Configuration Security Checks

The Configuration Security Checks analyze the configuration and settings of the database, instance, or server in the policy.

The Configuration Security Checks available on the Configure the Policy section are the following:

Name	Description
Analysis Services Running	Determine whether Analysis Services (OLAP) is running on the SQL Server.
Asymmetric Key Size	Check to verify that the encryption key length for asymmetric keys is 2048 bits and above. It is recommended that asymmetric keys are not created in the system databases (master, model, msdb, and tempdb).
Auto_Close set for contained databases	Check to see if Auto_Close is set for contained databases. Auto_close should be set to OFF for these databases.
Backups compliance with RTO and RPO requirements	Check for most recent backups and validate that they are in compliance with Recovery Point Objective (RPO) and Recovery Time Objective (RTO) policies.
BUILTIN /Administrators Is sysadmin	Determine whether BUILTIN/Administrators is a member of the sysadmin fixed server role.
CLR Enabled	Determine whether the CLR is Enabled on the server.
Common criteria compliance	Determine whether the Common criteria compliance is enabled.
Data Files On System Drive	Determine whether data files exist on the system drive.
Database-level Firewall Rules	Determine whether unapproved database-level firewall rules have been configured on Azure SQL Database.
Databases Are Trustworthy	Determine whether any unapproved databases are trustworthy on SQL Server 2005 or later.
Default Trace Enabled	Determine whether the Default Trace Enabled on the server.
Full-Text Search Running	Determine whether Full-Text Search is running on the SQL Server.
HADR is configured	Return each database that is configured in an HA configuration, and its current state. Possible configurations are Availability Groups, Database Mirroring or Log Shipping. Replication is not considered an HA technology for the purposes of this check, as it is not applied to the entire database.
Hide Instance Option is set	HideInstance' determines whether or not the SQL instance can be discovered by the SQL Server Browser service. Check examines registry setting for 'HideInstance'. If 1, the instance is hidden.
Integration Services	Determine whether permissions have been granted on Integration Services stored procedures.
Linked servers are configured	Determine whether linked servers are configured.

Max Number of concurrent sessions	Determine maximum number of allowed concurrent sessions.
Maximum number of error log files	Determine whether the Maximum number of error log files is more than 11.
Ole automation procedures	Determine whether the Ole automation procedures are enabled.
Other General Domain Accounts	Determine whether general domain accounts added to the instance.
Replication Enabled	Determine whether replication is enabled on the SQL Server.
sa Account Not Disabled	Determine whether the SQL Server sa account has been disabled on SQL Server 2005 or later.
sa Account Not Disabled Or Renamed	Determine whether the SQL Server sa account has been disabled or renamed on SQL Server 2005 or later.
Sample Databases Exist	Determine whether sample databases exist on the SQL Server.
Server Is Domain Controller	Determine whether the Server is a domain controller.
Server-level Firewall Rules	Determine whether unapproved server-level firewall rules have been configured on Azure SQL Database.
Shutdown SQL Server on Trace Failure	Determine if traces exist that will not cause SQL Server to shut down if the trace encounters an error.
SQL Agent Mail	Determine whether the SQL Server Agent has been configured to allow email.
SQL Mail Or Database Mail Enabled	Determine whether SQL Mail or Database Mail has been enabled on the SQL Server.
SQL Server Installation Directories On System Drive	Determine whether SQL Server installation directories are on the system drive.
SQL Server Version	Determine whether the SQL Server software is at an acceptable minimum version.
System Table Updates	Determine whether the "Allow Updates to System Tables" configuration option is enabled on SQL Server 2005 or later.
Transport Layer Security	Return a bit value indicating whether SQL Server is requiring encryption at the protocol layer. (0 for no, 1 for yes.) This indicates if the server is requiring encryption for connections over the network, though clients can still request an encrypted connection to SQL Server even if the server is not requiring it.

Unauthorized Account Check	Determine whether unauthorized accounts have sysadmin privileges on the SQL Server or has SoD roles like "CONNECT ANY DATABASE", "IMPERSONATE ANY LOGIN", "SELECT ALL USER SECURABLES", "ALTER ANY COLUMN MASTER KEY", "ALTER ANY COLUMN ENCRYPTION KEY", "VIEW ANY COLUMN MASTER KEY DEFINITION", "VIEW ANY COLUMN ENCRYPTION KEY DEFINITION", "ALTER ANY SECURITY POLICY", "ALTER ANY MASK", "UNMASK".
User created 'sa' account does not exist	Ensure that a user account has not been created, named 'SA'.
VSS Writer Running	Determine whether VSS Writer is running on the SQL Server.
xp_cmdshell Enabled	Determine whether the xp_cmdshell extended stored procedure is enabled on SQL Server 2005 or later.
xp_cmdshell Proxy Account Exists	Determine whether a Proxy Account is enabled on the SQL Server.