

Managed identity cannot be found due to tenant migration

Last updated by | Vitor Tomaz | Feb 18, 2021 at 3:24 AM PST

Contents

- **NOTE :**
- Issue:
- Known Issue:
- Mitigation:
 - Step-by-Step

****NOTE :**

Before using this TSG you need to verify that database doesn't have BYOK TDE when the server/database has TDE with BYOK (bring your own key) configuration. BYOK uses server's identity to get the key from azure key vault. When customer deleted the identity, database became unavailable**

Issue:

Vulnerability Assessment uses the managed identity of the SQL server to authenticate to the storage account by default.

Sometimes the authentication fails because the server's identity is in tenant XXXXXXXX while the server itself is in tenant YYYYYYYY.

Known Issue:

This is a known issue when you move the SQL server across tenant, the managed identity of the server does not move with it. The mitigation is to move it manually.

Mitigation:

To mitigate it, you need to unassigned the identity on the server, then re-assign it - which creates a new managed identity in your current tenant and re-save the VA policy - which connect the new managed identity to VA.

Step-by-Step

1. Delete the server's managed identity

For deleting the server's managed identity we need to used RESP API:

PUT <https://management.azure.com/subscriptions/<subscriptions-value>/resourceGroups/<resource-groups>/providers>

Body -

```
{
  identity: {
    type: "None",
  },
  location: "<resource-location>",
}
```

☐ Got to this [link](#) , using this link is easy to run a REST request.

☐ On the API description press "Try it"

The screenshot shows the Azure portal interface for the 'Servers - Create Or Update' page. The left sidebar contains a navigation menu with various Azure services. The main content area displays the 'Servers - Create Or Update' page for the 'SQL Database' service. The page includes a 'Try it' button, which is circled in red, and a 'URI Parameters' table. The 'Request Body' table is also visible.

URI Parameters

Name	In	Required	Type	Description
resourceGroupname	path	True	string	The name of the resource group that contains the resource. You can obtain this value from the Azure Resource Manager API or the portal.
servername	path	True	string	The name of the server.
subscriptionId	path	True	string	The subscription ID that identifies an Azure subscription.
api-version	query	True	string	The API version to use for the request.

Request Body

Name	Required	Type	Description
identity		Resource Identity	The Azure Active Directory identity of the server.
location	True	string	Resource location.
properties.administratorLogin		string	Administrator username for the server. Once created it cannot be changed.
properties.administratorLoginPassword		string	The administrator login password (required for server creation).
properties.minimalTlsVersion		string	Minimal TLS version. Allowed values: '1.0', '1.1', '1.2'
properties.publicNetworkAccess		ServerPublic Network Access	Whether or not public endpoint access is allowed for this server. Value is optional but if passed in, must be 'Enabled' or 'Disabled'
properties.version		string	The version of the server.

in Contents
Exit focus mode

Servers - Create Or Update

Service: SQL Database
API version: 2019-10-01-preview

Create or updates a server.

```

curl https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/{serverName}/api-version={apiVersion} \
  > 
```


URI Parameters

Name	In	Required	Type	Description
resourceGroup Name	path	True	string	The name of the resource group that contains the resource. You can obtain the value from the Azure Resource Manager API or the portal.
serverName	path	True	string	The name of the server.
subscriptionId	path	True	string	The subscription ID that identifies an Azure subscription.
api-version	query	True	string	The API version to use for the request.

Request Body

Name	Required	Type	Description
identity		ResourceIdentity	The Azure Active Directory identity of the server.
location	True	string	Resource location.
properties.administratorLogin		string	Administrator username for the server. Once created it cannot be changed.
properties.administratorLoginPassword		string	The administrator login password (required for server creation).
properties.minimalTlsVersion		string	Minimal TLS version. Allowed values: '1.0', '1.1', '1.2'.
properties.publicNetworkAccess		ServerPublicNetworkAccess	Whether or not public endpoint access is allowed for this server. Value is optional but if passed in, must be 'Enabled' or 'Disabled'.
properties.version		string	The version of the server.
tags		object	Resource tags.

Responses



- ```
Body -
{
 identity: {
 type: "None",
 },
 location: "<resource-location>",
}
```

## REST API Try It

Try the REST API with the inputs below.

Sign out

**Request URL**

PUThttps://management.azure.com/subscriptions/d32bb0ce-a0d0-4234-a7f4-1be3be0ec252/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/{serverName}

**Parameters**

resourceGroupName\*

serverName\*

subscriptionId\*DS-VulnerabilityAssessment\_Test\_assafak\_R&D\_60843

api-version\*2019-06-01-preview

name

value

+

**Headers**

Content-Type\*application/json

name

value

+

**Body**

```
{ "identity": { "type": "None", }, "location": "westus2"}
```

**Request Preview**

HTTP

Copy

☐ Run the command.

2. Re-save the VA policy

☐ Go to the SQL server in the portal

☐ Go to: Security → Advanced data security

The screenshot shows the Azure portal interface for a SQL server. In the left-hand navigation pane, the 'Security' section is expanded, and 'Advanced data security' is highlighted with a red box. The main content area displays a notification for the 'Advanced Data Security Free Trial' and a table of available resources.

| Name         | Type         | Status | Pricing tier |
|--------------|--------------|--------|--------------|
| SQL database | SQL database | Online | Basic        |

☐ Change storage account to "None"

The screenshot shows the 'Advanced Data Security' settings page. The 'Storage account' field is highlighted with a red box. The page includes sections for 'Vulnerability Assessment Settings' and 'Advanced Threat Protection Settings'.

**VULNERABILITY ASSESSMENT SETTINGS**

- Subscription: [Redacted]
- Storage account: [Redacted]
- Periodic recurring scans: ON
- Send scan reports to: [Redacted]
- Also send email notification to admins and subscription owners: [Checked]

**ADVANCED THREAT PROTECTION SETTINGS**

- Send alerts to: [Redacted]
- Also send email notification to admins and subscription owners: [Checked]
- Advanced Threat Protection types: All

Home / [redacted] / Advanced data security / Choose storage account / Create storage account

### Choose storage account

These are the storage accounts in the selected subscription and location 'West US 2'.

+ Create new

None

West US 2, Sta...

### Create storage account

Name \*

.core.windows.net

Account kind

Storage (general purpose v1)

Performance

Standard Premium

Replication

Locally-redundant storage (LRS)

OK

- ☐ Save the new setting.
- ☐ Set the correct storage account again.
- ☐ Save the new setting

**How good have you found this content?**

