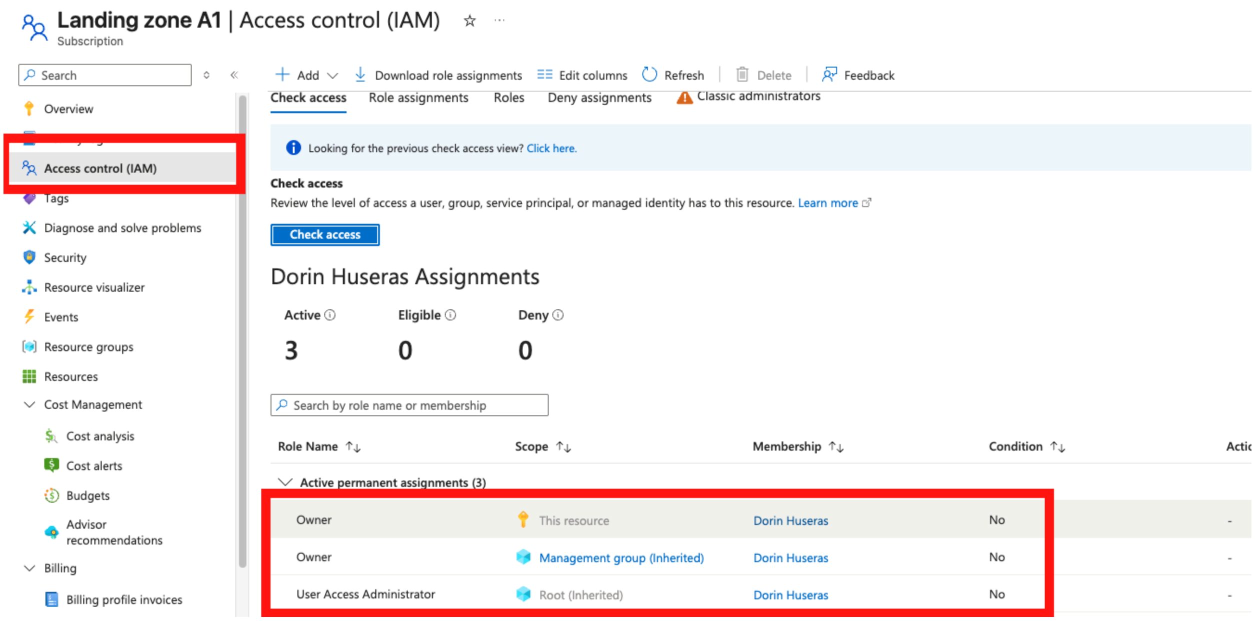
Exercise: Assign an RBAC Role to a User or Group in Azure Subscription

Role-Based Access Control (RBAC) in Azure is used to grant users or groups access to Azure resources within a particular scope. Here's an exercise that walks you through the steps to assign an RBAC role to a user or group for an Azure subscription:

1. **Sign in to Azure Portal**
    a. Navigate to https://portal.azure.com/
    b. Sign in with an account that has sufficient privileges to assign roles at the subscription level (e.g., **Owner** or **User Access Administrator**).



Landing zone A1 | Access control (IAM)
Subscription

Looking for the previous check access view? Click here.

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Check access

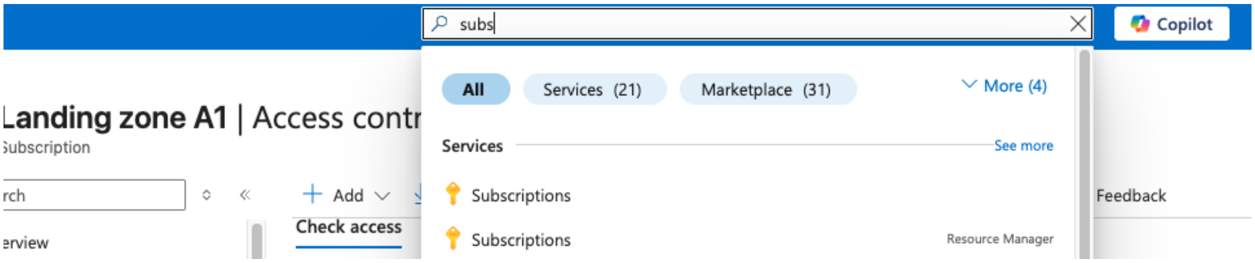
Dorin Huseras Assignments

Active	Eligible	Deny
3	0	0

Search by role name or membership

Role Name	Scope	Membership	Condition	Actic
Active permanent assignments (3)				
Owner	This resource	Dorin Huseras	No	-
Owner	Management group (Inherited)	Dorin Huseras	No	-
User Access Administrator	Root (Inherited)	Dorin Huseras	No	-

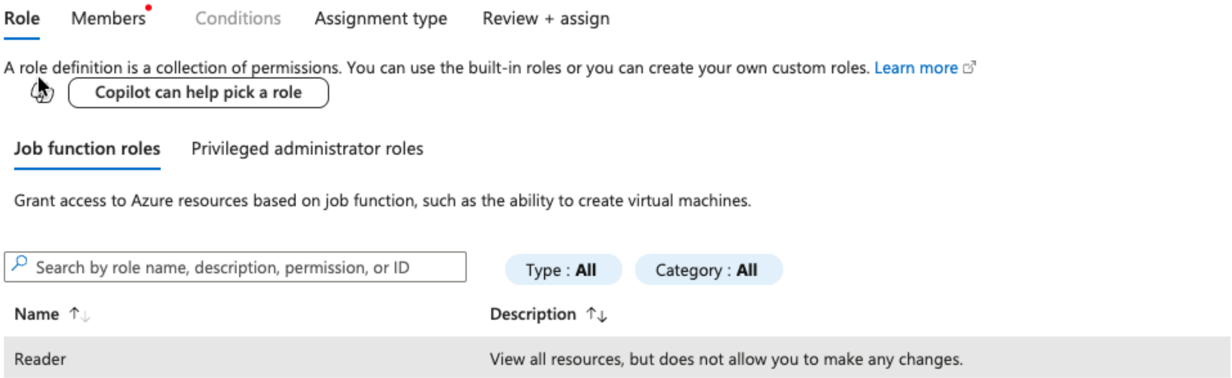
2. **Navigate to Subscriptions**
    a. In the search bar at the top, type “Subscriptions” and select “Subscriptions” from the dropdown results.



subs

3. **Select Your Subscription**
    a. From the list of available subscriptions, click on the subscription where you want to assign the role.

4. **Access Control (IAM)**
    a. In the subscription blade, click on “Access control (IAM)” from the left-hand menu.
5. **Add a Role Assignment**
    a. Click on the “+ Add” button and then select “Add role assignment”.
6. **Configure the Role Assignment**
    a. Role: Click on the "Role" dropdown. A list of roles like 'Contributor', 'Owner', 'Reader', etc., will be displayed.
    b. Select the **Reader Role**


Role
Members
Conditions
Assignment type
Review + assign
Copilot can help pick a role
Job function roles
Privileged administrator roles
Search by role name, description, permission, or ID
Type : All
Category : All

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name ↑↓	Description ↑↓
Reader	View all resources, but does not allow you to make any changes.

    c. Select: In the “Members” field, click on the “Select members” button.
        i. In the search box, type the name of the user or group you wish to assign the role to. (**Your User**)
        ii. From the search results, select the user or group.
        iii. Click on the "Select" button at the bottom.
    d. Confirm your selections.
7. **Save the Role Assignment**
    a. Click on the “Save” button. Azure will now assign the selected role to the chosen user or group for the specified subscription.
8. **Verify the Assignment**
    a. After assigning the role, you should be redirected back to the “Role assignments” tab under “Access control (IAM)”. You can search for the user or group to verify that they now have the intended role for that subscription.

Conclusion

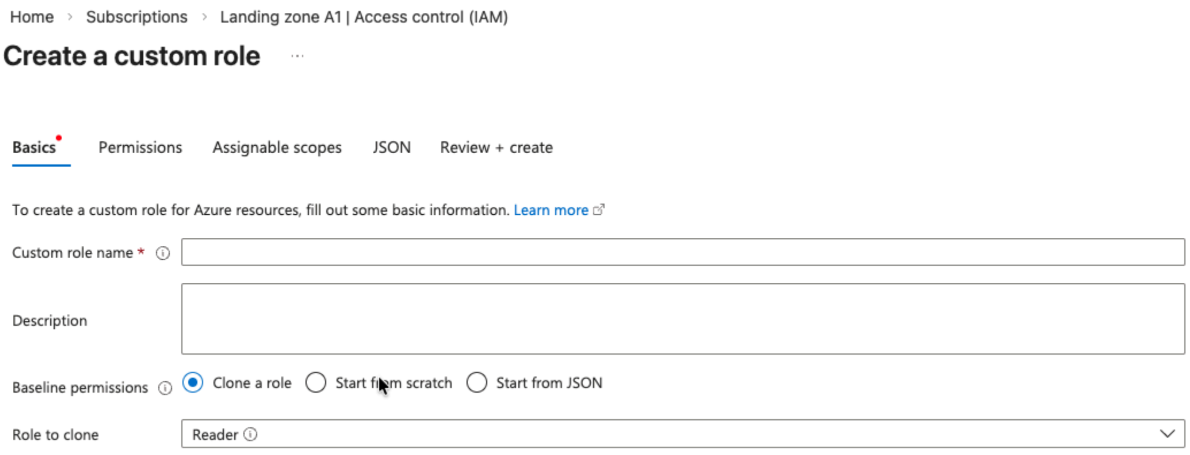
You've successfully assigned an RBAC role to a **user** or **group** for an Azure subscription! This user or group now has permissions based on the role you've assigned within the scope of that subscription.

Note: As always, adhere to the principle of **least privilege**. Grant users or groups only the permissions they require. Regularly review and audit permissions to ensure security and compliance.

Steps to Create a Custom Role from an Existing Role in an Azure Subscription using Azure Portal

Creating a custom role from an existing role in an Azure subscription involves leveraging the Azure Portal, Azure CLI, or Azure PowerShell. The Azure Portal provides a graphical interface to facilitate this, so we'll outline those steps here:

1. **Sign in to the Azure Portal**
   a. Go to https://portal.azure.com/
   b. Sign in with your Azure account.
2. **Navigate to Subscriptions**
   a. In the search bar at the top, type “Subscriptions” and select it from the dropdown results.
3. **Select Your Subscription**
   a. From the list of subscriptions, click on the one in which you wish to create the custom role.
4. **Access Control (IAM)**
   a. In the selected subscription blade, choose "Access control (IAM)" from the left-hand menu.
5. **Add a custom Role**
   a. Click on the “+ Add” button and then select “Add custom role”.
   b. Select clone a role from Baseline permissions.
      i. **Clone a Role**



To create a custom role for Azure resources, fill out some basic information. Learn more

Custom role name *

Description

Baseline permissions ● Clone a role ○ Start from scratch ○ Start from JSON

Role to clone: Reader

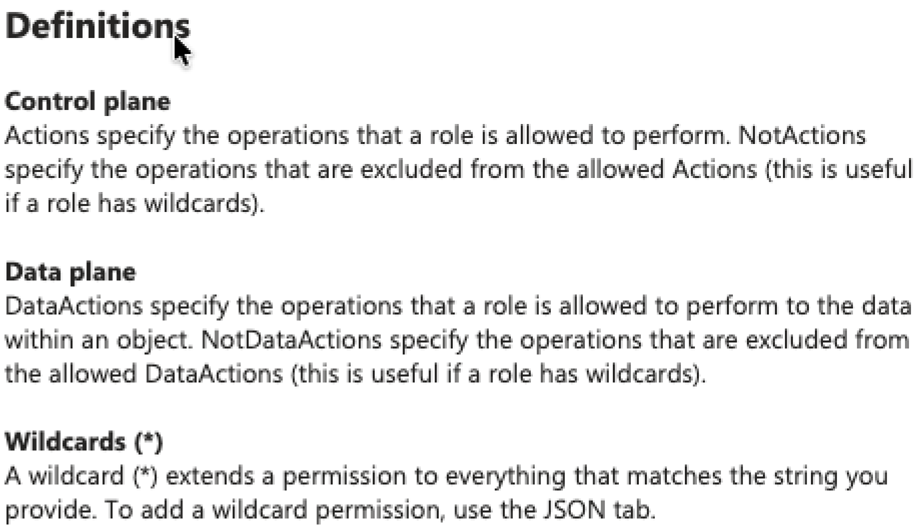
6. **Find and Select the Role to Copy**
   a. Scroll or search to find the existing role you wish to use as a basis for your custom role.
      i. **Reader**
7. **Define the Custom Role**
   a. Basics:
      i. **Name**: Provide a unique name for your custom role.

   ii. **Description**: Offer a short description detailing the purpose of this custom role or how it differs from the original.

b. Permissions:

   i. You'll see a list of permissions inherited from the original role. You can **add** or **remove** permissions based on your requirements.

   ii. Be mindful of



Definitions

Control plane

Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

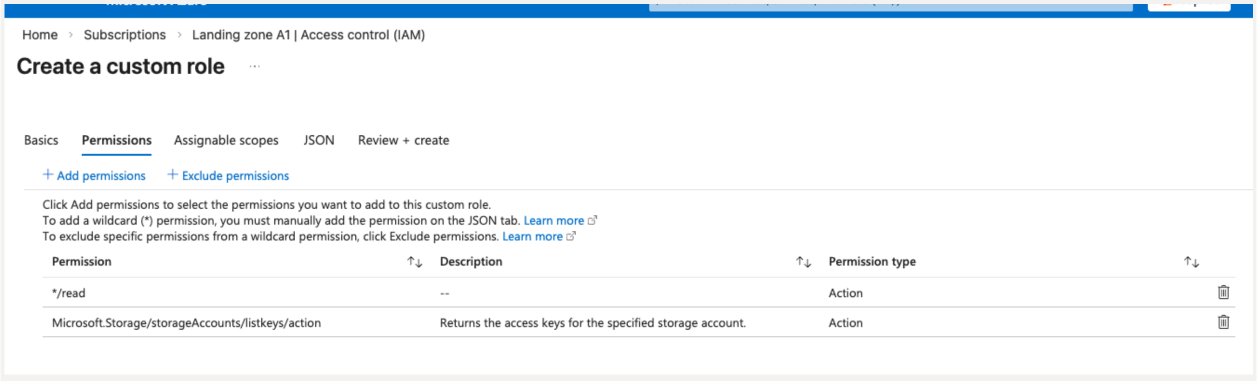
Data plane

DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role has wildcards).

Wildcards (*)

A wildcard (*) extends a permission to everything that matches the string you provide. To add a wildcard permission, use the JSON tab.

   iii. **Add**: `Microsoft.Storage/storageAccounts/listkeys/action`



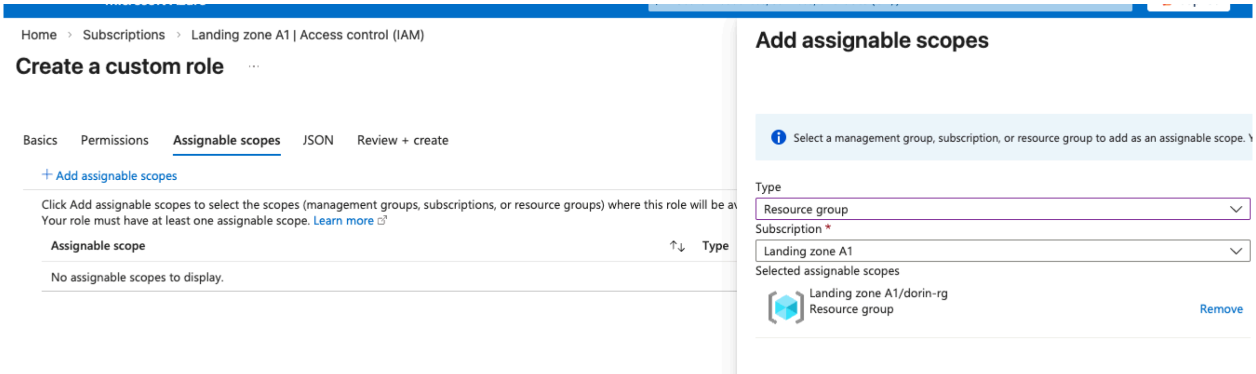
Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. Learn more
To exclude specific permissions from a wildcard permission, click Exclude permissions. Learn more

Permission	Description	Permission type
*/read	--	Action
Microsoft.Storage/storageAccounts/listkeys/action	Returns the access keys for the specified storage account.	Action

c. **Assignable Scopes**:

   i. By default, the scope might be set to the current subscription. If you need the custom role to be available for other subscriptions or specific resource groups, adjust the scopes accordingly.

      1. Assign it to your Resource Group **[yourname]-rg**



Home › Subscriptions › Landing zone A1 | Access control (IAM)

Create a custom role ···

Basics | Permissions | Assignable scopes | JSON | Review + create

+ Add assignable scopes

Click Add assignable scopes to select the scopes (management groups, subscriptions, or resource groups) where this role will be av
Your role must have at least one assignable scope. Learn more

Assignable scope	Type
No assignable scopes to display.	

Add assignable scopes

Select a management group, subscription, or resource group to add as an assignable scope. Y

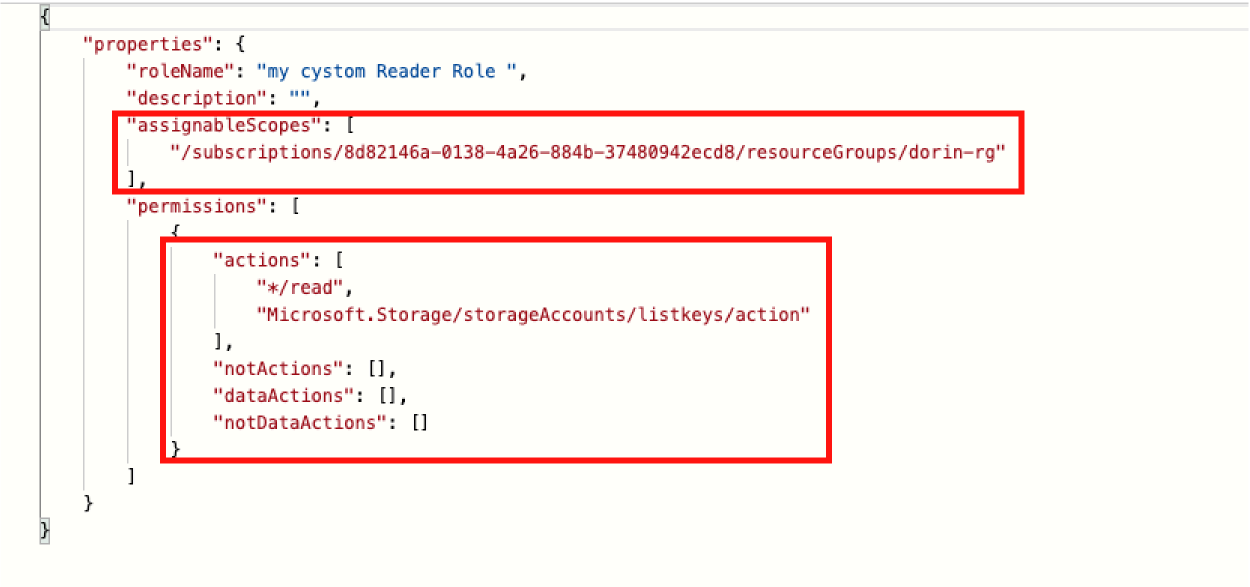
Type: Resource group

Subscription *: Landing zone A1

Selected assignable scopes

Landing zone A1/dorin-rg
Resource group — Remove

8. **Save the Custom Role**
   a. Once you've configured the role to your liking, click the “Save” or “Create” button to finalize your custom role.
   b. View the JSON configuration



```
{
    "properties": {
        "roleName": "my cystom Reader Role ",
        "description": "",
        "assignableScopes": [
            "/subscriptions/8d82146a-0138-4a26-884b-37480942ecd8/resourceGroups/dorin-rg"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

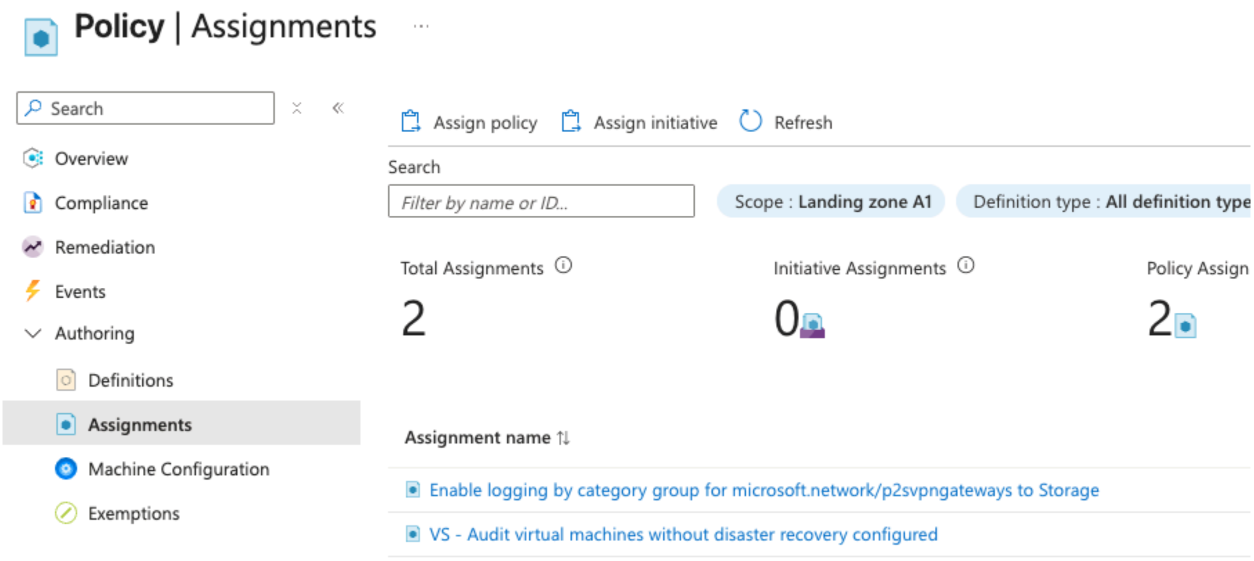
9. **Verification**
   a. Back in the “Role definitions” tab, you should see your newly created custom role in your RG only. Click on it to review the permissions and ensure they match your intentions.

Remember to practice the principle of **least privilege** when creating and assigning roles. This ensures that users, groups, or services have only the permissions necessary to perform their tasks, enhancing security and reducing the potential for unintended changes or access.

Steps to Assign a Policy to an Azure Subscription

Assigning a policy to an Azure subscription involves defining rules that enforce specific conditions or effects for resources within that subscription. Here are the steps to assign a policy to a subscription using the Azure Portal:

1. Sign in to Azure Portal
    a. Navigate to https://portal.azure.com/
    b. Log in with your Azure credentials.
2. Navigate to Policy Service
    a. In the search bar at the top, type “Policy” and select "Policy" from the dropdown results.
3. Go to Assignments
    a. On the Policy blade, click on “Assignments” in the left-hand menu.



Scope : **Landing zone A1**

Definition type : **All definition type**

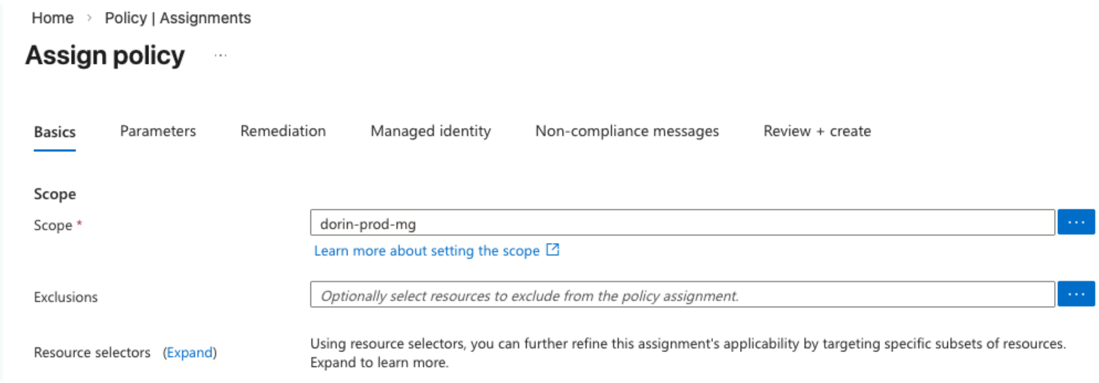
Total Assignments 2

Initiative Assignments 0

Policy Assign 2

Assignment name ⇅
Enable logging by category group for microsoft.network/p2svpngateways to Storage
VS - Audit virtual machines without disaster recovery configured

4. Add a Policy Assignment
    a. Click on the "+ Assign Policy" button at the top of the blade.
5. Select your Resource Group
    a. In the "Scope" section:
        i. Click on the ellipsis (...) next to the "Subscription" field.
        ii. Choose your Resource group **[yourname]-rg**



Scope

Scope *: dorin-prod-mg

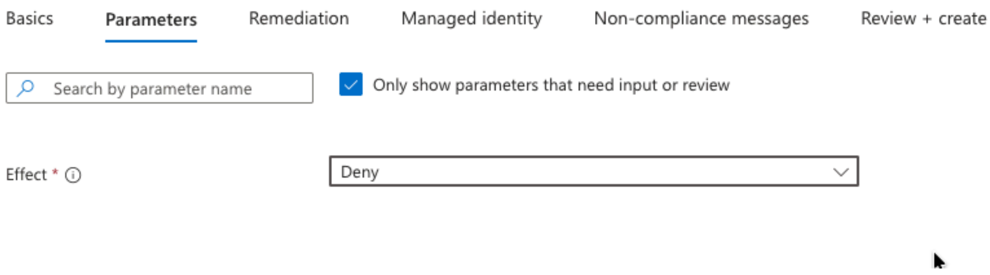
Learn more about setting the scope

Exclusions: *Optionally select resources to exclude from the policy assignment.*

Resource selectors: Using resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. Expand to learn more.

   iii. Click on the "Select" button at the bottom.

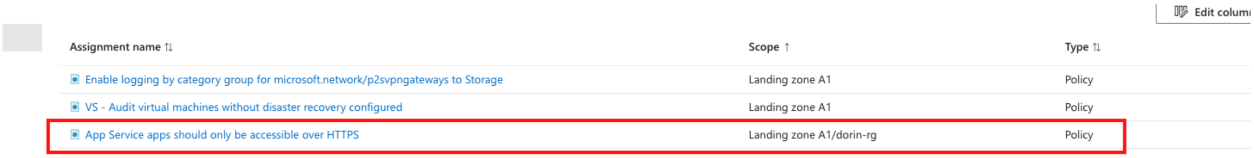
6. Select the Policy Definition
   a. Under the "Policy definition" section, click on the ellipsis (...).
      i. App Service apps should only be accessible over HTTPS
   b. Search and select the policy definition you want to assign.
   c. Click on the "Select" button.
7. Policy Assignment Settings
   a. Assignment name: Provide a name for the policy assignment.
   b. Description (Optional): Add a description for clarity, especially if other team members might manage or review this policy.
   c. Policy enforcement: Ensure it's set to "Enabled" if you want the policy to be enforced. If you're testing or auditing without enforcement, set it to "Disabled".
8. Parameters
   a. Effect: **Deny**



☑ Only show parameters that need input or review

Effect *: Deny

9. Review and Save
   a. After configuring the policy assignment settings, click on the “Review + create” button at the bottom.
   b. Ensure all details are correct, then click on the “Create” button to assign the policy to the chosen subscription.
10. Verification
   a. After assigning the policy, you'll return to the "Assignments" blade. Here, you can verify your policy assignment. It should be listed with the specified Resource Group scope.

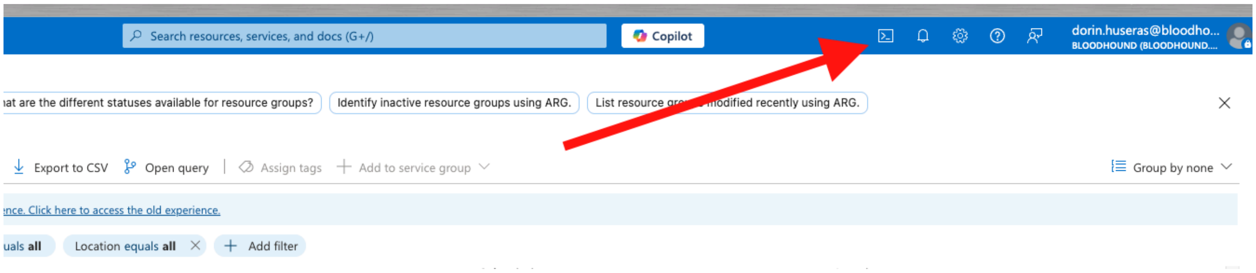


Assignment name ↑↓	Scope ↑	Type ↑↓
Enable logging by category group for microsoft.network/p2svpngateways to Storage	Landing zone A1	Policy
VS - Audit virtual machines without disaster recovery configured	Landing zone A1	Policy
App Service apps should only be accessible over HTTPS	Landing zone A1/dorin-rg	Policy

Remember, Azure Policy evaluates every resource in the scope for compliance with the conditions defined in the policy. Non-compliant resources are flagged, and depending on the policy effects, may be automatically corrected, audited, or even denied creation. Always test new policies in non-production environments first to understand their impact.

Test the policy

1. **Sign in to Azure Portal**
    a. Navigate to https://portal.azure.com/
    b. Log in with your Azure account.
    c. Click on the cloud shell button



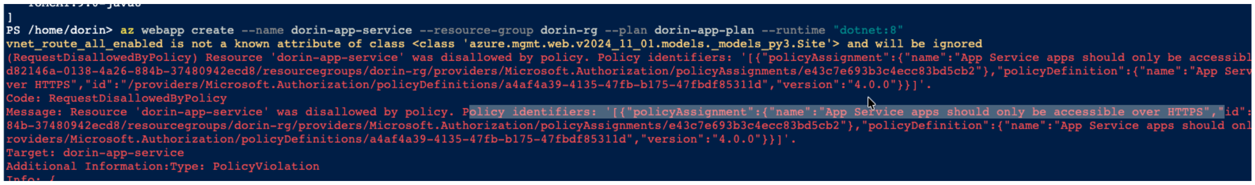
Search resources, services, and docs (G+/)
Copilot
dorin.huseras@bloodho...
BLOODHOUND (BLOODHOUND...
at are the different statuses available for resource groups?
Identify inactive resource groups using ARG.
List resource gro modified recently using ARG.
Export to CSV
Open query
Assign tags
Add to service group
Group by none
nce. Click here to access the old experience.
uals all
Location equals all
Add filter

    d. Run the commands:

```
az appservice plan create --name [yourname]-plan --resource-group
[yourname]-rg --location westeurope --sku B1

az webapp create --name [yourname]-app-service --resource-group
[yourname]-rg --plan [yourname]-plan --runtime "dotnet:8"
```

    e. Observe the error



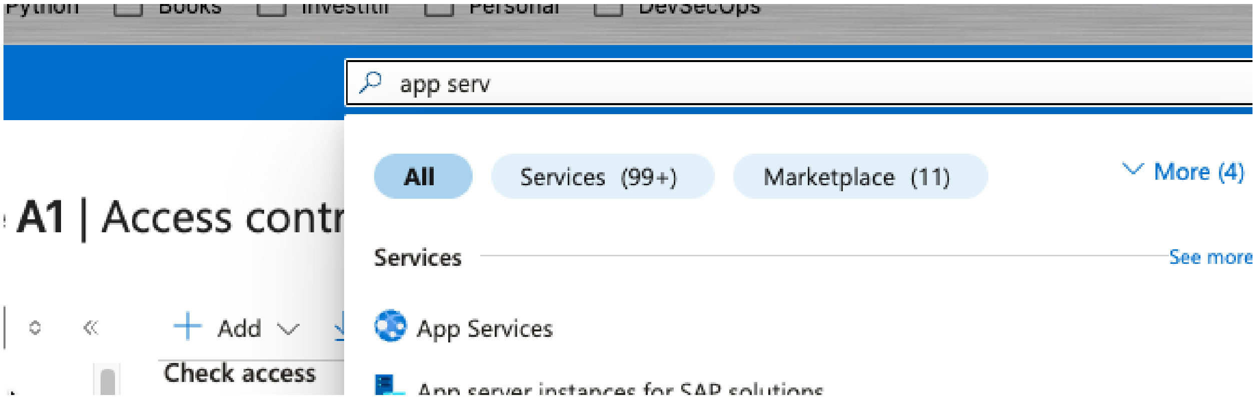
```
]
PS /home/dorin> az webapp create --name dorin-app-service --resource-group dorin-rg --plan dorin-app-plan --runtime "dotnet:8"
vnet_route_all_enabled is not a known attribute of class <class 'azure.mgmt.web.v2024_11_01.models._models_py3.Site'> and will be ignored
(RequestDisallowedByPolicy) Resource 'dorin-app-service' was disallowed by policy. Policy identifiers: '[{"policyAssignment":{"name":"App Service apps should only be accessibl
d82146a-0138-4a26-884b-37480942ecd8/resourcegroups/dorin-rg/providers/Microsoft.Authorization/policyAssignments/e43c7e693b3c4ecc83bd5cb2"},"policyDefinition":{"name":"App Serv
ver HTTPS","id":"/providers/Microsoft.Authorization/policyDefinitions/a4af4a39-4135-47fb-b175-47fbdf85311d","version":"4.0.0"}}]'.
Code: RequestDisallowedByPolicy
Message: Resource 'dorin-app-service' was disallowed by policy. Policy identifiers: '[{"policyAssignment":{"name":"App Service apps should only be accessible over HTTPS","id":
84b-37480942ecd8/resourcegroups/dorin-rg/providers/Microsoft.Authorization/policyAssignments/e43c7e693b3c4ecc83bd5cb2"},"policyDefinition":{"name":"App Service apps should onl
roviders/Microsoft.Authorization/policyDefinitions/a4af4a39-4135-47fb-b175-47fbdf85311d","version":"4.0.0"}}]'.
Target: dorin-app-service
Additional Information:Type: PolicyViolation
Info: {
```

    f. Try Again:

```
az webapp create --name [yourname]-app-service --resource-group
```

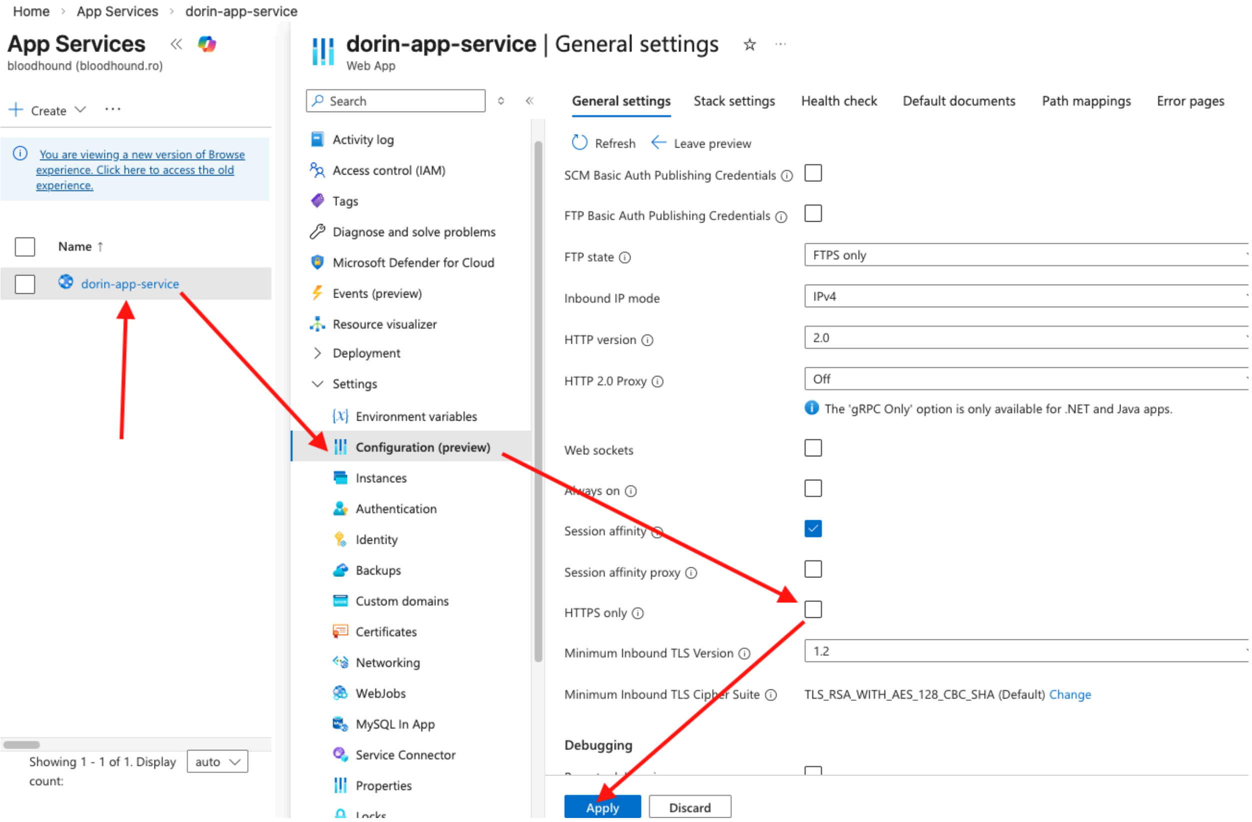
```
[yourname]-rg --plan [yourname]-plan --runtime "dotnet:8" --https-only true
```

Go to your App Service, and try to force the setting after creation:



app serv

Go to configurations and modify the setting



You are viewing a new version of Browse experience. Click here to access the old experience.

dorin-app-service | General settings

SCM Basic Auth Publishing Credentials □

FTP Basic Auth Publishing Credentials □

FTP state: FTPS only

Inbound IP mode: IPv4

HTTP version: 2.0

HTTP 2.0 Proxy: Off

The 'gRPC Only' option is only available for .NET and Java apps.

Web sockets □

Always on □

Session affinity ☑

Session affinity proxy □

HTTPS only □

Minimum Inbound TLS Version: 1.2

Minimum Inbound TLS Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (Default) Change

Debugging

Showing 1 - 1 of 1. Display count: auto

Get familiarized with the platform error.