

From The  Architects

Veeam Backup for Azure (Azure Private Deployments)

Author: David Bewernick

Contents

Executive summary.....	3
Introduction.....	4
Overview	4
Requirements	5
App registration and permissions.....	5
Veeam Appliance	5
Azure Service Bus.....	5
Storage Accounts for Repositories	7
Multi-Region and landing zones.	7
Azure Storage Accounts	7
Veeam Backup Repositories.....	9
Veeam Workers	12
Network Configuration.....	12
Azure Private DNS Integration.....	13
Azure Key Vault.....	14
Conclusion	17
Additional Topics	18
Azure Plug-in for Veeam Backup & Replication.....	18
Azure network hints.....	18
Virtual Network Service Endpoints	18
Firewall Ports	18
HTTP Proxy for Updates	19
Appendix A – JSON role template.....	19

Executive summary

Microsoft Azure is more than ever one of the preferred choices when it comes to public cloud computing. Customers and partners know that protecting the workloads in the cloud matter for various reasons. This is underlined by the Shared Responsibility Model, which defined that from the OS system onward or the data kept in PaaS and SaaS the customer is responsible for the data protection.

To protect their data from outsiders, customers are more frequently setting up isolated or restricted networks within Azure. Such environments are also called private deployments and are often seen in hardened environments based on the Microsoft Cloud Adaption Framework (CAF).

This document should give backup and Azure security administrators some guidance steps on running Veeam Backup for Azure in an environment where public access should be avoided.

Introduction

To provide an easier start with a basic setup in a private deployment, this document provides the initial steps and some hints on how to set up Veeam Backup for Microsoft Azure with a focus on the specialities of such environments.

Additionally, the general information can be found on the Helpcenter pages:

<https://helpcenter.veeam.com/docs/vbazure/guide/overview.html>

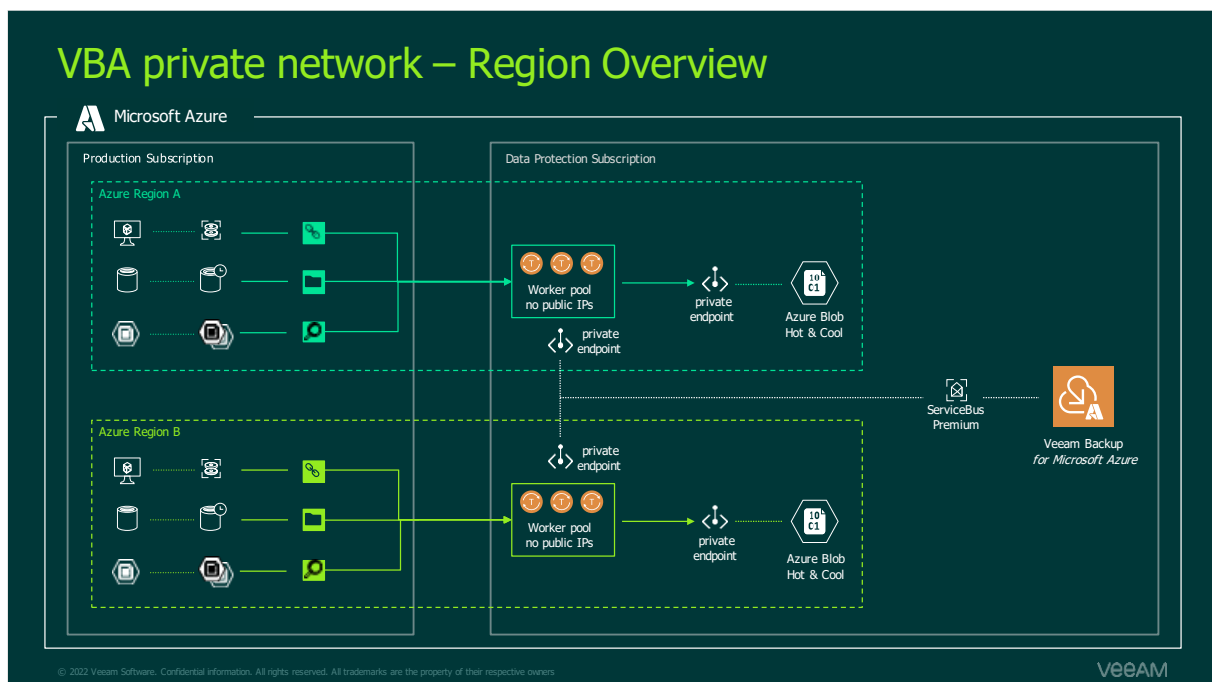
Please have a regular read through the Best Practices Guide to be up to date with some valuable tips and hints from field experience: <https://bp.veeam.com/vbcloud/guide/azure/>

The following steps are part of this document:

- Setting up App registration and permissions
- Deploying the Veeam Backup for Azure Appliance
- Enabling private network deployment and ServiceBus Premium
- Setting up Storage Accounts and Repositories
- Define Networks and private DNS
- Using Azure Key Vaults
- Additional topics that might be helpful

Overview

The following drawing provides a high-level overview of the setup and its connections. As we can see, the environment is split up into a production and a data protection subscription. Also, it is visible that different regions can be considered when deciding on where to place certain components.



This design gives us a basis for the setup described in this document.

Requirements

App registration and permissions

Veeam Backup for Microsoft Azure uses Azure AD Applications to connect and interact with Azure resources. They are named Azure Accounts and Repository Accounts within Veeam Backup for Microsoft Azure.

Their usage for operations starts with the enumeration of resources and building worker instances; they are involved in snapshot management and reach all the way to storing data in Azure Storage Accounts. Therefore, a range of permissions is needed.

We can find the detailed and most recent list of permissions here:

Azure Service Account Permissions

https://helpcenter.veeam.com/docs/vbazure/guide/service_account_permissions.html

Azure Repository Account Permissions

https://helpcenter.veeam.com/docs/vbazure/guide/repository_account_permissions.html

It is possible to leverage only one Azure Application. Still, using a dedicated account just for the backup repositories is recommended to minimise the required permissions for each connection. Also, the repositories can reside in a separate subscription and therefore need a separate Azure Application.

In this demo setup, we have added one Azure Application for the Production subscription and two for the Data Protection subscription. The two Azure Applications in the Data Protection subscription are used to split up the permissions of managing the Appliance and Worker on one side and the access to the Storage Accounts on the other side.

Azure Custom Roles have been defined with settings to reduce the permissions to the minimum requirements. The JSON templates for these roles can be found in Appendix A.

Veeam Appliance

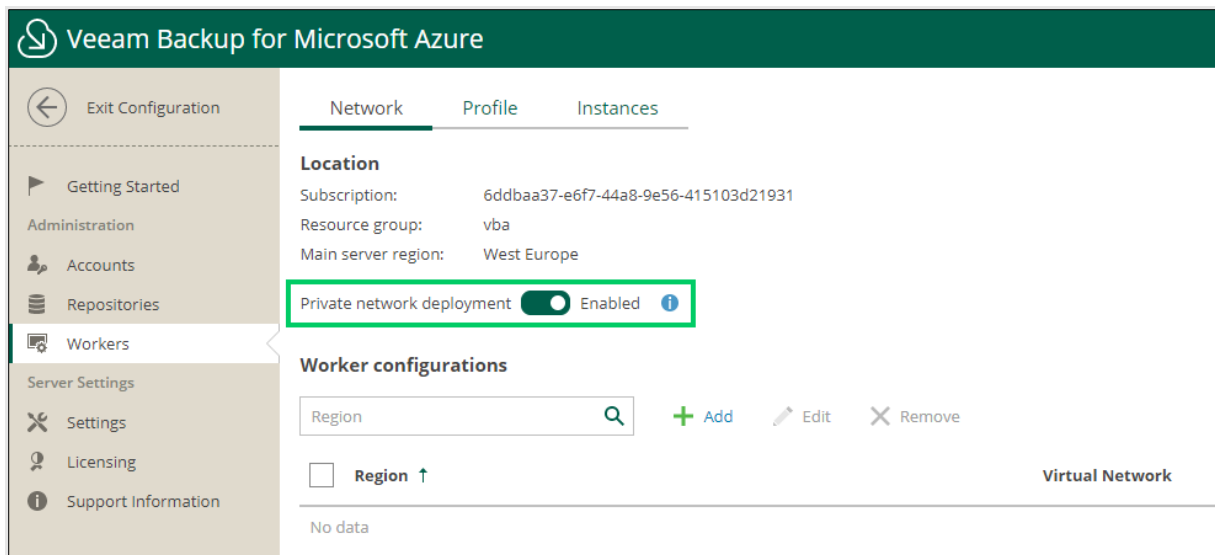
To simplify the deployment of Veeam Backup for Microsoft, we can find a virtual Machine template called “Veeam Backup for Microsoft Azure BYOL Edition” in the Azure Marketplace. Please use the Helpcenter Pages for the initial setup process:

https://helpcenter.veeam.com/docs/vbazure/guide/installing_vb.html

Veeam recommends using a Standard_B4ms machine, which can be adjusted to your needs. Ensure not to go below 2 vCPU and 4 GB RAM for small environments.

Azure Service Bus

For private environments, it is necessary to enable Azure Service Bus premium since this provides the functionality of private endpoints for a Service Bus. Veeam Backup for Microsoft Azure is managing this automatically once we activate the “Private network deployment” Option:



In the Azure Portal, we can see that a new premium Service Bus has been created. The process of activating the new Service Bus might take a while.

Veeam Backup for Azure needs to use the Azure Service Bus Premium to perform tasks in private environments. Depending on your environment, this comes with additional costs to consider.

Storage Accounts for Repositories

Multi-Region and landing zones.



As a best practice provide at least one Azure Storage Account within the data protection subscription per region in which you want to protect workloads to avoid the intensive costs generated by traffic leaving the region.

For security reasons, the Storage Accounts used for Repositories should not be within the same subscription as the production data. Separating them would also align with the landing zone concept provided by the Cloud Adoption Framework. Please see the Microsoft pages for more information:

<https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/>

Azure Storage Accounts

In this setup, we created a Storage Account in North Europe and one in West Europe:




<input type="checkbox"/> Name ↑↓	Type ↑↓	Kind ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/>  vbanortheuropedb	Storage account	StorageV2	vba	North Europe	Data Protection
<input type="checkbox"/>  vbawesteurope	Storage account	StorageV2	vba	West Europe	Data Protection


Each Storage Account has a container with a private access level defined:

Name	Last modified	Public access level
<input type="checkbox"/> \$logs	3.1.2023, 11:53:04	Private
<input type="checkbox"/> vbarepo	3.1.2023, 12:03:07	Private

Set the public network access to “Disabled”:

Firewalls and virtual networks Private endpoint connections Custom domain

 Save  Discard  Refresh



 Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

Public network access

☐ Enabled from all networks

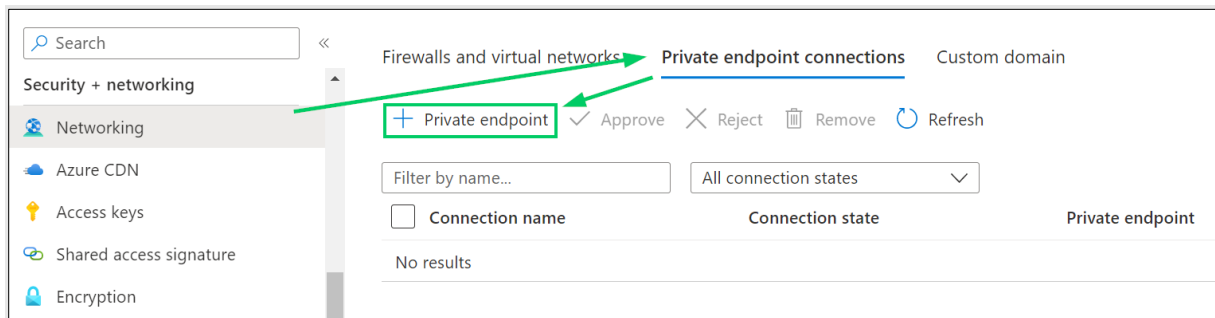
☐ Enabled from selected virtual networks and IP addresses

☒ Disabled

 Configure network security for your storage accounts. [Learn more](#) 

Create a private endpoint for every Storage Account in its region and one in the same network as the Veeam Appliance. The first is to enable the worker writing data during backups and the latter to manage the repository.

You can access the private endpoint settings by clicking “Networking” and “Private Endpoints” on the Storage Account.



Create a private endpoint ...

1 Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ Data Protection

Resource group * ⓘ vba

[Create new](#)

Instance details

Name * vbanortheuropedb ✓

Network Interface Name * vbanortheuropedb-nic ✓

Region * North Europe

Define the Target sub-resource as “Blob”:

✓ Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription Data Protection (6ddbba37-e6f7-44a8-9e56-415103d21931)

Resource type Microsoft.Storage/storageAccounts

Resource vbanortheuropedb

Target sub-resource * ⓘ blob

Select the related network in the region:

✓ Basics ✓ Resource **3 Virtual Network** 4 DNS 5 Tags 6 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ

Subnet * ⓘ

Network policy for private endpoints Disabled ([edit](#))

Private IP configuration

☒ Dynamically allocate IP address
☐ Statically allocate IP address

Keep the DNS settings with their defaults:

✓ Basics ✓ Resource ✓ Virtual Network **4 DNS** 5 Tags 6 Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No


Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-win...	<input type="text" value="Data Protection"/>	<input type="text" value="vba"/>	(new) privatelink.blob.cor...

If required, add tags and continue with Create.

Repeat this procedure for additional Storage Accounts that should be used as a repository.

Veeam Backup Repositories

Now that the Storage Accounts in Azure are prepared, we can add Repositories in Veeam Backup for Azure targeting them. Provide a name for the new Repository and select Next.

 Veeam Backup for Microsoft Azure

← Add Repository

Name

Settings

Options

Summary

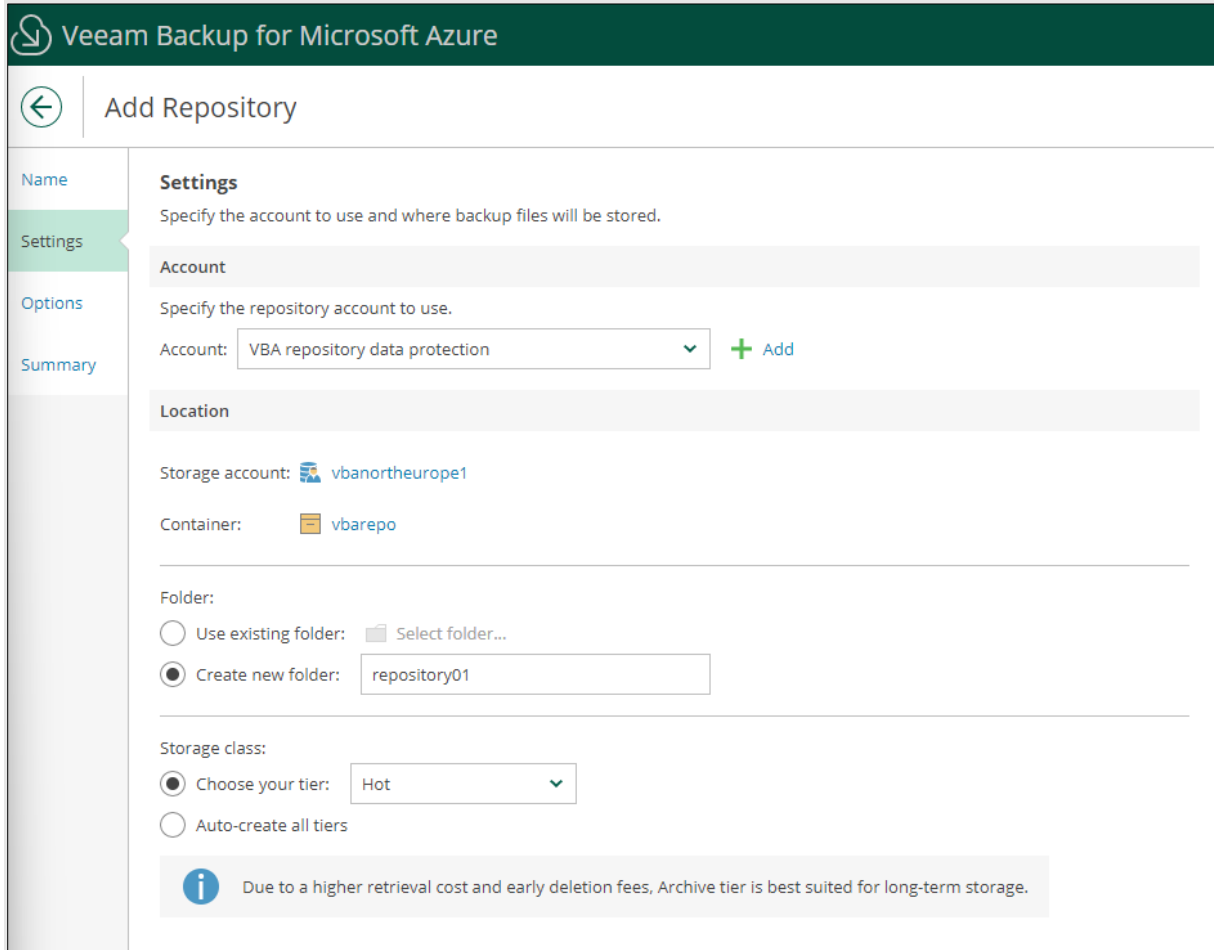
Name

Type in a name and description for the repository.

Name:

Description:


Select the dedicated account for repositories in the data protection subscription and the container to be used. If you have prepared a folder in the container, select it or create a new one instead. At last, define your required storage tier before continuing with Next.




The screenshot shows the 'Add Repository' configuration page in Veeam Backup for Microsoft Azure. The left sidebar contains a navigation menu with 'Name', 'Settings' (selected), 'Options', and 'Summary'. The main content area is titled 'Settings' and includes a sub-header 'Specify the account to use and where backup files will be stored.' The 'Account' section has a dropdown menu set to 'VBA repository data protection' and a '+ Add' button. The 'Location' section shows 'Storage account: vbanortheurope1' and 'Container: vbarepo'. The 'Folder' section has two options: 'Use existing folder' (disabled) and 'Create new folder' (selected), with a text input field containing 'repository01'. The 'Storage class' section has two options: 'Choose your tier' (selected) with a dropdown set to 'Hot', and 'Auto-create all tiers' (disabled). An information banner at the bottom states: 'Due to a higher retrieval cost and early deletion fees, Archive tier is best suited for long-term storage.'

Choose if you want to enable encryption of the backup data. You can use a dedicated password to encrypt or use an Azure Key Vault encryption key. Be aware that there is no way for Veeam to support with the decryption of backups if this key is ever lost. It is important to make sure that a copy is stored in a very safe place.

In this example we skip encryption and add the Repository after the summary page. Please see the steps below for using Azure Key Vaults if required.

 Veeam Backup for Microsoft Azure

Server time:
Feb 13, 2023 4:43 PM

 Add Repository

Name


Settings

Options

Summary

Summary

The repository settings have been saved successfully. Click finish to exit the wizard.

 [Copy to Clipboard](#)

General


Name: vbanortheurope
Description: Created by vba01\veeamadmin at 2/13/2023 4:35 PM

Repository

Account: VBA repository data protection
Storage account: vbanortheurope1
Container: vbarepo
Folder: repository1
Region: North Europe
Storage class: Hot

Options

Encryption: Disabled

 After you complete the wizard the repository will be created. To view the progress go to Sessions Log.


☒ Go to sessions log when I click Finish

Previous

Finish

Cancel

After the wizard is finished, we can find the added Repositories on the configuration page:

 Veeam Backup for Microsoft Azure

Server time:
Feb 13, 2023 4:45 PM

veeamadmin
Portal Administrator

Exit Configuration

Getting Started

Administration

Accounts

Repositories

Workers

Repository

+ Add

Edit

Remove

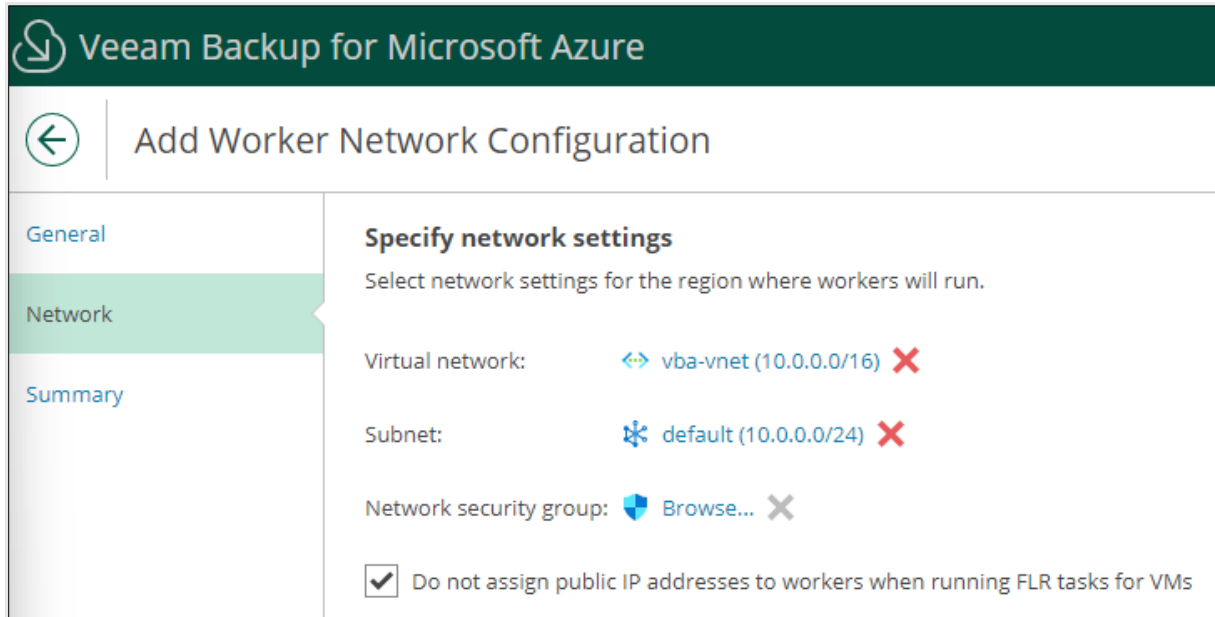
<input type="checkbox"/> Repository ↑	Description	Status	Storage Account	Container	Folder	Region	Encryption
Selected: 0 of 2							
<input type="checkbox"/> vbanortheurope	Created by vba01...	Ready	vbanortheurope1	vbarepo	repository1	North Europe	Disabled
<input type="checkbox"/> vbawesturope	Created by vba01...	Ready	vbawesturope	vbarepowest	repository1	West Europe	Enabled

Veeam Workers

Network Configuration

To be able to backup workloads in multiple regions, we need to add the Worker configuration. Since we enabled private network deployment, all workers will use private endpoints automatically.

During the wizard of adding a Worker configuration, make sure to enable the option **not** to assign public IP addresses to workers when running FLR tasks for VMs:



Veeam Backup for Microsoft Azure

← Add Worker Network Configuration


General


Network


Summary

Specify network settings

Select network settings for the region where workers will run.

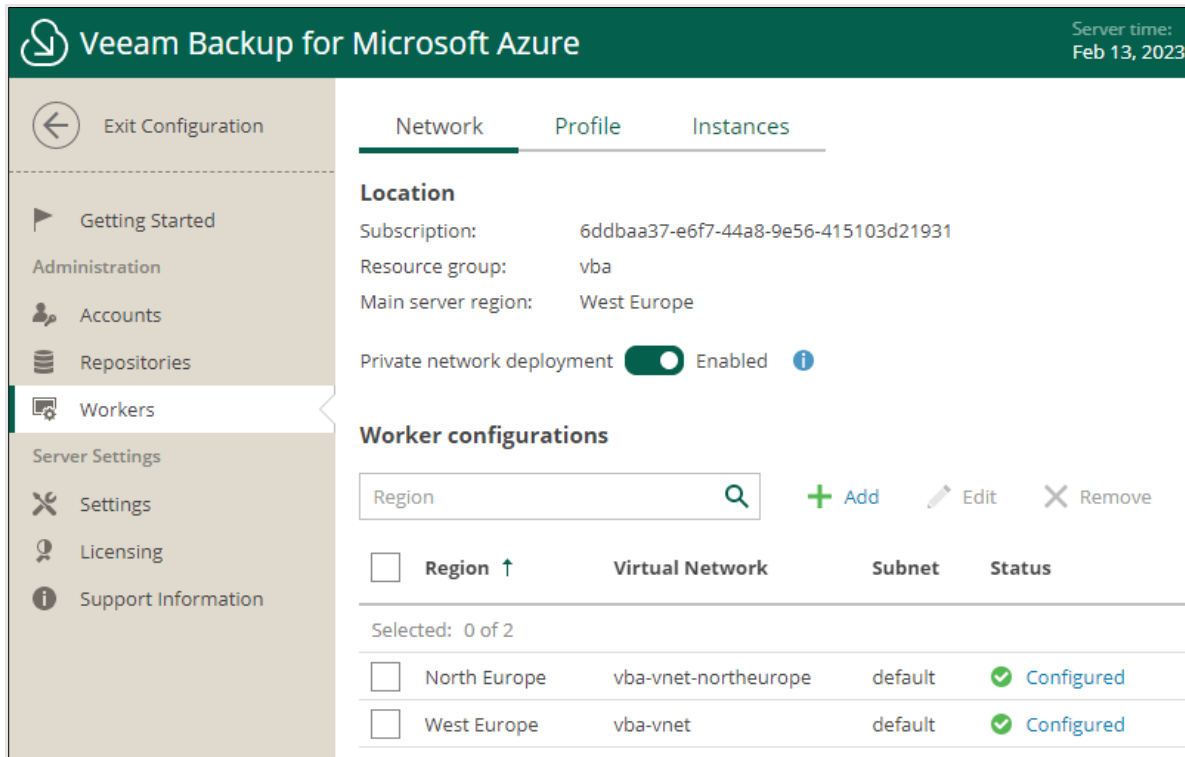
Virtual network:  vba-vnet (10.0.0.0/16) ✗

Subnet:  default (10.0.0.0/24) ✗

Network security group:  Browse... ✗

☒ Do not assign public IP addresses to workers when running FLR tasks for VMs

There needs to be a Worker configuration for every Azure region we want to protect:



Veeam Backup for Microsoft Azure Server time: Feb 13, 2023

← Exit Configuration

Getting Started

Administration

Accounts

Repositories

Workers

Server Settings

Settings

Licensing

Support Information


Network Profile Instances

Location





Subscription: 6ddbaa37-e6f7-44a8-9e56-415103d21931

Resource group: vba

Main server region: West Europe

Private network deployment  Enabled ⓘ

Worker configurations

Region   Add  Edit  Remove

<input type="checkbox"/>	Region ↑	Virtual Network	Subnet	Status
Selected: 0 of 2				
<input type="checkbox"/>	North Europe	vba-vnet-northeurope	default	✓ Configured
<input type="checkbox"/>	West Europe	vba-vnet	default	✓ Configured

Dedicated profiles for Worker instances can be set up in the Worker configuration. Since there is nothing special to private environments regarding the Worker profiles, please see the Helpcenter documentation for additional details on this topic:

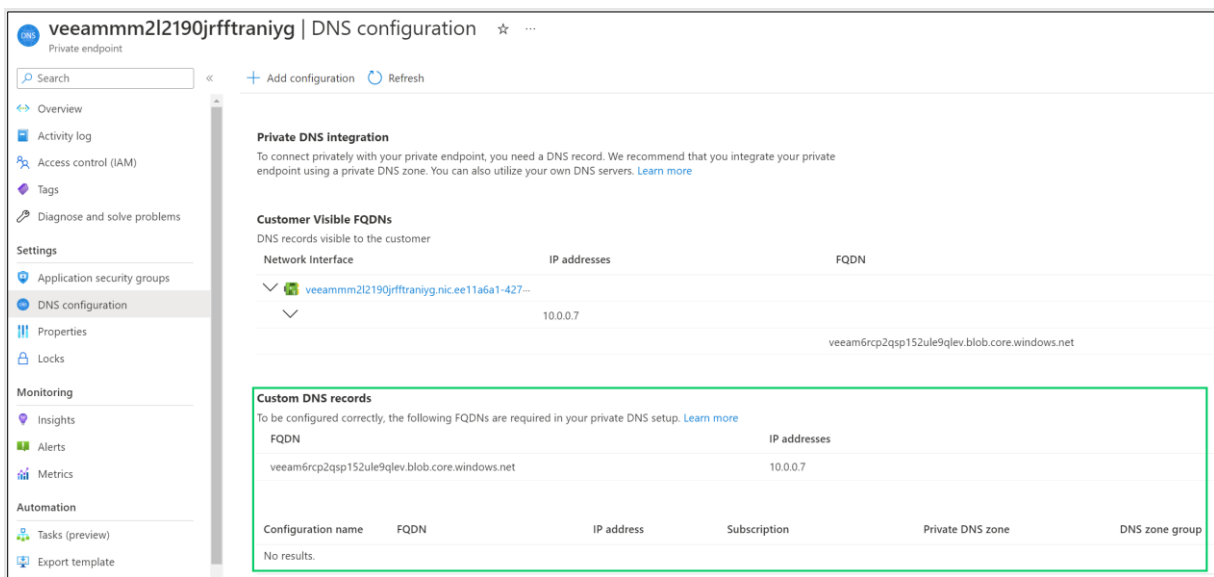
https://helpcenter.veeam.com/docs/vbazure/guide/managing_worker_profiles.html

Azure Private DNS Integration

The workers use a Storage Account per region to load their configuration. This Storage Account is automatically created with the first worker that gets deployed. In private deployments, this can lead to the issue that the Private Endpoint needs to be added to a Private DNS Zone. Veeam is evaluating options to improve and automate this in future product releases.

This will result in workers being unable to be provisioned because they cannot read a config.

To add the DNS record, open the DNS configuration of the Private Endpoint. Here we see that no Custom DNS record is present:



Private DNS integration
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint using a private DNS zone. You can also utilize your own DNS servers. [Learn more](#)

Customer Visible FQDNs
DNS records visible to the customer

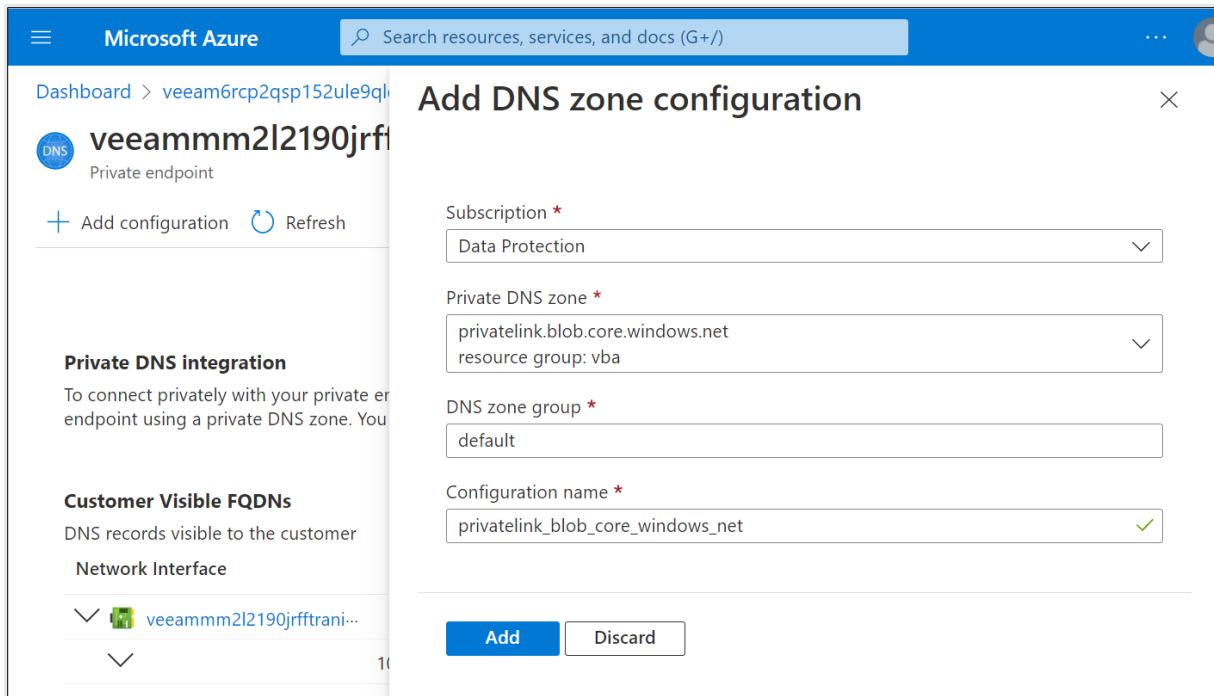
Network Interface	IP addresses	FQDN
✓ veeammm2l2190jrfftraniyg.nic.ee11a6a1-427...	10.0.0.7	veeam6rcp2qsp152ule9qlev.blob.core.windows.net

Custom DNS records
To be configured correctly, the following FQDNs are required in your private DNS setup. [Learn more](#)

FQDN	IP addresses
veeam6rcp2qsp152ule9qlev.blob.core.windows.net	10.0.0.7

Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
No results.					

Click on Add configuration at the top and add a custom DNS zone configuration:



Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > veeam6rcp2qsp152ule9ql...


veeammm2l2190jrftrani...
Private endpoint

+ Add configuration Refresh

Private DNS integration
To connect privately with your private endpoint using a private DNS zone. You can use a private DNS zone to connect to a private endpoint.

Customer Visible FQDNs
DNS records visible to the customer

Network Interface

▼  veeammm2l2190jrftrani... 10.0.0.7

Subscription *

Data Protection

Private DNS zone *

privatelink.blob.core.windows.net
resource group: vba

DNS zone group *

default


Configuration name *


privatelink_blob_core_windows_net ✓

Add Discard

After the configuration has been added, it is visible in the DNS configuration, and the workers can successfully be provisioned in this region:

Customer Visible FQDNs
DNS records visible to the customer


Network Interface	IP addresses	FQDN
▼  veeammm2l2190jrftraniyg.nic.ee11a6a1-4274...		
▼	10.0.0.7	veeam6rcp2qsp152ule9qllev.blob.core.windows.net

Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
▼ privatelink_blob_co...			Data Protection	 privatelink.blob.core.windows.net	default
▼	veeam6rcp2qsp152ule9qllev.privatel...	10.0.0.7		-	-

Azure Key Vault

If you decide to use Azure Key Vault Keys to encrypt backups stored by Veeam Backup for Microsoft Azure within a private deployment, it is necessary to add a private endpoint to the Azure Key Vault. Be aware that we need an Azure Key Vault in the same regions of the Azure Storage Accounts where you want to encrypt backup data.

For this setup, a dedicated Azure Key Vault and the key is created:

 Microsoft Azure

Search resources, services, and docs (G+)

Home > Key vaults >

Create a key vault

Basics

Access policy

Networking

Tags

Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Data Protection

Resource group *

vba

[Create new](#)

Instance details

Key vault name * ⓘ

vba-key-vault

Region *

West Europe

Pricing tier * ⓘ

Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete ⓘ

Enabled

Days to retain deleted vaults * ⓘ

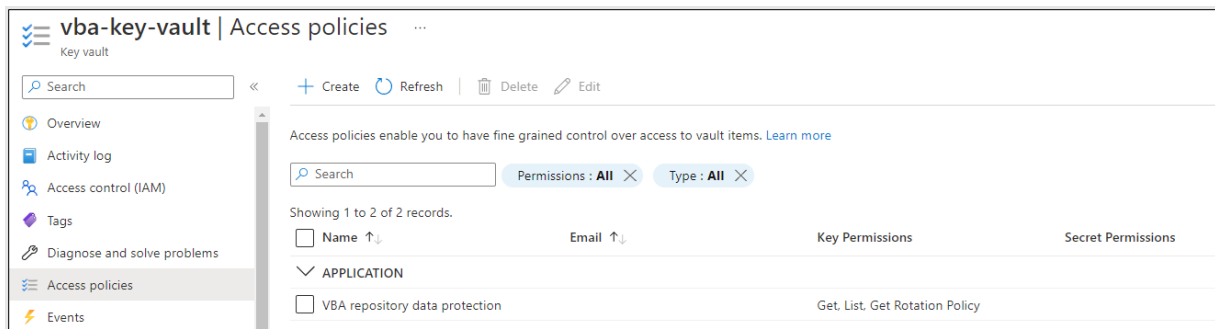
90

Purge protection ⓘ

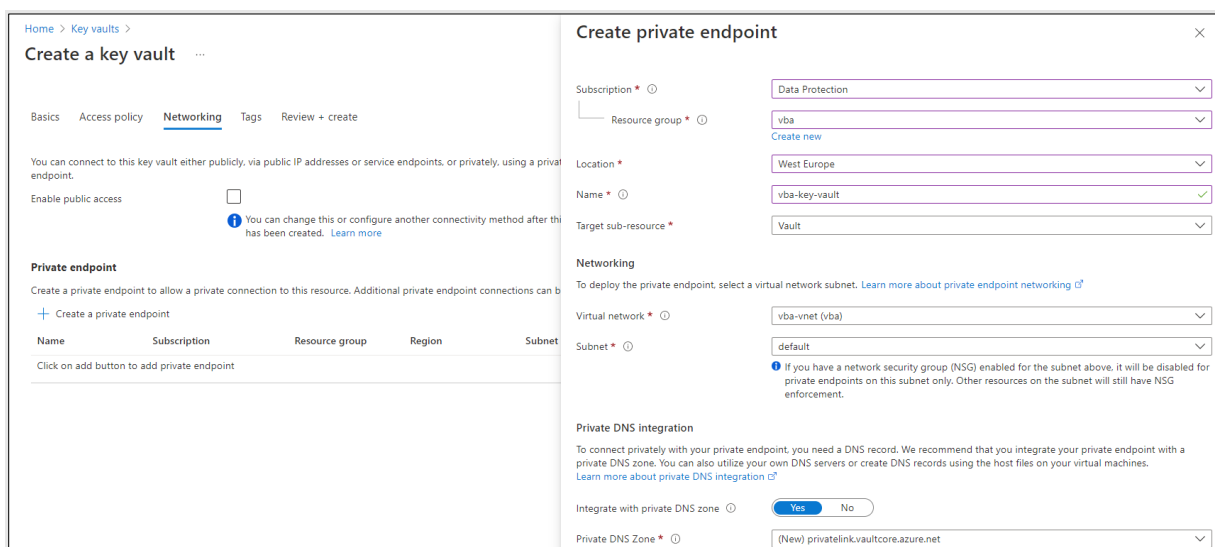
☒ Disable purge protection (allow key vault and objects to be purged during retention period)

☐ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

For the access policy, we add the Azure Application used for repository access with the key permissions Get, List, Get Rotation Policy:

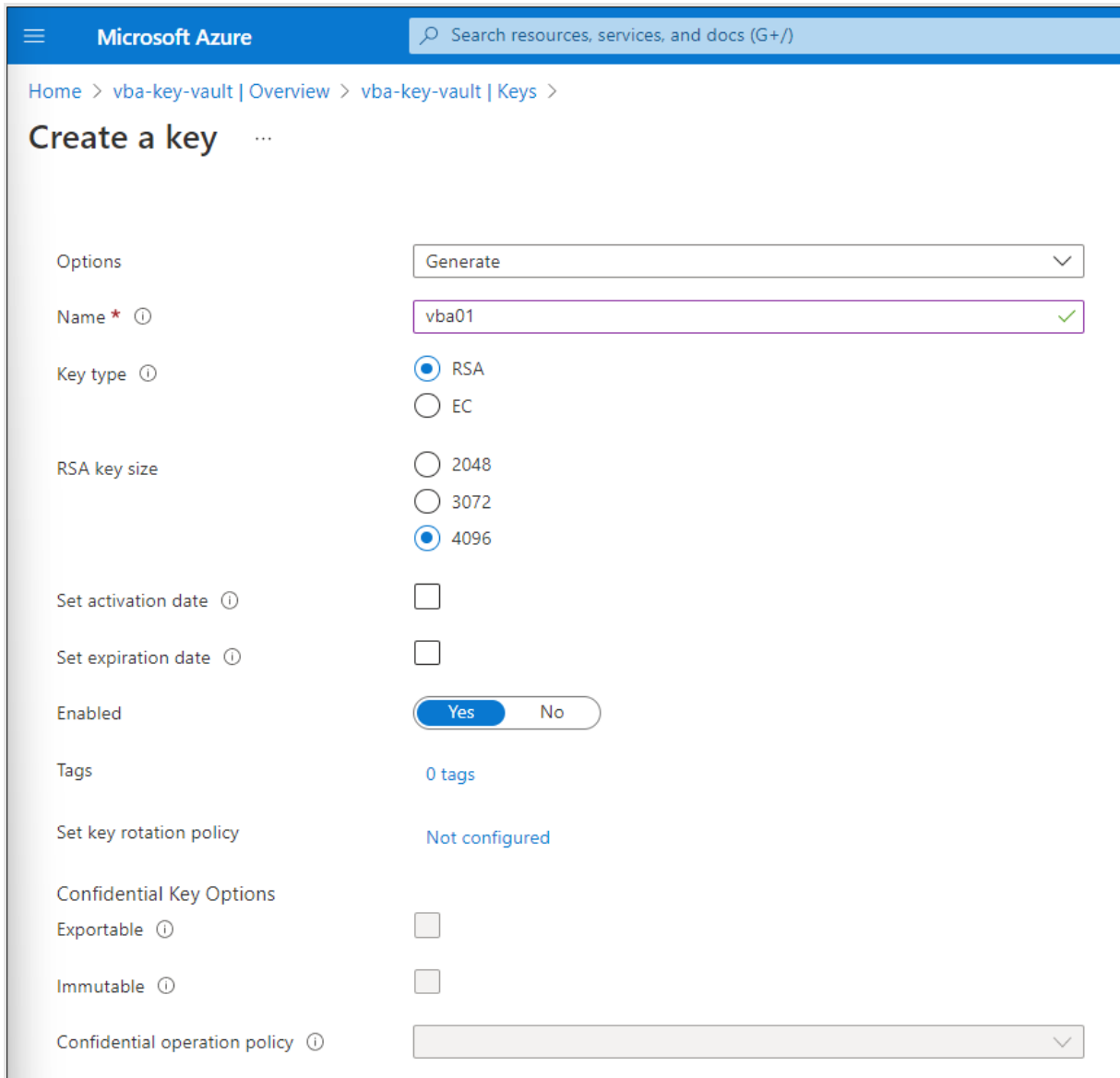


On the Networking page, we disable public access and create a private endpoint:



Review + Create the new Azure Key Vault.

Once the resource has been created, go on and create a key that should be used for the encryption of backup data:



The screenshot shows the 'Create a key' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > vba-key-vault | Overview > vba-key-vault | Keys >'. The page title is 'Create a key'. The form includes the following fields and options:

- Options:** A dropdown menu set to 'Generate'.
- Name:** A text field containing 'vba01' with a green checkmark icon on the right.
- Key type:** Radio buttons for 'RSA' (selected) and 'EC'.
- RSA key size:** Radio buttons for '2048', '3072', and '4096' (selected).
- Set activation date:** A checkbox that is unchecked.
- Set expiration date:** A checkbox that is unchecked.
- Enabled:** Toggle buttons for 'Yes' (selected) and 'No'.
- Tags:** A link that says '0 tags'.
- Set key rotation policy:** A link that says 'Not configured'.
- Confidential Key Options:**
 - Exportable:** A checkbox that is unchecked.
 - Immutable:** A checkbox that is unchecked.
- Confidential operation policy:** A dropdown menu that is currently empty.

This key can be used when adding a Veeam Backup for Microsoft Azure Repository within this region.

Conclusion

Private deployments do bring some challenges which you need to be aware of. In this document we described the settings and configuration steps that must be taken care of to run Veeam Backup for Microsoft Azure within such environments successfully.

At this stage you can create backup policies to achieve the desired state of protection for workloads in your private deployment in Azure.

If there are further questions or challenges to master, please see the Veeam Helpcenter documentation or raise a case with our support team.

Additional Topics

Azure Plug-in for Veeam Backup & Replication

If you want to use the Microsoft Azure Plug-in for Veeam Backup & Replication in a private deployment, make sure to have your firewall and routing for VPN or ExpressRoute set up so that communication between Veeam Backup & Replication and Veeam Backup for Microsoft Azure can be established. The required firewall ports can be found here:

https://helpcenter.veeam.com/docs/vbazure/vbr_integration/used_ports.html

Azure network hints

To avoid issues while connecting the Veeam Backup for Microsoft Azure appliance and workers to the Azure services, check the following settings in Azure:

- DNS configuration of the private endpoints.
- Peerings between the virtual networks involved.

This should be done for Storage Accounts used for backup repositories and Azure Key Vaults containing keys planned to encrypt backup data.

Virtual Network Service Endpoints



Make sure that the Service Endpoints contain Microsoft.KeyVault and Microsoft.Storage for all Azure virtual networks used by Veeam Workers and the Appliance:

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

2 selected

Service	Status	
Microsoft.KeyVault	Succeeded	
Microsoft.Storage	Succeeded	

Service endpoint policies

0 selected

Firewall Ports

For an up-to-date list of the firewall ports used by Veeam Backup for Microsoft Azure, please look at the related Helpcenter pages: <https://helpcenter.veeam.com/docs/vbazure/guide/ports.html>

HTTP Proxy for Updates

Suppose you have restricted internet access and use an HTTP and HTTPS proxy. In that case, you should configure the Veeam Backup for the Microsoft Azure appliance for this to receive OS and appliance updates.

Open an SSH connection to the appliance and perform these steps:

```
sudo -i
```

Modify or create the proxy.conf file:

```
vi /etc/apt/apt.conf.d/proxy.conf
```

Add the following information related to your proxy:

```
Acquire::http::Proxy "http://yourproxy.fqdn.com:8080/";
Acquire::https::Proxy "http://yourproxy.fqdn.com:8080/";
```

Save and exit the file and run a test:

```
apt-get update
```

Appendix A – JSON role template

The JSON template for roles in Production and Data Protection subscription where the Veeam Backup for Microsoft Azure appliance is located:

```
{
  "id": "/subscriptions/ABC-123-PROD/providers/Microsoft.Authorization/roleDefinitions/ABC456",
  "properties": {
    "roleName": "vba service account production",
    "description": "",
    "assignableScopes": [
      "/subscriptions/ABC-123-PROD",
      "/subscriptions/ABC-123-DP"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/roleAssignments/read",
          "Microsoft.Commerce/RateCard/read",
          "Microsoft.Compute/diskEncryptionSets/read",
          "Microsoft.Compute/disks/beginGetAccess/action",
          "Microsoft.Compute/disks/delete",
          "Microsoft.Compute/disks/endGetAccess/action",
          "Microsoft.Compute/disks/read",
          "Microsoft.Compute/disks/write",
          "Microsoft.Compute/snapshots/beginGetAccess/action",
          "Microsoft.Compute/snapshots/delete",
          "Microsoft.Compute/snapshots/endGetAccess/action",
          "Microsoft.Compute/snapshots/read",
          "Microsoft.Compute/snapshots/write",
          "Microsoft.Compute/virtualMachines/deallocate/action",

```

"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/runCommand/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.DevTestLab/Schedules/write",
"Microsoft.Insights/MetricDefinitions/Read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/keys/versions/read",
"Microsoft.KeyVault/vaults/read",
"Microsoft.Network/loadBalancers/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateLinkServices/privateEndpointConnections/read",
"Microsoft.Network/privateLinkServices/privateEndpointConnections/write",
"Microsoft.Network/privateLinkServices/privateEndpointConnections/delete",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/routeTables/join/action",
"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/delete",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/moveResources/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.ServiceBus/namespaces/delete",
"Microsoft.ServiceBus/namespaces/networkrulesets/delete",
"Microsoft.ServiceBus/namespaces/networkrulesets/read",
"Microsoft.ServiceBus/namespaces/networkrulesets/write",
"Microsoft.ServiceBus/namespaces/operationresults/read",
"Microsoft.ServiceBus/namespaces/queues/authorizationRules/ListKeys/action",
"Microsoft.ServiceBus/namespaces/queues/authorizationRules/read",
"Microsoft.ServiceBus/namespaces/queues/authorizationRules/write",
"Microsoft.ServiceBus/namespaces/queues/delete",
"Microsoft.ServiceBus/namespaces/queues/read",
"Microsoft.ServiceBus/namespaces/queues/write",
"Microsoft.ServiceBus/namespaces/read",

```

"Microsoft.ServiceBus/namespaces/write",
"Microsoft.ServiceBus/register/action",
"Microsoft.Sql/locations/*",
"Microsoft.Sql/managedInstances/databases/delete",
"Microsoft.Sql/managedInstances/databases/read",
"Microsoft.Sql/managedInstances/databases/write",
"Microsoft.Sql/managedInstances/encryptionProtector/read",
"Microsoft.Sql/managedInstances/read",
"Microsoft.Sql/servers/databases/azureAsyncOperation/read",
"Microsoft.Sql/servers/databases/delete",
"Microsoft.Sql/servers/databases/read",
"Microsoft.Sql/servers/databases/syncGroups/read",
"Microsoft.Sql/servers/databases/transparentDataEncryption/read",
"Microsoft.Sql/servers/databases/usages/read",
"Microsoft.Sql/servers/databases/write",
"Microsoft.Sql/servers/elasticPools/read",
"Microsoft.Sql/servers/encryptionProtector/read",
"Microsoft.Sql/servers/read",
"Microsoft.Storage/storageAccounts/blobServices/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/managementPolicies/write",
"Microsoft.Storage/storageAccounts/privateEndpointConnections/write",
"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write"
],
"notActions": [],
"dataActions": [
  "Microsoft.KeyVault/vaults/keys/encrypt/action",
  "Microsoft.KeyVault/vaults/keys/decrypt/action",
  "Microsoft.KeyVault/vaults/keys/read"
],
"notDataActions": []
}
]
}
}

```

The JSON template for a role in the subscription where the backup repositories are located:

```

{
  "id": "/subscriptions/DEF-123-DP/providers/Microsoft.Authorization/roleDefinitions/DEF456",
  "properties": {
    "roleName": "vba repository data protection",
    "description": "",
    "assignableScopes": [
      "/subscriptions/DEF-123-DPREPO"
    ],
    "permissions": [
      {

```

```

"actions": [
  "Microsoft.Authorization/roleAssignments/read",
  "Microsoft.KeyVault/vaults/deploy/action",
  "Microsoft.KeyVault/vaults/keys/versions/read",
  "Microsoft.KeyVault/vaults/read",
  "Microsoft.Network/privateEndpoints/delete",
  "Microsoft.Network/privateEndpoints/read",
  "Microsoft.Network/privateEndpoints/write",
  "Microsoft.Network/privateLinkServices/privateEndpointConnections/read",
  "Microsoft.Network/privateLinkServices/privateEndpointConnections/write",
  "Microsoft.Network/privateLinkServices/privateEndpointConnections/delete",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Storage/storageAccounts/blobServices/read",
  "Microsoft.Storage/storageAccounts/listKeys/action",
  "Microsoft.Storage/storageAccounts/privateEndpointConnections/write",
  "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",
  "Microsoft.Storage/storageAccounts/read"
],
"notActions": [],
"dataActions": [
  "Microsoft.KeyVault/vaults/keys/encrypt/action",
  "Microsoft.KeyVault/vaults/keys/decrypt/action",
  "Microsoft.KeyVault/vaults/keys/read"
],
"notDataActions": []
}
]
}
}

```

You can use and customize these JSON templates for your needs, but please check the latest Helpcenter information since required permissions might change with future development.
https://helpcenter.veeam.com/docs/vbazure/guide/account_permissions.html