Lab #10: **Setup of Resource-Level Logging**

Purpose:

- We'll configure resource-level logging, which includes activity from the data plane (**Key Vault** and **Blob Storage**). These logs will be sent to our Logs Analytics workspace.

Tasks:

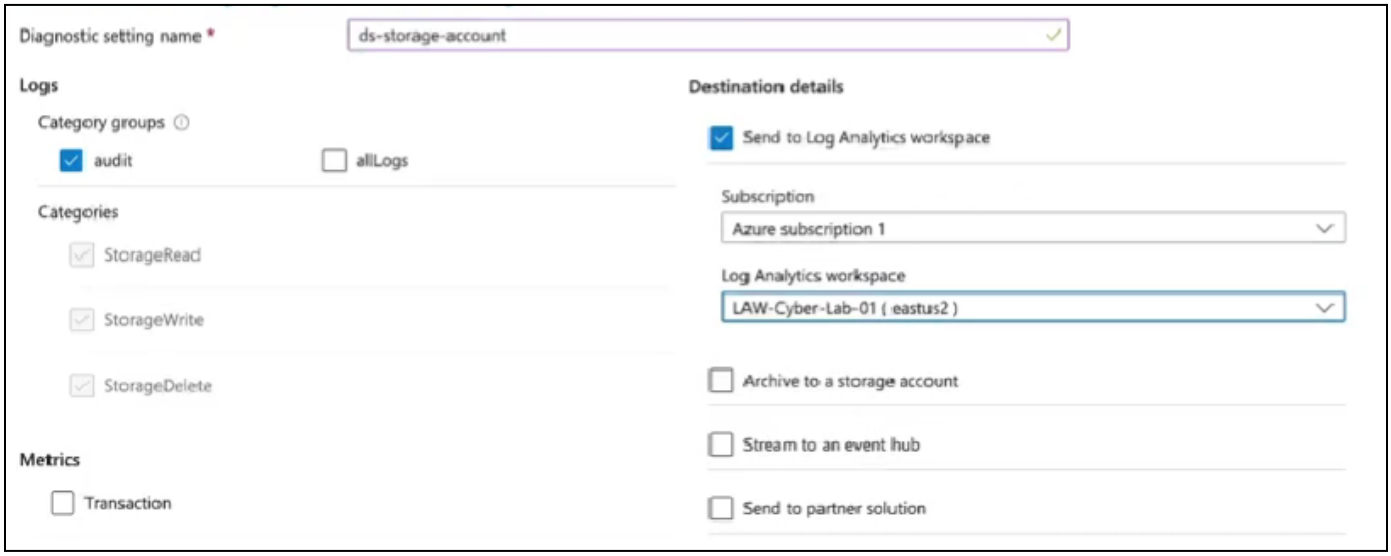
1. **Configure Logging for Azure Storage**
    - Send storage logs to Log Analytics workspace
    - Create a new container (and upload a file)
2. **Configure Logging for Key Vault**
    - Create a Key Vault Instance
    - Send Key Vault logs to Log Analytics workspace
    - Add a secret to Key Vault
3. **Observe the "Storage" and "Key Vault logs in Log Analytics Workspace**
    - Test the storage account logs
    - Test the Key Vault logs

Task 1: **Configure Logging for Azure Storage**

Send storage logs to Log Analytics workspace:

1. **Azure** account > **Storage accounts** > (select our storage account) > **Diagnostic Settings**
2. Select **blob** > **Add diagnostic setting**:

    a. **Name**: ds-storage-account
    b. Logs > **Category Groups**: (select the **Audit** box)
    c. Destination details > (select the **Send to Log Analytics workspace** box)
    d. Select **Save**.



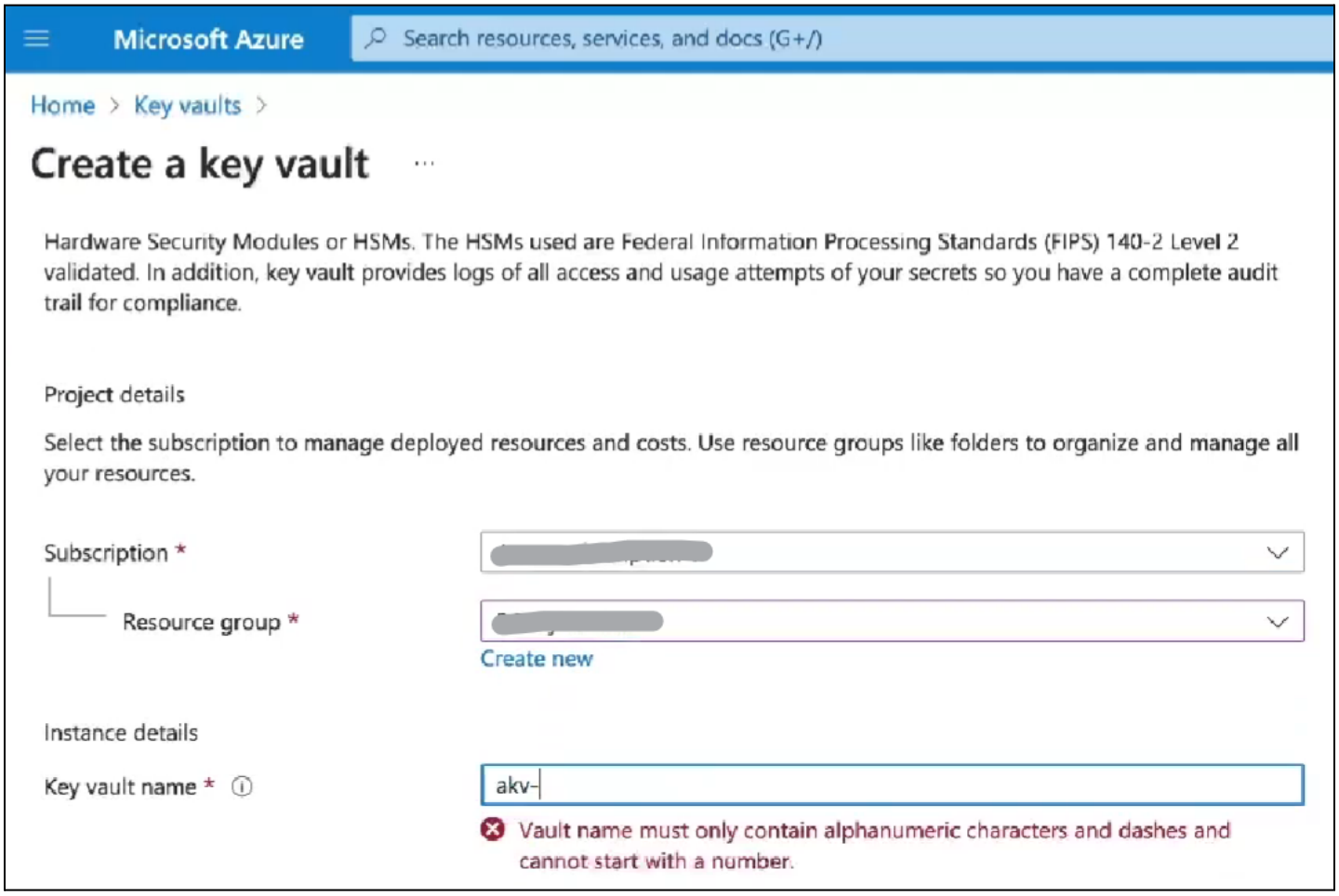
Create a new container (and upload a file):

1. **Azure** account > **Storage accounts** > **Containers** > **Create new container**:
    a. **Name**: test
2. Open the new container > **Upload** > (select a 'test-doc.txt' file that we created)
    a. Edit this document so it generates a log for us to view soon.

Task 2: Configure Logging for Key Vault

Create a Key Vault Instance:

1. **Azure** account > **Key Vault** > **Create**:
    a. **Name**: akv-..... (has to be globally unique)
    b. **Region**: East US 2
    c. **Pricing**: Standard
    d. (next page) **Permission model**: (select **Vault access policy**)
    e. Select **Review+Create**.



Send Key Vault logs to Log Analytics workspace:

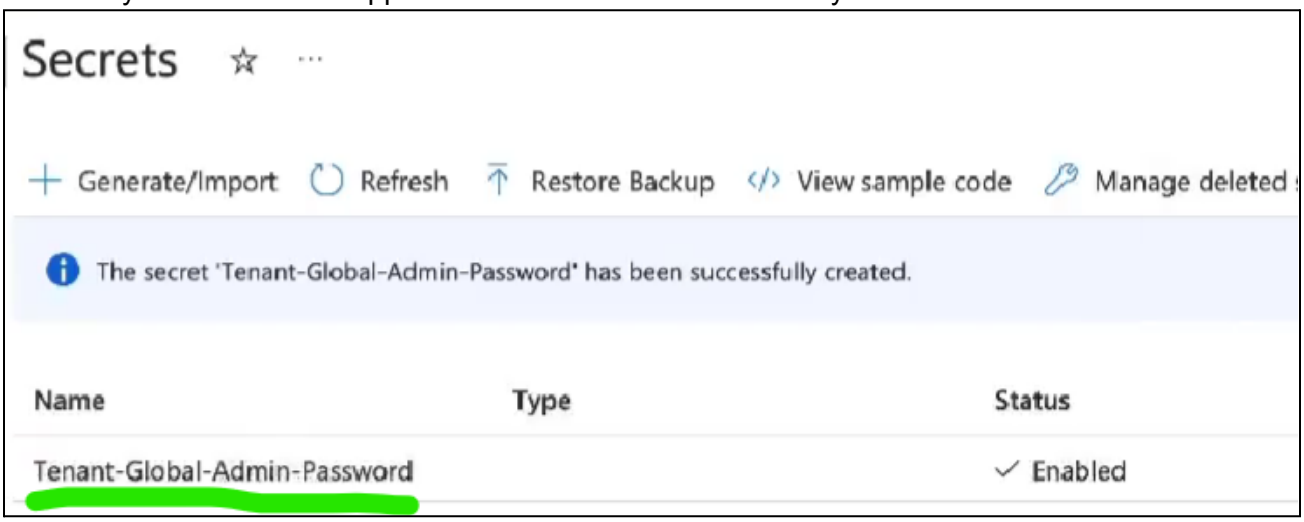
1. **Azure** account > **Key Vault** > (select our key vault) > **Diagnostic Settings**
2. Select **Add Diagnostic Settings**:
    a. **Diagnostic setting name:** ds-akv
    b. Logs > **Category Groups**: (select **Audit** checkbox)
    c. **Destination**: (select the **Send to Log Analytics workspace** checkbox)
        i. Select our subscription and workspace.
    d. Select **Save**.

Add a secret to Key Vault:

1. **Azure** account > **Key Vault** > (select our key vault) > **Secrets** > **Create a secret**:
    a. **Name**: Tenant-Global-Admin-Password
    b. **Secret Value**: (create a password)
    c. Select **Create**.

***Note**: This 'Secret' creation should've generated a log that we can view soon.*

2. This newly created 'secret' appears in our **Secrets** section of Key Vault:

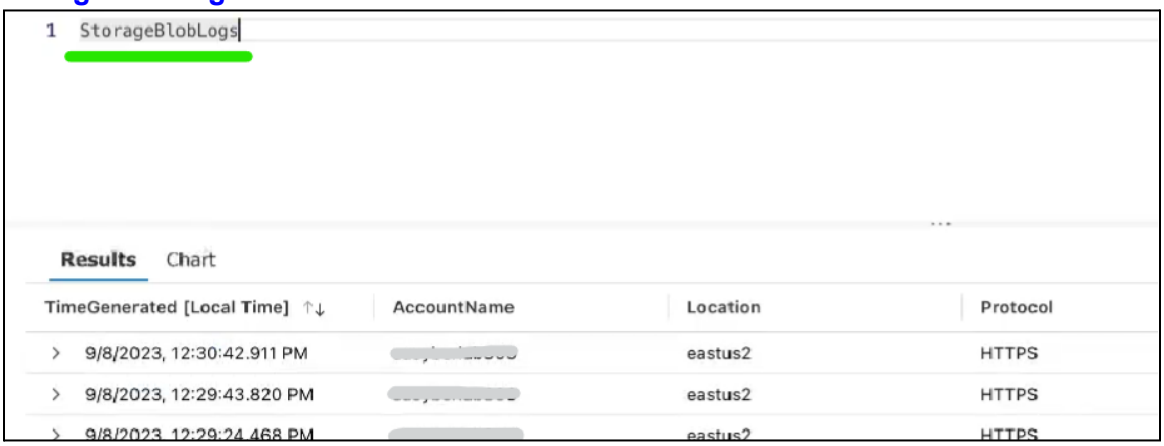


Task 3: Observe the "Storage" and "Key Vault logs in Log workspace

Test the storage account logs:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. **New Query** terminal >

a. View all storage logs:
StorageBlobLogs



b. View storage "Authorization Error" logs:
StorageBlobLogs
| where MetricResponseType **endswith** "Error"
| where StatusText **==** "AuthorizationPermissionMismatch"
| order by TimeGenerated asc

c. Reading a bunch of blobs:
StorageBlobLogs
| where OperationName **==** "GetBlob"

d. Deleting a bunch of blobs (in a short time period):
StorageBlobLogs | where OperationName **==** "DeleteBlob"
| where TimeGenerated **>** ago(24h)

e. Putting a bunch of blobs (in a short time period):
StorageBlobLogs | where OperationName **==** "PutBlob"
| where TimeGenerated **>** ago(24h)

f. Copying a bunch of blobs (in a short time period):
StorageBlobLogs | where OperationName **==** "CopyBlob"
| where TimeGenerated **>** ago(24h)

Test the Key Vault logs:

1. **Azure** account > **Log Analytics workspace** > select our workspace > **Logs** >
2. **New Query** terminal >
   a. List all Key Vault secrets:
   AzureDiagnostics
   | where ResourceProvider **==** "MICROSOFT.KEYVAULT"
   | where OperationName **==** "SecretList"

b. View passwords that **don't** exist:

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "SecretGet"
| where ResultSignature == "Not Found"
```

c. View passwords that **do** exist:

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "SecretGet"
| where ResultSignature == "OK"
```

d. View a specific password that does exist:

```
let CRITICAL_PASSWORD_NAME = "Tenant-Global-Admin-Password";
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "SecretGet"
| where ResultSignature == "OK"
```

e. Updating a password Success:

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "SecretSet"
```

f. Updating a specific existing password Success:

```
let CRITICAL_PASSWORD_NAME = "Tenant-Global-Admin-Password";
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "SecretSet"
| where id_s endswith CRITICAL_PASSWORD_NAME
| where TimeGenerated > ago(2h)
```

g. Failed access attempts:

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.KEYVAULT"
| where ResultSignature == "Unauthorized"
```

End:

- We configured our resource-level logs to be forwarded to our Log Analytics workspace.

  Note: *Soon, we'll set up our SIEM to query our Log Analytics workspace frequently (e.g., 1x/10min).*