Private Endpoints for Azure Backup

Azure Backup now allows you to use Private Endpoints for backing up and restoring your data from inside an isolated virtual network. More details on Private Endpoints can be found [here](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview).

This document will help you perform the following:

* Gain clarity on supported and unsupported scenarios for private endpoints with Backup.
* Enable the Azure subscription to use private endpoints for Recovery Services vaults inside the subscription
* Create a Recovery Services vault to back up your resources
* Enable managed identities for the vault and grant required permissions to create private endpoints
* Making DNS changes required for private endpoints
* Create and approve private endpoints for a vault inside a virtual network

# Support Matrix and Current Limitations

This section discusses the supported and unsupported scenarios for using private endpoints for Backup. The section also discusses certain limitations for the current solution. These limitations are being worked upon and will be removed in due course of time.

* Private Endpoints will be used for backup and restore of **SQL and SAP HANA workloads in an Azure VM and MARS agent** backup only, however, **you can use the vault for backup of other workloads as well** (these would not require private endpoints though). More details on support for workloads below.

|  |  |  |
| --- | --- | --- |
| **Workloads in Azure VM (SQL, SAP HANA), MARS Agent** | **Azure VM** | **Azure Files** |
| **Supported**  Use Private Endpoints to perform backup and restore of workloads running inside a secured virtual network.   * This document will help you understand how to use private endpoint for backing up these workloads. | **Not required**  You can backup and restore Azure VMs **without having to whitelist any IPs/FQDNs, thus maintaining network isolation,** and without the need for using Private Endpoints.   * File recovery is not supported if the vault contains private endpoints. * When using unmanaged disks, ensure the storage account containing the disks allows access to ‘trusted Microsoft services’ if it is ACL’ed. | **Not required**  Backups are stored in the local storage account only.   * Please allow ‘trusted Microsoft services’ to access ACL’ed storage accounts. |

* Private endpoints can be created for **new** Recovery Services vaults only (that do not have any items registered to the vault). Therefore, private endpoints **must be created before any items are attempted to be protected to the vault**.
* **Encryption at rest using customer managed keys is not supported for vaults using private endpoints**. Since CMK encryption is currently supported only for Azure VM backup, it is highly recommended you use a different vault (that uses CMK encryption) for backing up your Azure VMs. Azure VMs backup can be performed directly from inside a secured virtual network, without needing to open up to any public networks. Similarly, **a** **vault using private endpoints cannot be encrypted using customer managed keys.**
* Once a private endpoint is created for a vault, the vault will be locked down and **will not be accessible (for backups and restores) from networks apart from ones for which private endpoints exist**. If all private endpoints for the vault are removed, the vault will be accessible from all networks.
* While a Recovery Services vault is used by (both) Azure Backup and Azure Site Recovery, **this document discusses use of Private Endpoints for Azure Backup only**. Use of Azure Site Recovery is not currently supported.
* Azure AD currently does not support private endpoints Hence, IPs/FQDNs required for Azure AD to work in a region would need to be allowed outbound access from the secured network. You can also use NSG tags and Azure Firewall tags for allowing access to Azure AD, as applicable.
* Virtual networks with Network Policies are not supported for Private Endpoints. You would need to disable Network Polices before moving forward.

# Creating and using Private Endpoints for Backup

This section talks about the steps involved in creating and using private endpoints for Azure Backup inside your virtual networks

**Note**: It is highly recommended that you follow steps in the same sequence as mentioned in this document. Failure to do so may lead to the vault being rendered incompatible to use private endpoints and requiring you to restart the process with a new vault.

## Enable the Azure subscription to use Private Endpoints for Backup

By default, no Azure subscriptions currently allow you to create private endpoints for your Recovery Services vaults.

For enabling your subscriptions to use private endpoints for Azure Backup, please contact Microsoft (you would need to reach out to the Azure Backup product group). To do this, please fill out [this form](https://forms.office.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR0H3_nezt2RNkpBCUTbWEapUQk5EQ1QxRzVOWDNDS1Y1Q0xLTkdLQ0U0RC4u) and mail [azbackupnetsec@microsoft.com](mailto:azbackupnetsec@microsoft.com) about the same. Until this step is completed and confirmed, you would not be able to create and use private endpoints for your vaults. Hence, it is suggested that you proceed only once this is done.

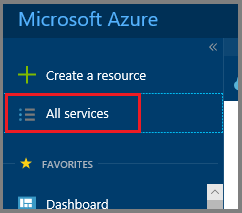
## Creating a Recovery Services vault

A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines. This section shows how to create a vault using the portal and the ARM client.

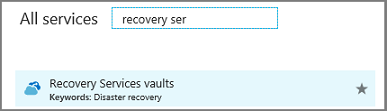
### Using the portal

To create a Recovery Services vault:

1. Sign into your subscription in the [Azure portal](https://portal.azure.com/).
2. On the left menu, select **All services**.

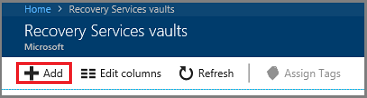


1. In the **All services** dialog box, enter **Recovery Services**. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.



The list of Recovery Services vaults in the subscription appears.

1. On the **Recovery Services vaults** dashboard, select **Add**.



The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location and create the vault.**

Learn more about to Recovery Services vaults [here](https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview).

### Using the ARM client

Alternately, you can create the Recovery Services Vault and enable its managed identity using the ARM client. A sample for doing the same is shared below:

armclient PUT /subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/Vaults/<vaultname>?api-version=2017-07-01-preview @C:\<filepath>\MSIVault.json

The above JSON should have the following content:

**Request JSON:**

{

"location": "eastus2",

"name": "<vaultname>",

"etag": "W/\"datetime'2019-05-24T12%3A54%3A42.1757237Z'\"",

"tags": {

"PutKey": "PutValue"

},

"properties": {},

"id": "/subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/Vaults/<vaultname>",

"type": "Microsoft.RecoveryServices/Vaults",

"sku": {

"name": "RS0",

"tier": "Standard"

},

"identity": {

"type": "systemassigned"

}

}

**Response JSON:**

{  
 "location": "eastus2",  
 "name": "<vaultname>",  
 "etag": "W/\"datetime'2020-02-25T05%3A26%3A58.5181122Z'\"",  
 "tags": {  
 "PutKey": "PutValue"  
 },  
 "identity": {  
 "tenantId": "<tenantid>",  
 "principalId": "<principalid>",  
 "type": "SystemAssigned"  
 },  
 "properties": {  
 "provisioningState": "Succeeded",  
 "privateEndpointStateForBackup": "None",  
 "privateEndpointStateForSiteRecovery": "None"  
 },  
 "id": "/subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/Vaults/<vaultname>",  
 "type": "Microsoft.RecoveryServices/Vaults",  
 "sku": {  
 "name": "RS0",  
 "tier": "Standard"  
 }  
 }

Please note that the vault created in this example through the ARM client is already created with a system-assigned managed identity.

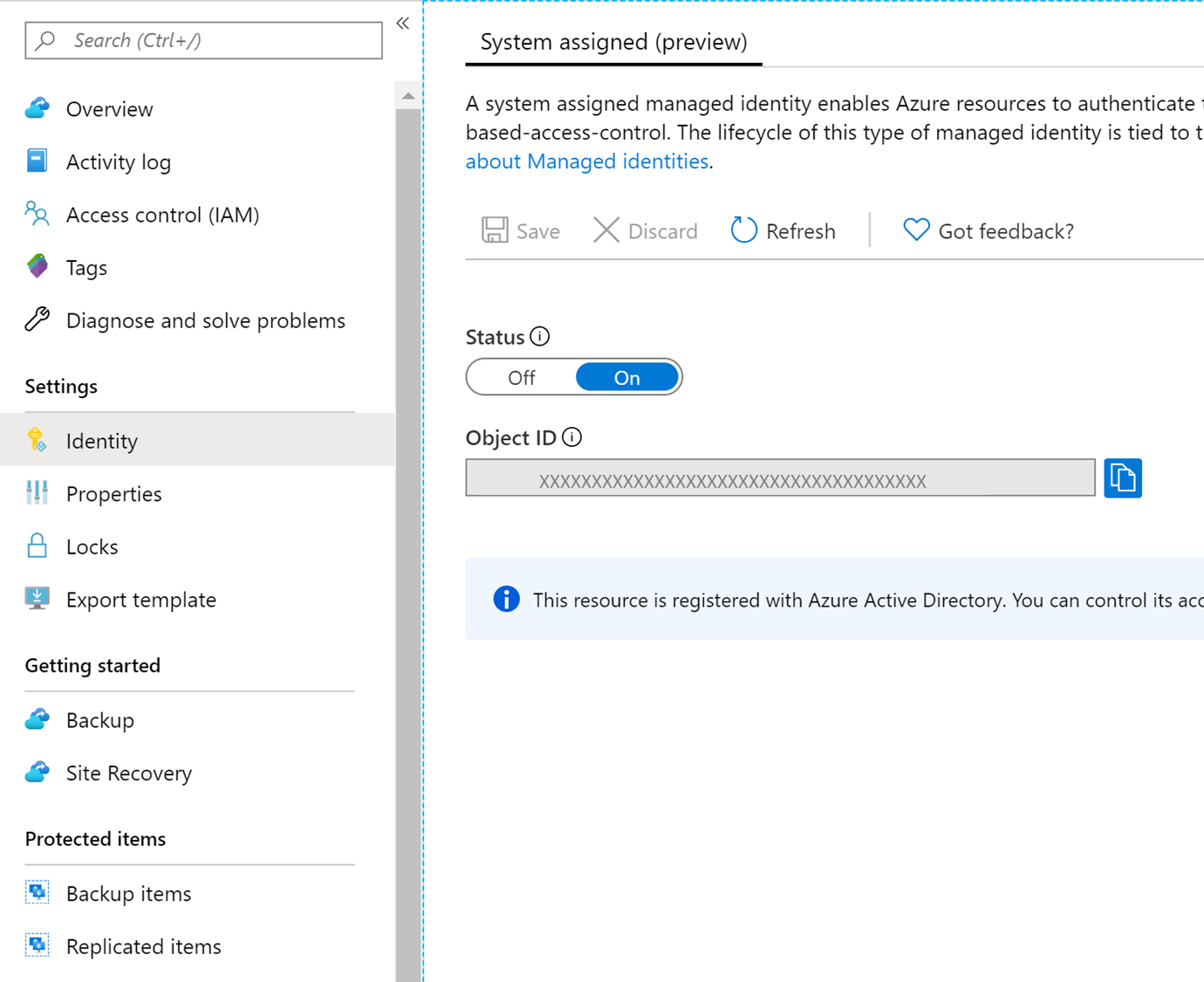
## Enable Managed Identity for your vault and grant required permissions

Managed identities allow the vault to create and use private endpoints. Hence, the vault must be granted permissions to create the required private endpoints in your resource group.

### Enable Managed Identity

Please note that the vault created through the ARM client in the example above is already created with a system-assigned managed identity. Therefore, this step for enabling managed identity is not required if you have created a vault using the same example (only part 1 of this section, part 2 for granting permissions is still required).

1. Go to your Recovery Services vault -> **Identity.** The ‘Identity’ option would be visible only after the subscription has been whitelisted.



1. Change the **Status** to ‘**On’** and click **Save**.
2. An Object ID is generated, which we will use in the next step to assign permissions to the vault.

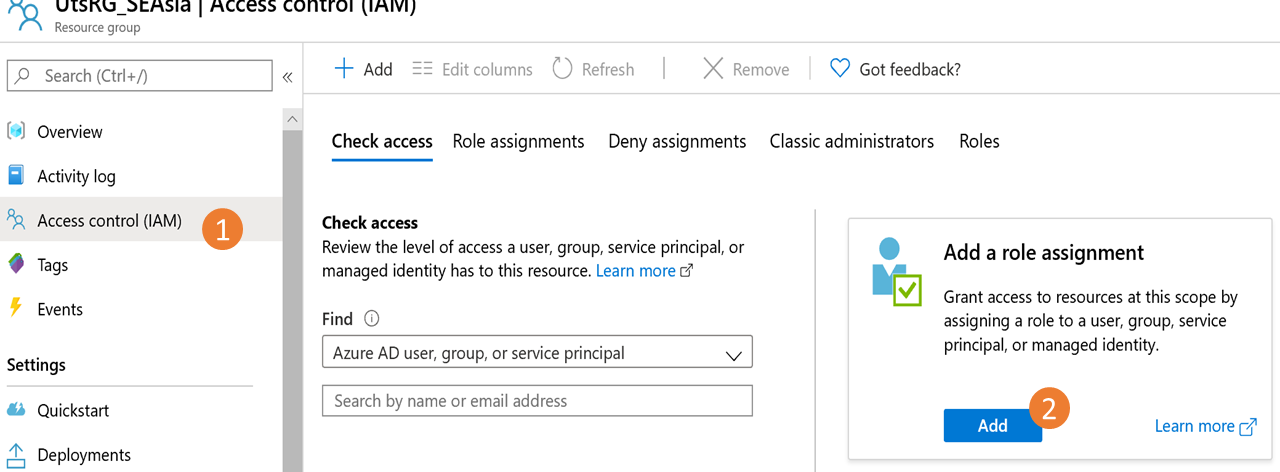
### 2. Grant permissions to the vault to create required private endpoints

In order to create the required private endpoints for Azure Backup, the vault (the Managed Identity of the vault) must have permissions to the following resource groups:

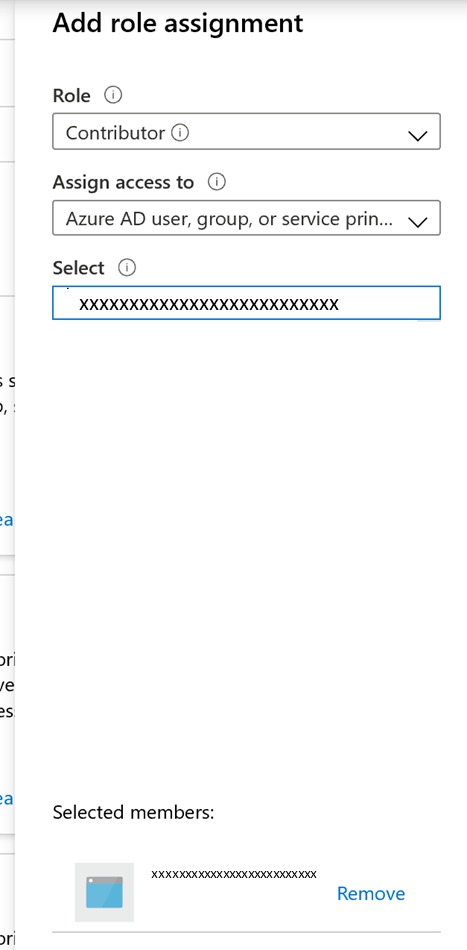
1. The Resource Group that contains the servers that need to be backed up
2. The Resource Group where the Private Endpoints are to be created
3. The Resource Group that contains the Private DNS zones

It is suggested that that you grant ‘Contributor’ role for the Vault (Managed Identity) to the above three Resource Groups. The following steps describe how to do it for a particular Resource Group (this needs to be done for each of the three resource groups):

1. Go to the Resource Group and navigate to **Access Control (IAM)** on the left bar.
2. Once in Access Control, go to **Add a role assignment**



1. In the **Add role assignment** blade, choose **Contributor** as the **Role**, and use the **Object ID** of the vault (this is the Managed Identity of the vault) observed in the previous step as the **Principal**. Click **Save** when done.



To manage permissions at a more granular level, refer to the Appendix.

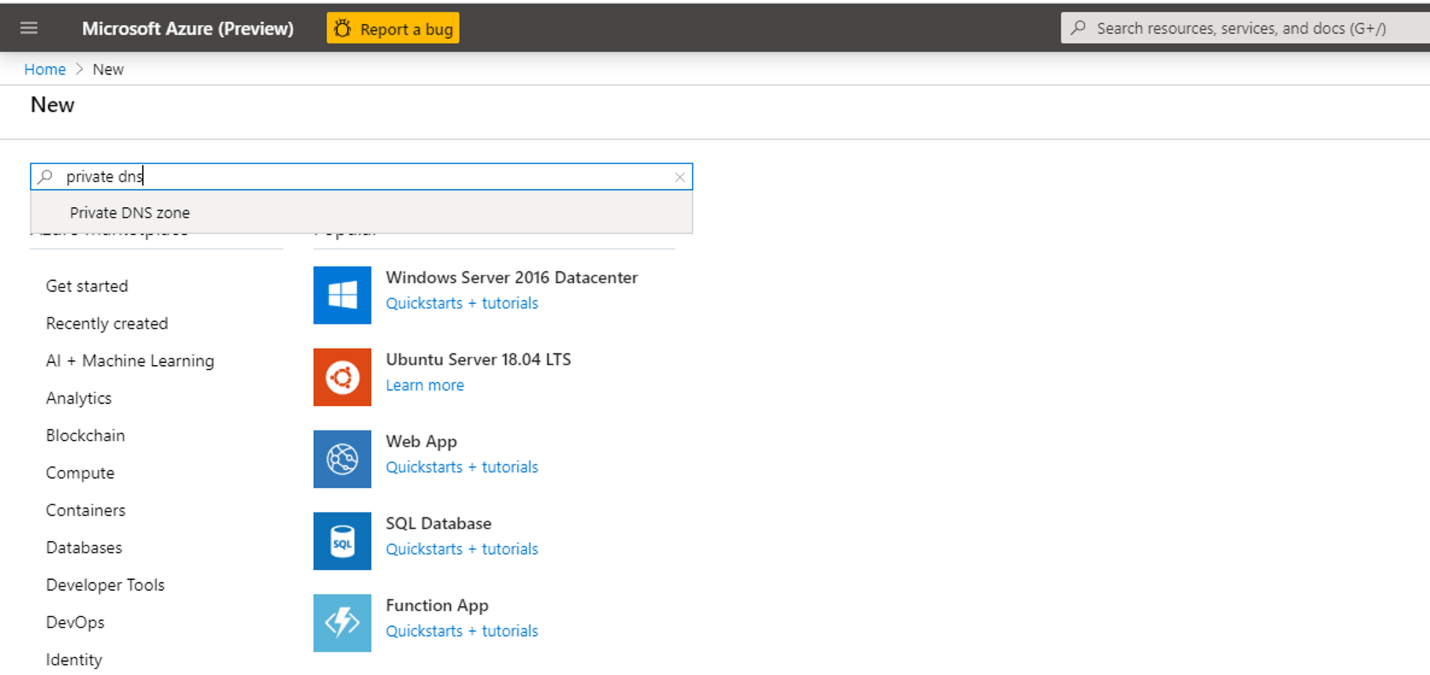
## DNS changes

You need to create the following Private DNS Zones in order to allow the Backup extension to resolve private link FQDNs to private IPs, thus requiring you to create three private DNS zones:

* privatelink.<geo>.backup.windowsazure.com (for service communication)
* privatelink.blob.core.windows.net (for backup/restore data)
* privatelink.queue.core.windows.net (for service communication)

### Creating a private DNS zone

1. Search for Private DNS Zone in the All services search bar, and select **Private DNS zones** from the drop down.

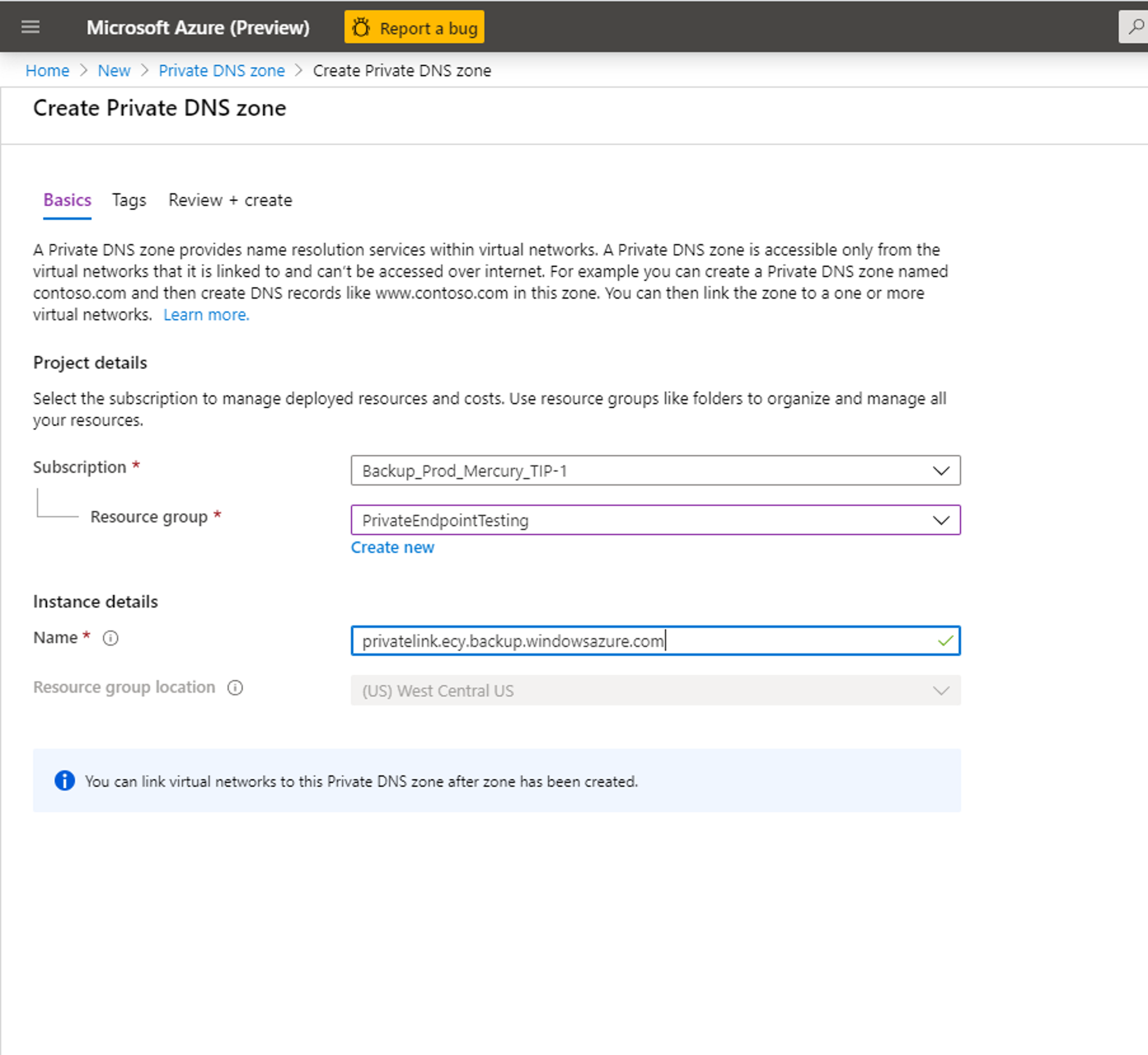


1. Once in the Private DNS zones blade, click the +Add button to start creating a new zone.
2. In the Create private DNS zone blade, fill in the details required. The subscription must be the same as where the private endpoint must be created.

The zones must be named as:

* privatelink.<geo>.backup.windowsazure.com
* privatelink.blob.core.windows.net
* privatelink.queue.core.windows.net

|  |  |  |
| --- | --- | --- |
| **Zone** | **Service** | **Subscription and Resource Group details** |
| privatelink.<geo>.backup.windowsazure.com | Backup | **Subscription**: Same as where Private Endpoint needs to be created  **RG**: Any RG within the subscription |
| privatelink.blob.core.windows.net | Blob | **Subscription**: Same as where private endpoint needs to be created  **RG**: Either the RG of the VNET or that of the Private Endpoint |
| privatelink.queue.core.windows.net | Queue |



For URL naming conventions in national geos:

China: <https://docs.microsoft.com/en-us/azure/china/resources-developer-guide#check-endpoints-in-azure>

Germany: <https://docs.microsoft.com/en-us/azure/germany/germany-developer-guide#endpoint-mapping>

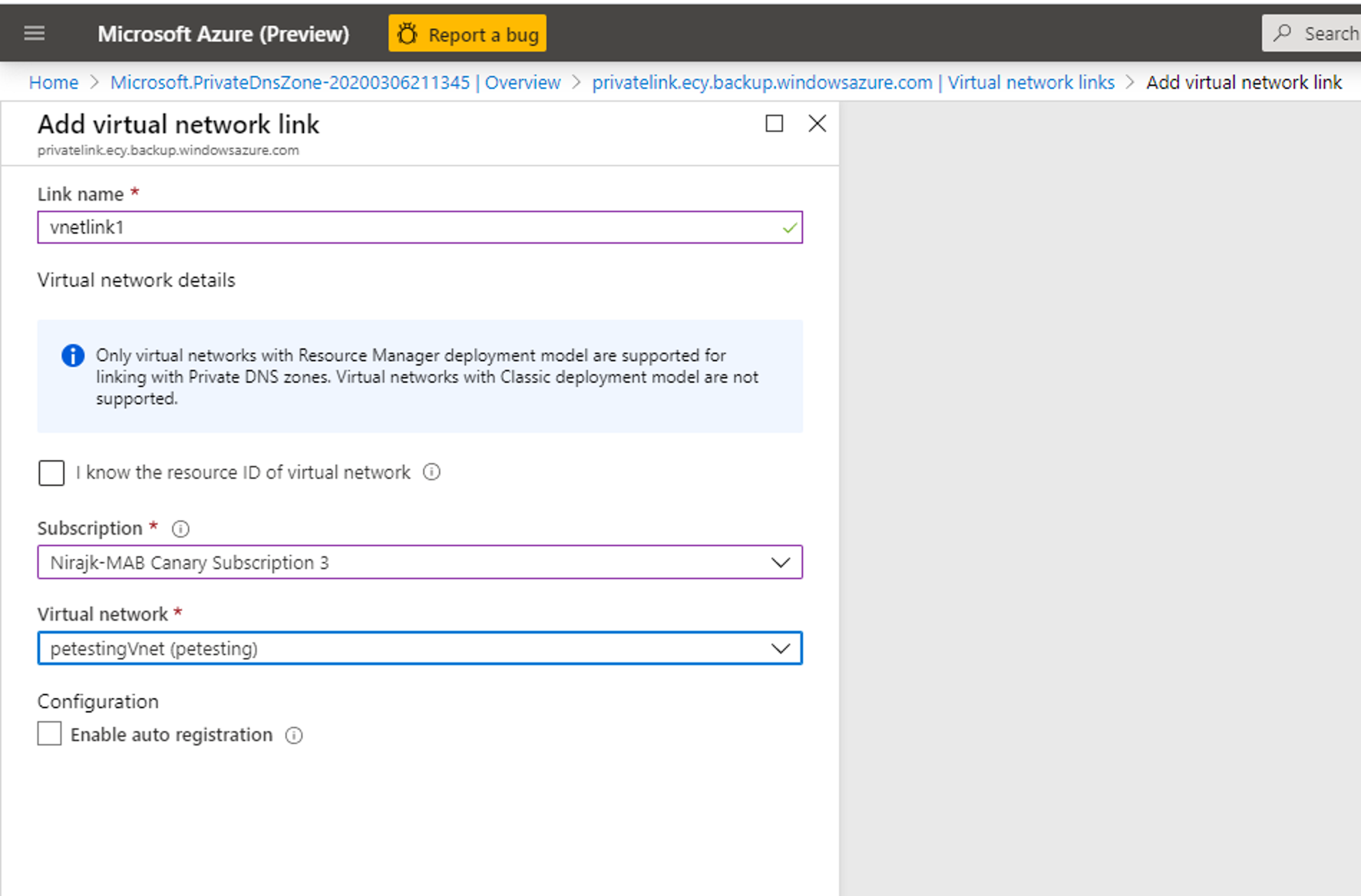
US Gov: <https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-developer-guide>

1. Once done, proceed to review and create the DNS zone.

### Linking private DNS zones with your virtual network

The DNS zones created above must now be linked to the virtual network where your servers are (that need to be backed up)

1. Go to your DNS zone (that you created in the previous step) and navigate to **Virtual network links** on the left bar. Once there, click the **+Add** button
2. Fill in the required details. The **Subscription** and **Virtual network** fields must be filled with corresponding details of the virtual network where your servers exist. The other fields must be left as is.



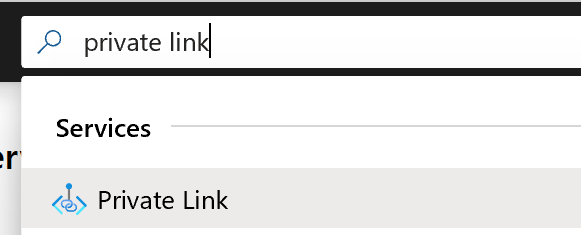
## Creating and approving Private Endpoints for Azure Backup

### Creating Private Endpoints for Backup

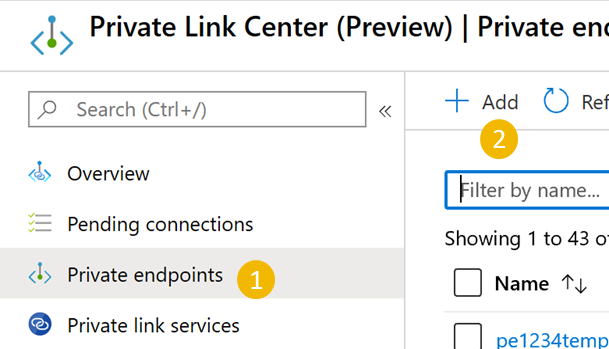
You can create private endpoints for your vault inside your virtual networks using the Private Link Center in the portal or through Azure PowerShell:

#### Portal

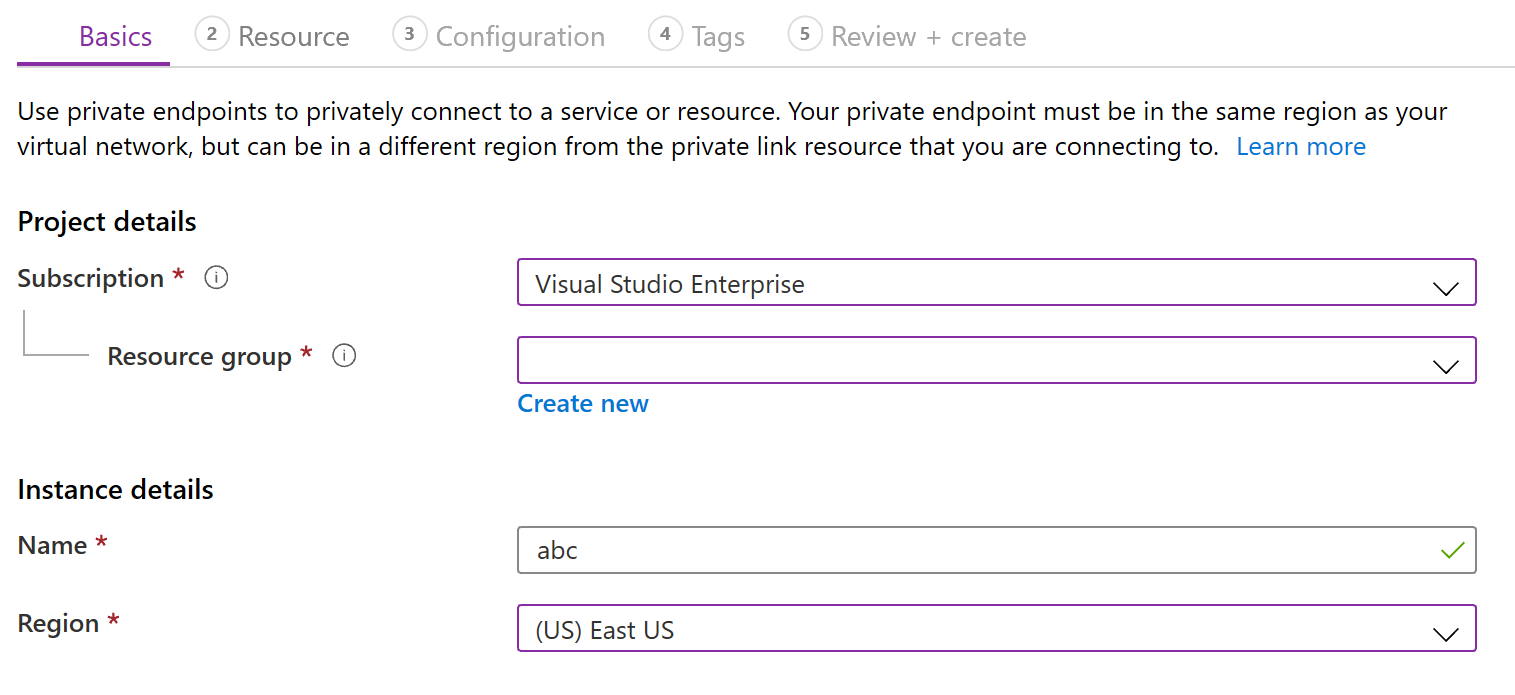
1. In the search bar, search for and select ‘Private Link’. This takes you to the Private Link Center.



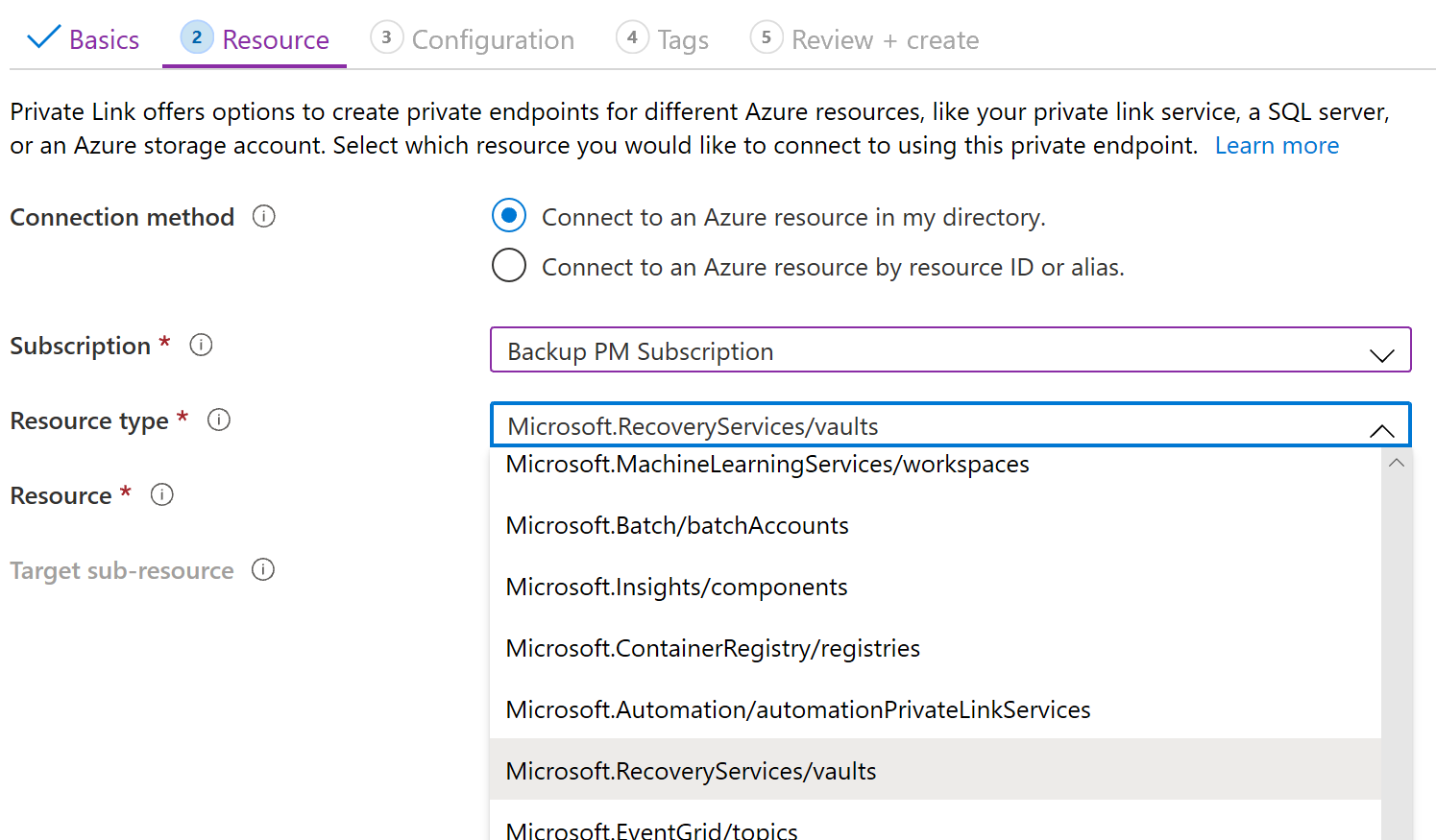
1. On the left navigation bar, click on Private Endpoints. Once in the Private Endpoints blade, click ‘+Add’ to start creating a Private Endpoint for your vault.



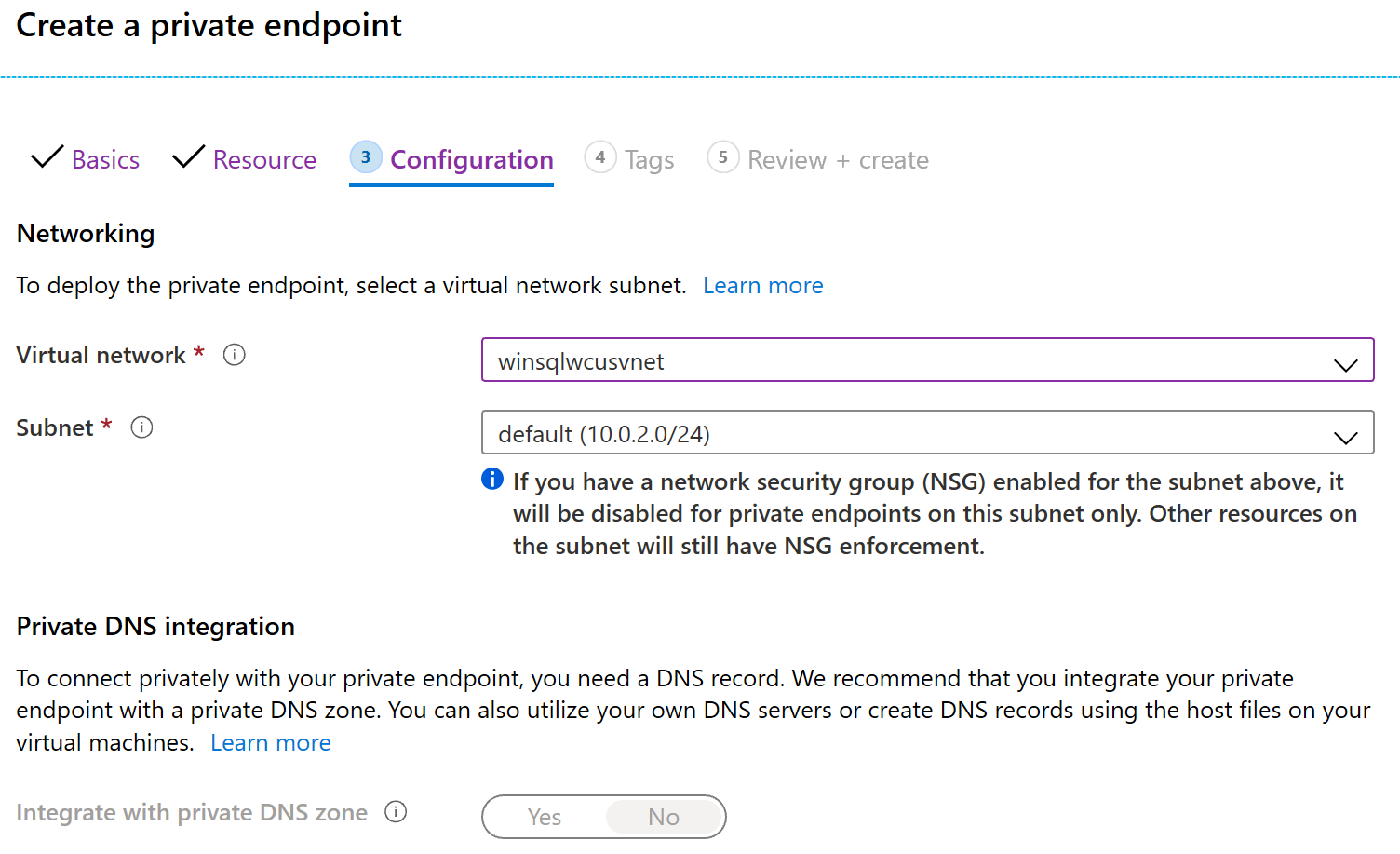
1. Once in the ‘Create Private Endpoint’ experience, you would be required to specify details for creating your private endpoint connection.
   1. **Basics:** Fill in the basic details for your private endpoints. The region should be the same as the vault and the resource.



* 1. **Resource:** This tab requires you to mention the PaaS resource for which you want to create your connection. Select ‘**Microsoft.RecoveryServices/vaults**’ from the resource type for your desired subscription. Once done, choose the name of your Recovery Services vault as the ‘Resource’ and ‘**AzureBackup**’ as the ‘Target sub-resource’.



* 1. **Configuration:** In configuration, specify the virtual network and subnet where you want the private endpoint to be created. This would be the net where the VM is present.



* 1. Optionally, you can add ‘Tags’ for your private endpoint.
  2. Proceed to ‘Review + create’ once done entering details. When the validation completes, click ‘Create’ to create the private endpoint.

#### Azure PowerShell

1. Use the following PowerShell commands to initiate creation of Private Endpoints:

Connect-AzAccount

Set-AzContext -SubscriptionId

$currentAzureContext = Get-AzContext

$azureRmProfile = [Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::Instance.Profile;

$profileClient = New-Object Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient($azureRmProfile);

$accessToken = $profileClient.AcquireAccessToken($currentAzureContext.Subscription.TenantId).AccessToken;

1. Create json file with manual Private Endpoint connection settings as per the following template:

<https://docs.microsoft.com/en-us/azure/templates/microsoft.network/2019-04-01/privateendpoints>

For e.g.,

{

"name": "<PEName>",

"type": "Microsoft.Network/privateEndpoints",

"location": "eastus2euap",

"tags": {},

"properties": {

"subnet": {

"id": "/subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.Network/virtualNetworks/<vnetname>/subnets/<subnetName>",

"name": "default"

},

"manualPrivateLinkServiceConnections": [

{

"id": "<PE\_connection\_Id>",

"properties": {

"privateLinkServiceId": "/subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/vaults/<vaultname>", "groupIds": [ "AzureBackup" ],

"requestMessage": "Backup Admin please manually approve my connection."

},

"name": "<PE\_connection\_Name>"

}

]

}

}

1. Run the following:

$json = [IO.File]::ReadAllText("")   
Invoke-WebRequest -Uri "<https://management.azure.com/subscriptions>/<subscriptionid>/resourceGroups/<rgname>/providers/[Microsoft.Network/privateEndpoints](http://Microsoft.Network/privateEndpoints)/<PEName>?api-version=2019-08-01" -Method PUT -ContentType "application/json" -Headers @{Authorization ="Bearer $accessToken"} -Body $json

### Approving Private Endpoints

If the user creating the private endpoint is also the owner of the Recovery Services vault, the private endpoint created above will be auto-approved. Else, the owner of the vault must approve the private endpoint before being able to use it. Currently, manual approval can be done using the ARM client only.

1. Use GetVault to get the Private Endpoint Connection ID for your private endpoint.

armclient GET /subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/vaults/<vaultname>?api-version=2017-07-01-preview

This would return the Private Endpoint Connection ID. The name of the connection can be arrived at using the first part of the connection ID as follows:

privateendpointconnectionid = {peName}.{vaultId}.backup.{guid}

1. Get the **Private Endpoint Connection ID** (and the **Private Endpoint Name**, wherever required) from the response and replace it in the following JSON and ARM URI and try changing the Status to “Approved/Rejected/Disconnected”, as demonstrated in the sample below:

armclient PUT /subscriptions/<subscriptionid>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/Vaults/<vaultname>/privateEndpointConnections/<privateendpointconnectionid>?api-version=2020-02-02-preview @C:\<filepath>\BackupAdminApproval.json

**JSON:**

{

"id": "/subscriptions/<subscriptionod>/resourceGroups/<rgname>/providers/Microsoft.RecoveryServices/Vaults/<vaultname>/privateEndpointConnections/<privateendpointconnectionid>",

"properties": {

"privateEndpoint": {

"id": "/subscriptions/<pesubscriptionid>/resourceGroups/<pergname>/providers/Microsoft.Network/privateEndpoints/pename"

},

"privateLinkServiceConnectionState": {

"status": "Disconnected", //choose state from Approved/Rejected/Disconnected

"description": "Disconnected by <userid>"

}

}

}

## Adding DNS records

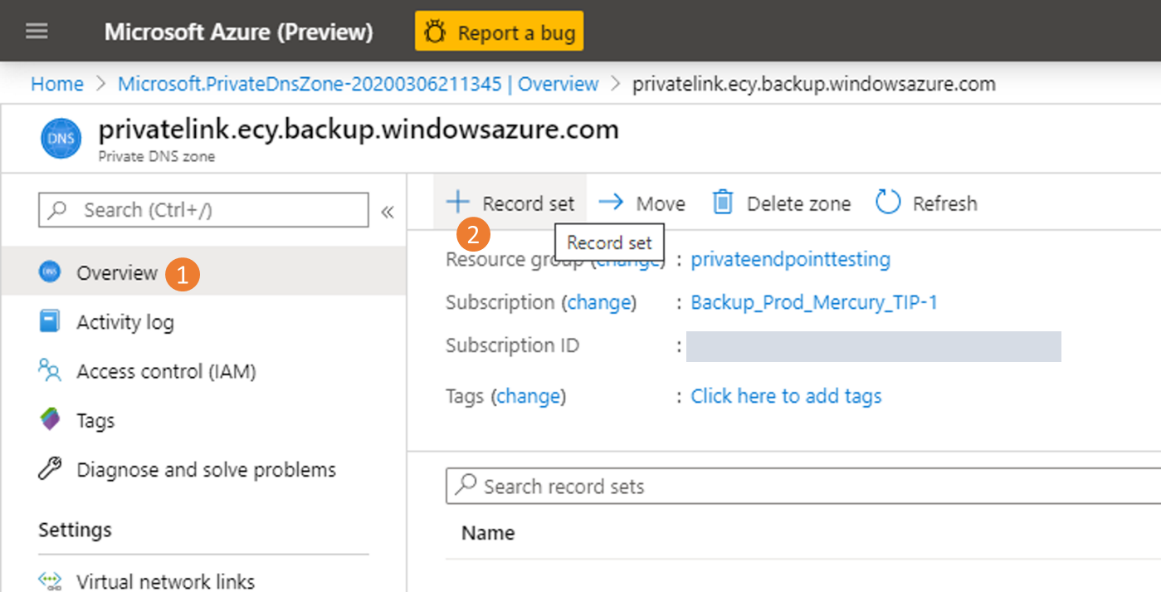
Once you have created the required private DNS zones and the private endpoints for your, you would need to add DNS records to your DNS zone. You can do this either manually or using a PS script. This needs to be done for your Backup DNS zone only, the same for Blobs and Queues will automatically be updated.

**Note**: In case you are using a custom private DNS zone, please make sure that similar entries are made as discussed below.

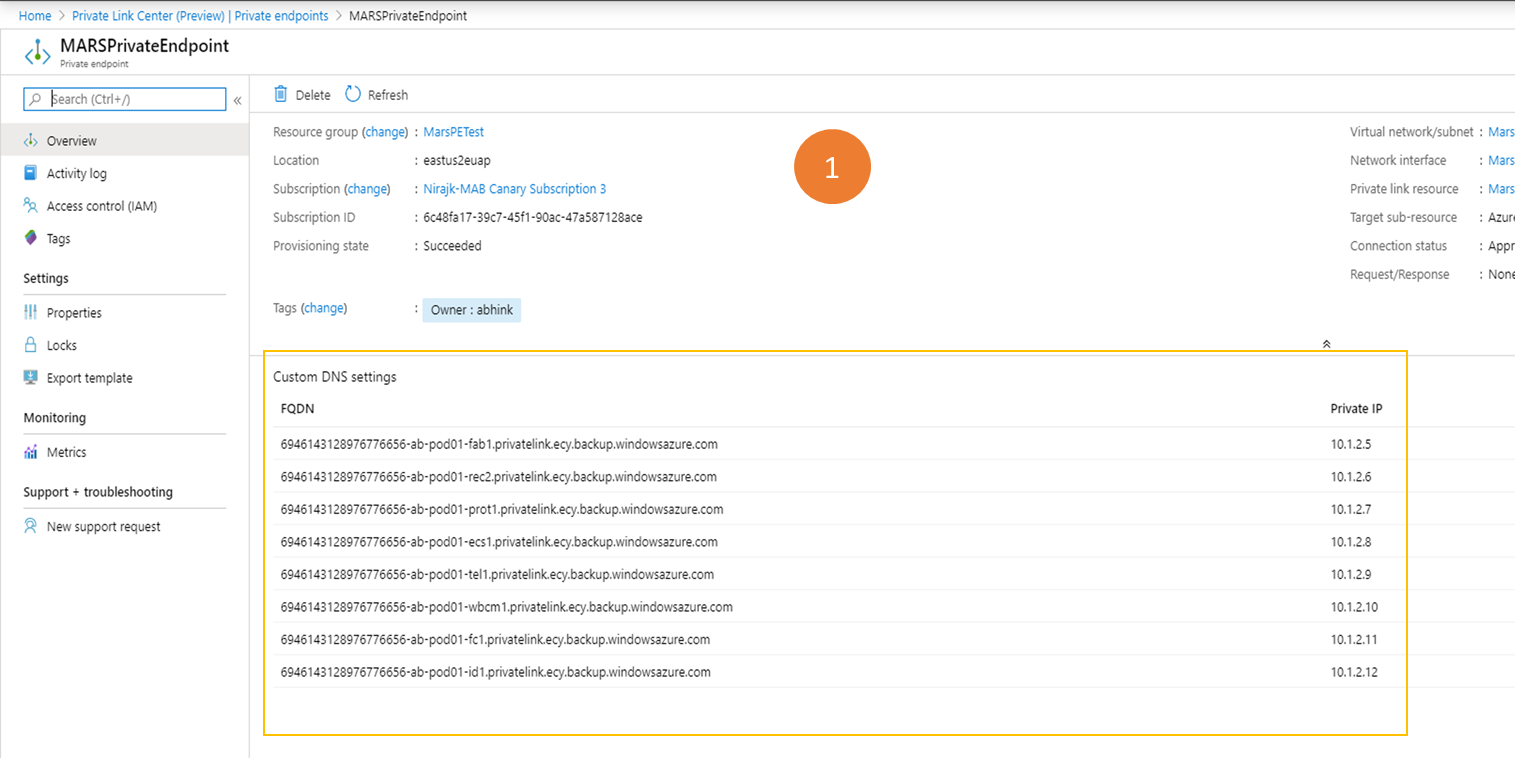
#### Add records manually

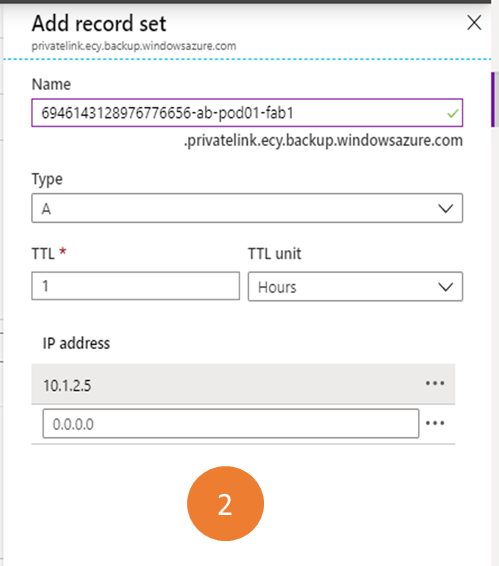
This requires you to make entries for your each FQDN in your private endpoint into your Private DNS Zone.

1. Go to your **private DNS zone** and navigate to the **Overview** option on the left bar. Once there, click **+Record set** to start adding records.



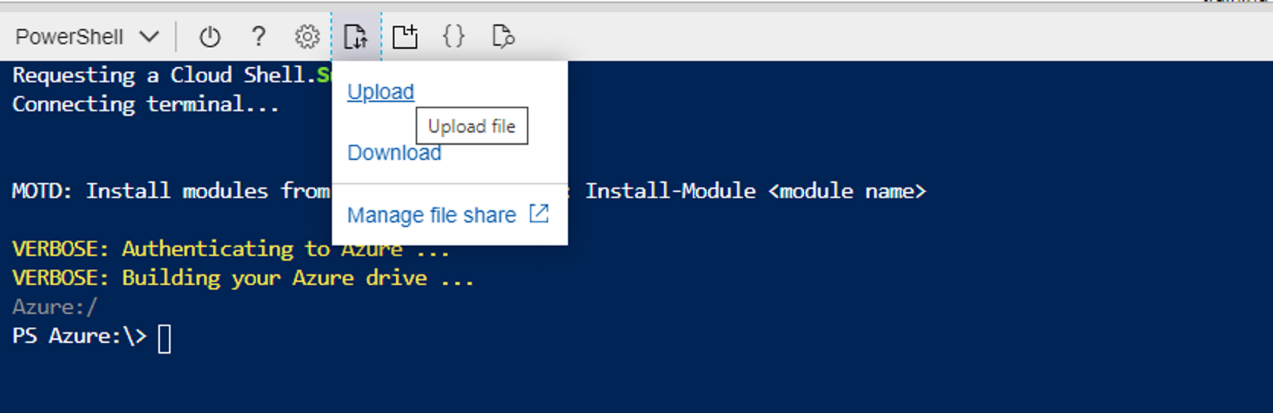
1. In the add record set blade that opens, add one entry for each FQDN and private IP as an A type record. The list of FQDNs and IPs can be obtained from your Private Endpoint (under Overview). As shown in the example below, the first FQDN from the private endpoint is being added to the record set in the private DNS zone.





#### Add records using PowerShell script

1. Start the **Cloud Shell** in the Azure portal and click on **Upload files** in the PS window.



1. Upload the following script

[DnsZoneCreation](https://download.microsoft.com/download/1/2/6/126a410b-0e06-45ed-b2df-84f353034fa1/dnszonerecordcreation.ps1)

1. Go to your home folder (e.g., cd /home/user)
2. Run the following:
3. ./dnszonerecordcreation.ps1 -subscription <SubscriptionId> -vaultPEName <VaultPE Name> -vaultPEResourceGroup <Vault PE RG> -dnsResourceGroup <Private DNS RG> -privatezone <privatednszone>

subscription: Subscription where the resources (vault's private endpoint and private DNS zone) reside

vaultPEName: Name of the private endpoint created for the vault

vaultPEResourceGroup: Resource group that contains the vault's private endpoint

dnsResourceGroup: Resource group that contains the private DNS zones

privatezone : name of the private DNS zone

## Using Private Endpoints for Backup

Once the private endpoints created for the vault in your VNet have been approved, you can start using the same for performing your backup and restores.

**Important:** Please ensure that you have completed all the steps mentioned above in the document successfully before proceeding. To recap, you must have:

1. Enabled your subscription to use Private Endpoints for Azure Backup
2. Created a Recovery Services Vault
3. Enabled the vault to use system assigned Managed Identity
4. Assigned relevant permissions to the Managed Identity of the vault
5. Created 3 Private DNS zones
6. Linked your Private DNS zones to your Azure Virtual Network
7. Created a Private Endpoint for your vault
8. Approved the Private Endpoint (if not auto approved)
9. Added required DNS records to your private DNS zone for Backup

### Backup and restore of workloads in Azure VM (SQL, SAP HANA)

Once the private endpoint is created and approved, no additional changes are required from the client side to use the private endpoint. All communication and data transfer from your secured network to the vault will be performed through the private endpoint.

### Backup and restore through MARS Agent

When using the MARS Agent to back up your on-prem resources, please make sure that your on-prem network (containing your resources to be backed up) is peered with the Azure VNET that contains a private endpoint for the vault, in order to be able to use it. You can then proceed install the MARS agent and configure backup as detailed [here](https://docs.microsoft.com/en-us/azure/backup/install-mars-agent). It must be, however, ensured that all communication for backup happens through the peered network only.

# Appendix

## Managing permissions on Resource Groups

The Managed Identity for the vault needs to have the following permissions in the resource group and virtual network where the private endpoints would be created:

1. “Microsoft.Network/privateEndpoints/\*"  
   This is required to perform CRUD on private endpoints in the resource group. It should be assigned on the resource group.
2. “Microsoft.Network/virtualNetworks/subnets/join/action”  
   This is required on the virtual network where private IP is getting attached with the private endpoint.
3. "Microsoft.Network/networkInterfaces/read"  
   This is required on the resource group to get the network interface created for the private endpoint
4. Private DNS Zone Contributor Role   
   This role already exists and can be used to provide "Microsoft.Network/privateDnsZones/A/\*" and "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read" permissions.

You can use one of the following methods to create roles with required permissions:

### Create roles and permissions manually

Create the following JSON files and use the PS command at the end of the section to create roles:

**//PrivateEndpointContributorRoleDef.json**

{

  "Name": "PrivateEndpointContributor",

  "Id": null,

  "IsCustom": true,

  "Description": "Allows management of Private Endpoint",

  "Actions": [

    "Microsoft.Network/privateEndpoints/\*",

  ],

  "NotActions": [],

  "AssignableScopes": [

    "/subscriptions/00000000-0000-0000-0000-000000000000"

  ]

}

**//NetworkInterfaceReaderRoleDef.json**

{

  "Name": "NetworkInterfaceReader",

  "Id": null,

  "IsCustom": true,

  "Description": "Allows read on networkInterfaces",

  "Actions": [

    "Microsoft.Network/networkInterfaces/read"

  ],

  "NotActions": [],

  "AssignableScopes": [

    "/subscriptions/00000000-0000-0000-0000-000000000000"

  ]

}

**//PrivateEndpointSubnetContributorRoleDef.json**

{

  "Name": "PrivateEndpointSubnetContributor",

  "Id": null,

  "IsCustom": true,

  "Description": "Allows adding of Private Endpoint connection to Virtual Networks",

  "Actions": [

    "Microsoft.Network/virtualNetworks/subnets/join/action"

  ],

  "NotActions": [],

  "AssignableScopes": [

    "/subscriptions/00000000-0000-0000-0000-000000000000"

  ]

}

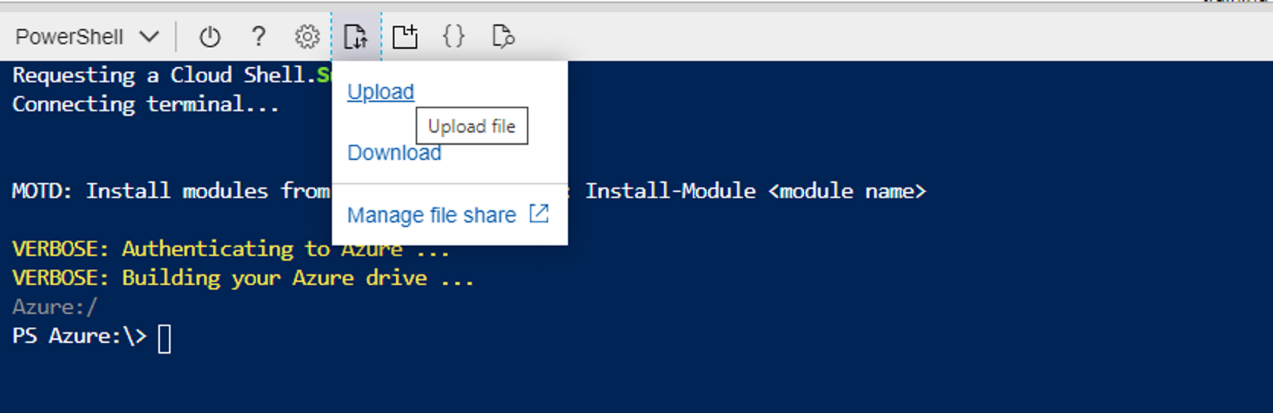
 New-AzRoleDefinition -InputFile "PrivateEndpointContributorRoleDef.json"

 New-AzRoleDefinition -InputFile "NetworkInterfaceReaderRoleDef.json"

 New-AzRoleDefinition -InputFile "PrivateEndpointSubnetContributorRoleDef.json"

### Use a script

1. Start the **Cloud Shell** in the Azure portal and click on **Upload files** in the PS window.



1. Upload following the script:

[VaultMsiPrereqScript](https://download.microsoft.com/download/1/2/6/126a410b-0e06-45ed-b2df-84f353034fa1/VaultMsiPrereqScript.ps1)

1. Go to your home folder (e.g., cd /home/user)
2. Run the following:

./VaultMsiPrereqScript.ps1 -subscription <subscription-Id> -vaultPEResourceGroup <vaultPERG> -vaultPESubnetResourceGroup <subnetRG> -vaultMsiName <msiName>

subscription: SubscriptionId which has resource group where private endpoint for the vault is to be created and the subnet where vault's private endpoint is getting attached

vaultPEResourceGroup: Resource group where private endpoint for the vault is getting created

vaultPESubnetResourceGroup: Resource group of the subnet to which private endpoint is to be joined

vaultMsiName: Name of the vault's MSI which that same as VaultName

1. Complete the authentication and the script will take the context of the given subscription provided above and create the appropriate roles if missing from tenant and will assign roles to the vault's MSI.