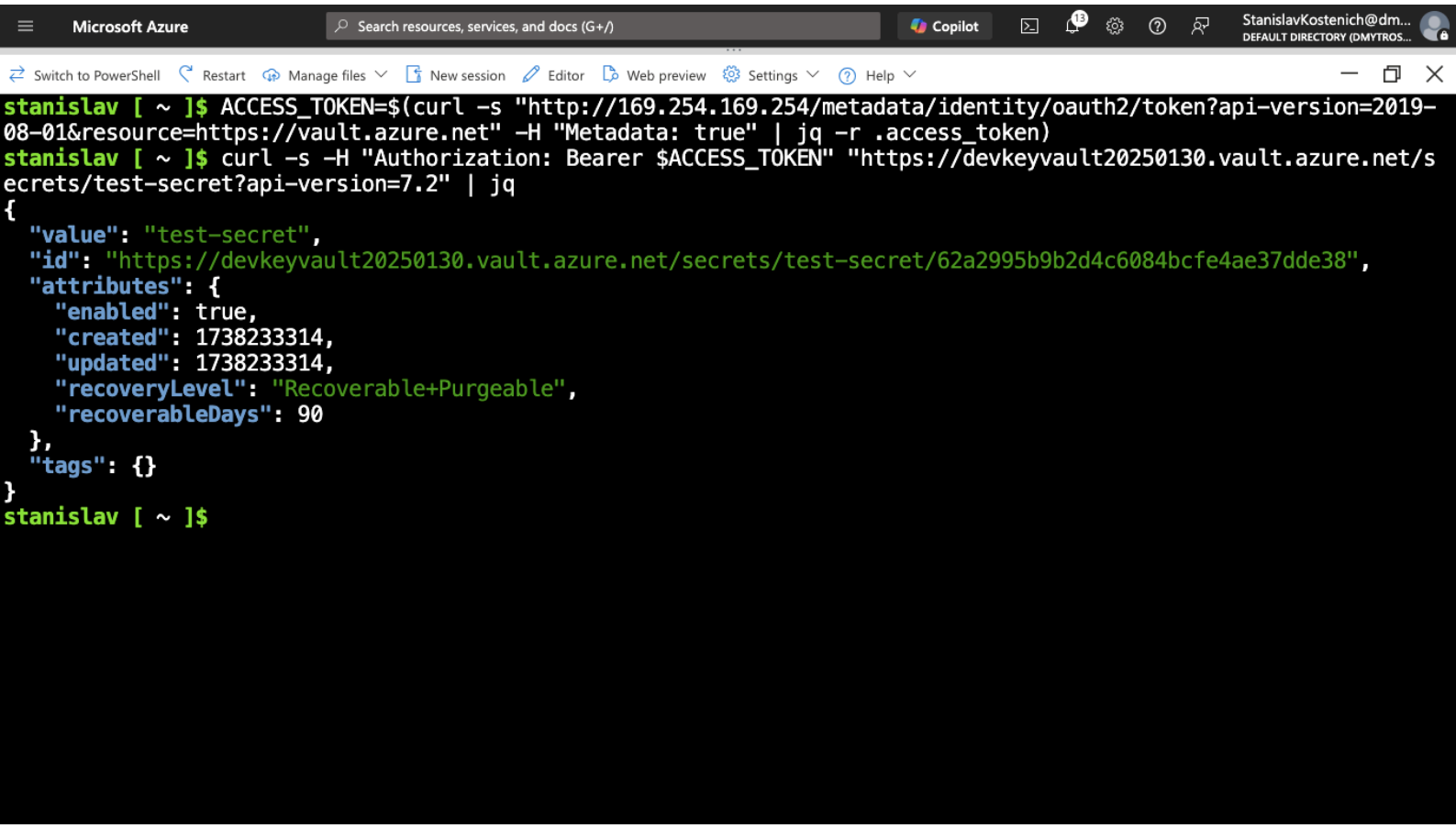
3. Stop all ACI instances after completing the testing to reduce ongoing costs.

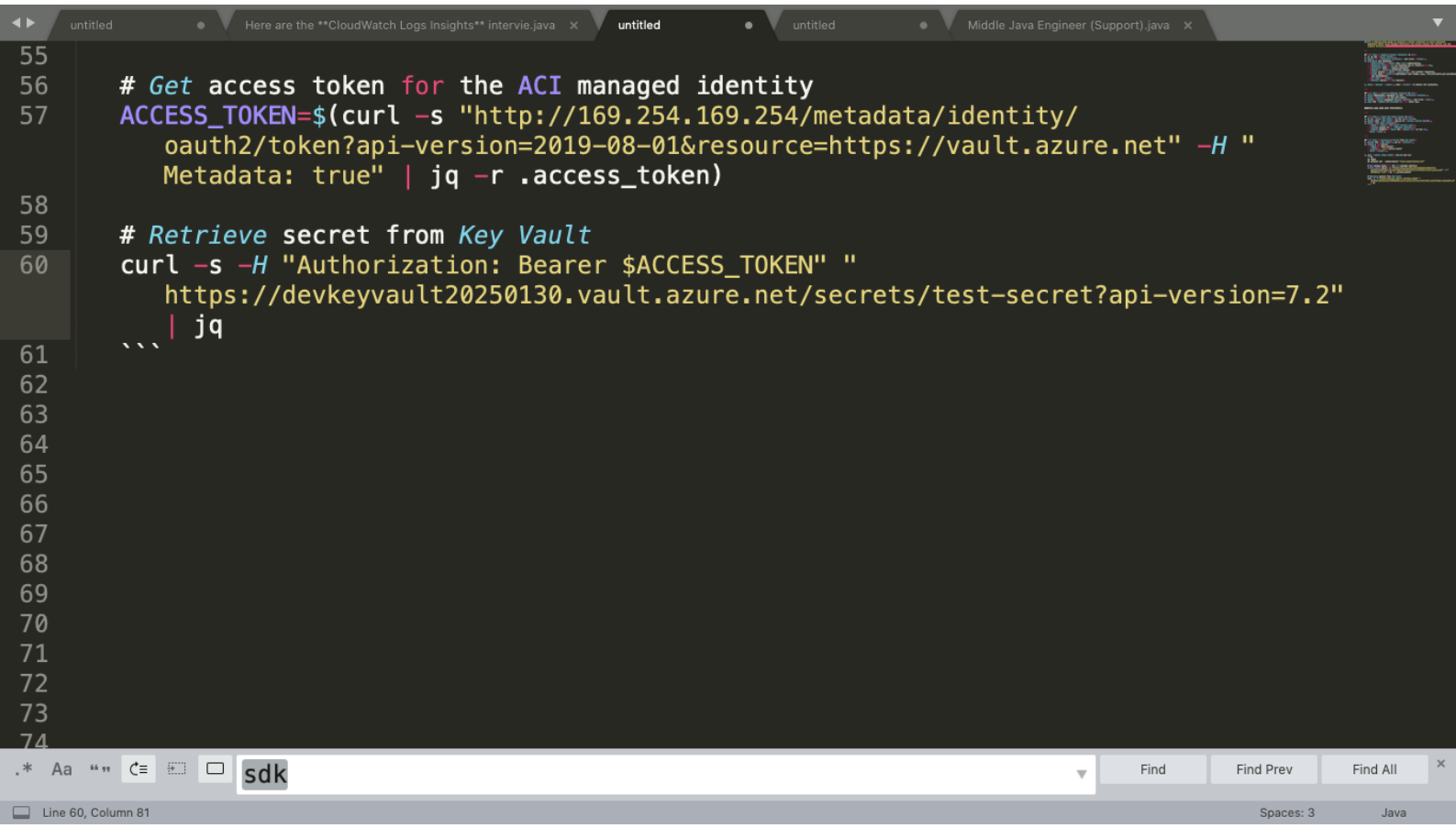
Practical Task 4: Secure a Docker Container in ACI with Managed Identity via Azure Portal

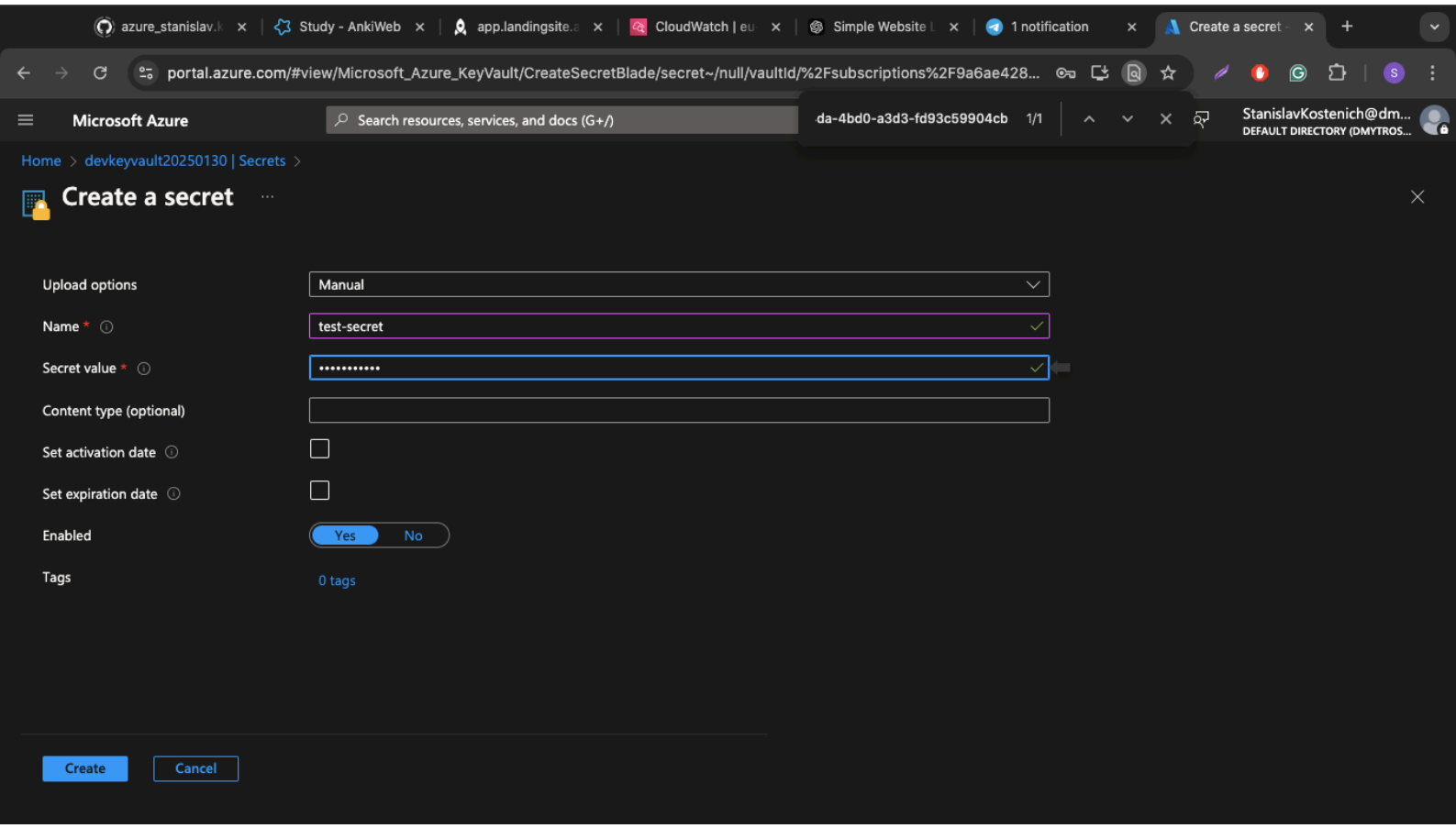
Requirements:

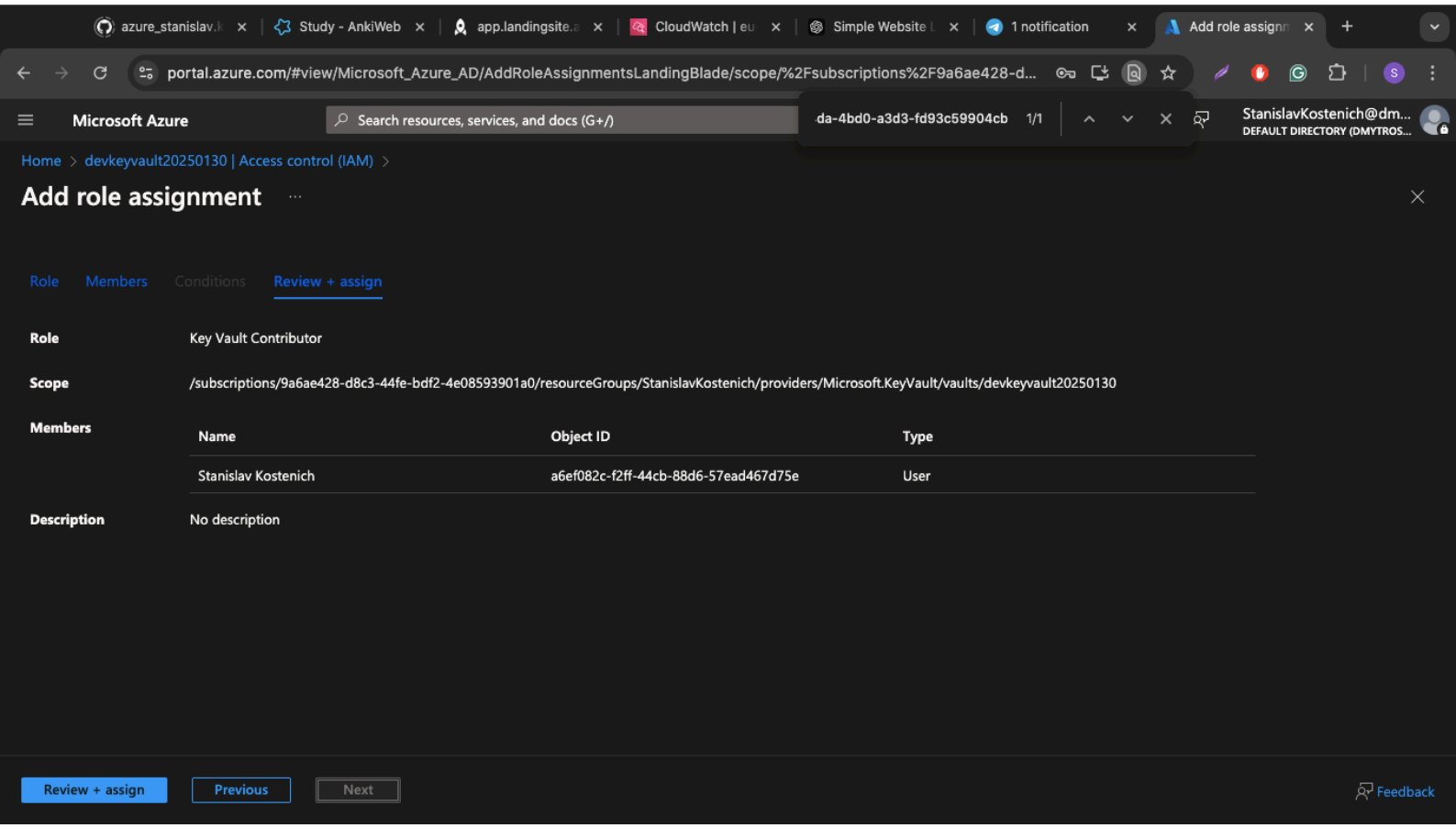
1. Deploy a Docker container to Azure Container Instances using the existing lightweight ACI setup from previous tasks.
2. Configure a Managed Identity for the ACI and securely access an Azure service (e.g., Azure Key Vault) with minimal permissions and access scope.

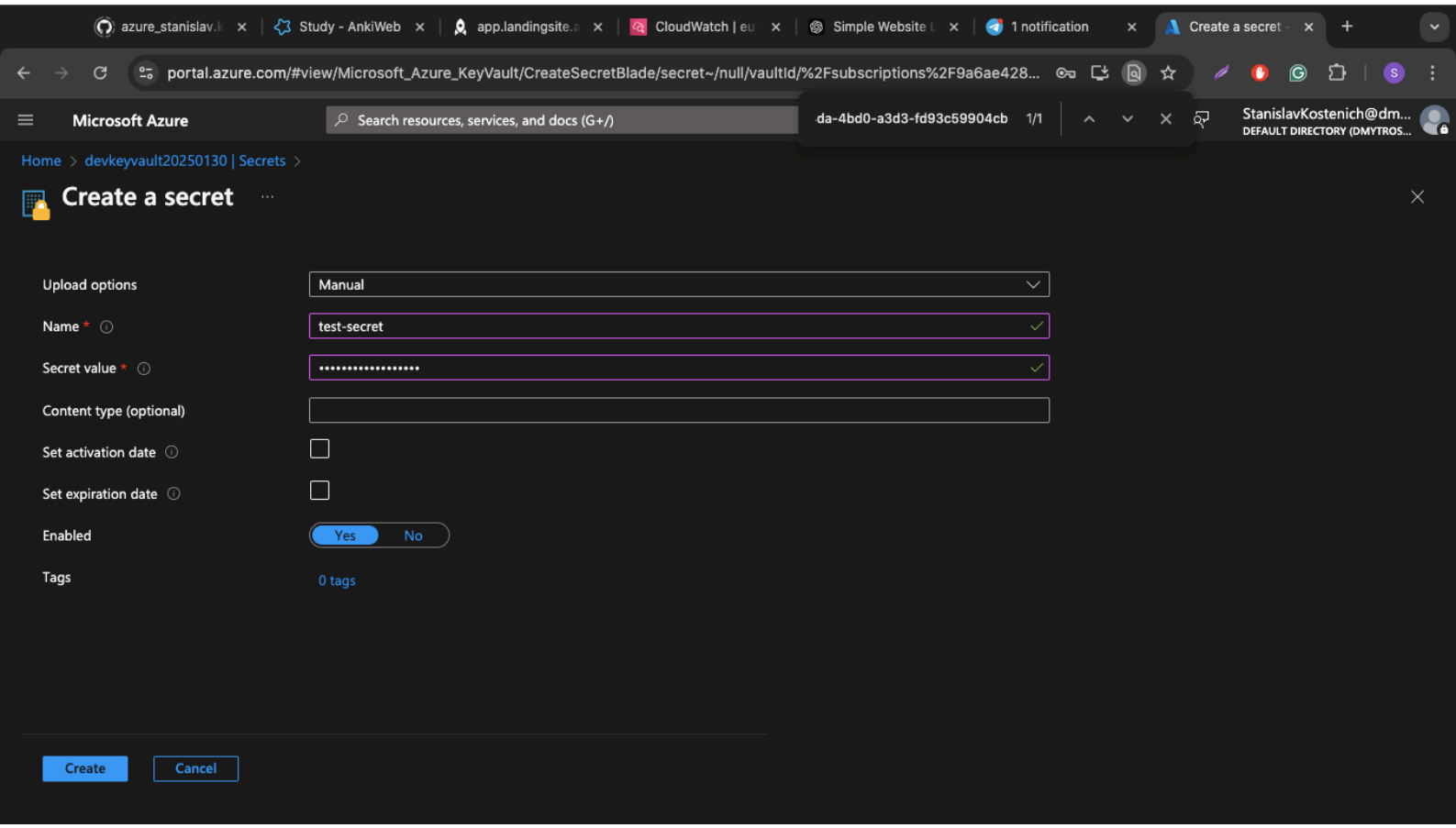
3. Retrieve only a single secret from Azure Key Vault for testing purposes.
4. Remove the ACI container after verifying secure access.

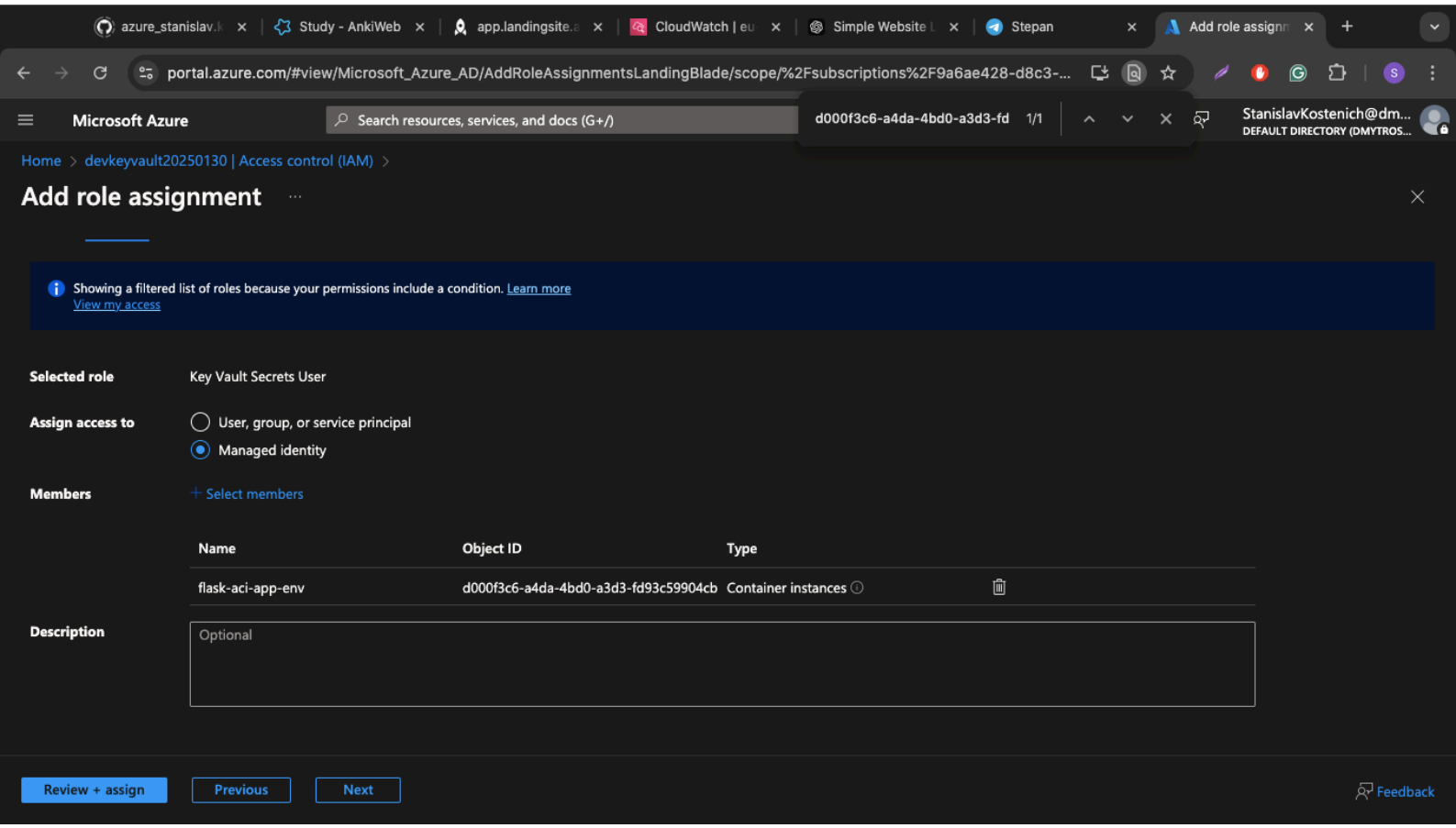

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Switch to PowerShell
Restart
Manage files
New session
Editor
Web preview
Settings
Help
stanislav [~]$ ACCESS_TOKEN=$(curl -s "http://169.254.169.254/metadata/identity/oauth2/token?api-version=2019-08-01&resource=https://vault.azure.net" -H "Metadata: true" | jq -r .access_token)
stanislav [~]$ curl -s -H "Authorization: Bearer $ACCESS_TOKEN" "https://devkeyvault20250130.vault.azure.net/secrets/test-secret?api-version=7.2" | jq
{
"value": "test-secret",
"id": "https://devkeyvault20250130.vault.azure.net/secrets/test-secret/62a2995b9b2d4c6084bcfe4ae37dde38",
"attributes": {
"enabled": true,
"created": 1738233314,
"updated": 1738233314,
"recoveryLevel": "Recoverable+Purgeable",
"recoverableDays": 90
},
"tags": {}
}
stanislav [~]$

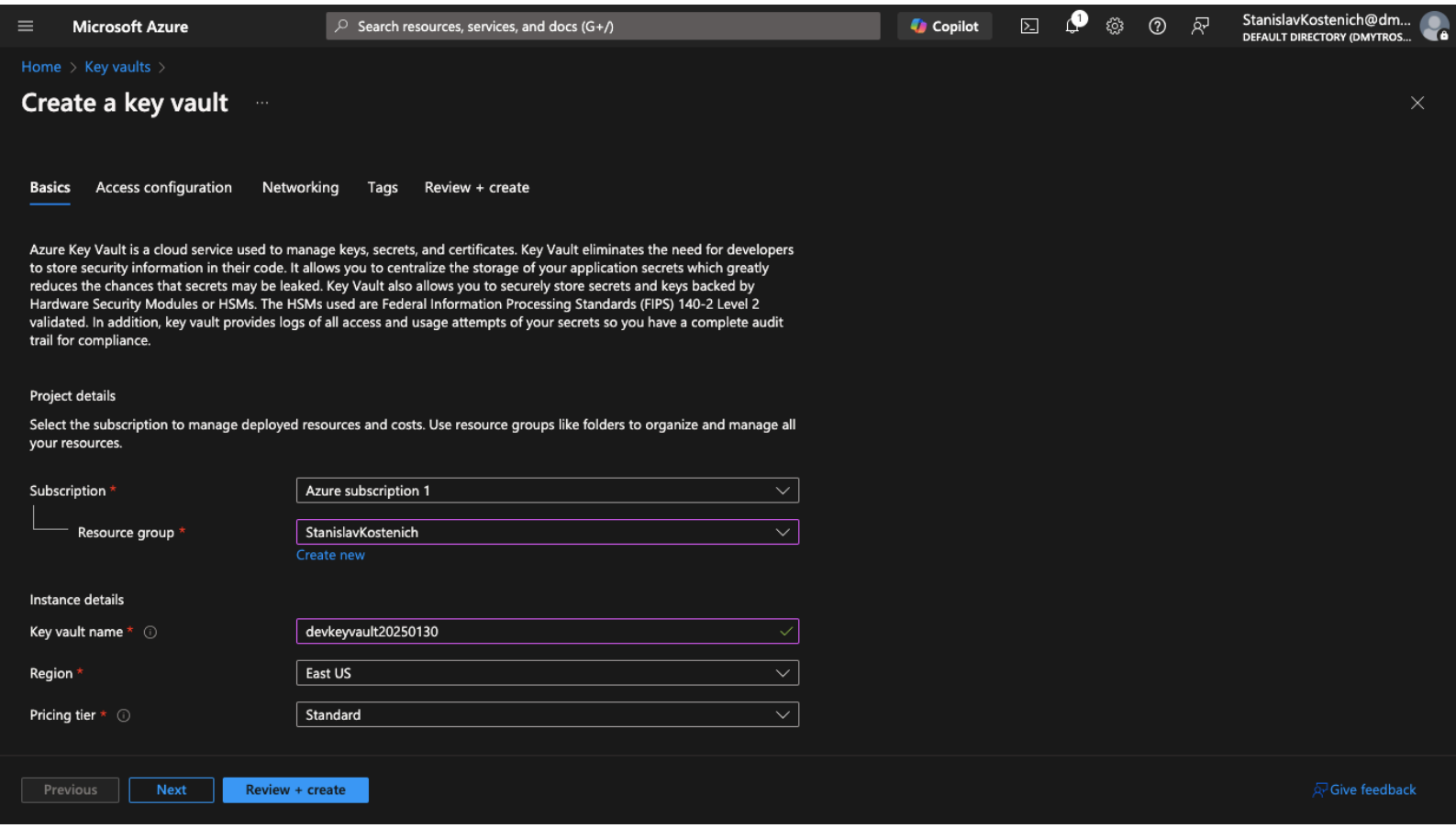

untitled
Here are the **CloudWatch Logs Insights** intervie.java
untitled
untitled
Middle Java Engineer (Support).java
55
56 # Get access token for the ACI managed identity
57 ACCESS_TOKEN=$(curl -s "http://169.254.169.254/metadata/identity/
oauth2/token?api-version=2019-08-01&resource=https://vault.azure.net" -H "
Metadata: true" | jq -r .access_token)
58
59 # Retrieve secret from Key Vault
60 curl -s -H "Authorization: Bearer $ACCESS_TOKEN" "
https://devkeyvault20250130.vault.azure.net/secrets/test-secret?api-version=7.2"
| jq
61 ```
62
63
64
65
66
67
68
69
70
71
72
73
74
.* Aa
sdk
Find
Find Prev
Find All
Line 60, Column 81
Spaces: 3
Java

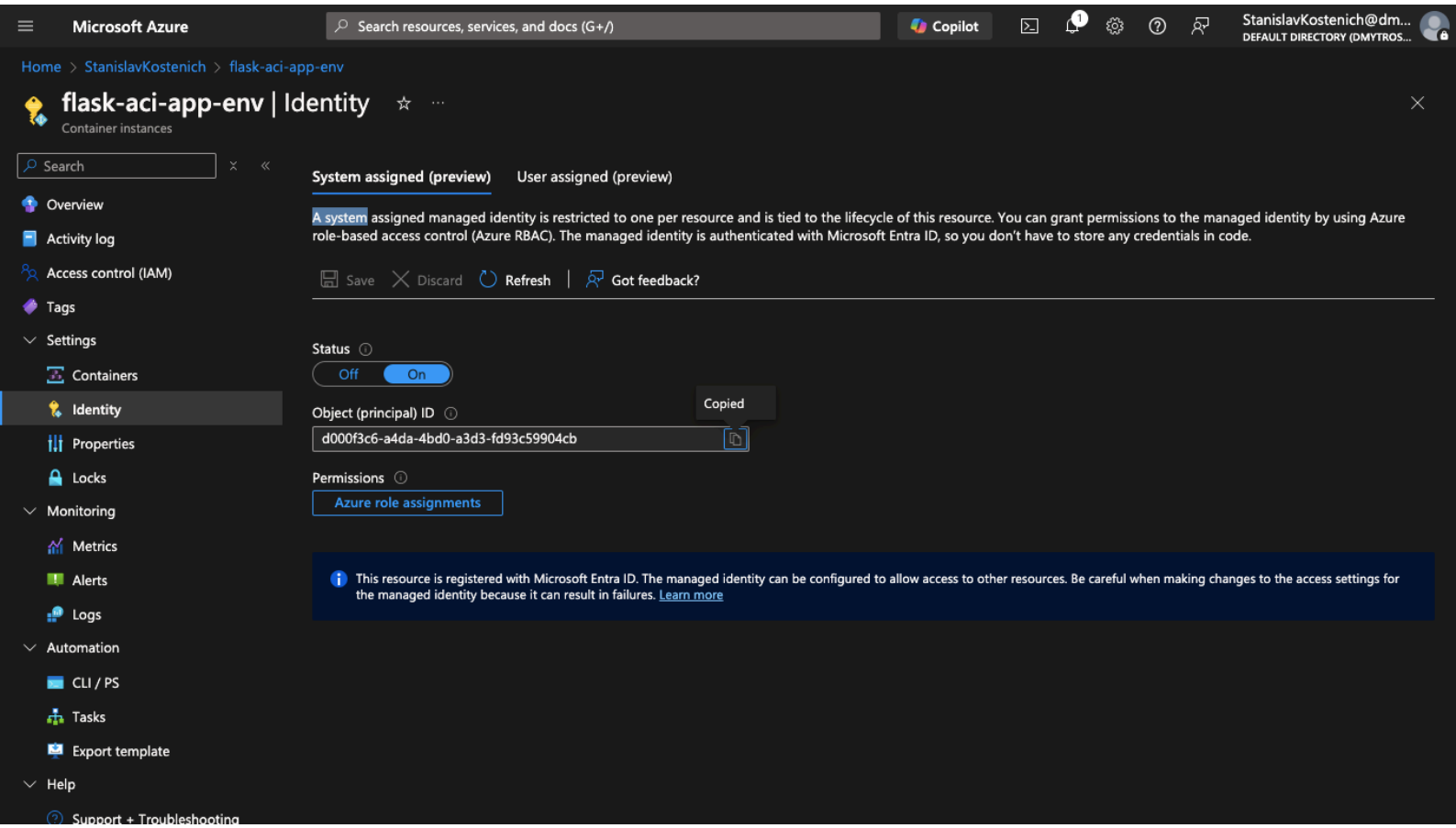

azure_stanislav.k
Study - AnkiWeb
app.landingsite.a
CloudWatch | eu
Simple Website
1 notification
Create a secret
portal.azure.com/#view/Microsoft_Azure_KeyVault/CreateSecretBlade/secret~/null/vaultId/%2Fsubscriptions%2F9a6ae428...
Microsoft Azure
Search resources, services, and docs (G+/)
da-4bd0-a3d3-fd93c59904cb
1/1
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home
devkeyvault20250130 | Secrets
Create a secret
Upload options
Manual
Name *
test-secret
Secret value *
Content type (optional)
Set activation date
Set expiration date
Enabled
Yes
No
Tags
0 tags
Create
Cancel


azure_stanislav.k
Study - AnkiWeb
app.landingsite.a
CloudWatch | eu
Simple Website L
1 notification
Add role assignm
portal.azure.com/#view/Microsoft_Azure_AD/AddRoleAssignmentsLandingBlade/scope/%2Fsubscriptions%2F9a6ae428-d...
Microsoft Azure
Search resources, services, and docs (G+/)
da-4bd0-a3d3-fd93c59904cb 1/1
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home > devkeyvault20250130 | Access control (IAM) >
Add role assignment
Role Members Conditions Review + assign
Role Key Vault Contributor
Scope /subscriptions/9a6ae428-d8c3-44fe-bdf2-4e08593901a0/resourceGroups/StanislavKostenich/providers/Microsoft.KeyVault/vaults/devkeyvault20250130
Members
Name Object ID Type
Stanislav Kostenich a6ef082c-f2ff-44cb-88d6-57ead467d75e User
Description No description
Review + assign
Previous
Next
Feedback


azure_stanislav.k
Study - AnkiWeb
app.landingsite.a
CloudWatch | eu
Simple Website L
1 notification
Create a secret -
portal.azure.com/#view/Microsoft_Azure_KeyVault/CreateSecretBlade/secret~/null/vaultId/%2Fsubscriptions%2F9a6ae428...
Microsoft Azure
Search resources, services, and docs (G+/)
da-4bd0-a3d3-fd93c59904cb 1/1
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home > devkeyvault20250130 | Secrets >
Create a secret
Upload options
Manual
Name *
test-secret
Secret value *
Content type (optional)
Set activation date
Set expiration date
Enabled
Yes
No
Tags
0 tags
Create
Cancel


azure_stanislav.k
Study - AnkiWeb
app.landingsite.a
CloudWatch | eu
Simple Website L
Stepan
Add role assignn
portal.azure.com/#view/Microsoft_Azure_AD/AddRoleAssignmentsLandingBlade/scope/%2Fsubscriptions%2F9a6ae428-d8c3-...
Microsoft Azure
Search resources, services, and docs (G+/)
d000f3c6-a4da-4bd0-a3d3-fd 1/1
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home > devkeyvault20250130 | Access control (IAM) >
Add role assignment
Showing a filtered list of roles because your permissions include a condition. Learn more
View my access
Selected role
Key Vault Secrets User
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
flask-aci-app-env
d000f3c6-a4da-4bd0-a3d3-fd93c59904cb
Container instances
Description
Optional
Review + assign
Previous
Next
Feedback


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home
Key vaults
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure subscription 1
Resource group *
StanislavKostenich
Create new
Instance details
Key vault name *
devkeyvault20250130
Region *
East US
Pricing tier *
Standard
Previous
Next
Review + create
Give feedback


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
StanislavKostenich@dm...
DEFAULT DIRECTORY (DMYTROS...
Home > StanislavKostenich > flask-aci-app-env
flask-aci-app-env | Identity
Container instances
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Containers
Identity
Properties
Locks
Monitoring
Metrics
Alerts
Logs
Automation
CLI / PS
Tasks
Export template
Help
Support + Troubleshooting
System assigned (preview)
User assigned (preview)
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.
Save
Discard
Refresh
Got feedback?
Status
Off
On
Object (principal) ID
Copied
d000f3c6-a4da-4bd0-a3d3-fd93c59904cb
Permissions
Azure role assignments
This resource is registered with Microsoft Entra ID. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more

3. Stop all ACI instances after completing the testing to reduce ongoing costs.

Practical Task 4: Secure a Docker Container in ACI with Managed Identity via Azure Portal

Requirements:

1. Deploy a Docker container to Azure Container Instances using the existing lightweight ACI setup from previous tasks.
2. Configure a Managed Identity for the ACI and securely access an Azure service (e.g., Azure Key Vault) with minimal permissions and access scope.

3. Retrieve only a single secret from Azure Key Vault for testing purposes.
4. Remove the ACI container after verifying secure access.