**DefenderFileScanNotifier** Resource Deployment Guidance

As part of resource deployments, we have two bicep files as mentioned below

1. common.bicep
2. malwarescanner.bicep

* **common bicep file**

**Parameter file:** DFSNotifierResourcesDeployment\deployabletemplates\commonResources\parameters\common-westus2.parameters.json

**Bicep File:**

DFSNotifierResourcesDeployment\deployabletemplates\commonResources\common.bicep

* It will create these resource types: **App Configuration**, **Key Vault** & **Log Analytics workspace.**
* Please find naming conventions related parameters to avoid deployment errors

**featureName** is important parameter and used by all resource types

* + **App Configuration**: In Parameter file please update **featureName** as per your project requirement or go with any available name.

Final name will be decided by **appConfiguration.bicep** module file as mentioned below,

var appConfigurationName = environment != 'prod' ? '${featureName}-${subFeatureName}-configuration-${empty(shortLocation) ? deploymentLocation : shortLocation}-${environment}' : '${featureName}-${subFeatureName}-configuration-${empty(shortLocation) ? deploymentLocation : shortLocation}'

Example: **dfn-common-configuration-westus2**

**Refer App configuration resource naming rules**:

<https://azure.github.io/PSRule.Rules.Azure/en/rules/Azure.AppConfig.Name/>

* **Key Vault**:

Module file: DFSNotifierResourcesDeployment\modules\configurationstore\keyVault.bicep

var envBasedName = environment != 'prod' ? '${featureName}-${subFeatureNameForKeyVault}-${empty(shortLocation) ? deploymentLocation : shortLocation}-${environment}' : '${featureName}-${subFeatureNameForKeyVault}-${empty(shortLocation) ? deploymentLocation : shortLocation}'

var keyVaultName\_var = length(envBasedName) > 24 ? '${featureName}-${subFeatureNameForKeyVault}-${environment}' : envBasedName

Example**:** **dfn-kv-westus2**

**Refer App configuration resource naming rules**:

<https://azure.github.io/PSRule.Rules.Azure/en/rules/Azure.KeyVault.Name/>

* **Log Analytics workspace:**

Module file: DFSNotifierResourcesDeployment\modules\monitoring\loganalyticsworkspace.bicep

var logAnalyticsName = environment != 'prod' ? '${featureName}-${subFeatureName}${applicationType}-law-${deploymentLocation}-${environment}' : '${featureName}-${subFeatureName}${applicationType}-law-${deploymentLocation}'

Example: **dfn-commonservice-law-westus2**

You can update resource names as per your requirements.

Pre-requisites

Install Azure Modules through powershell script (Az modules)

Steps to execute common bicep:

1. Open Powershell or CMD CLI window and execute azure login

**az login --tenant <tenanted>**

1. Execute bicep:

az deployment group create --resource-group "<**ResourceGroupName**>" --template-file "<**localpath**>\DFSNotifierResourcesDeployment\deployabletemplates\commonResources\common.bicep" --parameters "<**localpath**>\DFSNotifierResourcesDeployment\deployabletemplates\commonResources\parameters\common-westus2.parameters.json"

A screenshot of a computer

Description automatically generated

* **malwarescanner.bicep**

**Parameter file:** DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\parameters\malwarescanner-easus.parameters.json

**Bicep File:**

DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\malwarescanner.bicep

Before executing above bicep file we need to update few attributes in “**malwarescanner-easus.parameters.json**” file as mentioned below.

**appconfigName** value should be updated asper resource created at **common bicep file** For example this value should be **dfn-common-configuration-westus2** because it’s created by common bicep file.

**commonLogAnalyticsWorkspace** This is also same as appconfigName.

For example: **dfn-commonservice-law-westus2**, it’s created by common bicep file.

**kvName** This is also same as appconfigName.

For example: **dfn-kv-westus2**, it’s created by common bicep file.

**Script to execute malwarescanner bicep file**

az deployment group create --resource-group "<**ResourceGroupName**>" --template-file "<**localpath**>\DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\malwarescanner.bicep" --parameters "<**localpath**>\DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\parameters\malwarescanner-easus.parameters.json"

A screenshot of a computer

Description automatically generated

And we need to configure **Microsoft Defender for Cloud** for storage account to send scan result to **Event Grid Topic**.

Storage account that is used for processing files to verify malware results,

Parameter Path: DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\parameters\malwarescanner-easus.parameters.json  
  
"**storageAccountNameFile\_Variable**": {

"value": "dfsnfilestorageacnt"

}

Bicep Path:

DFSNotifierResourcesDeployment\deployabletemplates\malwarescanner\malwarescanner.bicep

By using above bicep file, it will generate Event grid topic as mentioned below   
name: 'ScanResults-${dfsnProcessorStorageAccount.name}'

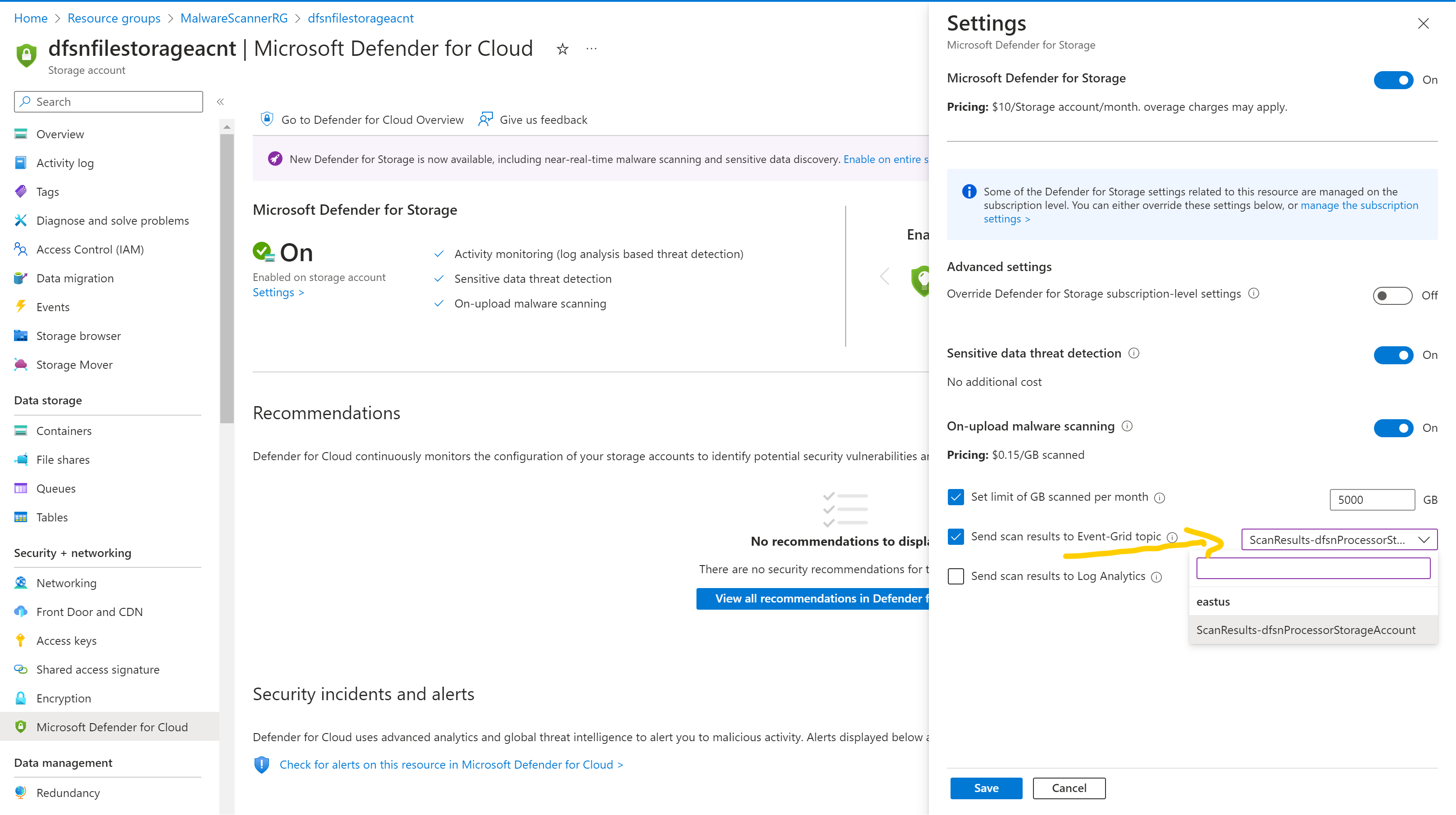
Finally the resource name will be : **ScanResults-<storageAccountNameFile\_Variable >**

Example: **ScanResults-dfsnProcessorStorageAccount**

Steps to configure **Microsoft Defender for Cloud** for storage account

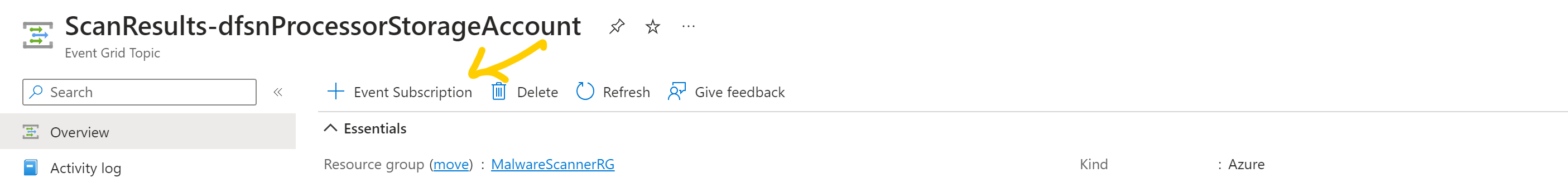
A screenshot of a computer

Description automatically generated



And save the configuration.

Next Deploy the azure function code base, And then configuration Subscription under Event Grid Topic: **ScanResults-dfsnProcessorStorageAccount**



A screenshot of a computer

Description automatically generated

Provide name and select azure function as an Endpoint Type, then Configure function name under endpoint settings save all these settings.

Add below settings in Azure App Configuration section for example: Example: This is App Configuration Name **dfn-common-configuration-westus2**

|  |  |  |
| --- | --- | --- |
| Sno | Configuration Name | Configuration Value |
| 1 | MalwareScanner:MalwareScannerConfigs:AntimalwareScanEventTypes | Microsoft.Security.AntiMalwareScan,Microsoft.Security.MalwareScanningResult |
| 2 | MalwareScanner:MalwareScannerConfigs:AntimalwareScanSuccessIdentifier | **No threats found** |
| 3 | MalwareScanner:MalwareScannerConfigs:ScannerContainerMapping | [{"sourceBlobContainerName":"malwarescanner","sourceStorageConstringAppConfigName":"BlobConfigOptions:ConnectionString","destinationBlobContainerName":"malwarefreedocuments","destinationStorageConstringAppConfigName":"BlobConfigOptions:ConnectionString","destinationFolderstructure":"userid/attachmenttype/","isTagEnabled":false}] |
| 4 | MalwareScanner:MalwareScannerConfigs:SourceBlobReadSasTokenPeriodInMinutes | 2 |
| 5 | Common:BlobConfigOptions:ConnectionString | Here we need to add keyvault reference of malware storage account (for example : here we select **CommonStorage** KeyVault secret key related to **dfsnrfilestgacnt** storage account connection string) |
| 6 | Common:BlobConfigOptions:ConnectionString | Here we need to add keyvault reference of malware storage account (for example : here we select **CommonStorage** KeyVault secret key related to **dfsnrfilestgacnt** storage account connection string) |
|  |  |  |