Lab 02b - Manage Governance via Azure Policy

Objectives

In this lab, we will:

* Task 1: Create and assign tags via the Azure portal
* Task 2: Enforce tagging via an Azure policy
* Task 3: Apply tagging via an Azure policy

## Task 1: Assign tags via the Azure portal

In this task, we will create and assign a tag to an Azure resource group via the Azure portal.

First we need to start a PowerShell session in the Cloud Shell. There we will run the command ‘df’. We will get the next output:

PS /home/ana> df 
Filesystem 
Used Available 
U sex 
Mounted 
/ dev 
on 
overlay 
32584448 
tmpfs 
e 
tmpfs 
e 
/dev/sdal 
32584448 
shm 
e 
18e19384 
65536 
2ø13272 
1019384 
65536 
/ sys Ifs/ cgroup 
[home 
/ dev/shm 
//csb1øe32øe2884bb15d.file.core.windows.net/cs-nikolovska-anal-outlook-com-1032øe2884bb15d 
524288B 
tmpfs 
e 
tmpfs 
e 
tmpfs 
e 
/dev/loopø 
1B48576 
2013272 
2Ø13272 
2B13272 
4795484 
84% 
1% 
/usr/csuser/clouddrive 
/proc/acpi 
/proc/scsi 
/ sys/ firmware 
/home/ana 
1K-b10cks 
50620216 
65536 
2e13272 
50620216 
65536 
6291456 
2913272 
2e13272 
2e13272 
se74592 
PS /home/ ana> 

We can notice here the first part of the fully qualified path designating the Cloud Shell home drive mount: //csb10032002884bb15d.file.core.windows.net/cloudshell (..) /usr/csuser/clouddrive

Here is the storage account we identified in the previous step:

Storage accounts 
Default Directory 
Filter for any field... 
Showing 1 to 1 of 1 records. 
Name 
D csb10032002884bb15d 
O 
Manage view v 
Subscription equals all 
Type 
Refresh 
Export to CSV 
Open query I Assign tags Delete 
v More (2) 
Storage account 
+7 Add filter 
Kind 
StorageV2 
Resource group 
cloud-shell-storage•wm 
Location 
West Europe 

Next, we will create some Tags, with the following settings:

| Setting | Value |
| --- | --- |
| Name | **Role** |
| Value | **Infra** |

After this we go back to the storage account blade to note that the new tag was not automatically assigned to the storage account.

csb10032002884bb15d 
Storage account 
-O Search 
Overview 
Activity log 
Tags 
Diagnose and solve problems 
Access Control (IAM) 
Data migration 
f Events 
Storage browser 
Data storage 
Containers 
File shares 
Queues 
Delete 
x 
CD 
'SON View 
Upload Open in Explorer 
A Essentials 
Resource group (!ILQUe) 
cloud-shell-storage-westeurope 
Location 
West Europe 
Subscription Cnove) 
Azure Pass - Sponsorship 
Subscription ID 
cef4a15b3 
Disk State 
Available 
Tags (edit) 
Move v 
performance 
Standard 
Replication 
Locally-redundant storage (LRS) 
Account kind 
StorageV2 (general purpose v2) 
provisioning state 
Succeeded 
Created 
3/26/2023, 6:01:55 PM 

## Task 2: Enforce tagging via an Azure policy

In this task, we will assign the built-in *Require a tag and its value on resources policy* to the resource group and evaluate the outcome.

In order to do this, we go to Policy in the Azure portal. There we go to Definitions from the Authoring section and browse through the list of built-in policy definitions that are available for us to use. We click the entry that is representing the **Require a tag and its value on resources** built-in policy and review its definition. There we click Assign and specify the Scope by selecting the following values:

| Setting | Value |
| --- | --- |
| Subscription | the name of the Azure subscription you are using in this lab |
| Resource Group | the name of the resource group containing the Cloud Shell account you identified in the previous task |

We configure the Basics properties:

| Setting | Value |
| --- | --- |
| Assignment name | **Require Role tag with Infra value** |
| Description | **Require Role tag with Infra value for all resources in the Cloud Shell resource group** |
| Policy enforcement | Enabled |

The Parameters values:

| Setting | Value |
| --- | --- |
| Tag Name | **Role** |
| Tag Value | **Infra** |

Next, we review the Remediation tab, and leave Create a Managed Identity – unchecked. After this we click Create. After this we will verify that the new policy assignment is in effect by attempting to create another Azure Storage account in the resource group. For **Storage account name** we chose academydevops. When we try to deploy it, we will get the Deployment failed message.

Create a storage account 
Validation failed. Required information is missing or not valid. 
x 
Basics Advanced 
Basics 
Subscription 
Resource Group 
Storage account name 
Networking Data protection 
Encryption 
Tags O 
Deployrnent model 
Performance 
Replication 
Advanced 
Secure transfer 
Allow storage account key access 
Allow cross-tenant replication 
Azure Pass - Sponsorship 
cloud-shell-storage-westeurope 
academydevops 
Resource manager 
Standard 
Read-access geo-redundant storage (RA-C;RS) 
Enabled 
Enabled 
Enabled 

## Task 3: Apply tagging via an Azure policy

In this task, we will use a different policy definition to remediate any non-compliant resources.

In the Azure portal we select Policy, and in the Authoring section se click Assignments. There, form the list of assignments we select the **Require Role tag with Infra value** policy assignment and use the **Delete assignment** menu item to delete the assignment.

After this we Assign new policy and specify the Scope for that new policy, with the following values:

| Setting | Value |
| --- | --- |
| Subscription | the name of the Azure subscription you are using in this lab |
| Resource Group | the name of the resource group containing the Cloud Shell account you identified in the first task |

Then we specify Policy definition. For this we search and select **Inherit a tag from the resource group if missing**.

We configure the remaining Basics properties of the assignment by specifying the following settings:

| Setting | Value |
| --- | --- |
| Assignment name | **Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing** |
| Description | **Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing** |
| Policy enforcement | Enabled |

For Parameters:

| Setting | Value |
| --- | --- |
| Tag Name | **Role** |

On Remediation tab we configure the following settings:

| Setting | Value |
| --- | --- |
| Create a remediation task | enabled |
| Policy to remediate | **Inherit a tag from the resource group if missing** |

At the end we click Create.

We navigate back to the blade of the resource group hosting the storage account used for the Cloud Shell home drive, which we identified in the first task. There we create a new Storage Account. On the Basics tab of the Create storage account blade, we will verify that we are using the Resource Group that the Policy was applied to and specify the following settings:

| Setting | Value |
| --- | --- |
| Storage account name | academydevops |

Next, we verify that the validation passed and we click Create. After this we **Go to resource** of the newly created storage account and we note that the tag Role with the value Infra Is automatically assigned to the resource.

academydevops 
Storage account 
P Search 
Overview 
Activity log 
Tags 
Diagnose and solve problems 
Access Control (LAM) 
Data migration 
Events 
Storage browser 
Data storage 
Containers 
File shares 
Queues 
Tables 
Upload Open in Explorer 
Essentials 
Resource group (move 
cloud-shell-storage-westeurope 
Location 
East US 
Primary/Secondary Location 
Primary. East US, Secondary. West US 
Subscription (move) 
Azure Pass - Sponsorship 
Subscription ID 
9947c7d8-0002-4f95-9be2-e61cef4a15b3 
Disk state 
Primary: Available, Secondary: Available 
Tags (edit) 
•ple : Infre 
Delete 
Move v 
Performance 
Standard 
Replication 
O 
Refresh 
JSON View 
Read-access geo-redundant storage (RA-G RS) 
Account kind 
StorageV2 (general purpose v2) 
Provisioning state 
Succeeded 
Crea ted 
3/27/2023, AM 