SQL Managed Instance provisioning via portal stuck on external admin States

Last updated by | Akio Hose | Dec 22, 2021 at 10:45 PM PST

Contents

Note: A fix for this issue has been deployed, thus for any stuck/failed provisioning of SQL MI from Portal should be investigated from scratch. This TSG is provided as an FYI.

Issue

We expect to see some incidents on the Managed Instance Provisioning Path where the ‘UpsertManagedServerRequestStateMachine’ gets stuck in WaitingForExternalServerAdminCreate or related states involving an “External Administrator”, rolls back and fails MI creation when the customer supplies an external administrator with special characters i.e. ‘[]’.

Root Cause

These incidents occur due to a bug on portal, where in cases when the user Display Name has a '[]' or an unsupported T-SQL character in the name, the AAD Admin creation fails. This happens since in the recent portal deployment we started using "Display Name" in the external admin name instead of UPN i.e. User Principal Name.

Investigation

In case you get a similar incident please perform the following:

1. Confirm that the Managed Instance create operation was attempted via portal.
2. It is likely that the operation times out and rollbacks MI creation since the AAD Admin name is buggy, so we need to query Kusto - MonManagement Logs and not CMS itself.

```
let req_id = '<Request ID>';
MonManagement
| where TIMESTAMP > ago(3h)
| where request_id contains req_id
| project TIMESTAMP, error, exception, exception_message, stack_trace, error_message, message,ClusterName
| where stack_trace != "" or message != ""
| order by TIMESTAMP desc
```

Here the callstack will show the following exception:

Exception rethrown at [0]:

```
at
Microsoft.Xdb.NodeAgent.Exports.INodeAgentService.ManagedInstanceExternalAdminLoginPrincipalType(String instanceName, String masterDbName, Guid externalAdminSid, String externalAdminName, Nullable`1 principalType, Boolean isRollback, Guid oldExternalAdminSid)
at Microsoft.Xdb.InstanceManager.ManagedServerExternalAdminStateMachine.
<>c__DisplayClass91_0./<AddExternalAdministratorToMetadata/>b__1(INodeAgentService na) in
d:\dbs\sh\5uj5\1209_185906\cmd\8\sql\xdb\manifest\svc\mgmt\fsm\ManagedServerExternalAdminStateMachine.cs:line 1390
at Microsoft.SqlServer.Management.Service.FiniteStateMachines.BasePhysicalDatabaseStateMachine.
<>c__DisplayClass41_0.<TryExecuteOnNodeAgent>b__0(INodeAgentService na) in
d:\dbs\sh\5uj5\1209_185906\cmd\8\sql\xdb\manifest\svc\mgmt\fsm\BasePhysicalDatabaseStateMachine.cs:line 189
at Microsoft.SqlServer.Management.Service.Clients.NodeAgentConnectionFactory.NodeAgentConnection.
<>c__DisplayClass2_0`2.<ExecuteNodeAgentAction>b__4(X509Certificate2 cert) in
d:\dbs\sh\5uj5\1209_185906\cmd\5\Sql\xdb\manifest\svc\mgmt\clients\NodeAgentConnectionFactory.cs:line 169
```

3. Check with the customer if the AAD Admin Name they were using contains '[]' or any special characters not supported by T-SQL.

Mitigation

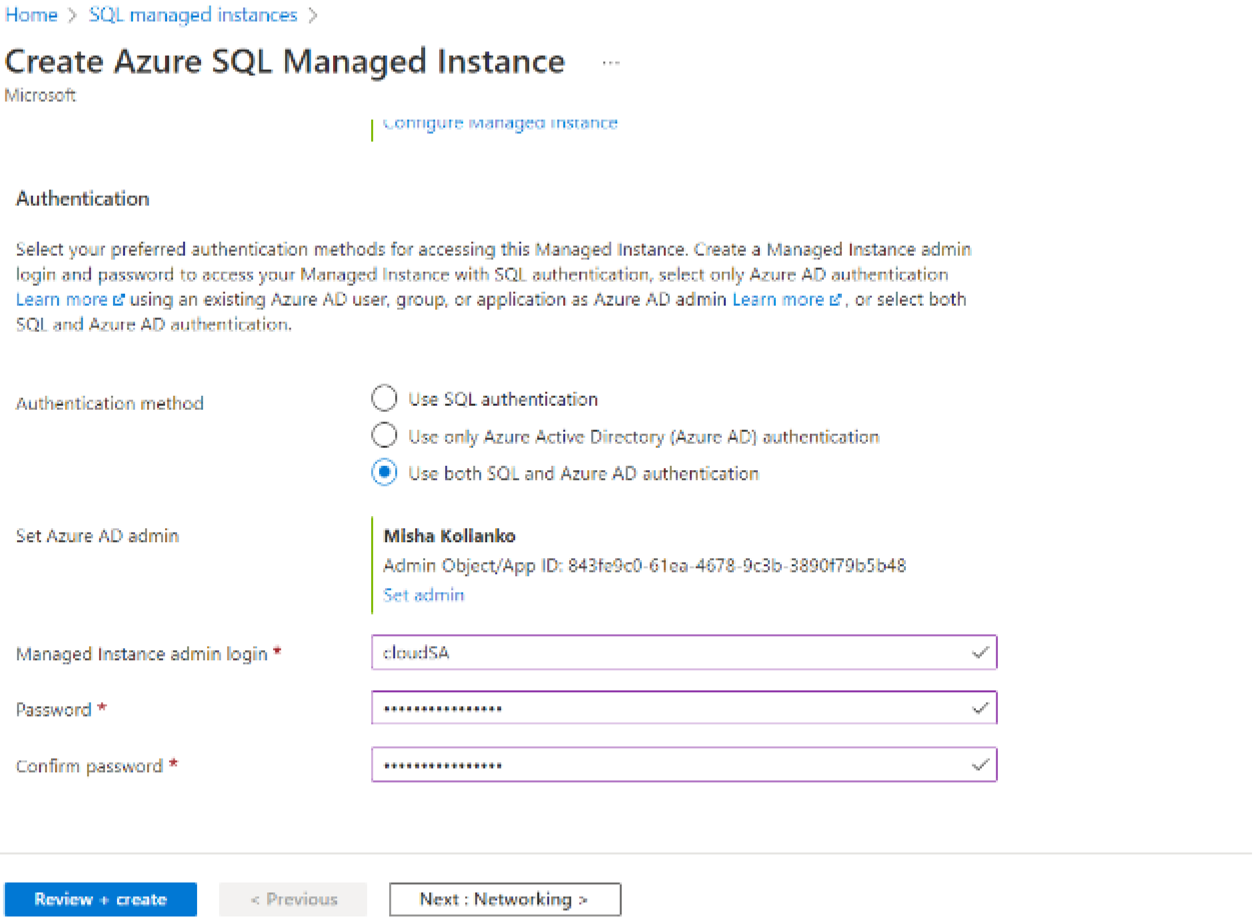
In case the customer wants to use an AAD Admin which has '[]' or certain special characters in the Display Name during Managed Instance create, please ask them to attempt the operation with UPN i.e. User Principal Name using Powershell, Rest APIs or ARM Templates until the portal side fix is deployed.

Documentation and samples for the same can be obtained here: [Create server with Azure AD-only authentication enabled in Azure SQL](#)

Work around steps from Portal

In case the customer wants to use the portal, they can use the following workaround:

1. Fill out all the parameters on all the different pages as usual:



Home > SQL managed instances >

Create Azure SQL Managed Instance ...

Microsoft

Configure managed instance

Authentication

Select your preferred authentication methods for accessing this Managed Instance. Create a Managed Instance admin login and password to access your Managed Instance with SQL authentication, select only Azure AD authentication Learn more using an existing Azure AD user, group, or application as Azure AD admin Learn more, or select both SQL and Azure AD authentication.

Authentication method
○ Use SQL authentication
○ Use only Azure Active Directory (Azure AD) authentication
● Use both SQL and Azure AD authentication

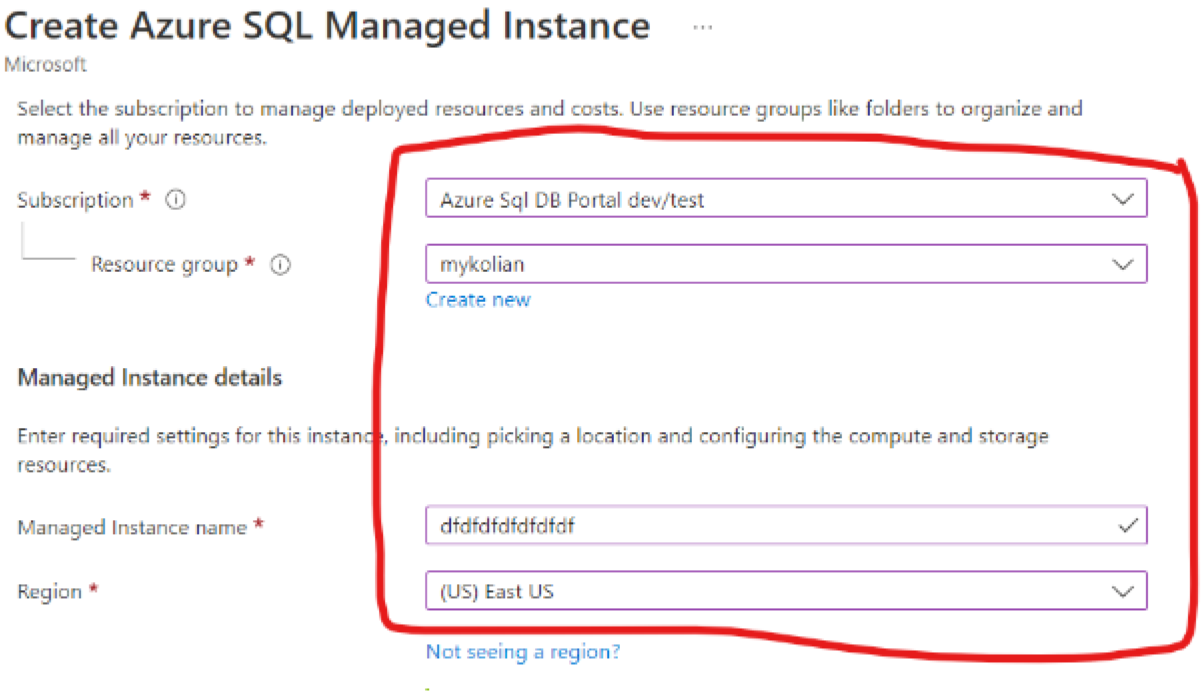
Set Azure AD admin: Misha Kollanko
Admin Object/App ID: 843fe9c0-61ea-4678-9c3b-3890f79b5b48
Set admin

Managed Instance admin login *: cloudSA

Password *: ••••••••••••••••

Confirm password *: ••••••••••••••••

2. Remember this information from Basics Tab: subscription, resource group, region, if used as both AAD and Sql Server auth remember password (or create new one later).



Create Azure SQL Managed Instance ...

Microsoft

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Azure Sql DB Portal dev/test

Resource group *: mykolian

Create new

Managed Instance details

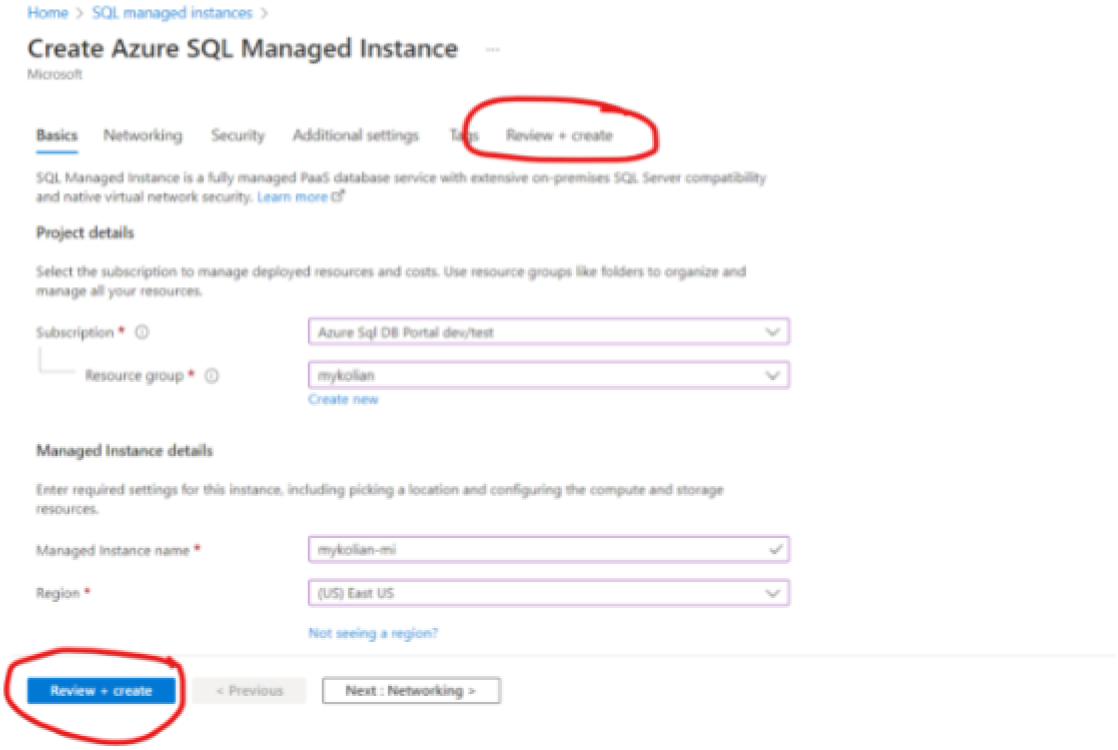
Enter required settings for this instance, including picking a location and configuring the compute and storage resources.

Managed Instance name *: dfdfdfdfdfdfdf

Region *: (US) East US

Not seeing a region?

3. After finishing all the preparations go to "Review+create" tab



Home > SQL managed instances >

Create Azure SQL Managed Instance ...

Microsoft

SQL Managed Instance is a fully managed PaaS database service with extensive on-premises SQL Server compatibility and native virtual network security. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure Sql DB Portal dev/test

Resource group * : mykolian

Create new

Managed Instance details

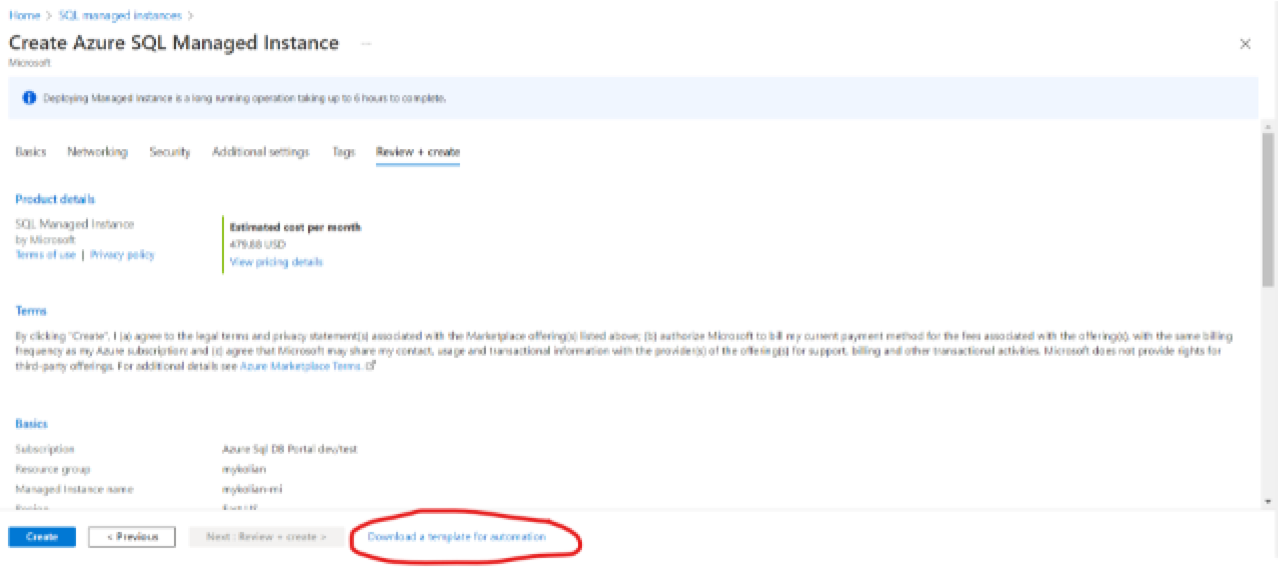
Enter required settings for this instance, including picking a location and configuring the compute and storage resources.

Managed Instance name * : mykolian-mi

Region * : (US) East US

Not seeing a region?

4. Go to "Download a template for automation"



Home > SQL managed instances >

Create Azure SQL Managed Instance ...

Microsoft

Deploying Managed Instance is a long running operation taking up to 6 hours to complete.

Product details

SQL Managed Instance
by Microsoft
Terms of use | Privacy policy

Estimated cost per month
479.88 USD
View pricing details

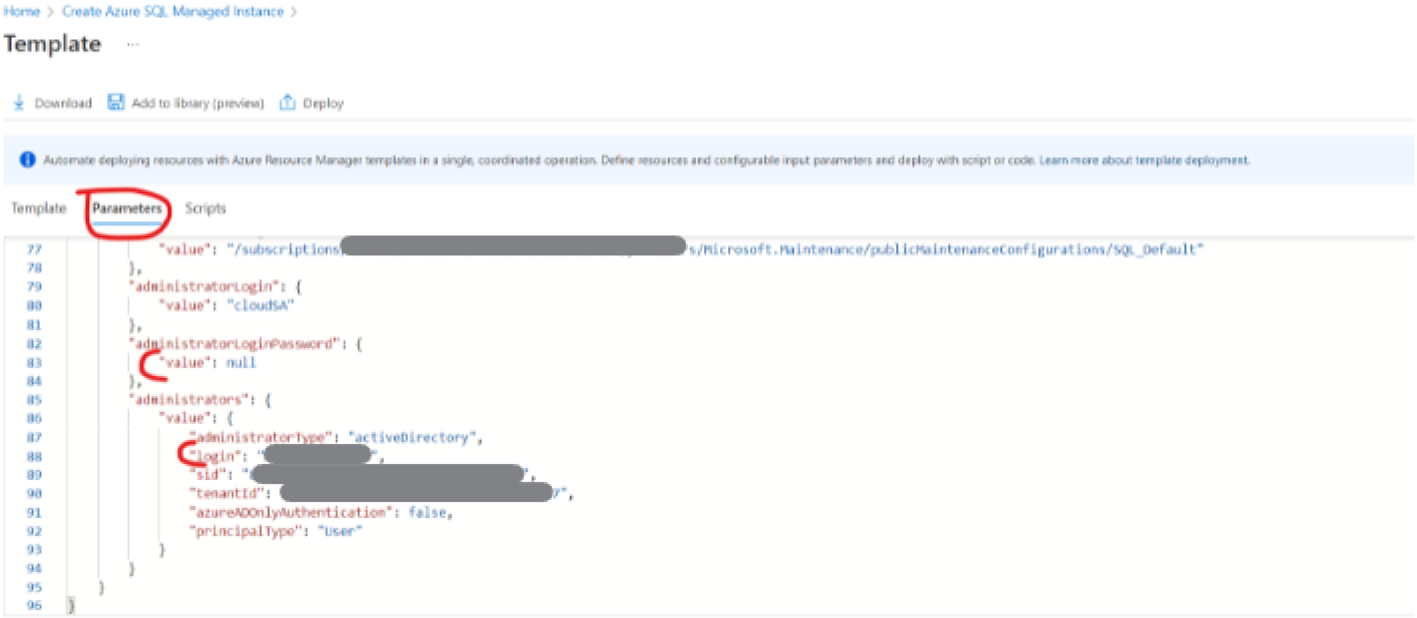
Terms

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details see Azure Marketplace Terms.

Basics

Subscription	Azure Sql DB Portal dev/test
Resource group	mykolian
Managed Instance name	mykolian-mi
Region	East US

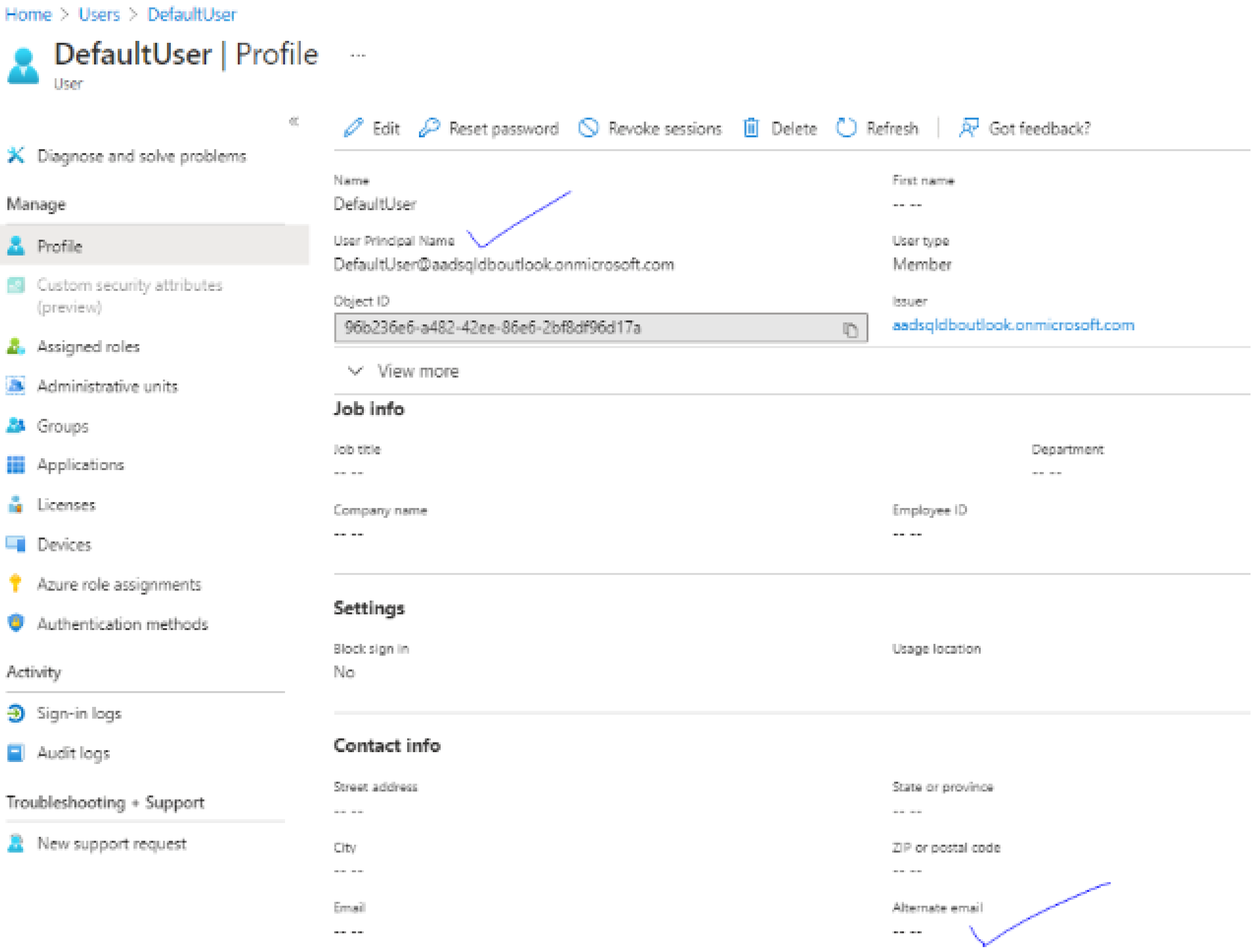
5. Now either download whole template and change 2 parameters: Under "administrators" change login to your UPN if it is a regular AAD account or email if it is a Guest account. If SQL Auth also present don't forget to provide password that passes the same validations as on basic tab.



Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resources and configurable input parameters and deploy with script or code. Learn more about template deployment.

```
            "value": "/subscriptions[redacted]s/Microsoft.Maintenance/publicMaintenanceConfigurations/SQL_Default"
        },
        "administratorLogin": {
            "value": "cloudSA"
        },
        "administratorLoginPassword": {
            "value": null
        },
        "administrators": {
            "value": {
                "administratorType": "activeDirectory",
                "login": "[redacted]",
                "sid": "[redacted]",
                "tenantId": "[redacted]",
                "azureADOnlyAuthentication": false,
                "principalType": "User"
            }
        }
    }
}
```

6. In order to fetch the UPN or email ID use the User Profile link:



Name: DefaultUser
First name: -- --
User Principal Name: DefaultUser@aadsqldboutlook.onmicrosoft.com
User type: Member
Object ID: 96b236e6-a482-42ee-86e6-2bf8df96d17a
Issuer: aadsqldboutlook.onmicrosoft.com

Job info

Job title: -- --
Department: -- --
Company name: -- --
Employee ID: -- --

Settings

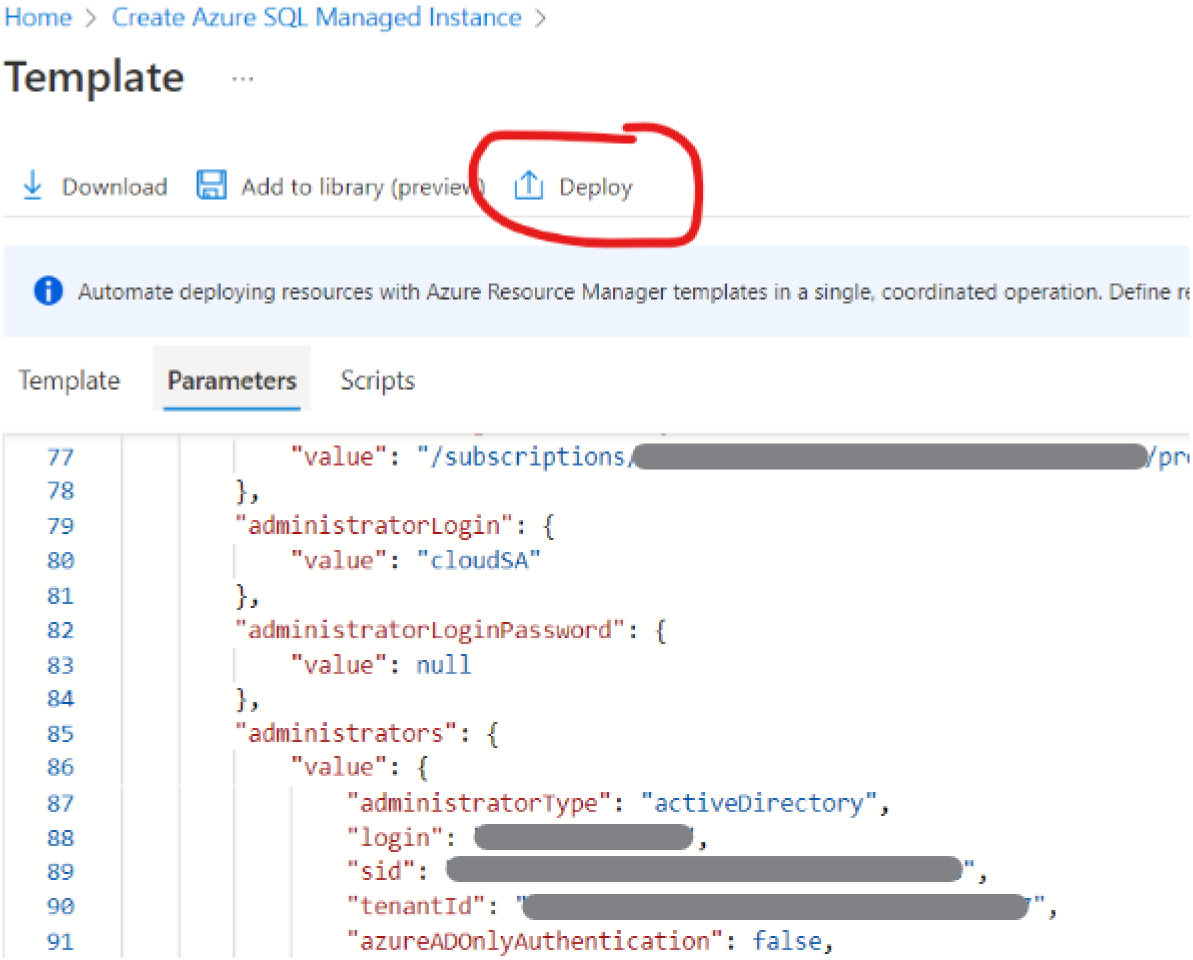
Block sign in: No
Usage location:

Contact info

Street address: -- --
State or province: -- --
City: -- --
ZIP or postal code: -- --
Email: -- --
Alternate email: -- --

Work around steps with deploy feature

1. From the Deploy tab

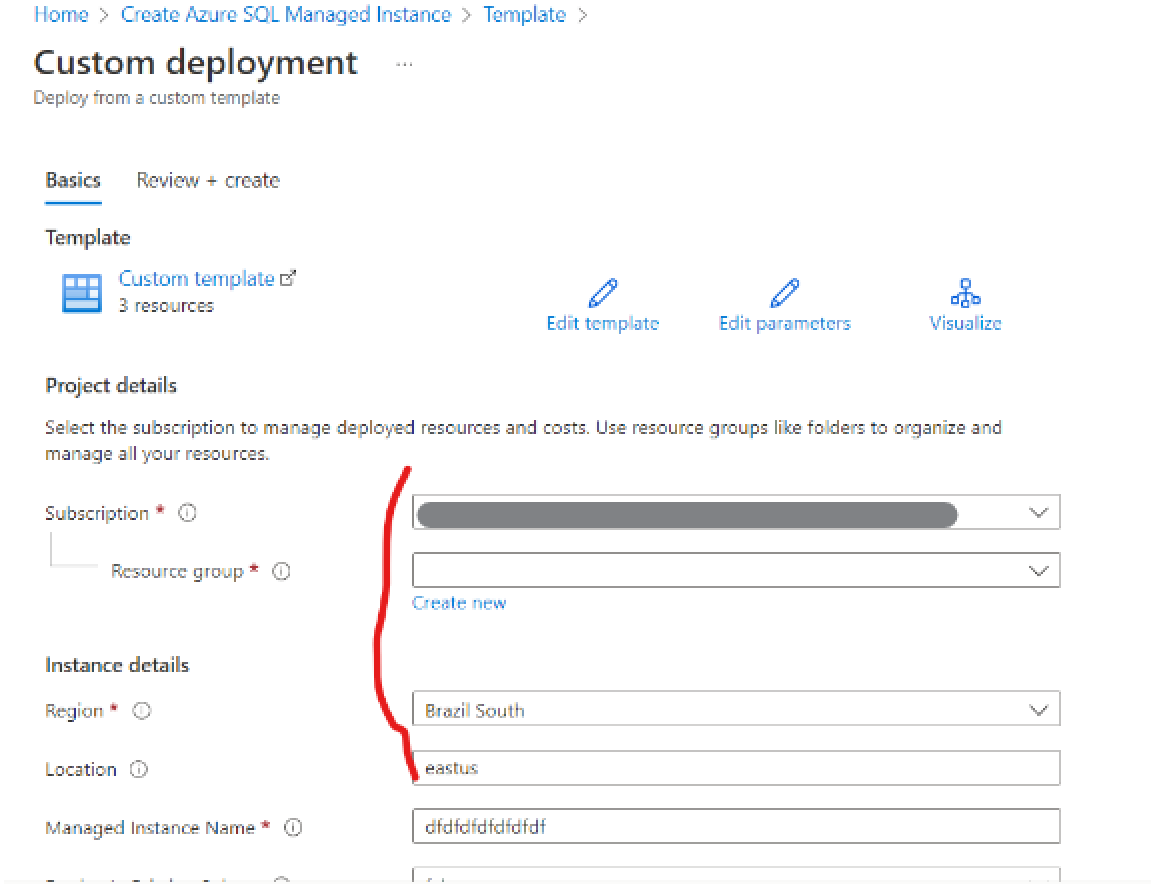


Template ...

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define re

```
            "value": "/subscriptions/[redacted]/pr
        },
        "administratorLogin": {
            "value": "cloudSA"
        },
        "administratorLoginPassword": {
            "value": null
        },
        "administrators": {
            "value": {
                "administratorType": "activeDirectory",
                "login": [redacted],
                "sid": [redacted]",
                "tenantId": "[redacted]",
                "azureADOnlyAuthentication": false,
```

2. Put subscription resource group and region from basics tab



Home > Create Azure SQL Managed Instance > Template >

Custom deployment ...

Deploy from a custom template

Template

Custom template
3 resources

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : [redacted]

Resource group * :

Create new

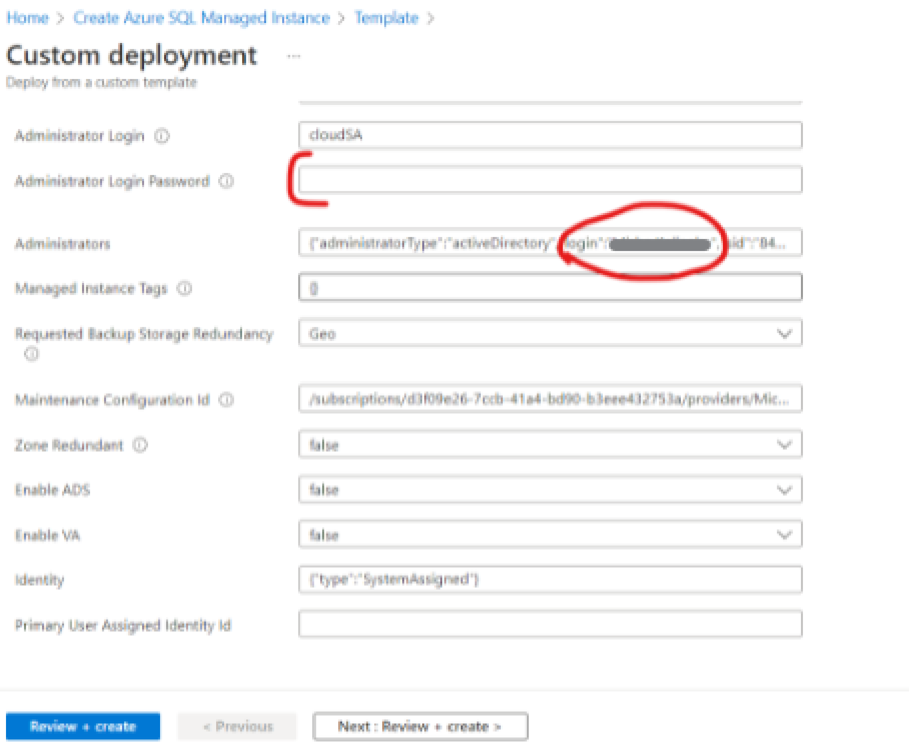
Instance details

Region * : Brazil South

Location : eastus

Managed Instance Name * : dfdfdfdfdfdfdf

3. Change login under administrators property the same way as described in step 5, if Sql Auth used put Login Password the same way as described in Step 5 of the Portal work around.



Home > Create Azure SQL Managed Instance > Template >

Custom deployment ...

Deploy from a custom template

Administrator Login : cloudSA

Administrator Login Password :

Administrators : {"administratorType":"activeDirectory","login":"[redacted]","sid":"84...

Managed Instance Tags : {}

Requested Backup Storage Redundancy : Geo

Maintenance Configuration Id : /subscriptions/d3f09e26-7ccb-41a4-bd90-b3eee432753a/providers/Mic...

Zone Redundant : false

Enable ADS : false

Enable VA : false

Identity : {"type":"SystemAssigned"}

Primary User Assigned Identity Id :

4. "Review + create" and "Create" to start deployment.

Internal Reference

IcM 278209162

How good have you found this content?

🙂 🙁