

# Connector MSI authentication failed due to ADF moved to different tenant

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST

## Contents

- [Issue](#)
- [Root Cause](#)
- [Suggestion](#)

## Issue

Connector (storage, sql, etc.) MSI authentication failed

If you look into this issue, you can get the following detail info:

```
ApiOperationEvent
| where env_time > ago(15h)
| where SubscriptionId =~ 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx'
| where DataFactoryName =~ "<dataFactoryName>"
| where operationName contains "createOrUpdate"
| where resultType != 'Success'
```

Get any TraceCorrelationId about the failed one.

```
AdfTraceEvent
| where TraceCorrelationId == "f7ddb856-dd2e-495b-8ab1-7ef5596bc5b6"
```

Error details:

```
ResourceControllerBase.CreateMsiAsync[426]: Failed to write MSI identity to MSI store: resource name: <dataFac
Exception translates to response with HttpStatusCode: InternalServerError, Action: CreateOrUpdateDataFactoryAs
at Microsoft.DataTransfer.MsiStoreService.Client.ManagedServiceIdentityOperations.<CreateOrUpdateWithHttpMe
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at Microsoft.DataTransfer.MsiStoreService.Client.ManagedServiceIdentityOperationsExtensions.<CreateOrUpdate
--- End of stack trace from previous location where exc
```

```
cluster('Azuredmprod').database("AzureDataMovement").MsiTraceInfo
| where DatafactoryName == "<dataFactoryName>"
| where SubscriptionId == 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx'
| where Operation == "PutManagedServiceIdentity"
| project SubscriptionId, DatafactoryName, IdentityPrincipalId, IdentityTenantId, Detail, StatusCode
```

## You will see a lot of failure:

SubscriptionId	DataFactoryName	IdentityPrincipalId	IdentityTenantId	Detail	StatusCode
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500
5b4b0c5f-1e10-4b10-8110-4110	mbwaychallengeadfprodv2	e72b053b-2bbe-4666-a4f2-1cd74df6f664	ea590c8e-692e-402e-a380-f42240d66165	Error getting value from 'RenewAfter' on 'Microsoft.Hdis.AgentService.BusinessLogic.Store.Msi.ManagedServiceIdentity'.	500

```
cluster('Azuredmprod').database("AzureDataMovement").MsiTraceVerbose
| where ActivityId in ((
MsiTraceInfo
| where DataFactoryName == "<dataFactoryName>"
| where SubscriptionId == 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx'
| where Operation == "PutManagedServiceIdentity"
| where StatusCode == long(500)
| distinct ActivityId
| take 1
))
```

In Detail column, we can get the identityUrl = <https://control-westeurope.identity.azure.net/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx/resourcegroups/<ResourceGroupName>/providers/Microsoft.DataFactory/factories/<dataFactoryName>/credentials/v2/systemassigned?arpid=fca13624-4990-4747-95d4-020eddfca98d&said=f4e8dab4-acf6-4e1c-a676-44e8f2b7dde0>

Begin call ManagedServiceIdentityLogic.PutManagedServiceIdentityAsync, with subscriptionId=xxxxxxxx-xxxx-xxxx-



In Error column, we can see MSI returns HTTP Code: Forbidden, Reason: Forbidden.

```
In PutManagedServiceIdentityAsync, MsiServiceRPCClient.GetIdentityMetadataAsync caught MsiServiceException: HTT
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at Microsoft.DataTransfer.MsiServiceClient.MsiServiceRPCClient.<>c__DisplayClass2_0.<<GetIdentityMetadataAsy
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at Microsoft.DataTransfer.MsiServiceClient.MsiServiceRPCClient.<GetIdentityMetadataAsync>d__2.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at Microsoft.Hdis.AgentService.BusinessLogic.Logics.ManagedServiceIdentityLogic.<PutManagedServiceIdentityA
```



## Root Cause




We have a data factory for example: "mbwaychallengeadfprodv2" which was moved between tenants, causing ADF failed to use identityUrl to call Msi service RP to get managed identity, with following exception:

MsiServiceRPCClient.GetIdentityMetadataAsync caught MsiServiceException: HTTP Code: Forbidden, Reason: Forbidden  
Please help to investigate and delete the old managed identity.  
Identity Url: https://control-west europe.identity.azure.net/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx

## Suggestion

If you encounter such issue, firstly confirm with customer on whether they have moved data factory from other tenants. If yes, please go ahead to raise ICM to MSI PG that we need to delete the MSI from old tenant in order to refresh a new one on new tenant. Before doing that, we need to get approval from customer to delete the old MSI from old tenant.

How to create ICM to MSI PG:

- Template: <https://portal.microsofticm.com/imp/v3/incidents/create?tmpl=r2R1P1> 
- Provide the principalId, tenantId and identityUrl we get from MsiTraceInfo and MsiTraceVerbose
- Sample: <https://portal.microsofticm.com/imp/v3/incidents/details/200590930/home> ,  
<https://portal.microsofticm.com/imp/v3/incidents/details/171724619/home> 

After MI team cleans up the now-orphaned backing service principal in the old tenant, customer should publish new pipeline changes or follow this document to generate the managed identity:

<https://docs.microsoft.com/en-us/azure/data-factory/data-factory-service-identity#generate-managed-identity-using-powershell> 

Set-AzDataFactoryV2 -ResourceGroupName <resourceGroupName> -Name <dataFactoryName> -Location <region>

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

