System Managed Identity Issue

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:28 AM PST

- Issue : customer is trying to configure auditing to storage account behind vnet and its failing for system managed identity with an error "identity not found" from the stoarge account we can see identity is enabled.

- Cause : there is a descrepency with the identity

- Solution :

  Resaving the Managed Identity might help to resolve any issues with it.. So can we please request the customer to perform these 3 steps:

  1. Turn off Managed Identity

```
# Log in first with Connect-AzAccount if not using Azure Cloud Shell$azContext = Get-AzContext
$azProfile = [Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::Instan
$profileClient = New-Object -TypeName Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient -Ar
$token = $profileClient.AcquireAccessToken($azContext.Subscription.TenantId)
$authHeader = @{
'Content-Type'='application/json''Authorization'='Bearer ' + $token.AccessToken
}
$body = '{
"identity": {
"type": "None",
},
"properties": {
"fullyQualifiedDomainName": "<SERVERNAME>.database.windows.net",
"administratorLogin": "<ADMINNAME>",
"administratorLoginPassword": "<SECUREPASSWORD>",
"version": "12.0",
"state": "Ready"
},
"location":"<LOCATION>"
}'# Invoke the REST API

$restUri = 'https://management.azure.com/subscriptions/<SUBSCRIPTION_ID>/resourceGroups/<RESOURCE_GROUP>/
$response = Invoke-RestMethod -Uri $restUri -Method PUT -Headers $authHeader -Body $body
```

  2. Turn it back on

     The only difference between step 2 and step 1 is the change in "type" ("type": "None" changes to "type": "SystemAssigned")

```
# Log in first with Connect-AzAccount if not using Azure Cloud Shell
$azContext = Get-AzContext
$azProfile = [Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::I
$profileClient = New-Object -TypeName Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClien
$token = $profileClient.AcquireAccessToken($azContext.Subscription.TenantId)
$authHeader = @{
'Content-Type'='application/json'
'Authorization'='Bearer ' + $token.AccessToken
}
$body = '{
"identity": {
"type": "SystemAssigned",
},
"properties": {
"fullyQualifiedDomainName": "<SERVERNAME>.database.windows.net",
"administratorLogin": "<ADMINNAME>",
"administratorLoginPassword": "<SECUREPASSWORD>",
"version": "12.0",
"state": "Ready"
},
"location":"<LOCATION>"
}'
# Invoke the REST API
$restUri = 'https://management.azure.com/subscriptions/<SUBSCRIPTION_ID>/resourceGroups/<RESOURCE_GR
$response = Invoke-RestMethod -Uri $restUri -Method PUT -Headers $authHeader -Body $body
```

3. Try resaving the audit policy by switching it 'off' and back 'on' through portal. Through Portal, the creation of this storage blob data contributor role will be done automatically.

How good have you found this content?