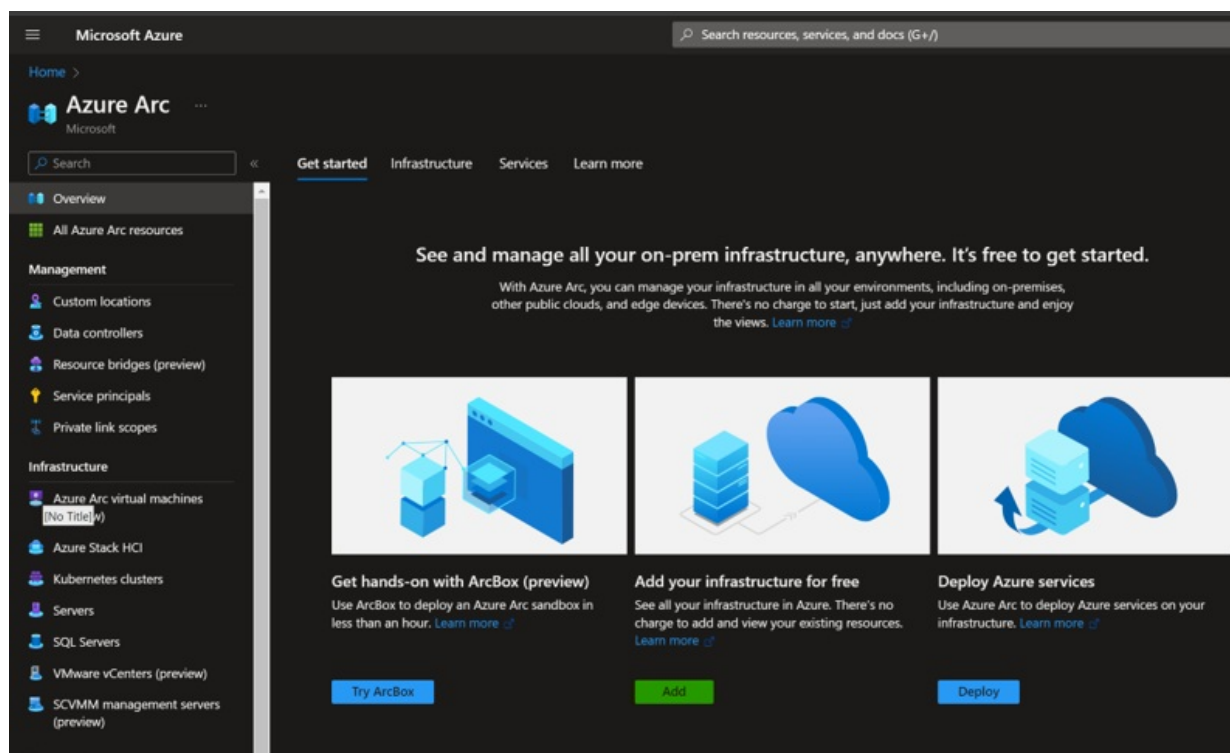


Figure 2. Azure Arc overview on Azure portal

3. Select Platform > VMware vSphere

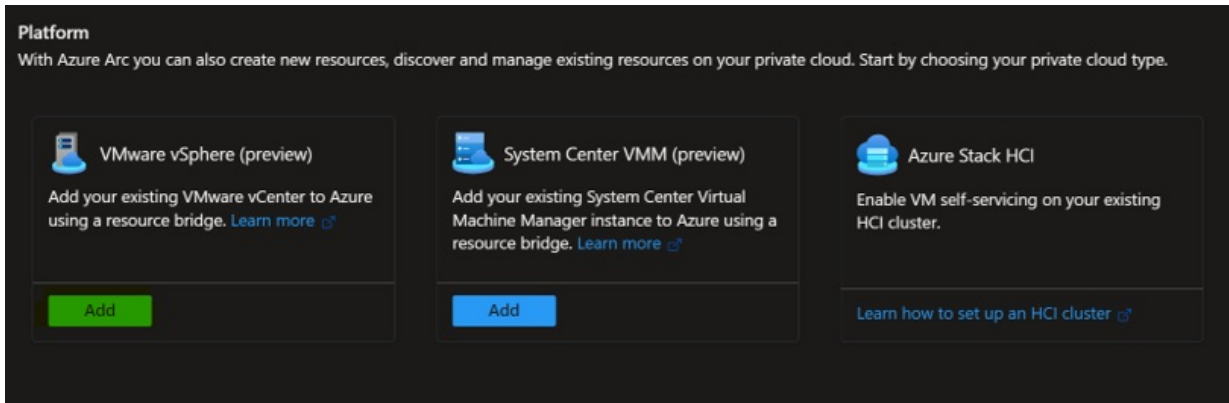


Figure 3. Azure Arc add infrastructure on Azure portal

4. Create a new Resource Bridge

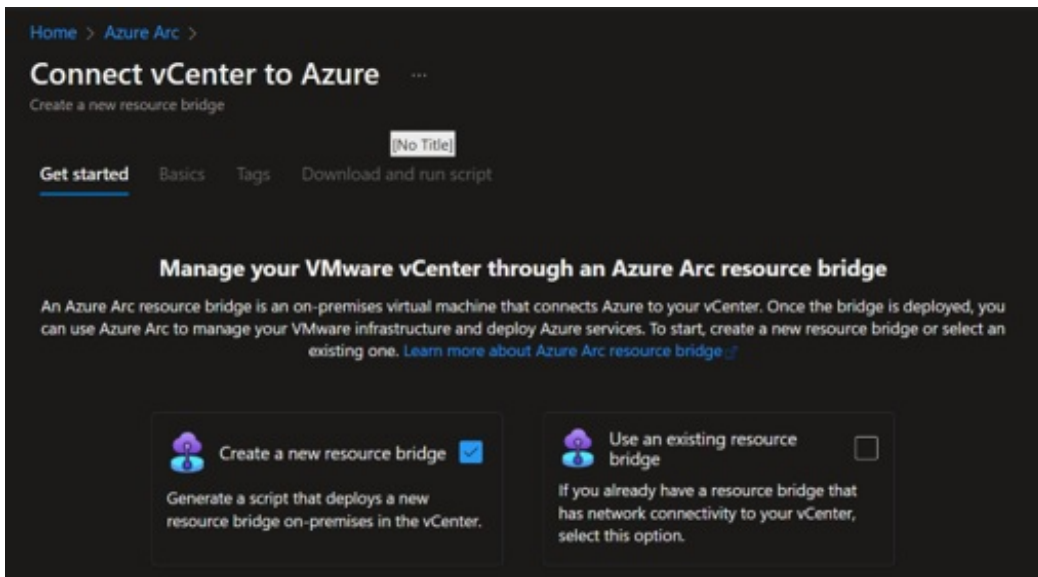


Figure 4. Azure Arc connect vCenter on Azure portal

5. Select the Resource group and define the custom location

Get started **Basics** Tags Download and run script

The information you enter below will be used to generate a script, which will connect your vCenter to Azure and create resources in Azure that represent your vCenter, custom location, and resource bridge.

### Resource bridge

An Azure Arc resource bridge is a virtual machine that will be used to connect your vCenter to Azure. It'll run on-premises, but it'll be fully managed by Microsoft, including updates. Select the Azure region closest to your datacenter. This is where the Azure metadata for your VMware resources will be stored. [Learn more about resource bridge](#)

Name \* ⓘ

Subscription \* ⓘ

Resource group \* ⓘ

Region \* ⓘ

**i** The same region will be used for the custom location and vCenter.

### Custom location

A custom location is an Azure resource that represents your vCenter deployment location. As part of the resource bridge creation process, we'll create a custom location that contains your vCenter resources. [Learn more about custom locations](#)

Name \* ⓘ

Use the same subscription and resource group as your resource bridge

### vCenter

An Azure resource will represent your vCenter in Azure.

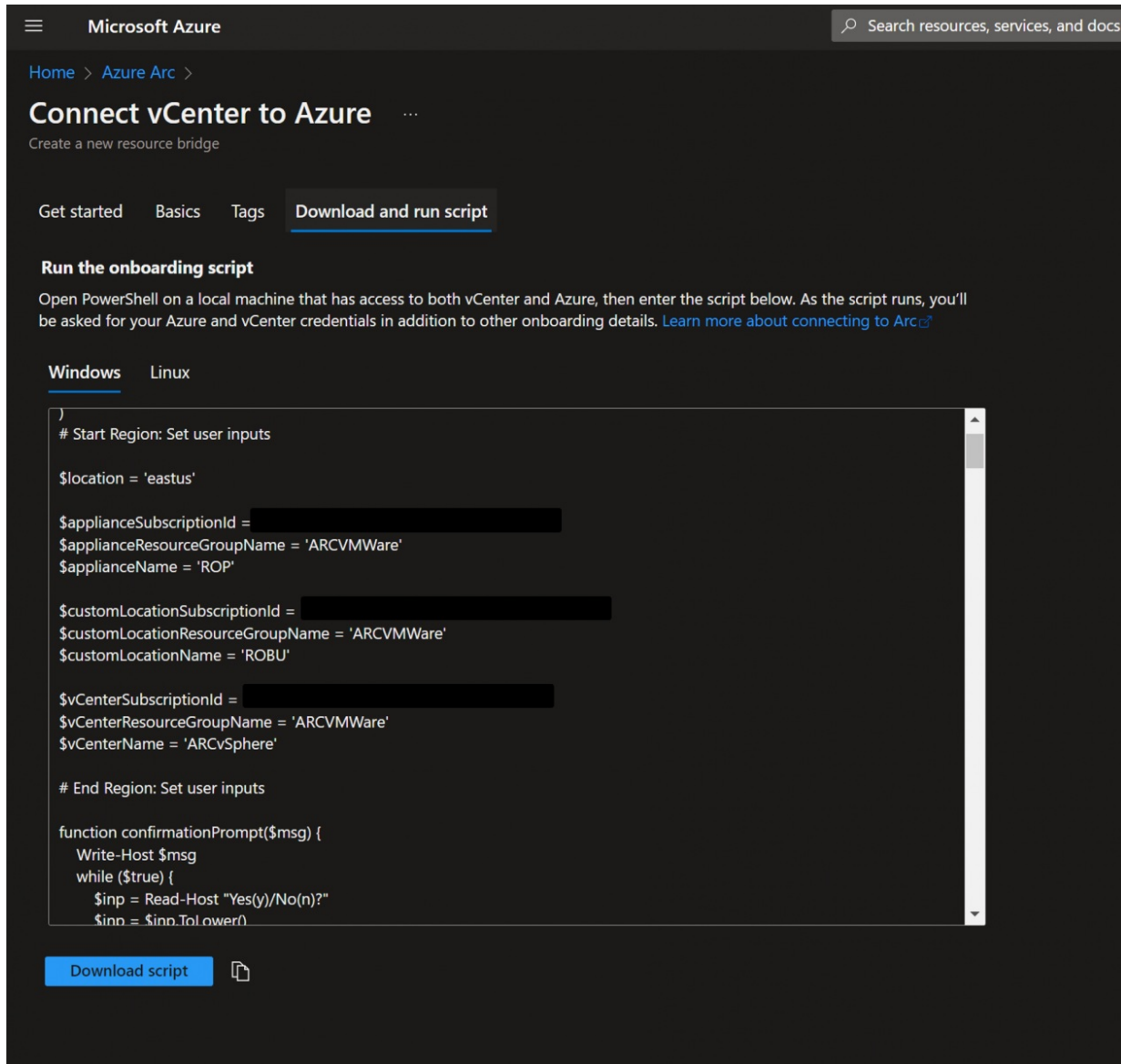
vCenter name in Azure \* ⓘ

Use the same subscription and resource group as your resource bridge

Figure 5. Azure Arc Resource Bridge deployment on Azure portal

## Step 4: Onboarding vCenter to Azure

After you provide the required information in the Basic tab, it will generate an Onboarding Script that will be run on any VM that can access both vCenter and vSphere.



The screenshot shows the Microsoft Azure portal interface for connecting vCenter to Azure. The page title is "Connect vCenter to Azure" and it is under the "Download and run script" tab. The script content is as follows:

```
)  
# Start Region: Set user inputs  
  
$location = 'eastus'  
  
$applianceSubscriptionId = [REDACTED]  
$applianceResourceGroupName = 'ARCVMWare'  
$applianceName = 'ROP'  
  
$customLocationSubscriptionId = [REDACTED]  
$customLocationResourceGroupName = 'ARCVMWare'  
$customLocationName = 'ROBU'  
  
$vCenterSubscriptionId = [REDACTED]  
$vCenterResourceGroupName = 'ARCVMWare'  
$vCenterName = 'ARCvSphere'  
  
# End Region: Set user inputs  
  
function confirmationPrompt($msg) {  
    Write-Host $msg  
    while ($true) {  
        $inp = Read-Host "Yes(y)/No(n)?"  
        $inp = $inp.ToLower()  
    }  
}
```

At the bottom of the script area, there is a blue "Download script" button and a copy icon.

Figure 6. Onboarding script in Azure Arc on Azure portal

Azure Arc-enabled VMware vSphere uses the vSphere account credentials you provided during the onboarding to communicate with your vCenter server. These credentials are only persisted locally on the Arc resource bridge VM. As part of your security practices, you might need to rotate credentials for your vCenter accounts. As credentials are rotated, you must also update the credentials provided to Azure Arc to ensure the functioning of Azure Arc-enabled VMware services. You can also use the same steps in case you need to use a different vSphere account after onboarding. You must ensure the new account also has all the [required vSphere permissions](#).

## Step 5: Run the Onboarding Script

Before run the script execute the following: **Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass**

Copy the Onboarding script in PowerShell or execute the file containing the script and follow the instructions by providing network details and credentials of the vCenter and the script will deploy the arc appliance.

```
Create Config
Starting createconfig
cli.azext_arcappliance.telemetry_helpers: Custom telemetry: {'Context.Default.AzureCLI.ApplianceDeploymentId': '/subscriptions/4a5bd4d32', 'Context.Default.AzureCLI.Provider': 'vmware', 'Context.Default.AzureCLI.PortalTraceId': '00000000-0000-0000-0000-000000000000', 'Context.Default.AzureCLI.CurrentDateTime': '2023-02-02T15:42:55Z', 'Context.Default.AzureCLI.CurrentRunCreateConfig': '2023-02-02T15:42:55Z'}
Please enter vCenter FQDN/Address:
Please enter vCenter username: administrator@vsphere.local
Please enter vCenter password:
Initializing chart values for provider: vsphere 2023-02-02T07:43:19-08:00 INFO Client Created with vcenter url: 1
2023-02-02T07:43:19-08:00 INFO vsphereProvider: createConfigHelper

Please select datacenter:
1) /Datacenter
Enter number: 1
You Selected: /Datacenter

Please select network:
1) VM Network
Enter number: 1
You Selected: VM Network
Do you want to configure Appliance for DHCP or Static IP deployment? Please select Y for DHCP and N for Static IP (y/n)?d
Do you want to configure Appliance for DHCP or Static IP deployment? Please select Y for DHCP and N for Static IP (y/n)?y

Please select resourcepool:
1) S/Resources (Complete path - /Datacenter/host/S/Resources)
2) ARC (Complete path - /Datacenter/host/S/Resources/ARC)
Enter number: 2
You Selected: ARC (Complete path - /Datacenter/host/S/Resources/ARC)

Please select datastore:
1) datastore1
Enter number: 1
You Selected: datastore1

Please select folder:
1) Discovered virtual machine (Complete path - /Datacenter/vm/Discovered virtual machine)
2) vCLS (Complete path - /Datacenter/vm/vCLS)
Enter number: 1
You Selected: Discovered virtual machine (Complete path - /Datacenter/vm/Discovered virtual machine)

Please provide Appliance cluster configuration
Please enter Appliance control plane IP:
Do you want to configure Appliance proxy settings? (y/n) n

All configuration files created successfully
Appliance Configuration YAML was created here: C:\Users\Administrator\ARCWMA-appliance.yaml
Resource Configuration YAML was created here: C:\Users\Administrator\ARCWMA-resource.yaml
Infrastructure Configuration YAML was created here: C:\Users\Administrator\ARCWMA-infra.yaml
```

Figure 7. Onboarding script execution on the local appliance



## Step 6: Enable VMware vCenter resource in Azure

Visit the VMware vCenter section in Azure Arc Center to view all the connected vCenters.

From there, you'll see your virtual machines (VMs), resource pools, templates, and networks. From the inventory of your vCenter resources, you can select and enable one or more resources in Azure.

When you enable a vCenter resource in Azure, it creates an Azure resource that represents your vCenter resource. You can use this Azure resource to assign permissions or conduct management operations while managing the resources in the custom location defined.

To enable your VMware vSphere resources in Azure, start by accessing the vCenter's blade on Azure Arc Center through your browser. From there, navigate to the inventory resources blade.

Next, choose the specific resource or resources that you wish to enable and select the "Enable in Azure" option.

Then, you'll need to select your Azure Subscription and Resource Group before clicking on the "Enable" button. This will trigger a deployment process and create a representation of your VMware vSphere resources in Azure.

By doing so, you'll gain the ability to manage access to these resources through Azure role-based access control (RBAC) in a granular manner.

Finally, repeat the same steps for any other resources such as network, resource pool, and VM template, that you wish to enable.

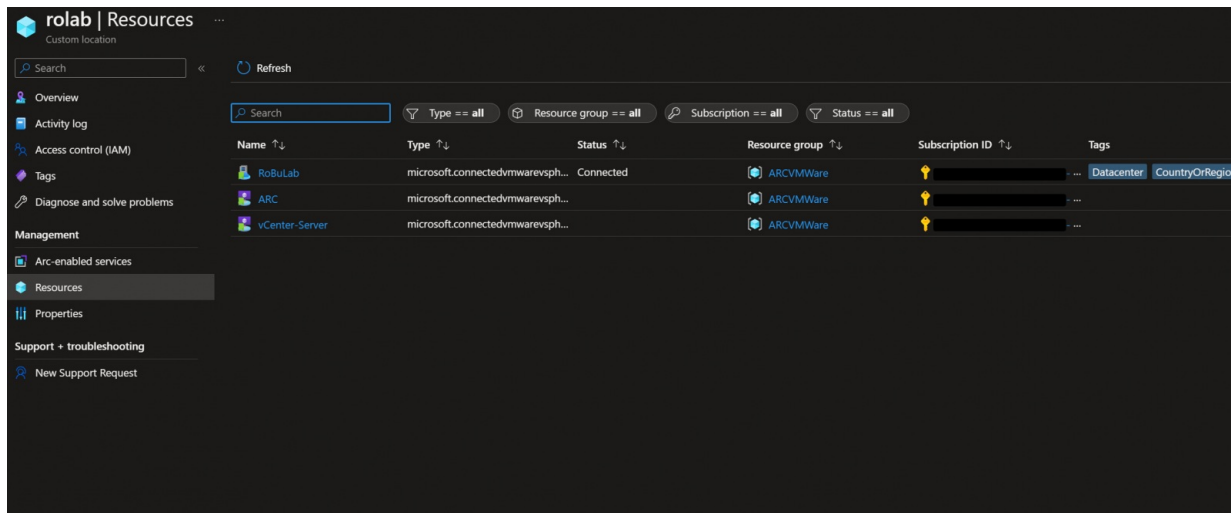


Figure 8. Resources inside the custom location created in Azure portal

## Step 7: Enable existing virtual machines in Azure

From your browser, go to the vCenter's blade on Azure Arc Center and navigate to your vCenter.

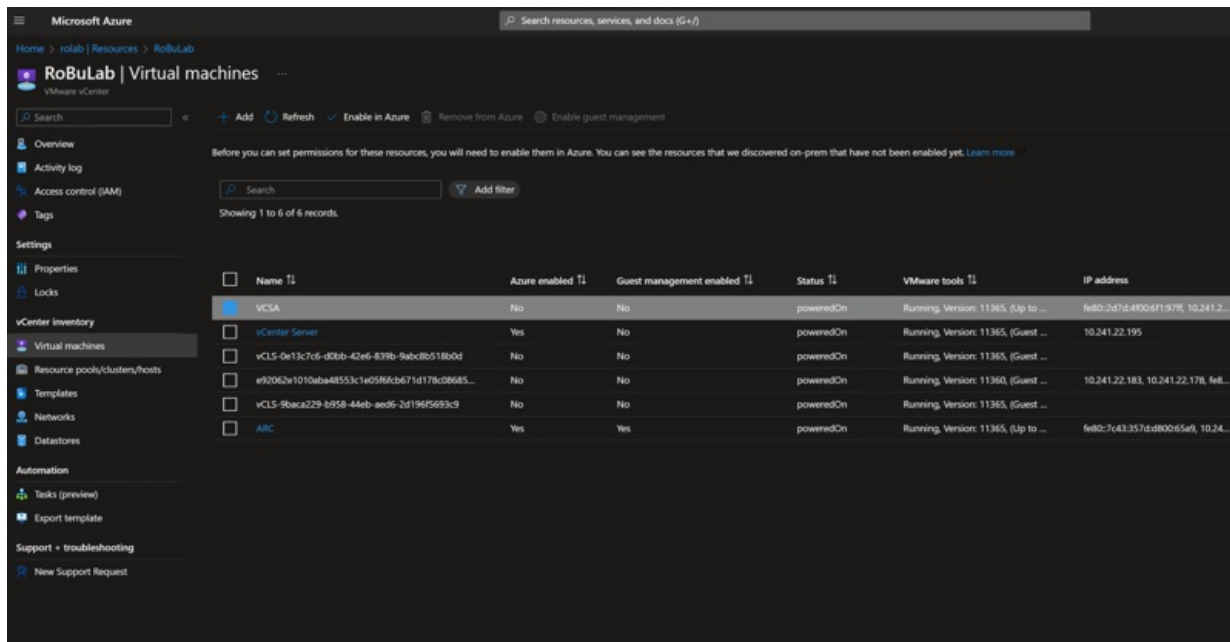


Figure 9. vCenter virtual machine exposed in Azure portal

1. Navigate to the VM inventory resource, select the VMs you want to enable, and then select Enable in Azure.
2. Select your Azure Subscription and Resource Group.
3. (Optional) Select Install guest agent and then provide the Administrator username and password of the guest operating system.
4. The guest agent is the Azure Arc connected machine agent. You can install this agent later by selecting the VM in the VM inventory view on your vCenter and selecting.
5. Select Enable to start the deployment of the VM represented in Azure.

Once your VMware vCenter resources have been enabled in Azure, the final step in setting up a self-service experience for your teams is to provide them access. [This article](#) describes how to use built-in roles to manage granular access to VMware resources through Azure and allow your teams to deploy and manage VMs.

## Step 8: Arc-enabled VMware vSphere built-in roles

There are three built-in roles to meet your access control requirements. You can apply these roles to a whole subscription, resource group, or a single resource.

- **Azure Arc VMware Administrator role** - a predefined role that grants full permissions for all operations related to the Microsoft.ConnectedVMwarevSphere resource provider. This role is intended for administrators who manage Azure Arc enabled VMware vSphere deployments. You can assign this role to individual users or groups.
- **Azure Arc VMware Private Cloud User role** - a preconfigured role that allows users to access VMware vSphere resources through Azure. This role is intended for individuals or groups who need to create, modify, or delete VMs. It is recommended that you assign this role at the resource pool, host, or cluster level, as well as for the virtual network or template that the user will use to deploy VMs. This will ensure that the user has the appropriate permissions to perform their tasks while maintaining security and access control.
- **Azure Arc VMware VM Contributor role** - a built-in role that provides permissions to conduct all VMware virtual machine operations. Assign this role to any users or groups that need to deploy, update, or delete VMs. We recommend assigning this role at the subscription or resource group you want the user to deploy VMs.

### Assigning the roles to users/groups

1. Go to the Azure portal.
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 VMware vSphere resources like resource pools, clusters, hosts, datastores, networks, or virtual machine templates:
  1. navigate to the resource group and select the Show hidden types checkbox.
  2. search for "VMware".
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 VMware Administrator, Azure Arc VMware Private Cloud User, or Azure Arc VMware VM Contributor).
7. Search for the Azure Active Directory (Azure AD) user or group to which you want to assign this role.
8. Select the Azure AD user or group name. Repeat this for each user or group to which you want to grant this permission.
9. Repeat the above steps for each scope and role.

## Step 9: Create a virtual machine on VMware vCenter using Azure Arc

### Prerequisites

- You need an Azure subscription and resource group for which you have the Arc VMware VM contributor role.
- You must have the Arc Private Cloud Resource User Role for the resource pool/cluster/host where you want to deploy your VM.
- You must also have the Arc Private Cloud Resource User Role for the virtual machine template resource you want to use.
- Finally, you need to have the Arc Private Cloud Resource User Role for the virtual network resource you plan to attach the VM to.

## Step 10: How to create a VM in the Azure portal

1. Open your web browser and navigate to the Azure portal.
2. Find the virtual machines browse view and click on it.
3. You will see a unified browsing experience for both Azure and Arc virtual machines. Click on "Add" and choose "Azure Arc machine" from the drop-down menu.
4. Choose the subscription and resource group where you want to deploy the virtual machine.
5. Provide a name for the virtual machine and select a custom location that has been shared with you by your administrator.
6. If multiple kinds of virtual machines are supported, select "VMware" from the virtual machine kind drop-down menu.
7. Select the resource pool/cluster/host where you want to deploy the virtual machine.
8. Choose the datastore that you want to use for storage.
9. Select a template based on which you will create the virtual machine.
10. If you have selected a Windows template, provide a username and password for the administrator account.
11. If necessary, you can change the disks and network interfaces that are configured in the template. For example, you can add more disks or update existing ones, and you can add or update network interface (NIC) cards.
12. You can also change the network to which the NIC will be attached, provided that you have the appropriate permissions to the network resource.
13. If necessary, you can add tags to the virtual machine resource.
14. Review all the properties and click on "Create" to provision the virtual machine. It may take a few minutes for the virtual machine to be created.

## Why Lenovo?

Lenovo is a US\$70 billion revenue Fortune Global 500 company serving customers in 180 markets around the world. Focused on a bold vision to deliver smarter technology for all, we are developing world-changing technologies that power (through devices and infrastructure) and empower (through solutions, services and software) millions of customers every day.

## For More Information

To learn more about this Lenovo solution contact your Lenovo Business Partner or visit:  
<https://www.lenovo.com/us/en/servers-storage/solutions/>

## Related product families

Product families related to this document are the following:

- [Microsoft Alliance](#)
- [ThinkAgile MX Series for Microsoft Azure Stack HCI](#)
- [VMware Alliance](#)
- [VMware vSphere](#)

## Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.  
8001 Development Drive  
Morrisville, NC 27560  
U.S.A.  
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2024. All rights reserved.

This document, LP1713, was created or updated on March 31, 2023.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:  
<https://lenovopress.lenovo.com/LP1713>
- Send your comments in an e-mail to:  
[comments@lenovopress.com](mailto:comments@lenovopress.com)

This document is available online at <https://lenovopress.lenovo.com/LP1713>.

## Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at <https://www.lenovo.com/us/en/legal/copytrade/>.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®

ThinkAgile®

The following terms are trademarks of other companies:

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Active Directory®, Arc®, Azure®, PowerShell, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.