Managed Instance Restore

Last updated by | Radhika Shah | Feb 17, 2023 at 10:03 AM PST

Contents

IMPORTANT: Only the subscription owner/admin can approve the request for recovering a dropped Azure SQL Managed Instance. From PG side, this is an important step to ensure that we are not restoring the server to an un-authorized customer. Getting subscription owner permission is essentially our only security. Get this approval as soon as possible.

Issue

Restore of managed instances is not an officially supported feature and we are doing this on a best-effort basis. These kind of incidents are therefore not sev2. Please read through the warnings below carefully and closely follow the instructions. PG have a CAS command that they execute to restore the managed instance with all its databases, but it is does not always work perfectly and some extra steps are needed before they are executing it. Also, the restore doesn't work as SQL DB server restore does, here the PG create a new instance with the same setup as the dropped instance and then they restore system and all user databases on top.

This TSG consists of explaining the restore process and how to monitor the restore progress.

Note: If the customer has set up BYOK (which can be checked in CMS managed_servers view, field encryption_protector_type - if it is AzureKeyVaultUri than the customer has BYOK - AKV setup) PG can perform the restore of only system databases and unencrypted user databases, the restore of encrypted user databases will fail. In this case after the instance is restored with system databases (encrypted user database restores are failed due to missing certs) PG need to hydrate ARM and ask customer to setup the access to the AKV, once the customer does that PG can perform the restore of encrypted user databases using a CAS for individual restore of a dropped databases from a dropped server.

Customer Ready content (Before filing ICM)

Thank you for reaching out to us. Restoring a dropped instance is not something that we generally support at this moment, and work that will be done to restore this instance will be on a best effort basis. If the server was

dropped more than 7 days ago, we will not be able to recover the server or the database(s). The restored instance will be created in an adhoc manner and there is no guarantee that any complex scenario associated with the original instance will be working with the new instance. Hence, we will not be providing any SLA for it.

Please share/confirm the following information:

- Azure Region (e.g. West Europe)
- Server Name
- Is this a Production server? (Yes /No)
- Do you need all databases within the server to be restored? If not, please share the list of the databases that needs to be recovered.
- Was the server dropped directly? Or did you attempt to drop the resource group which resulted in force drop of the server?
- How was the server dropped (e.g. via portal, terraform script, third party tool etc.)?
- Approximate date and time that the server was dropped?
- Have you tried to re-create the server with the same name after the original server was dropped? If yes, for future occurrences, you should avoid re-creating server with same name if it needs to be recovered.
- What was the encryption type on the server (Service-managed key or Customer-managed key (BYOK))?
- Could you please provide a business justification for the requested restore.
- Request Approval from **Subscription Owner** for any restore operation of dropped server.

Please note: The instance, once restored, will be named with a "-restored" suffix appended to the original instance name. The restored instance will be in UTC time zone, regardless of the original instance time zone.

Investigation/Analysis

Check/confirm when the managed instance was dropped via below kusto:

```
MonManagementOperations
| where operation_parameters contains '{ServerName}'
| where operation_type == 'DropManagedServer'
| project TIMESTAMP , subscription_id , request_id , operation_type , event, database_name , operation_paramet
```

Restoring the dropped server

1. The procedure requires that there is no newly created server of the same name. Check if there is a newly created server of the same name. (the dropped one is in 'WaitingForCleanup' state)

CMS query:

```
select name, state, managed_server_id, create_time, dropped_date
from managed_servers
where name = '<***server_name***>'
```

Kusto Query:

```
MonManagedServers
| where LogicalServerName == '{ServerName}' or name == '{ServerName}'
| summarize arg_max(TIMESTAMP,*) by name
| project TIMESTAMP, customer_subscription_id, managed_server_id, name, state, encryption_protector_type, crea
```

2. If the managed server is "stuck" in WaitingForInstanceCapacity PG might have to resize the ring which can take up to 2h or if a new PDC is necessary it might take up to 6h.

3. A single user databases restore failing does not mean the entire instance restore will fail. The restore works on a best effort basis. If this happens PG can perform individual restores of the databases from the dropped server to the restored server. For example, if user the has BYOK - AKV encryption setup the instance restore will only restore system databases and unencrypted user databases at which point PG need Hydrate ARM and ask the customer to setup AKV on the restored instance and issue individual restore requests for the encrypted databases. Below we have couple of known issue for failing restores.

4. Once the Managed Instance is restored, the restored managed instance does not have identity & AAD Admin. Customer will need to reset the identity and set the AAD Admin again on the restored instance. See the Steps to set up AAD Admin.

Monitoring Progress

Once the restore starts, you can monitor it using the following CMS query:

```
select state, last_exception, last_state_change_time, request_id, managed_server_id
from managed_servers
where name = '<restoring_server_name>'
```

Or using below kusto query:

```
MonManagedServers
| where LogicalServerName == '{restoring_server_name}' or name == '{restoring_server_name}'
| summarize arg_max(TIMESTAMP,*) by name
| project TIMESTAMP, customer_subscription_id, managed_server_id, name, state, last_exception, last_state_chan
```

Databases which were dropped at the moment of dropping the server are not restored during instance restore as the last state of the server is taken into consideration when issuing instance restore. Confirm with the customer if all the databases were restored.

Checking cleanup period for dropped instance

Check CleanupServerExpiry FSM property in CMS, that is going to be cleanup date.

```
select fsm_extension_data, name from managed_servers
where name = '<managed_server_name>'
```

Using Kusto:

```
MonManagedServers
| where LogicalServerName == '{ServerName}' or name == '{ServerName}'
| where state == 'WaitingForCleanup'
| summarize arg_max(TIMESTAMP,*) by name
| extend result = parse_xml(fsm_extension_data).FiniteStateMachineExtensionData.Properties.PropertyExtendedDat
| mv-expand result
| where result contains"CleanupServerExpiry"
| extend CleanupServerExpiryDate = tostring(parse_xml(result).Value)
| project TIMESTAMP, customer_subscription_id, managed_server_id, name, CleanupServerExpiryDate, dropped_date,
```

Mitigation

Warning: Create the ICM with the Backup/Restore team as soon as possible, since there is a limited time available before the cleanup process removes the backups and the information from the dropped Managed Instance that are required to increase the success of the recovery operation.

Use the information collected from customer to create the ICM so Engineering team is aware about the details and scenarios associated with the dropped instance.

Note: ICM to restore dropped instance is not eligible for Sev2 **unless** we are closing in on the 7-day mark since the server drop. If this is the case, please make a note of it on the ICM.

Warnings and heads-up for CSS and Customer

Warning: Restoring a dropped instance is not something we offer to customers. We do this on a best-effort basis. No SLA is given to the restored instance. Customer should be informed on this!

- Restoring a dropped instance is not something that we generally support at this moment, and work that will be done to restore this instance is on a best effort basis. The restored instance will be created in an ad hoc manner and there is no guarantee any complex scenario is working for that instance, so we will not be providing any SLA for it.
- Given the upper "no SLA" statement, once the restored instance is up, the customer is advised to evacuate the data to a new instance - e.g. using a cross instance PITR: https://techcommunity.microsoft.com/t5/Azure-SQL-Database/Cross-instance-point-in-time-restore-in-Azure-SQL-Database/ba-p/386208
- Once the data is evacuated by some means, the customer should drop the restored instance. **Note that this temporary created instance is customer billed**, so customer should drop it as soon as it's not needed anymore.
- If the customer starts creating a new instance immediately or at any point before the restored instance is up, they should NOT give the instance the same name as the original instance. The restored instance will be named with a "-restored" suffix appended to the original instance name. The restored instance will be in UTC time zone, regardless of the original instance time zone.

Customer Ready content (after managed instance is restored)

If customer the has BYOK - AKV encryption setup, the instance restore will only restore system databases and unencrypted user databases at which point PG will need to Hydrate ARM and ask the customer to setup AKV on

the restored instance. Once the customer completes AKV set up, PG will issue individual restore requests for the encrypted databases.

Scenario1 - Dropped instance had BYOK, pending restore of encrypted DBs

We have managed to restore the dropped instance as *<new restored instance name>*. We noted that the dropped instance was encrypted using Customer-managed key (BYOK). Please enable access to AKV for the newly restored instance in order for us to further proceed restoring the dropped databases.

Scenario2 - All restore completed successfully

We have managed to successfully restore the managed instance and all requested databases with it.

Please review below carefully:

- The restored instance has been created, but we do not provide any SLA for this restored instance. Once the restored instance is up, you are advised to evacuate the data from the restored instance to a new instance as soon as possible - e.g. using a cross instance PITR.
- Once the data is evacuated by some means, the customer should drop the restored instance. **Note that this temporary created instance will be billed**, so you should drop it as soon as it's not needed anymore.
- If you had identity and AAD admin on the older (dropped) instance, the restored managed instance does not have identity & AAD Admin. You will need to reset the identity and set the AAD Admin again on the restored instance. Please see below steps to set up AAD Admin.

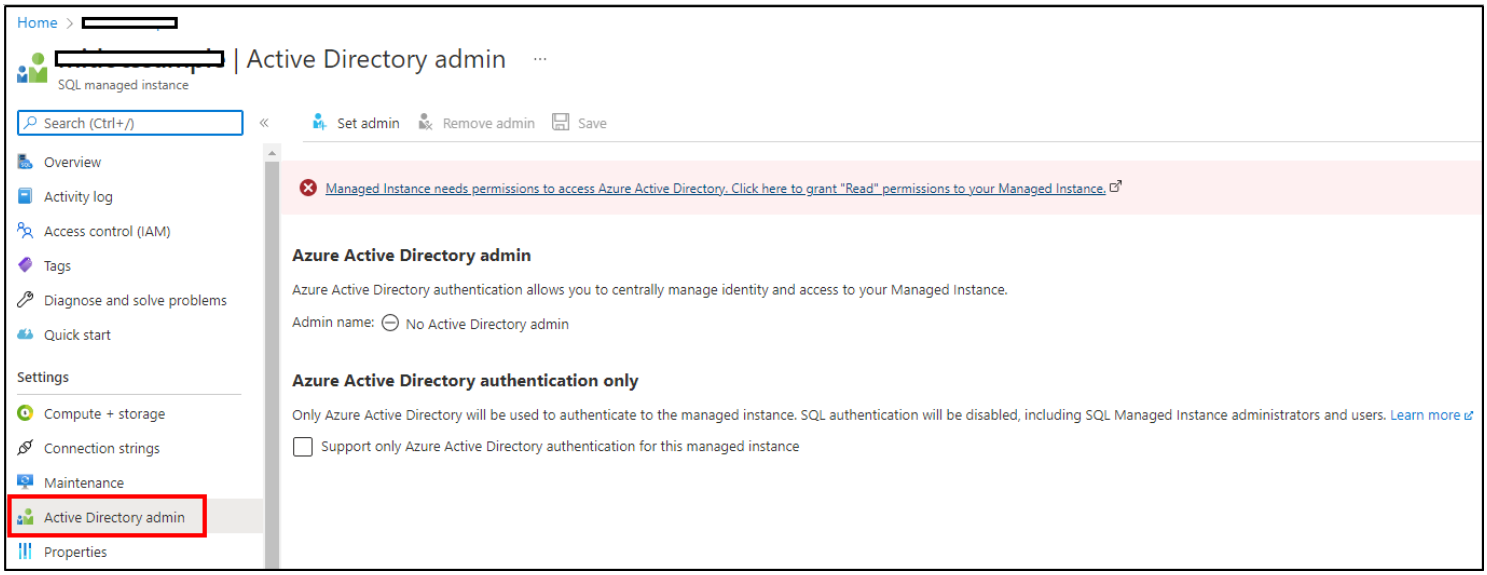
Steps to set up AAD Admin

Below are the steps:

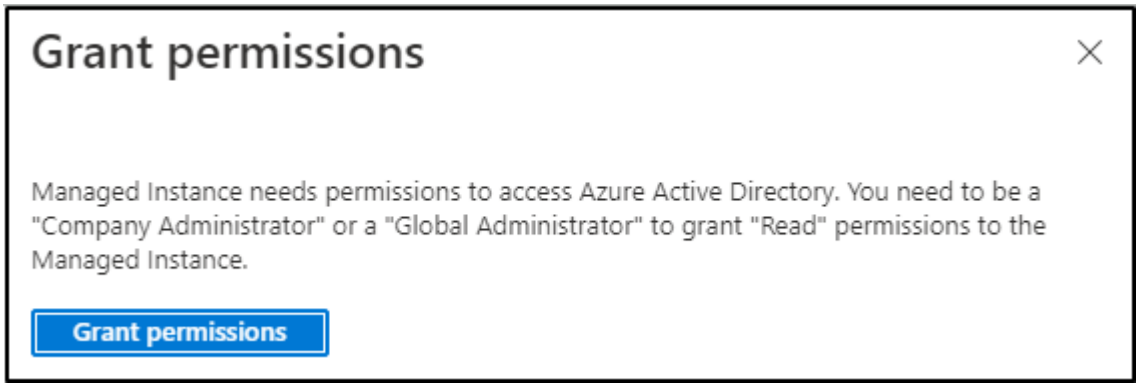
- To reset identity:

```
Connect-AzAccount - TenantId {CustomerTenantId} -SubscriptionId {CustomerSubscriptionId}

Set-AzSqlInstance -Name {RestoreManagedInstanceName} -ResourceGroupName {ResourceGroupName} -AssignIdentity -I

Set-AzSqlInstance -Name {RestoreManagedInstanceName} -ResourceGroupName {ResourceGroupName} -AssignIdentity -I
```

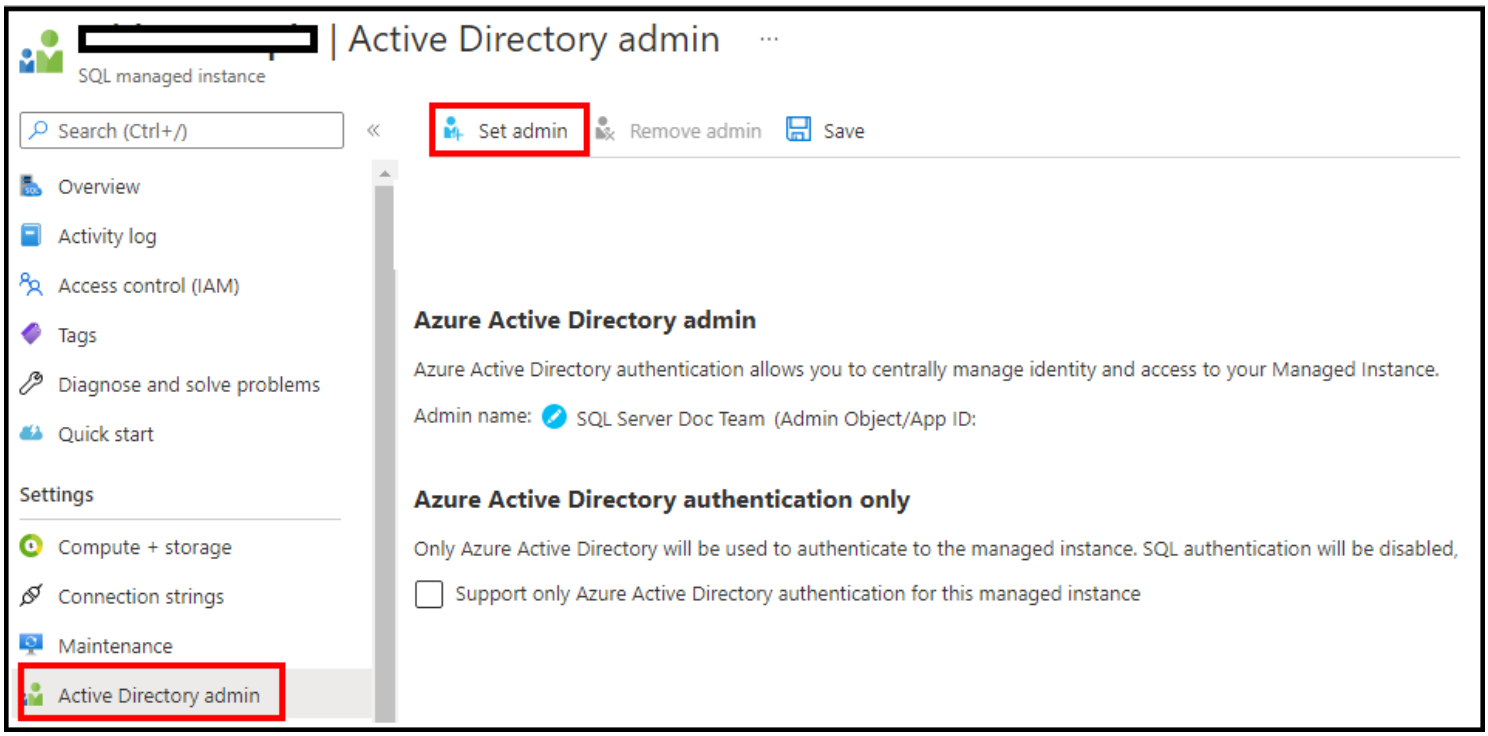
- Once the identity is assigned, set the AAD Admin. From Azure portal, click on 'Active Directory admin':



Grant permissions:



Then set the AAD admin using the 'Active Directory admin' blade:



RCA

This RCA should only be shared when the restore is not possible. (For example, if the restore request is from beyond 7 days).

Dear <customer>,

Restoring deleted SQL Managed Instance from short-term backups (PITR) is currently not supported. This is because once a Managed Instance is dropped all short-term backups are placed on the drop path as well. Hence, there is no guarantee that the data will be available. And hence, no guarantee can be given to customers that we can recover the instance.

For future reference, in case you have sensitive data that you would like to protect against occurrence such as this one, please consider using our long-term backup service LTR (Long Term Retention). This service can retain your backups up to 10 years and they can be restored even in the case managed instance has been dropped. Alternatively, if you do not want to use the LTR service, you can manually backup your sensitive data (using copy-only backup) to Azure blob storage, or other storage type of your choice.

While we are doing everything in our power to exceed expectations of our customers, in this case we were not able to help. We thank you for your patience and understanding.

Public Doc Reference

Deleted database restore

How good have you found this content?