Regression with Managed Instance identity (service principal)

Last updated by | Vitor Tomaz | Feb 13, 2023 at 1:31 AM PST

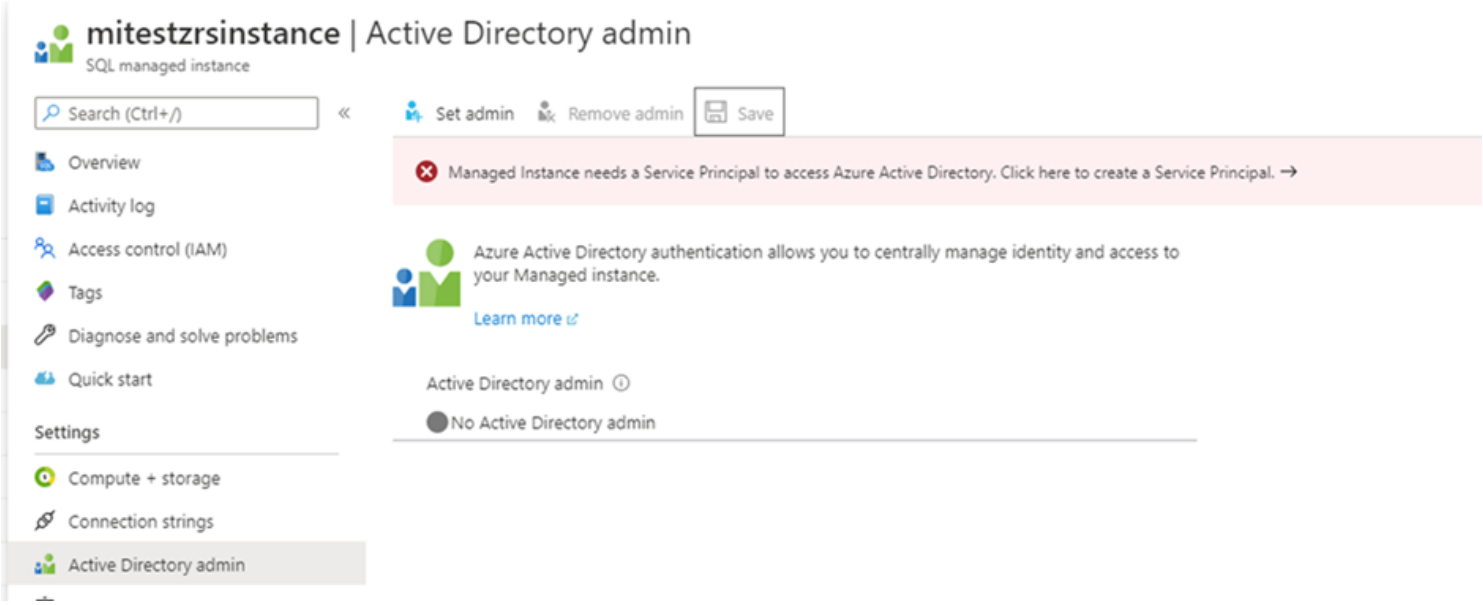
What has happened

Your Managed Instance is experiencing issues with Service Principal used to access Azure Active Directory and Azure Key Vault services. As a result following features may be impacted:

1. Azure Active Directory authentication - you may be experiencing intermittent connectivity issues, or not be able to run statements like CREATE LOGIN/USER FROM EXTERNAL PROVIDER or EXECUTE AS LOGIN/USER.
2. Transparent Database Encryption - setting up TDE with customer-managed key on a new instance. This feature will not be impacted on existing instances.

Mitigation

We have already deployed the fix that prevents this URL from being removed, however instances where URL was already removed may hit issue if certain conditions are met (explained below in the section Root cause details). We are proactively working on mitigating affected instances, however, we may not be 100% successful, as there are instances where identity URL cannot be retrieved. In those cases we need the customer to mitigate this manually from Azure Portal using the following instructions. Go to Azure Portal, access SQL Managed Instance Active Directory admin blade. Verify if you can see the error message "Managed Instance needs a Service Principal to access Azure Active Directory. Click here to create a Service Principal" as on the example screenshot below. In case you have encountered this error message, click on it, and follow the step by step instructions provided until this error have been resolved.



PowerShell or CLI from Azure Portal is a fast & easy to try the mitigation

1. Open Cloud Shell

2. Update the instance name and resource group name and use on of the following commands

- (PowerShell): Set-AzSqlInstance -Name "a" -ResourceGroupName "a" -AssignIdentity
- (CLI): az sql mi update --assign-identity --name a--resource-group a

Next steps

To minimize the impact we will proactively monitor the system and mitigate the issue when we detect it. The bug that is causing this issue is understood, fix is coded and deployed. In case this issues is still active on your SQL MI please see the instructions in the Mitigation section.

Root cause details

Identity service provides an URL where SQL Managed Instance (SQL MI) service pulls credentials from for the system-assigned identity (Service Principal). The SQL MI service uses this URL to periodically refresh the certificate. Due to a bug in our code, this URL was removed from SQL service by unrelated internal operation. Removal of the URL property will not immediately lead to issues, as MI process will retain previous certificate for a while. The issue will occur when one of two conditions are met:

1. Customer changes the SQL MI pricing tier (e.g. resize operation);
2. Current certificate expires.

We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future.

How good have you found this content?