

SFA Homework #11

Elizabet Ivanova

Lab 02b - Manage Governance via Azure Policy

*For conciseness, *not every single* step of the assignment is included here*

Task 1: Assign tags via the Azure portal

1. After creating a storage account using the Shell, I created the following tag:

The screenshot shows the Azure portal interface. The browser address bar displays the URL: `https://portal.azure.com/#@lilaliza9898outlook.onmicrosoft.com/resource/subscriptions/e29abe6c-d392-4ef5-9c66-5d25436f079`. The page title is "Storage accounts" and the breadcrumb navigation shows "Home > Storage accounts > csb100320028a63be23". The left sidebar contains a list of services, with "Tags" selected. The main content area shows the "Tags" page for the storage account "csb100320028a63be23". It includes a search bar, a "Delete all" button, and a table of tags. The table has two columns: "Name" and "Value". The first row shows "ms-resource-usage" with the value "azure-cloud-shell". The second row shows "Role" with the value "Infra". Below the table, there is a summary of the tags for the storage account and buttons for "Apply" and "Discard changes".

Name	Value
ms-resource-usage	azure-cloud-shell
Role	Infra

csb100320028a63be23 (Storage account)

ms-resource-usage : azure-cloud-shell Role : Infra

No changes

Apply Discard changes

Task 2: Enforce tagging via an Azure policy

2. Assigning a policy to the resource group:


The screenshot shows the 'Require a tag and its value on resources' policy assignment page in the Microsoft Azure portal. The breadcrumb trail is 'Home > Policy | Definitions > Require a tag and its value on resources >'. The page title is 'Require a tag and its value on resources'. Below the title, there is a section 'Assign policy' with a dropdown menu showing 'Require a tag and its value on resources'. The 'Assignment name' field is labeled with a red asterisk and contains the text 'Require Role tag with Infra value' with a green checkmark. The 'Description' field contains the text 'Require Role tag with Infra value for all resources in the Cloud Shell resource group'. The 'Policy enforcement' section has two buttons: 'Enabled' (selected) and 'Disabled'. The 'Assigned by' field contains the name 'Elizabet Ivanova'. At the bottom, there are four buttons: 'Review + create' (blue), 'Cancel', 'Previous', and 'Next'.

3. As expected, the deployment failed because of the set policy:

The screenshot shows the 'newstorage2ndattempt_1679648463951 | Overview' page in the Microsoft Azure portal. The breadcrumb trail is 'Home >'. The page title is 'newstorage2ndattempt_1679648463951 | Overview'. Below the title, there is a section 'Deployment' with a search bar and buttons: 'Delete', 'Cancel', 'Redeploy', 'Download', and 'Refresh'. The 'Overview' tab is selected. A red banner at the top of the main content area says 'Deployment failed. Click here for details ->'. Below this, the heading 'Your deployment failed' is followed by a green square icon with a white 'X'. The deployment details are: 'Deployment name: newstorage2ndattempt_1679648463951', 'Subscription: Azure Pass - Sponsorship', 'Resource group: cloud-shell-storage-west europe', 'Start time: 3/24/2023, 11:01:06 AM', and 'Correlation ID: dea507a0-eba2-40b9-92d5-addbdf3ee87'. Below the details, there is a section 'Deployment details' with a table. The table has four columns: 'Resource', 'Type', 'Status', and 'Operation details'. The table is empty with the text 'No results.' below it. On the right side, there is a 'Deployment failed' notification box with a red 'X' icon. The text in the box says: 'Deployment to resource group 'cloud-shell-storage-west europe' failed. Additional details from the underlying API that might be helpful: At least one resource deployment operation failed. Please list deployment operations for details. Please see https://aka.ms/arm-deployment-operations for usage details.' Below the notification box, there is a 'Microsoft Defender for Cloud' section with a green shield icon. The text says: 'Secure your apps and infrastructure. Go to Microsoft Defender for Cloud >'. Below this, there is a 'Free Microsoft tutorials' section with the text: 'Start learning today >'.

4. Viewing the raw error tab with details of the failed deployment:

Home >

 newstorage2ndattempt_1679648463951 | Overview

Deployment

Delete

Cancel

Redeploy

Download

Refresh

Overview


Inputs

Outputs

Template

Deployment failed. Click here for details →

Your deployment failed



Deployment name: newstorage2ndattempt_1679648463951


Subscription: [Azure Pass - Sponsorship](#)

Resource group: [cloud-shell-storage-west europe](#)

Start time: 3/24/2023,

Correlation ID: dea507

Deployment details

Resource	Type	Status
 newstorage2ndattempt	Microsoft.Storage/storageAcc...	Forbidden

Errors

Summary

Raw Error

```
1 {
2   "code": "DeploymentFailed",
3   "message": "At least one resource deployment operation
4   failed. Please list deployment operations for details. Please
5   see https://aka.ms/arm-deployment-operations for usage details.
6   ",
7   "details": [
8     {
9       "code": "RequestDisallowedByPolicy",
10      "message": "Resource 'newstorage2ndattempt' was
disallowed by policy. Policy identifiers: '[
{\\\"policyAssignment\\\":{\\\"name\\\":\\\"Require Role tag with Infra
value\\\",\\\"id\\\":\\\"/subscriptions/
e29abe6c-d392-4ef5-9c66-5d25436f0796/resourceGroups/
cloud-shell-storage-west europe/providers/Microsoft.
Authorization/policyAssignments/069d41a5be844ac1a9e4342e\\\"},
\\\"policyDefinition\\\":{\\\"name\\\":\\\"Require a tag and its value on
resources\\\",\\\"id\\\":\\\"/providers/Microsoft.Authorization/
policyDefinitions/1e30110a-5ceb-460c-a204-c1c3969c6d62\\\"}]'."
8     }
9   ]
10 }
```

Task 3: Apply tagging via an Azure policy

5. After setting the policy definition to inherit the tag, I created a storage account – **newnewstor22** – and verified that the tag was automatically assigned to it.

The screenshot displays the Microsoft Azure portal interface. At the top, the header shows 'Microsoft Azure' and a search bar. The user's profile 'lizaliza9898@outlook.co...' is visible in the top right corner. The main content area is titled 'newnewstor22 Storage account'. Below the title, there is a search bar and a set of action buttons: 'Upload', 'Open in Explorer', 'Delete', 'Move', 'Refresh', and 'Open in mobile'. The left sidebar contains a navigation menu with categories: 'Overview', 'Data storage', and 'Security + networking'. The 'Overview' section is currently selected, showing various tabs like 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', and 'Storage browser'. The 'Tags' tab is active, displaying a table of tags. The table has two columns: 'Name' and 'Value'. The first tag is 'cloud-shell-storage-westeurope' with a value of 'Standard'. The second tag is 'Azure Pass - Sponsorship' with a value of 'Succeeded'. Below the table, there is a 'Role : Infra' button. The 'Properties' tab is also visible, showing details about the storage account, including 'Resource group', 'Location', 'Primary/Secondary Location', 'Subscription', 'Subscription ID', 'Disk state', and 'Tags'. The 'Blob service' section shows 'Hierarchical namespace' as 'Disabled', 'Default access tier' as 'Hot', and 'Blob public access' as 'Enabled'. The 'Security' section shows 'Require secure transfer for REST API operations' as 'Enabled', 'Storage account key access' as 'Enabled', and 'Minimum TLS version' as '1.2'.

Name	Value
cloud-shell-storage-westeurope	Standard
Azure Pass - Sponsorship	Succeeded

Role : Infra

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob public access: Enabled

Security

- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: 1.2