

Azure Database Migration Service

Last updated by | Vitor Tomaz | Nov 16, 2022 at 5:43 AM PST

Contents

- [Self-help content presented in Azure Portal](#)
- [Database migration service](#)
 - [Fix this problem now using our expert solution](#)
 - [Recommended steps](#)
 - [Recommended resources](#)

Self-help content presented in Azure Portal



Database migration service

Fix this problem now using our expert solution

Expert solutions are written by Azure engineers to help you quickly resolve the problem on your own.




You can use the Azure Database Migration Service to migrate the databases from an on-premises SQL Server instance to an Azure SQL Managed Instance. When you migrate databases to Azure by using Azure Database Migration Service, you can do an offline or an online migration. With an offline migration, application downtime starts when the migration starts. With an online migration, downtime is limited to the time to cut over at the end of migration. We suggest that you test an offline migration to determine whether the downtime is acceptable; if not, do an online migration.

Recommended steps

- Ensure that your VNet Network Security Group rules don't block the following inbound communication ports to Azure Database Migration Service: 443, 53, 9354, 445, 12000. For more detail on Azure VNet NSG traffic filtering, see [Filter network traffic with network security groups](#) .
- Configure your [Windows Firewall for source database engine access](#) .
- Open your Windows Firewall to allow the Azure Database Migration Service to access the source SQL Server, which by default is TCP port 1433.
- If you're running multiple named SQL Server instances using dynamic ports, you may wish to enable the SQL Browser Service and allow access to UDP port 1434 through your firewalls so that the Azure Database Migration Service can connect to a named instance on your source server.
- If you're using a firewall appliance in front of your source databases, you may need to add firewall rules to allow the Azure Database Migration Service to access the source database(s) for migration, as well as files via SMB port 445.
- Ensure that the logins used to connect the source SQL Server and the target managed instance are members of the sysadmin server role.

- Provide an SMB network share that contains full database backup files and subsequent transaction log backup files the Azure Database Migration Service can use for database migration.
- Ensure that the service account running the source SQL Server instance has write privileges on the network share that you created and that the computer account for the source server has read/write access to the same share.

Recommended resources

- [Tutorial: Migrate SQL Server to an Azure SQL Managed Instance online using DMS](#) 
- [Tutorial: Migrate SQL Server to an Azure SQL Managed Instance offline using DMS](#) 
- [Network topologies for Azure SQL DB Managed Instance migrations using the Azure Database Migration Service](#) 

How good have you found this content?



-