

Barracuda CloudGen Firewall Managed Identities in Microsoft Azure

<https://campus.barracuda.com/doc/95259343/>

Microsoft introduced the notion of managed identities for Azure resources. This feature permits Azure Resources like the Barracuda CloudGen Firewall to be integrated much faster and easier during the provisioning process into the cloud infrastructure. The VM can issue calls towards the Azure backend to read routing tables and the location of the resources and to adapt routing on HA failover.

For more information, see the Microsoft documentation website:

- <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Managed identities for Azure resources support was added in version 7.2.2 of the Barracuda CloudGen Firewall.

Enable Managed Identities for Azure Resources

During Deployment

During deployment of the Barracuda CloudGen Firewall using ARM templates, you can add the following snippet in the 'Microsoft.Compute/virtualMachines' resource on the same level as the "type": "Microsoft.Compute/virtualMachines" property.

```
"identity": {  
  "type": "SystemAssigned"  
},
```

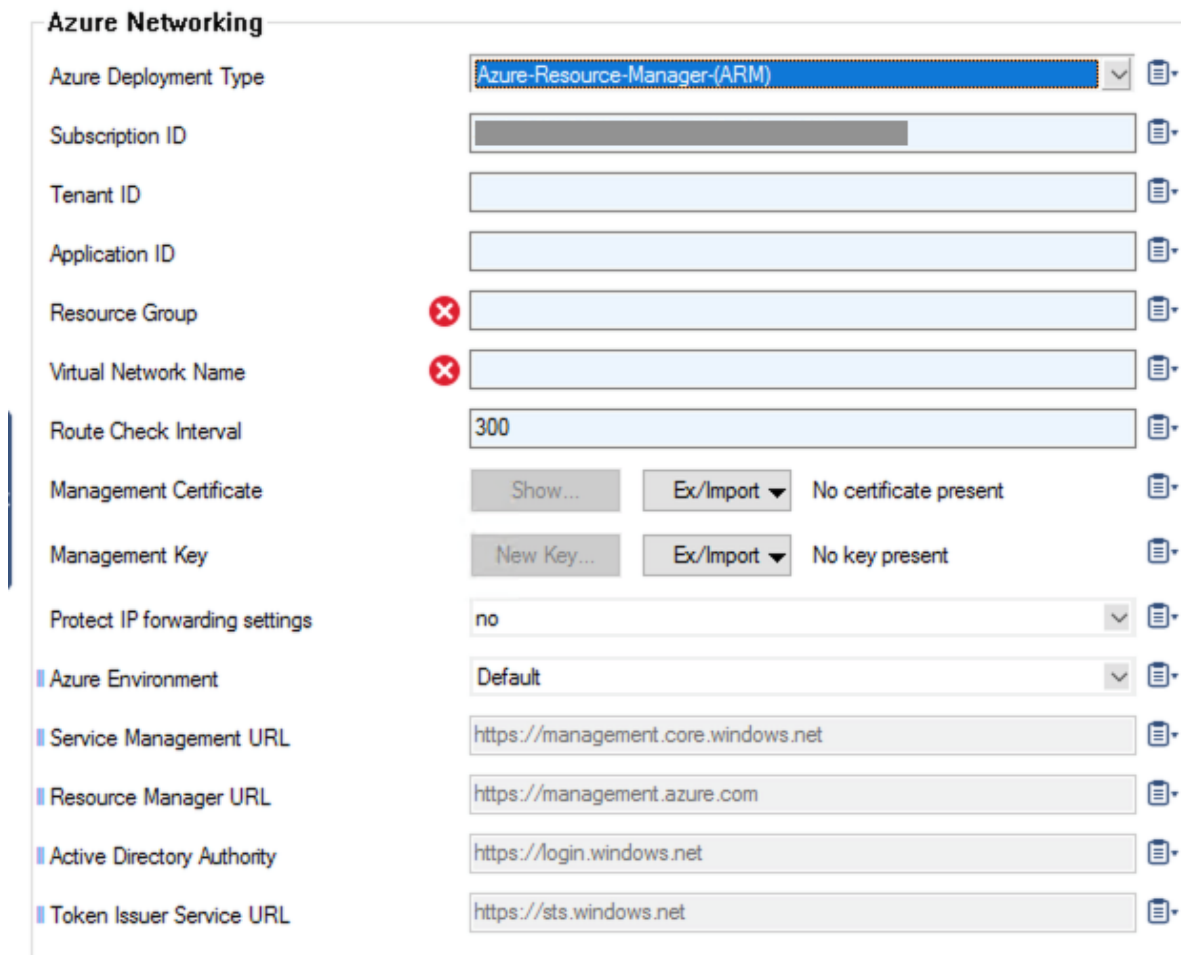
More information is available on the Microsoft documentation website:

- <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-template-windows-vm>

An example ARM template can be found here:

- <https://github.com/jvhoof/ngf-azure-templates/tree/master/NGF-Quickstart-HA-1NIC-AS-ELB-STD>

The Barracuda CloudGen Firewall will automatically detect when managed identity is enabled, and enable cloud integration and fill in known fields: Enable **Cloud Integration** and **Subscription ID** (masked in the screenshot with a gray bar).

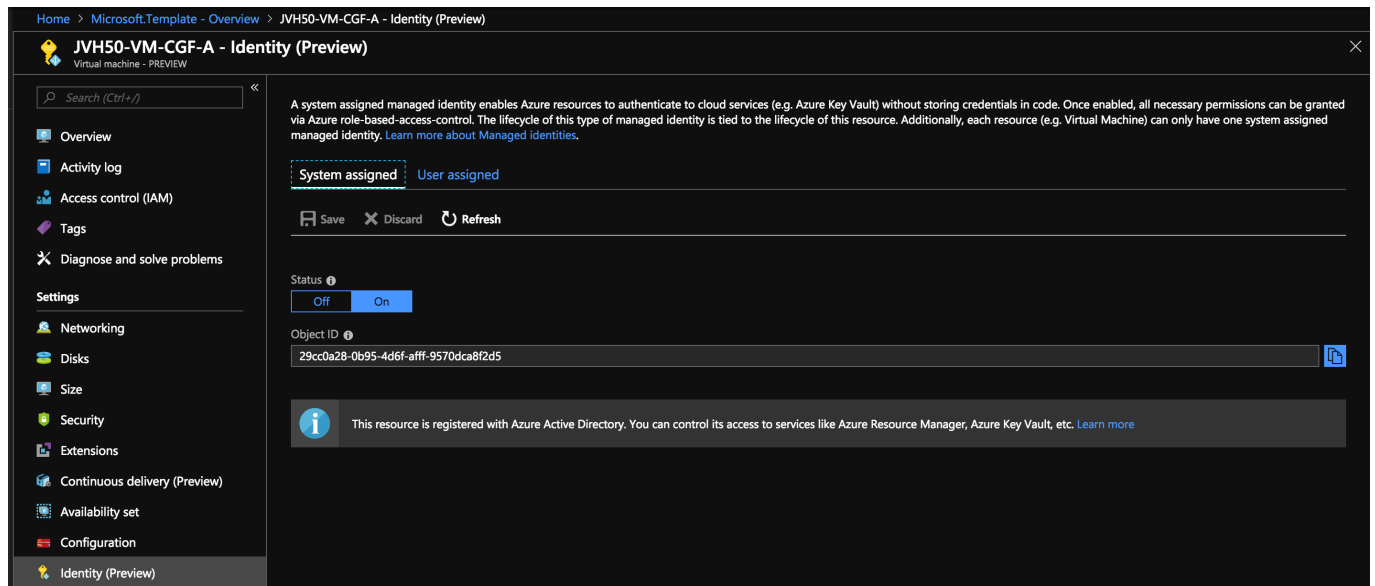


Azure Networking	
Azure Deployment Type	Azure-Resource-Manager-(ARM)
Subscription ID	[Masked]
Tenant ID	
Application ID	
Resource Group	[Red X]
Virtual Network Name	[Red X]
Route Check Interval	300
Management Certificate	Show... Ex/Import No certificate present
Management Key	New Key... Ex/Import No key present
Protect IP forwarding settings	no
Azure Environment	Default
Service Management URL	https://management.core.windows.net
Resource Manager URL	https://management.azure.com
Active Directory Authority	https://login.windows.net
Token Issuer Service URL	https://sts.windows.net

After Deployment

If you already have the Barracuda CloudGen Firewall deployed in your environment but want to enable a managed identity for Azure resources, you can do so via the Microsoft Portal, Azure CLI, Powershell, or other means.

In the Azure Portal, find your Barracuda CloudGen Firewall VM and open the Identity settings. To enable a managed identity for Azure resources, you need to set the **System assigned** option to **on**.



Other options are documented on the Microsoft documentation website:

- <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-cli-windows-vm>

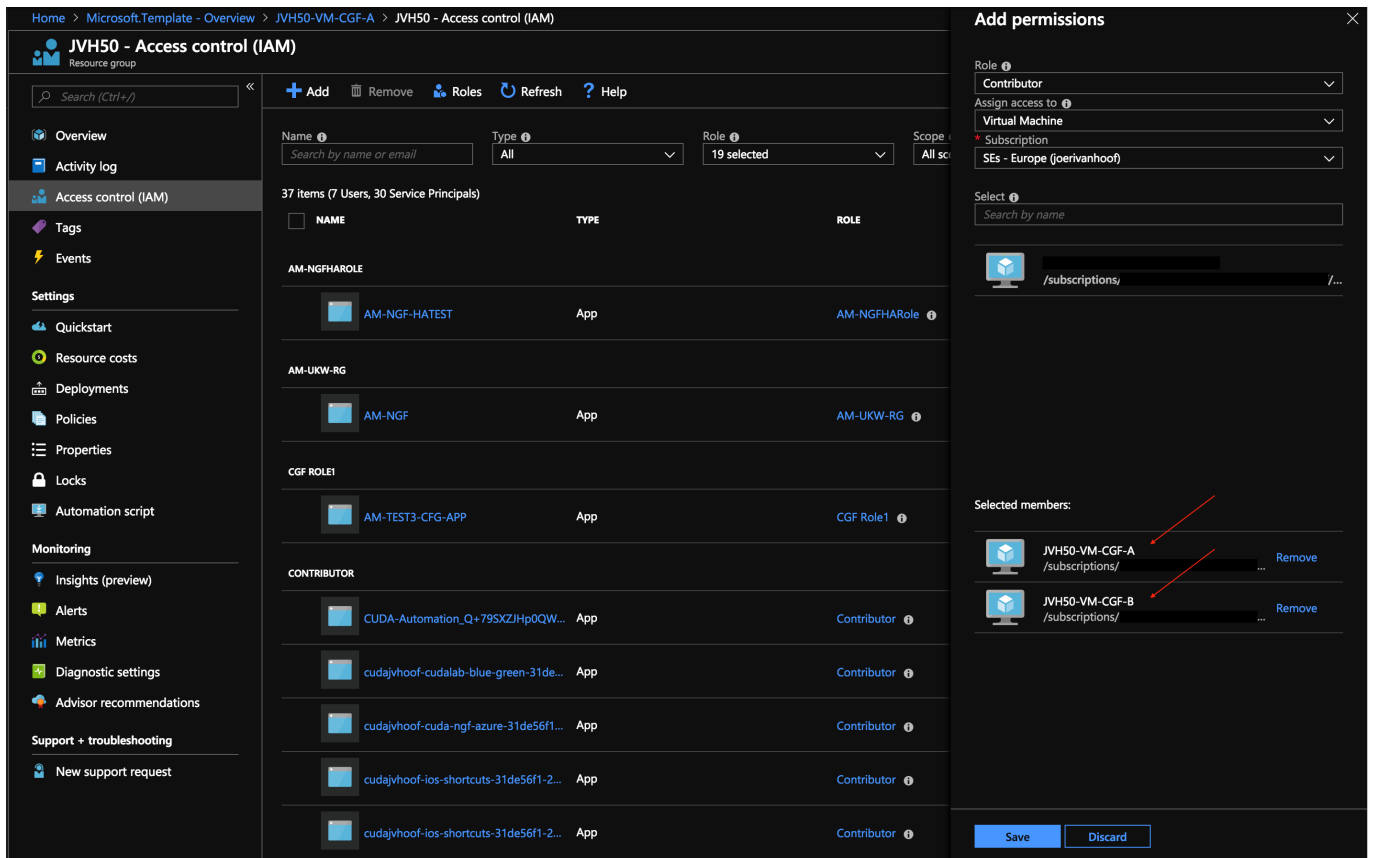
Granting Access to Resources

After enabling the managed identity, you need to grant access to the different resources that the Barracuda CloudGen Firewall needs access to.

Both Barracuda CloudGen Firewall VMs need access as a Contributor to the following Azure resources:

- Barracuda CloudGen Firewall virtual machine
- Barracuda CloudGen Firewall network interface
- Routing tables
- VNET

If all of them are in the same resource group, you can enable access to the whole Azure resource group as shown in the picture below.



Home > Microsoft.Template - Overview > JVH50-VM-CGF-A > JVH50 - Access control (IAM)

JVH50 - Access control (IAM)
Resource group

Search (Ctrl+/)

+ Add Remove Roles Refresh ? Help

37 items (7 Users, 30 Service Principals)

NAME	TYPE	ROLE
AM-NGFHAROLE		
AM-NGF-HATEST	App	AM-NGFHARole
AM-UKW-RG		
AM-NGF	App	AM-UKW-RG
CGF ROLE1		
AM-TEST3-CFG-APP	App	CGF Role1
CONTRIBUTOR		
CUDA-Automation_Q+79SXZJHp0QW...	App	Contributor
cudajvhooof-cudalab-blue-green-31de...	App	Contributor
cudajvhooof-cuda-ngf-azure-31de56f1...	App	Contributor
cudajvhooof-ios-shortcuts-31de56f1-2...	App	Contributor
cudajvhooof-ios-shortcuts-31de56f1-2...	App	Contributor

Add permissions

Role: Contributor
 Assign access to: Virtual Machine
 Subscription: SEs - Europe (joerivanhoof)

Select: Search by name

/subscriptions/ /...

Selected members:

- Jvh50-VM-CGF-A /subscriptions/ Remove
- Jvh50-VM-CGF-B /subscriptions/ Remove

Save Discard

Cloud Integration

After the permissions are in place on the Azure level, the Barracuda CloudGen Firewall VM has access and can perform the following tasks:

- Retrieve cloud information like location, instance size, instance name, public ip, ...
- Retrieve routing tables that are linked to the firewall
- Provide failover and update of the routing table in case of failover in a HA cluster
- Command-line tool to retrieve additional information in scripts: cloud-api

The Barracuda CloudGen Firewall will automatically detect if a managed identity is enabled, and enable cloud integration and fill in known fields: Enable **Cloud Integration** and **Subscription ID** (masked in the screenshot with a gray bar).

If the managed identity was not configured during deployment, the **Cloud Integration** needs to be enabled manually and the **Subscription ID** needs to be filled in manually.

Azure Networking

Azure Deployment Type	<input type="text" value="Azure-Resource-Manager-(ARM)"/>	
Subscription ID	<input type="text"/>	
Tenant ID	<input type="text"/>	
Application ID	<input type="text"/>	
Resource Group	<input type="text"/>	
Virtual Network Name	<input type="text"/>	
Route Check Interval	<input type="text" value="300"/>	
Management Certificate	<input type="button" value="Show..."/> <input type="button" value="Ex/Import"/> No certificate present	
Management Key	<input type="button" value="New Key..."/> <input type="button" value="Ex/Import"/> No key present	
Protect IP forwarding settings	<input type="text" value="no"/>	
Azure Environment	<input type="text" value="Default"/>	
Service Management URL	<input type="text" value="https://management.core.windows.net"/>	
Resource Manager URL	<input type="text" value="https://management.azure.com"/>	
Active Directory Authority	<input type="text" value="https://login.windows.net"/>	
Token Issuer Service URL	<input type="text" value="https://sts.windows.net"/>	

To have all functionalities working, you need to fill in the **Resource Group** containing the VNET and the VNET containing the Barracuda CloudGen Firewall.

Azure Networking

Azure Deployment Type	Azure-Resource-Manager-(ARM)	
Subscription ID		
Tenant ID		
Application ID		
Resource Group	✓ JVH50	
Virtual Network Name	✓ JVH50-VNET	
Route Check Interval	300	
Management Certificate	Show... Ex/Import No certificate present	
Management Key	New Key... Ex/Import No key present	
Protect IP forwarding settings	no	
Azure Environment	Default	
Service Management URL	https://management.core.windows.net	
Resource Manager URL	https://management.azure.com	
Active Directory Authority	https://login.windows.net	
Token Issuer Service URL	https://sts.windows.net	

To make sure IP forwarding is always on, which is essential on the Barracuda CloudGen Firewall to operate correctly in Microsoft Azure, you can enable a guard for it as well.

Figures

1. managed_id_01.png
2. managed_id_02.png
3. managed_id_03.png
4. managed_id_04.png
5. managed_id_05.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.