

HANDS-ON LAB: Azure Administration

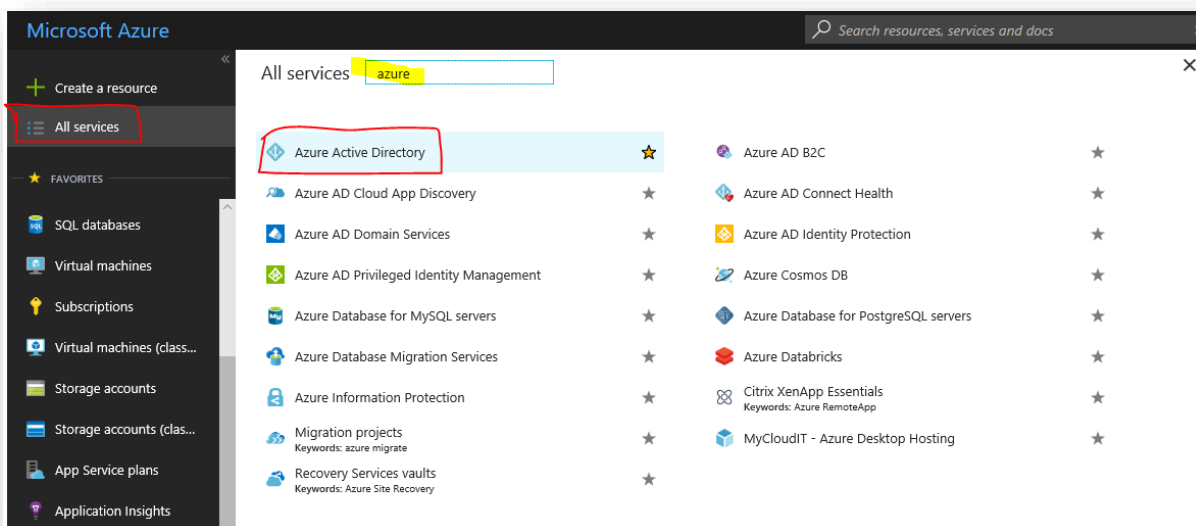
Admin User Access to Subscriptions

As the person who created your subscription in the first place, you will have OWNER / SERVICE ADMINISTRATOR rights on it however there may be a time when you want to give someone else access into your subscription... This happens all the time in corporate environments and so needs to be well managed.

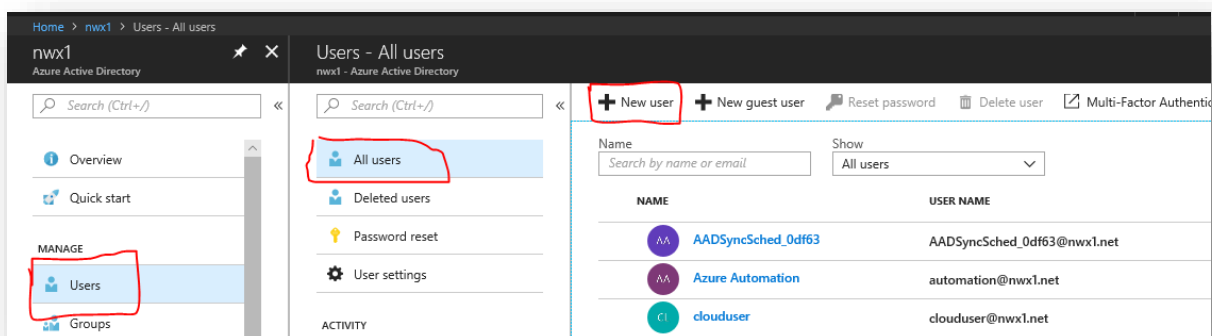
Open a web browser and head to <https://portal.azure.com>

Sign in with the Microsoft Account credentials you used when setting up your subscription.

When in the Azure portal, click ALL SERVICES, type AZURE to begin searching for "Azure Active Directory" then select it when it appears.



Select USERS, ALL USERS, New User:



Add some user details and click CREATE. Ensure the username is within your own directory, not my "nwx1.net" directory. Notice that the user's directory role is set to USER... this is what we want as we are not wanting this user to be able to administer our Directory, just Azure resources.

User
nwx1

* Name ⓘ
Jane Black ✓

* User name ⓘ
jane@nwx1.net ✓

Profile ⓘ
Not configured >

Properties ⓘ
Default >

Groups ⓘ
0 groups selected >

Directory role ⓘ
User >

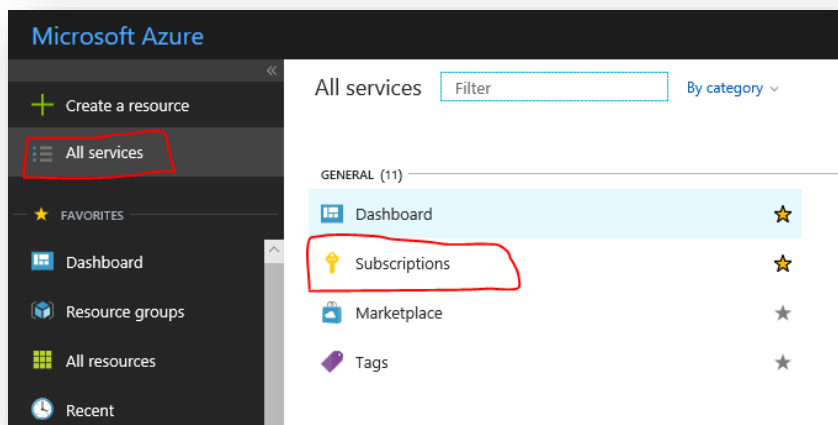
Password
••••••••

☐ Show Password

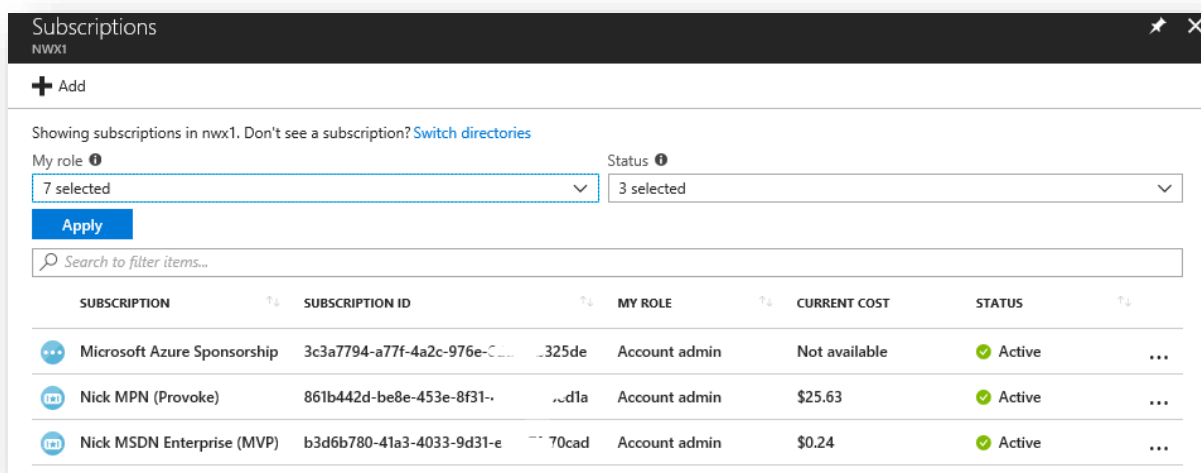
Ensure you select SHOW PASSWORD to record the password for use later.

You'll now see this user added to your directory, ready to be granted rights to Azure services.

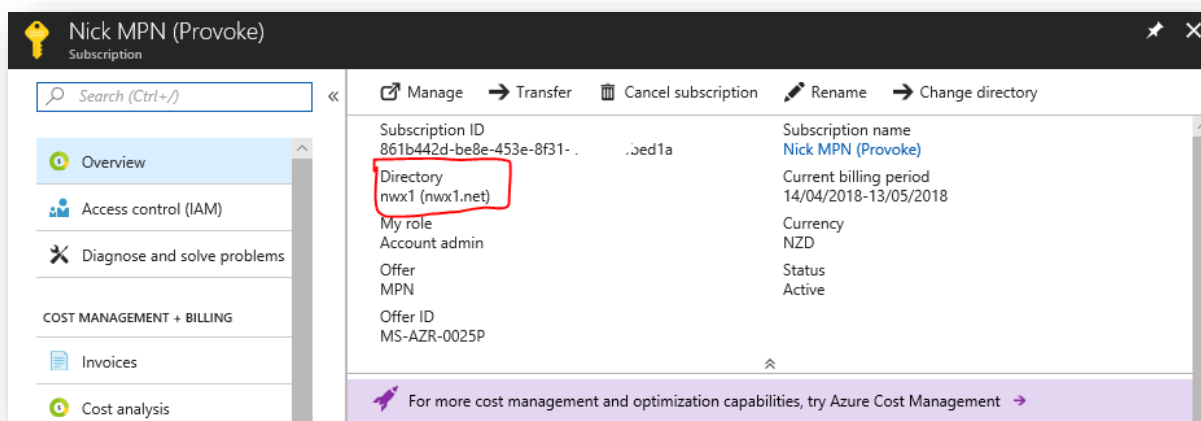
When in the Azure portal, click ALL SERVICES then Subscriptions:



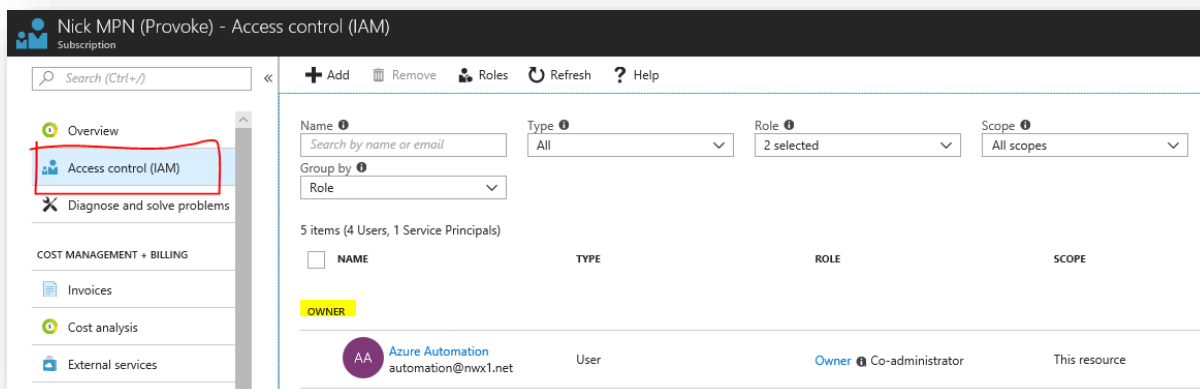
This will show you your list of subscriptions, click on one of them to select



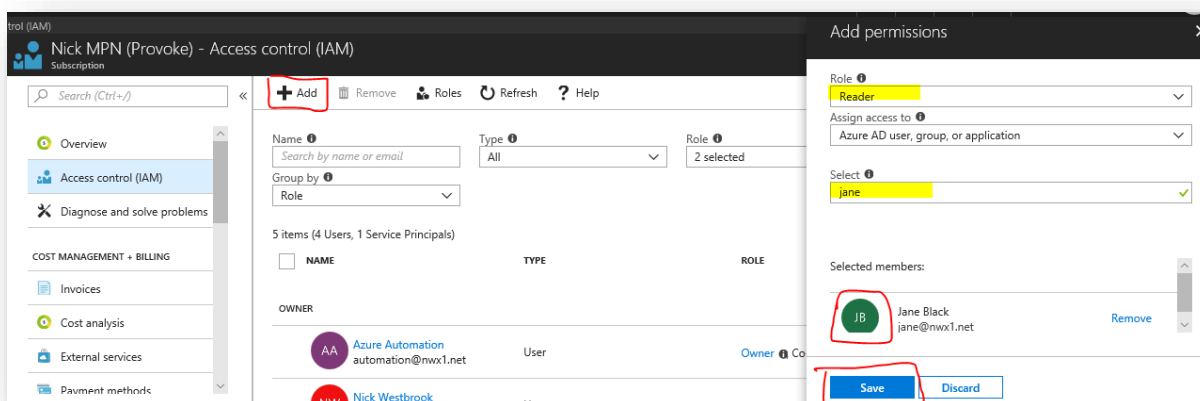
In the subscription overview, you'll notice the directory that this subscription trusts for authentication. This is the directory we added our user to earlier:



Click on ACCESS CONTROL (IAM) in the menu, this allows us to see which users currently have access to our subscription in order to perform administrative work. You'll see one or now OWNERS listed... These users have full control over your Azure subscription.



Say we want to add our user from earlier with read-only access to our subscription, we can click ADD, select her role as READER, find her in our list of users and click SAVE:

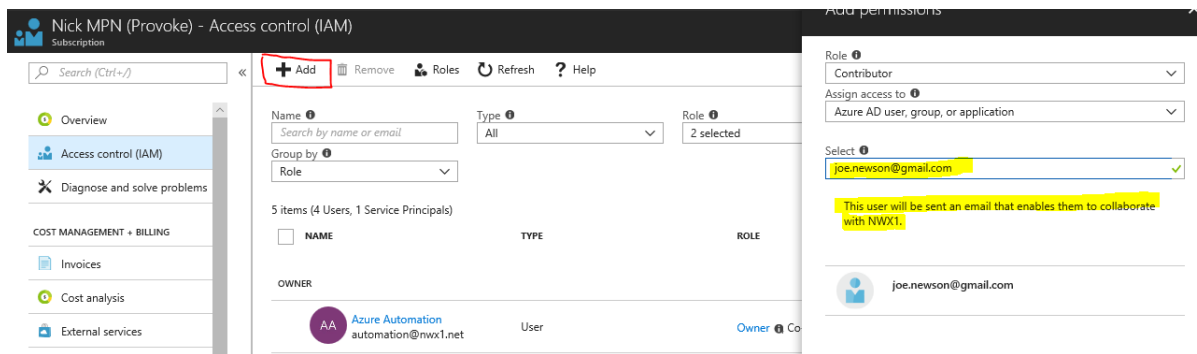


Optional:

Open a new incognito / in private window in your web browser and log into <https://portal.azure.com> with the new user's details... you should notice that you can access the subscription but only have read-only access.

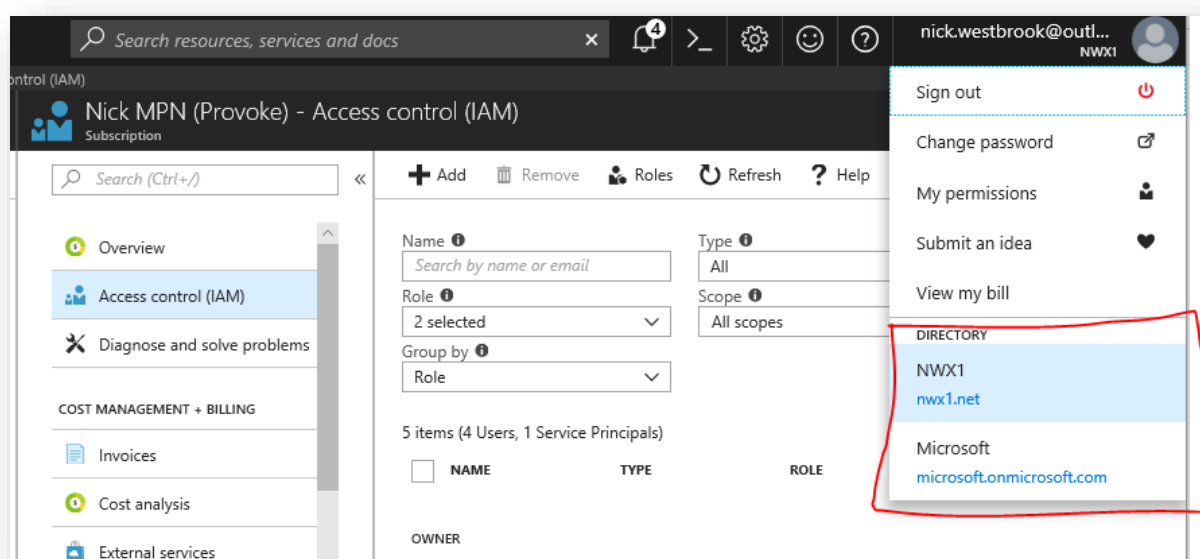
If you don't want to create new user accounts in your directory for people to collaborate with you, you can also invite them as a guest user by adding their normal email address:

On the Access Control (IAM) screen, click ADD, select a role of your choice then just add their email address. Note the notice reading an email will be sent to them to enable collaboration with your directory.



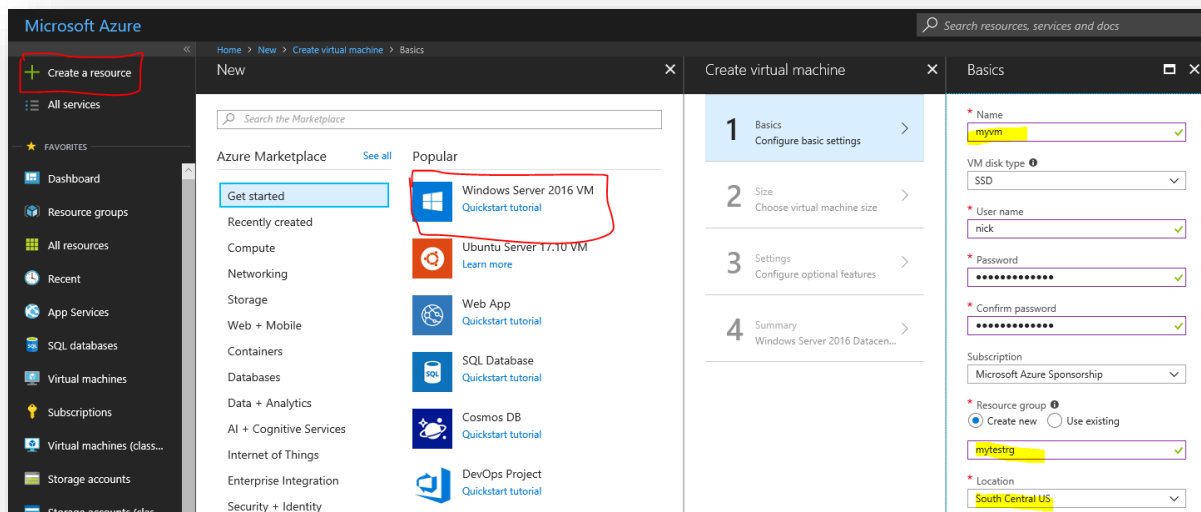
NOTE:

If this user then signs into the Azure Portal, they'll notice a new directory available in the dropdown on their account... This is YOUR directory which you've just invited them to.

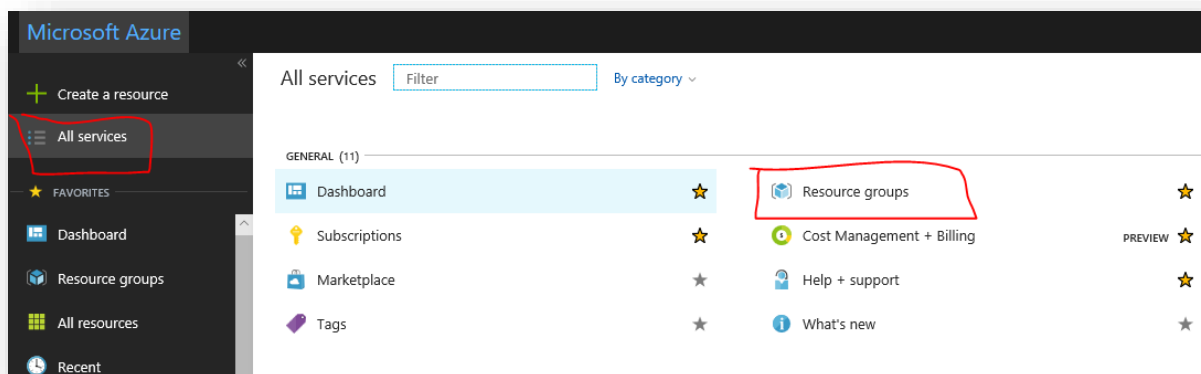


RESOURCE GROUPS

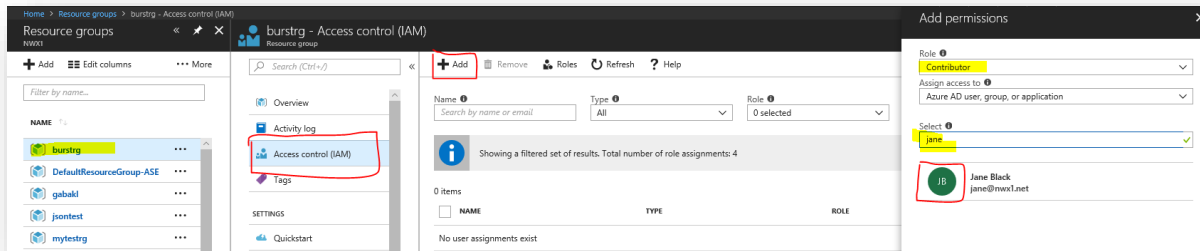
OK, let's create a new resource group and place a virtual machine inside it. Click NEW SERVICE, select WINDOWS SERVER 2016, complete all fields as necessary but for LOCATION, select someplace other than Australia. For Size, choose whatever's cheapest. All other settings can remain as default.



Once deployed, let's take a look at the resource group that got created... Click ALL SERVICES... RESOURCE GROUPS



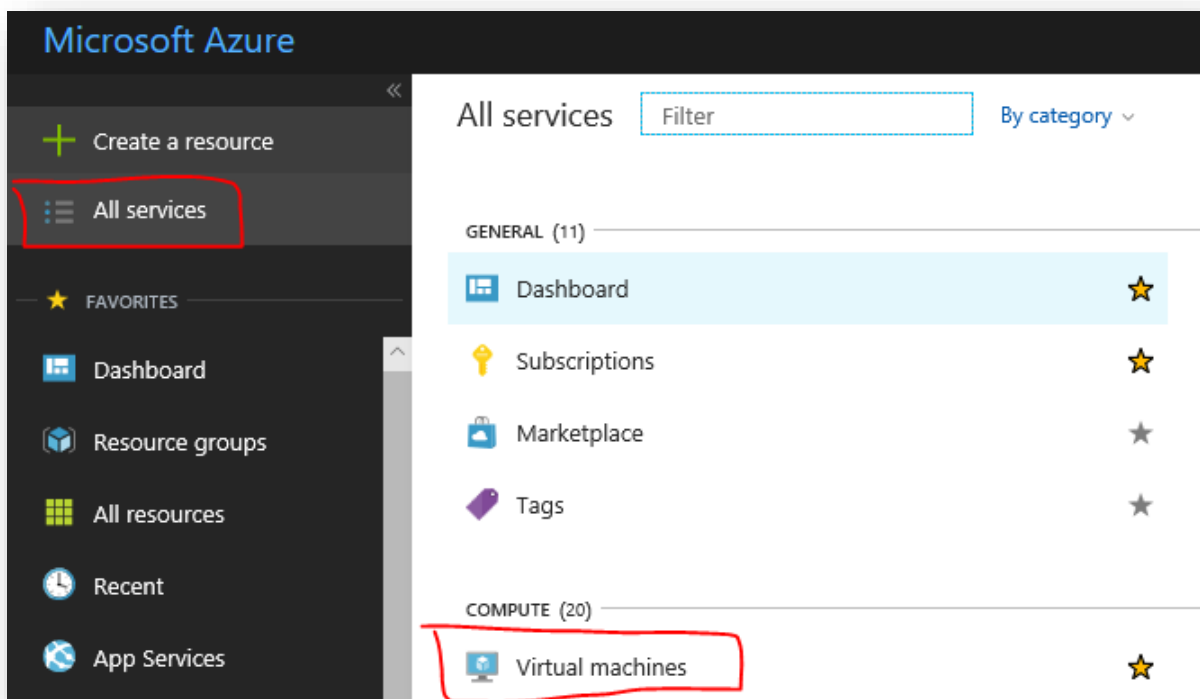
Select the resource group you created, select ACCESS CONTROL (IAM) then click ADD. We can now add our user above as a CONTRIBUTOR on this resource group even though they were only a READER on the subscription. This means they'll now be able to make changes on resources that exist within this group but not anywhere else in the subscription.



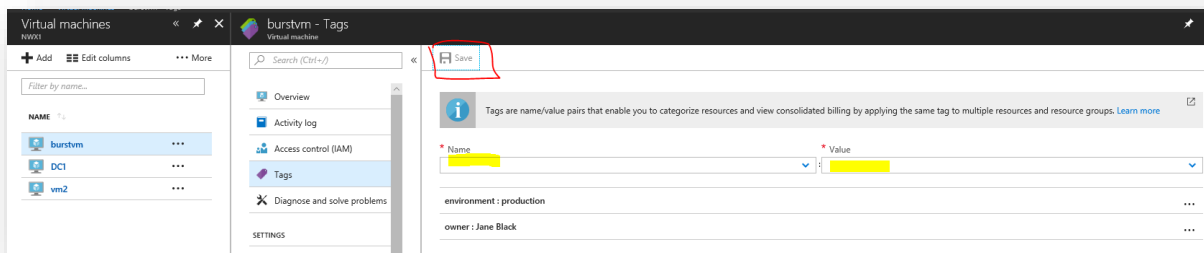
TAGGING

Once you start building more and more resources in your subscription, it can be hard to track what each of them are for or who is responsible for them. Tagging allows us to have greater visibility of our resources.

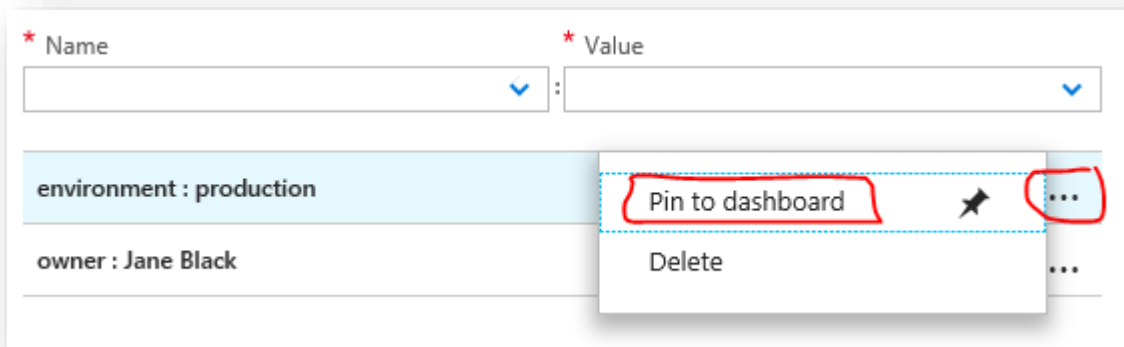
Click ALL SERVICES... VIRTUAL MACHINES to find the VM we created earlier



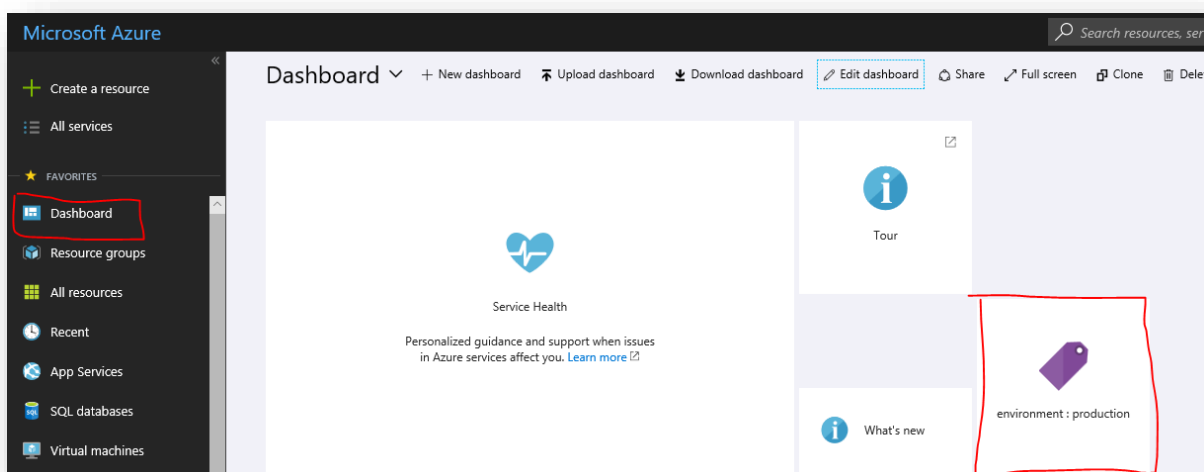
Select the VM we created above, then click on the TAGS menu item. Here we can add key:value tag pairs to the resource such as OWNER: Jane Black or ENVIRONMENT: Production. After adding each tag, click SAVE.



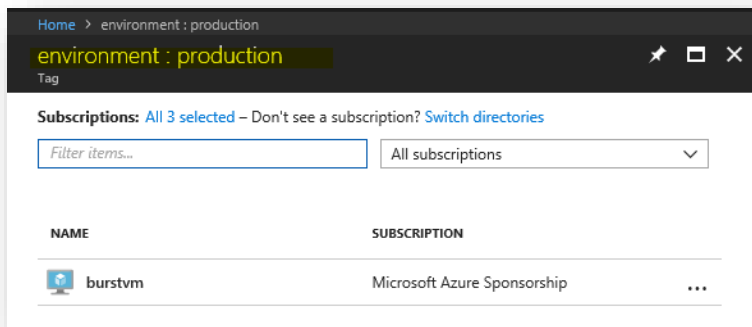
We can now add this tag to our dashboard in order to get a quick list of all production resources.



Clicking DASHBOARD will allow us to now see this quick reference list to the tag.

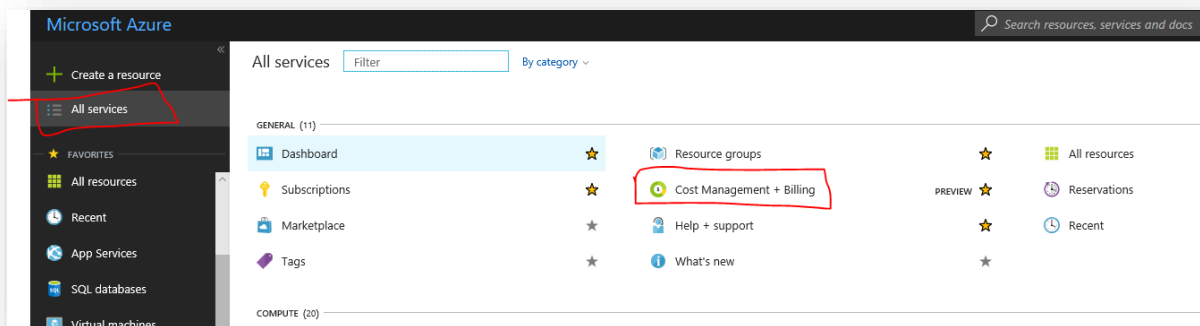


Clicking it will show us all resources tagged with this tag:

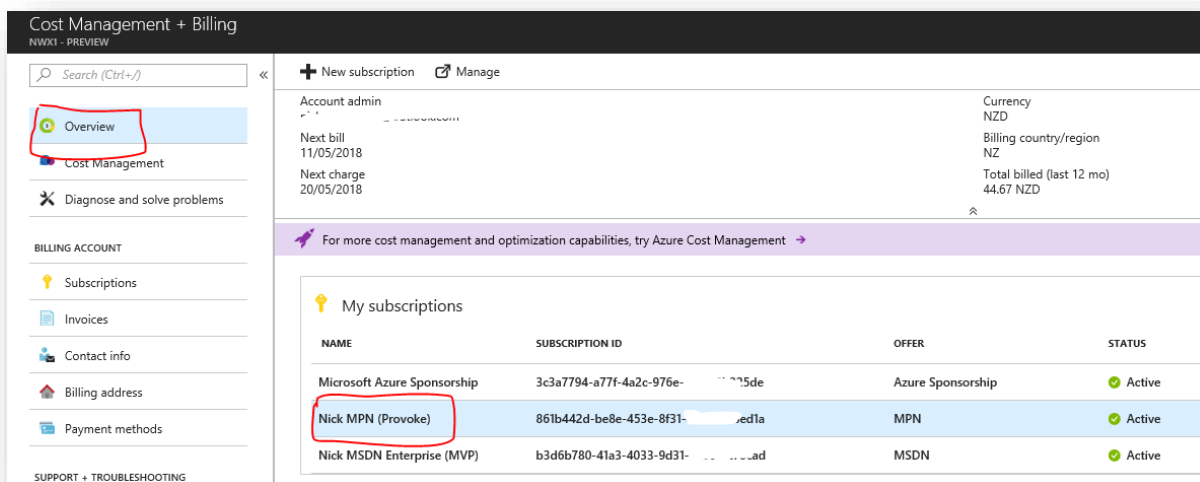


We can also see how much all Jane's resources are costing...

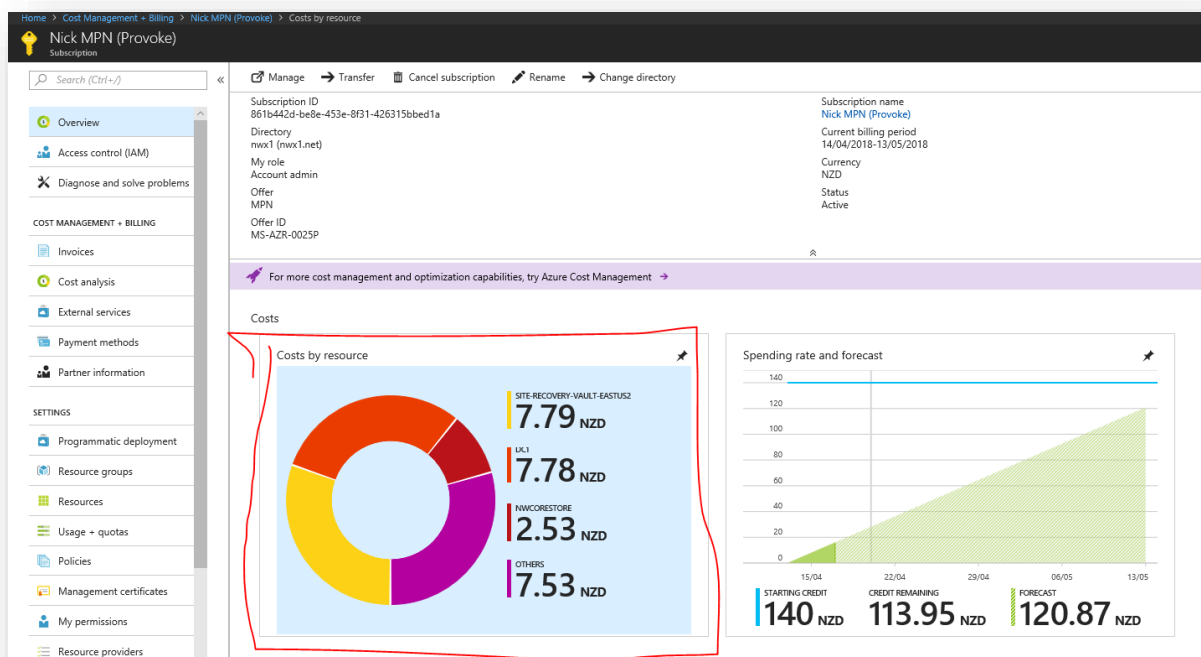
From the portal, select ALL SERVICES... Cost Management and Billing...



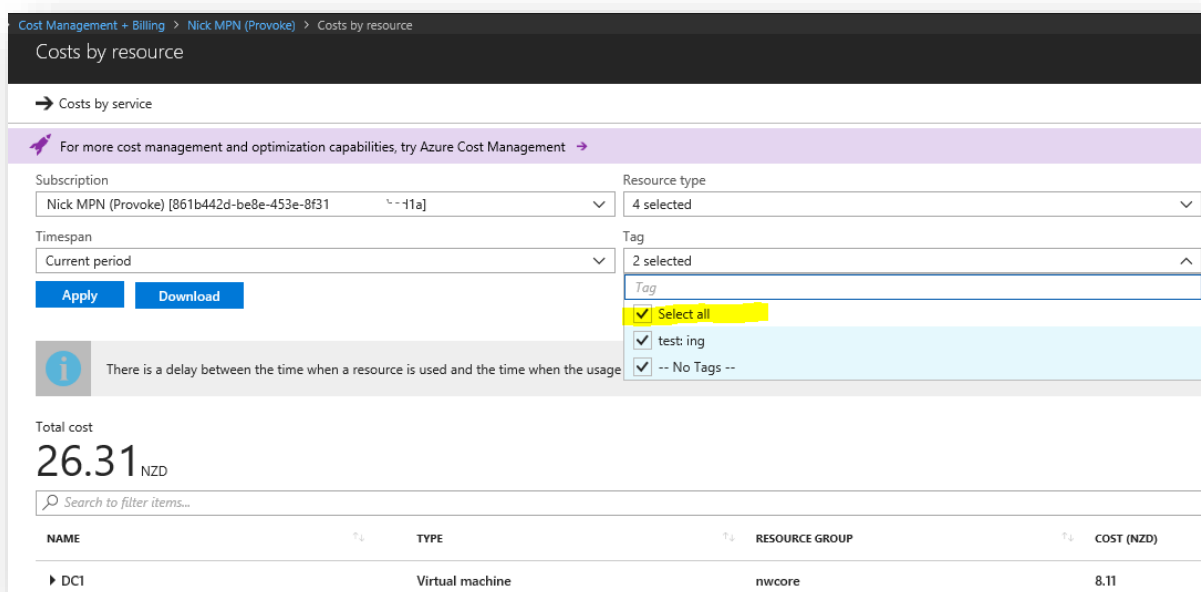
Select your subscription:



Click on Costs by Resource:



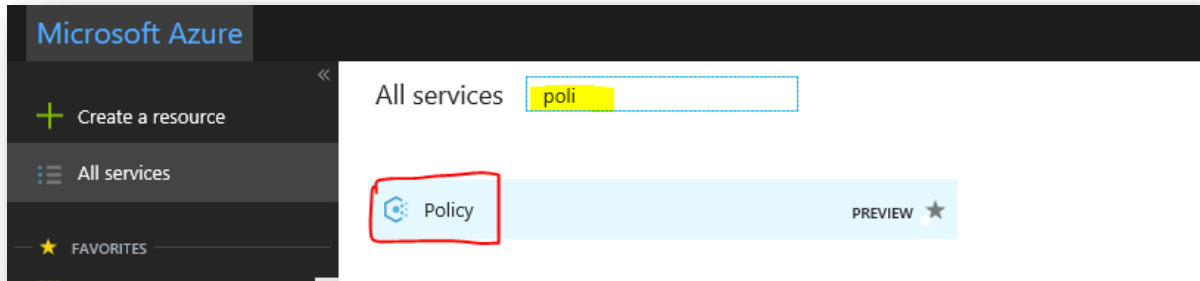
Then select which tags you're interested in filtering on:



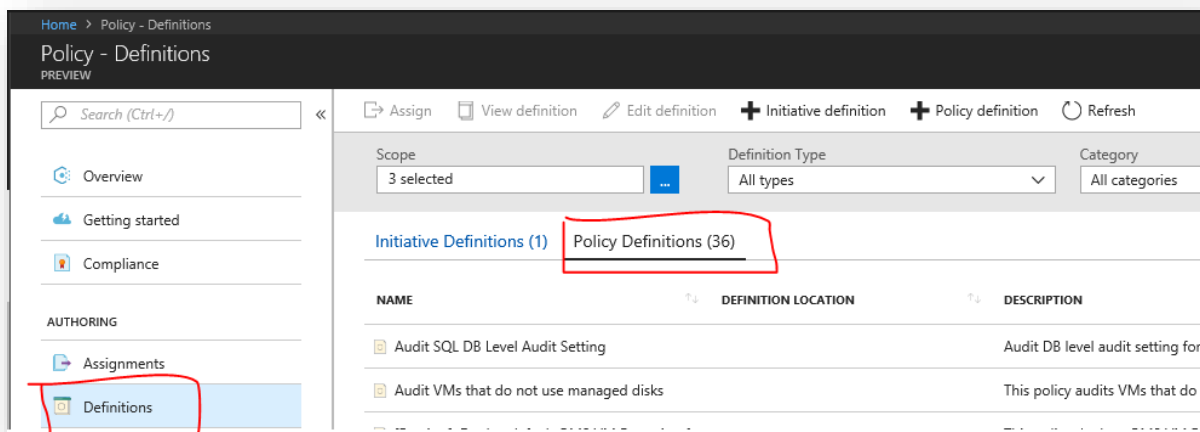
POLICY

Instead of just restricting users with all or nothing access (i.e. contributor vs reader), what if we could restrict the types of things they're allowed to do? Well we can with POLICY. Lets go ahead and ensure that all resources in our subscription are only allowed to be created in one of the Australian datacenters.

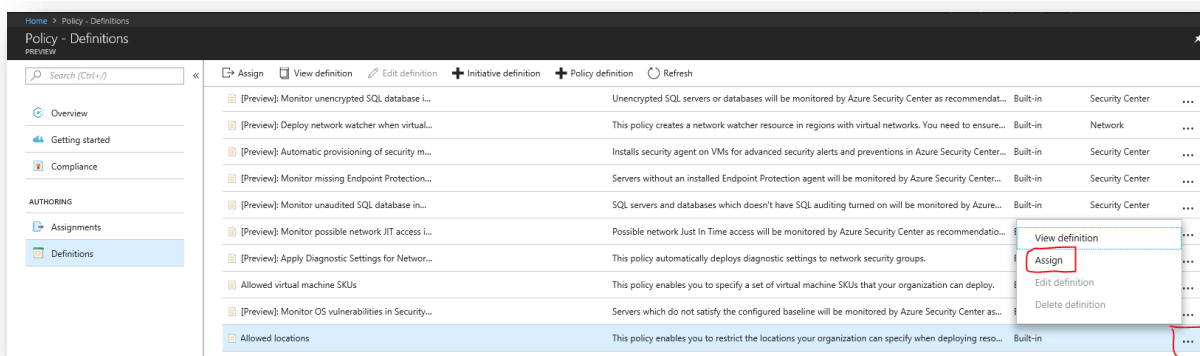
From the Azure portal, click ALL SERVICES, search for and then click POLICY



In the policy screen that appears, select DEFINITIONS then POLICY DEFINITIONS



Scroll to the bottom and select ALLOWED LOCATIONS then click the "... " menu and select ASSIGN:



In the configuration pane, customize the policy name if you wish, select the SCOPE of the policy to be your subscription and in PARAMETERS, select the 4 Australian datacenters then click ASSIGN.

Home > Policy - Definitions > Allowed locations

Allowed locations

Assign Policy - PREVIEW

BASICS

* Policy
Allowed locations

* Name ⓘ
Australia Only Allowed locations ✓

Description
Resources can only be deployed in Australian datacenters

Assigned by
Nick Westbrook

* Pricing Tier (Learn more about Pricing Tiers)
Standard
To get compliance evaluation, select Standard pricing tier.

SCOPE

* Scope (Learn more about setting the scope)
Nick MPN (Provoke) ✓

Exclusions

PARAMETERS

* Allowed locations ⓘ
4 selected

Assign Cancel

You can now head over to the COMPLIANCE tab to see if the current resources you have deployed are compliant with this policy. They SHOULDN'T be as the VM we created above was not in an Austalian datacenter. It may take some time for this to show accurately... come back to take a look later.

Policy - Compliance

Assign Policy Assign Initiative Refresh

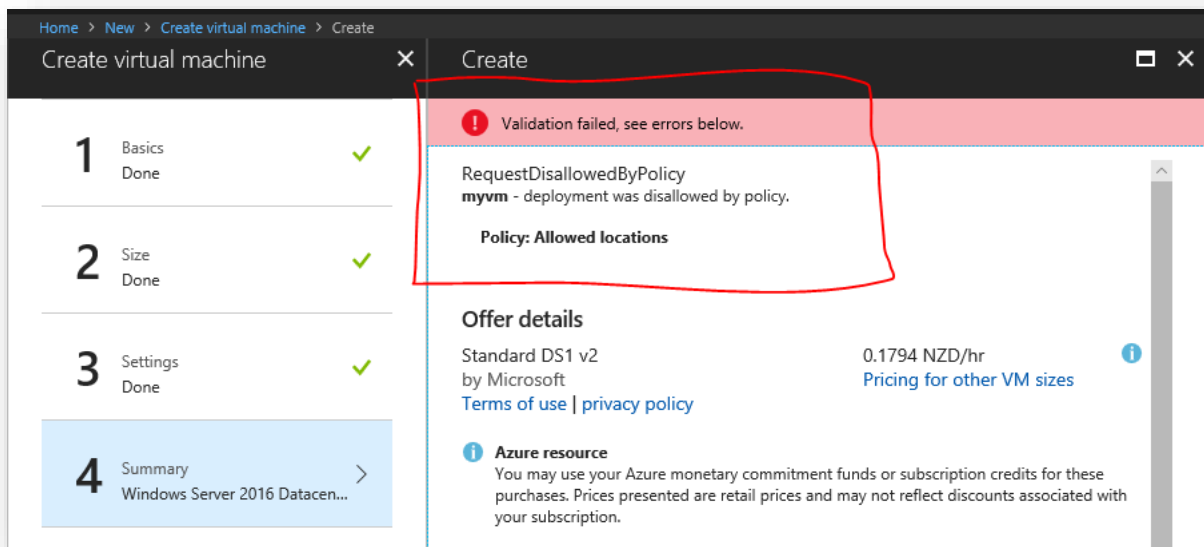
Scope: 3 selected Type: All types Compliance State: All compliance states Search: Filter by name or id...

Non-compliant initiatives: 0 out of 0 Non-compliant policies: 0 out of 1 Non-compliant resources: 25

NAME	SCOPE	COMPLIANCE	TYPE	NON-COMPLIANT POLICIES	NON-COMPLIANT RESOURCES
Allowed locations	Microsoft Azure Sponsorship	Compliant	Policy	0	0

Go ahead and try to create another virtual machine in a non-Australian datacenter (CREATE A RESOURCE... Windows Server 2016... etc)

You should now see a VALIDATION FAILED message due to the ALLOWED LOCATIONS policy disallowing the operation.



ALERTS

Want to get alerted if someone tries to create a resource against your policy? Select ALL RESOURCES... MONITOR. From the Azure Monitor service, select ACTIVITY LOG. This is where all activity against your subscription is logged. Find the failed operation (VALIDATE... DENY), click it and then click ADD ACTIVITY LOG ALERT:

Monitor - Activity log

Search (Ctrl+/)

Columns Export Log Analytics

Query returned 41 items. [Click here to download all the items as csv.](#)

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION
Write PolicyAssignments	Succeeded	6 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Write VirtualMachines	Succeeded	21 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Write VirtualMachines	Succeeded	32 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Delete PolicyAssignments	Succeeded	32 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Activated	Succeeded	33 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Activated	Succeeded	33 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Validate	Failed	49 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Deny	Failed	49 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship
Update resource group	Succeeded	49 min ago	Fri Apr 20 20...	Microsoft Azure Sponsorship

Deny

[+ Add activity log alert](#)

[+ Create new support request](#)

Summary JSON

Operation name
Deny

On the CREATE RULE dialog, click SELECT TARGET then change FILTER BY RESOURCE TYPE to "ALL", click on your subscription, then click DONE.

Create rule

Rules management

1. Define alert condition

Alert condition configuration requires 1) Target selection and 2) Alert criteria definition where signal(s) and alert logic is configured. Start by selecting a Target.

Alert target

Target Hierarchy

Microsoft Azure Sponsorship

[+ Select target](#)

Alert criteria

No criteria defined, click on 'Add criteria' to select a signal and define its logic

[+ Add criteria](#)

2. Define alert details

3. Define action group

Select a resource

For metric and log based alert rules please select a specific target, for activity log alert rules you can select a subscription, a resource type or a resource group.

Filter by subscription

Microsoft Azure Sponsorship

Filter by resource type

All

Search to filter items...

RESOURCE

Microsoft Azure Sponsorship

BURSTRG

burstvm_OsDisk_1_3cf2939b8bf048fca5a9e844ad58c

burstrg

AzureBackup.burstvm

Selection preview

Available signal(s) : Activity Log

Microsoft Azure Sponsorship

Click ADD CRITERIA, set SIGNAL TYPE to ACTIVITY LOG and MONITOR SERVICE to ACTIVITY LOG – POLICY then select ALL POLICY OPERATIONS

Create rule

Rules management

1. Define alert condition

Alert condition configuration requires 1) Target selection and 2) Alert criteria definition where signal(s) and alert logic is configured. Start by selecting a target and then defining alert criteria.

Alert target

Target Hierarchy

Microsoft Azure Sponsorship

+ Select target

Alert criteria

No criteria defined, click on 'Add criteria' to select a signal and define its logic

+ Add criteria

2. Define alert details

3. Define action group

Define your alert criteria by choosing a signal below and defining your alert condition on the next screen.

All signals (149)

Signal type ⓘ Monitor service ⓘ

Activity Log Activity Log - Policy

Search by signal name, e.g: Percentage CPU

SIGNAL NAME	SIGNAL TYPE	MONITOR SERVICE
All Policy operations	Activity Log	Policy
Create new database fro...	Activity Log	Policy
List/Get Azure SQL Serv...	Activity Log	Policy
Create/Update Azure S...	Activity Log	Policy
Delete Azure SQL Server...	Activity Log	Policy
Creates a restore point (...)	Activity Log	Policy
Upgrade a data warehou...	Activity Log	Policy
Export an existing datab...	Activity Log	Policy
Pause a Datawarehouse...	Activity Log	Policy
Resume a Datawarehou...	Activity Log	Policy

In ALERT LOGIC, change EVENT LEVEL to ERROR and STATUS to FAILED then click DONE

Alert logic

Event Level ⓘ Status ⓘ Event initiated by ⓘ

Error Failed

Condition preview

Done

Next up, we DEFINE ALERT RULES:

2. Define alert details

* Alert rule name ⓘ

Policy denied events

* Description

Triggers whenever a policy denies an operation

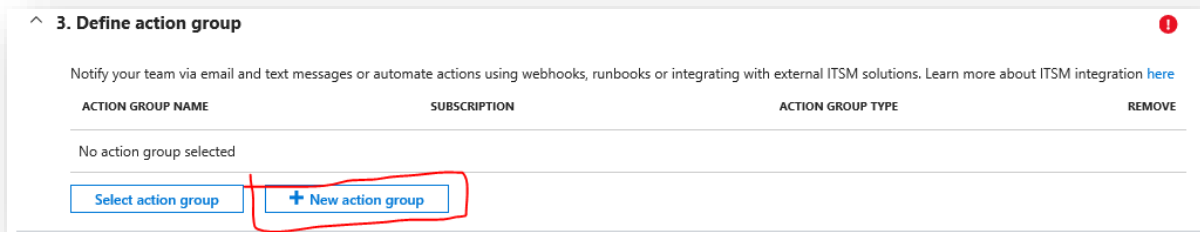
* Save alert to resource group ⓘ

Type to start filtering ...

Enable rule upon creation

Yes No

Next we define an ACTION GROUP... This is where you choose who to notify when this alert is triggered. You can also send Push Notifications to the Azure mobile App if you have it set up.



^ 3. Define action group !

Notify your team via email and text messages or automate actions using webhooks, runbooks or integrating with external ITSM solutions. Learn more about ITSM integration [here](#)

ACTION GROUP NAME	SUBSCRIPTION	ACTION GROUP TYPE	REMOVE
No action group selected			

[Select action group](#) [+ New action group](#)

AZURE MOBILE APP

If you haven't yet taken a look at the Azure mobile app, open Google Play store or the App Store on your phone, search for "Azure" and dive in!