SQL Server Hardening

SQL Server Hardening Considerations

Top SQL Hardening Considerations

Top SQL Hardening considerations:

1. Do not install SQL Server on an Active Directory Domain Controller.
2. Install the latest updates for SQL Server from Microsoft.
3. Set a strong password for the sa account before installing ICM.
4. Always install SQL Server service to run using a least privilege account. Never install SQL Server to run using the built-in Local System account. Instead, use the Virtual account.

   See the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html for more information.
5. Enable SQL Server Agent Service and set to Automatic for database maintenance in Unified ICM.

Note Installing the latest updates for SQL Server from Microsoft might require you to disable the SQL Server Agent service. So before performing the cumulative update installation, reset this service to *disabled*. When the installation is complete, stop the service and set it back to *enabled*.

6. Disable the SQL guest account.
7. Restrict sysadmin membership to your Unified ICM administrators.
8. Block TCP port 1433 (default) and UDP port 1434 at the network firewall, unless the Administration & Data Server is not in the same security zone as the Logger.
9. Change the recovery actions of the Microsoft SQL Server service to restart after a failure.

10. Remove all sample databases.
11. Enable auditing for failed sign-ins.

The following table lists the settings and the corresponding default and supported values for SQL hardening.

Setting Name	Default Value	Supported Value
Scan for Startup Procedures	Disabled |0|	0 or 1 supported. Unified CCE does not require it to be enabled; however, enabling it would not create any problem.
Ad Hoc Distributed Queries	Disabled |0|	0 or 1 supported. 0 is more secure.

Related Topics

SQL Server Users and Authentication, on page 2
Virtual Accounts, on page 5

SQL Server Users and Authentication

When creating a user for the SQL server account, create Windows accounts with the least possible privileges for running SQL server services. Create the accounts during the installation of SQL server.

The local user or the domain user account that is created for the SQL server service account follows the Windows or domain password policy respectively. Apply a strict password policy on this account. However, don’t set the password to expire. If the password expires, the SQL server service ceases to function and the Administration, & Data server fails.

Site requirements can govern the password and account settings. Consider minimum settings like the following:

Table 1: Password and Account Settings

Setting	Value
Enforce Password History	24 passwords remembered
Minimum Password Length	12 characters
Password Complexity	Enabled
Minimum Password Age	1 day
Account Lockout Duration	15 minutes
Account Lockout Threshold	3 invalid logon attempts
Reset Account Lockout Counter After	15 minutes

During automated SQL server hardening, if the sa password is found blank, a strong password is generated at random to secure the sa account. You can reset the sa account password after installation by logging on to the SQL server using a Windows Local Administrator account.

UCCE supports renaming or removal of default built-in MS SQL sa account. If the sa account is used to integrate with UCCE solution components like Finesse, CUIC or any other third-party integrations, the login credentials have to be reconfigured with the renamed sa account.

Note Renaming or removing the sa account has no correlation with SQL Server hardening that happens during installation or upgrade.

SQL Server Security Considerations

Microsoft SQL server provides granular access control and runs with lower privileges by default. In addition to the security provided by SQL server, CCE provides utility to harden the SQL server further. Details are available in the following sections.

Automated SQL Server Hardening

The SQL Server Security Automated Hardening utility performs the following:

- Enforces Mixed Mode Authentication.
- Ensures that the Named Pipe (np) is listed before TCP/IP (tcp) in the SQL Server Client Network Protocol Order.
- Disables SQLWriter and SQLBrowser Services.
- Forces SQL server user 'sa' password if found blank.

SQL Server Security Hardening Utility

The SQL Server Security Hardening utility allows you to harden or roll back the SQL Server security on Logger and Administration & Data Server/HDS components. The Harden option disables unwanted services and features. If the latest version of the security settings is already applied, then the Harden option does not change anything. The Rollback option allows you to return to the state of SQL services and features that existed before your applying the last hardening.

You can optionally apply the SQL Server Security Hardening as part of Unified CCE installation and upgrade or via the Security Wizard tool. The utility is internally managed by running the Windows PowerShell script ICMSQLSecurity.ps1. You can also apply the hardening by directly running the PowerShell script.

Note Run the Security Wizard tool or Windows PowerShell script as an administrator.

Utility Location

The utility is located at:

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity
```

HARDEN Command

At the Windows PowerShell command line, enter:

```
Powershell .\ICMSQLSecurity.ps1 HARDEN
```

Note The current SQL Server configuration is backed up to `<ICMInstallDrive>:\CiscoUtils\SQLSecurity\icmsqlsecuritybkp.xml` before the utility applies the SQL Server hardening.

ROLLBACK Command

The ROLLBACK command rolls back to the previous SQL Server configuration, if hardening was applied before.

To roll back to the previous SQL Server configuration, enter the following command:

```
Powershell .\ICMSQLSecurity.ps1 ROLLBACK
```

Note The following settings are required for Unified CCE to function properly. They are not reverted to their original state when automated rollback is performed:

1. Named Pipe (np) listed before TCP/IP(tcp) in the SQL Server Client Network Protocol Order.
2. Mixed mode authentication.

Help for Commands

If you use no argument with the command line, the help appears.

Output Log

All output logs are saved in the file:

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity\Logs\ICMSQLSecurity.log
```

Manual SQL Server Hardening

By default, SQL Server disables VIA endpoint and limits the Dedicated Administrator Connection (DAC) to local access. Also, by default, all logins have GRANT permission for CONNECT using Shared Memory, Named Pipes, TCP/IP, and VIA endpoints. Unified ICM requires only Named Pipes and TCP/IP endpoints.

Procedure

- Enable both Named Pipes and TCP/IP endpoints during SQL Server setup. Make sure that the Named Pipes endpoint has a higher order of priority than TCP/IP.

Note The SQL Server Security Hardening utility checks for the availability and order of these endpoints.

- Disable access to all unrequired endpoints. For instance, deny connect permission to VIA endpoint for all users/groups who have access to the database.

Virtual Accounts

Virtual Accounts are preferred over Network or Local Services account for SQL Services because of the former's higher level of security. Virtual accounts run with the lowest privileges. The CCE installer adds the Perform Volume Maintenance Tasks privilege to the SQL account. This privilege is needed to perform database-related operations, such as creating and expanding the database.

If your corporate policy does not allow the use of this privilege, you can remove it. However, performing database-related operations such as creating and expanding the database takes more time (depending on the size of your database).