

USING SERVICE ACCOUNT INSTEAD OF NETWORK SERVICE FOR INTEGRATED DATABASE AUTHENTICATION

Contents

A.	Preamble	2
B.	CM configuration	2
1.	SDL Web MMC	2
2.	Database configuration.....	3
3.	Tridion Service CM Logins	5
4.	IIS config.....	6
5.	Add service user account to the SDLSearchUsers group	7
6.	Other CM functionality tested	7
7.	Component service configuration.....	7
8.	Topology Manager configuration	9
C.	CD configuration	9
1.	Microservice configuration	10
D.	Addendum.....	11

A. Preamble

This document is a supplement to the SDL Web 8.5 online documentation, and describes in more detail how to install the Content Manager, Topology Manager, and Content Delivery with integrated database authentication.

The document was verified for SDL Web 8.5 (SQL Server), and tested on Windows 2012 R2 (x64) with SQL Server 2014 (SP3) (KB4022619). Minor differences in interface and functionality when referenced for prior major versions of SDL Web. Compatibility with future versions of SDL Web (ie Tridion Sites 9.0) is not assured.

Verified on a test server only, further configuration changes may be required in a production environment. Not all configuration specifications may be necessary for integrated authentication.

B. CM configuration

1. SDL Web MMC

The screenshot displays three separate windows of the SDL Web Content Manager Management Console (MMC) interface:

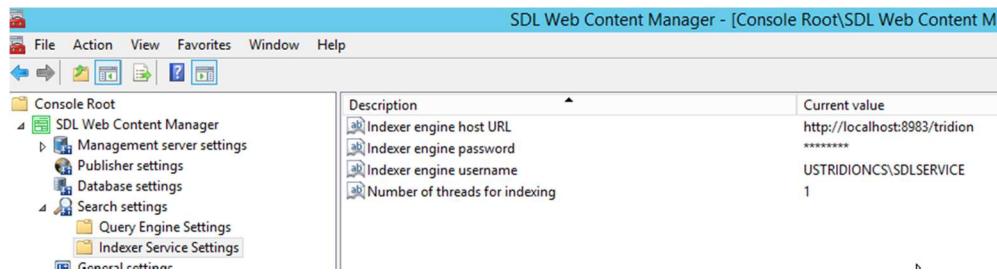
- Top Window (Database settings):** Shows the "Database advanced connection settings" node expanded. The table lists the following settings:

Description	Current value
Enlist=false	Enlist=false
Integrated	Integrated
*****	*****
TCM_WEB85_W12R220	TCM_WEB85_W12R220
USCSDB09	USCSDB09
MSSQL70	MSSQL70
- Middle Window (WindowsUser):** Shows the "WindowsUser" node expanded. The table lists two users:

Type
windows
windows

The entries are:
 - NT AUTHORITY\NETWORK SERVICE
 - USTRIDIONCS\SDLSERVICE
- Bottom Window (Query engine settings):** Shows the "Query engine settings" node expanded. The table lists the following settings:

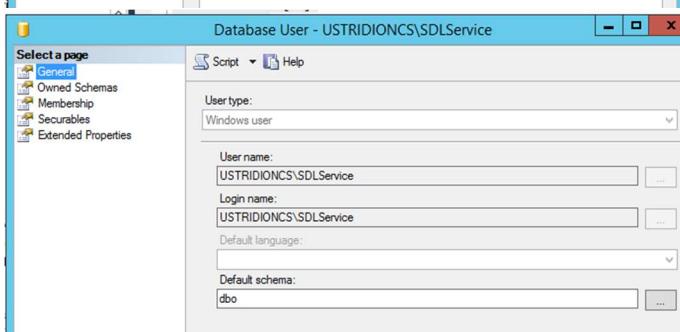
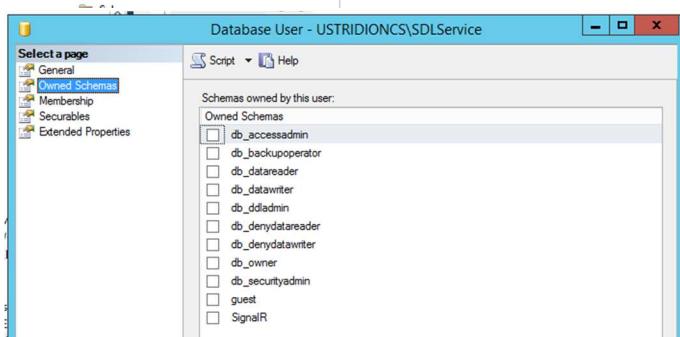
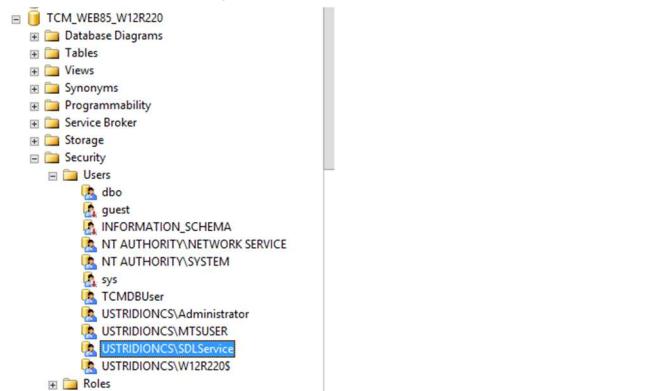
Description	Current value
Query engine host URL	http://localhost:8983/tridion
Query engine password	*****
Query engine username	USTRIDIONCS\SDLSERVICE

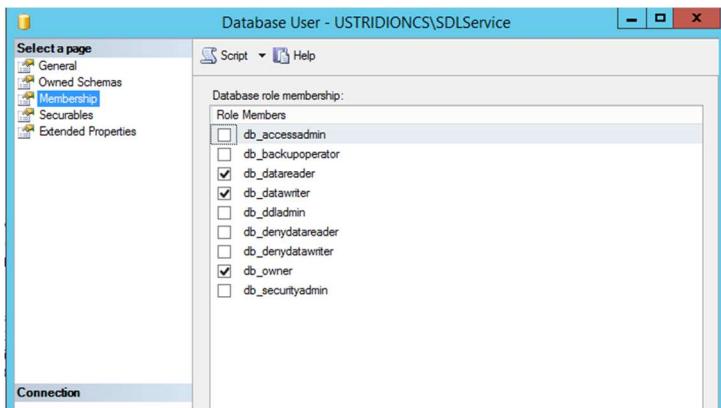


2. Database configuration

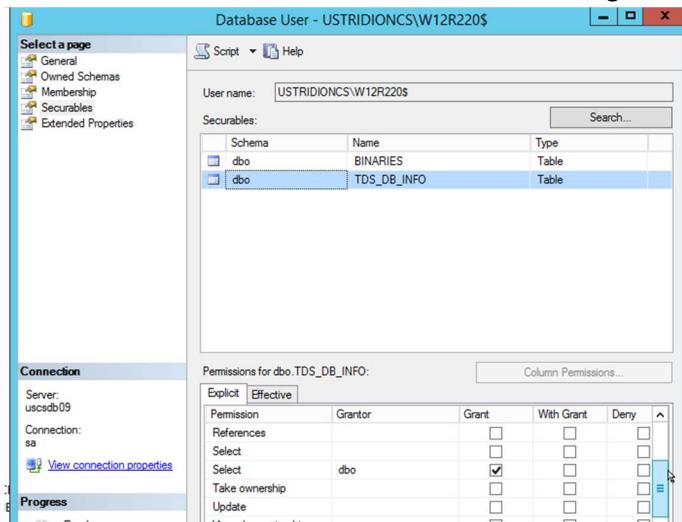
1. SSMS > TCM DB > Security > Users

- User USTRIDIONCS\SDLService is added



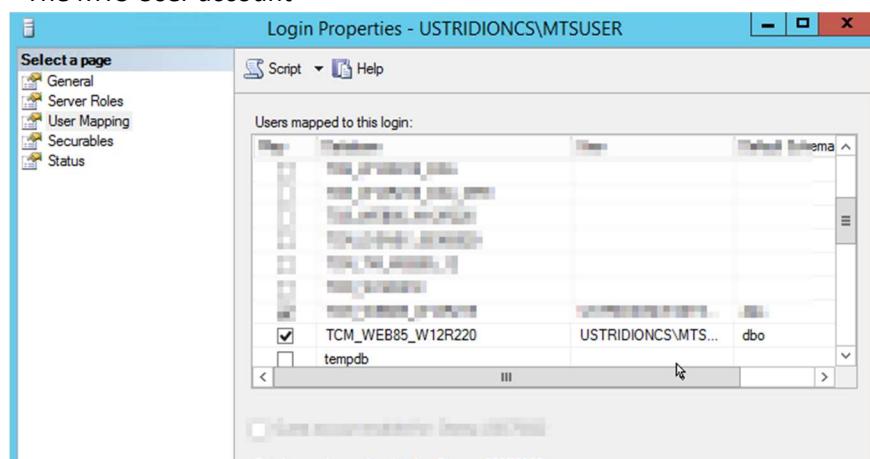


- Permissions for SDLService does *not* need to be granted to the BINARIES and TDS_DB_INFO tables.



2. Ensure that the user accounts of any users that need to access your database are listed under Security > Logins . You typically would have specified these user accounts during installation or configuration. Ensure that they include:

- The MTS User account



- SDLService account

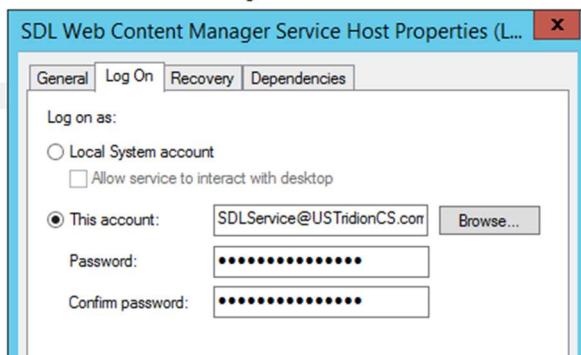
- The user who was logged in when you ran the Content Manager installer.

5. Ensure that these new users have administrator-level access to the software. You do this by setting the value of the privilege column to "1" for this user.

ID	NAME	ENABLED	IS_PREDEFINED	ITEM_TYPE	PRIVILEGE	IS_DEFAULT_GROUP	DELETED	DESCRIPTION
1 12	USTRIDIONCS\Administrator	1	0	65552	1	0	0	SDL Web Content Management Administrator
2 13	USTRIDIONCS\MTSUser	1	1	65552	1	0	0	System Account
3 14	USTRIDIONCS\SDLService	1	1	65552	1	0	0	SDLService account
4 15	W12R220\Admin	1	0	65552	1	0	0	Admin
5 16	W12R220\MTSUSER	1	1	65552	1	0	0	MTSUSER
6 17	NT AUTHORITY\NETWORK SERVICE	1	1	65552	1	0	0	NULL

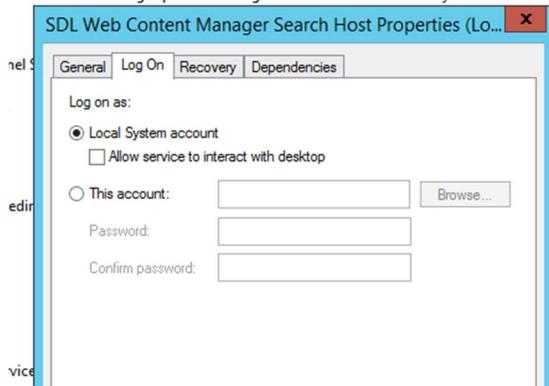
3. Tridion Service CM Logins

1. Log on for Tridion services is the SDLService account as in screenshot.



- Transport service
- Publisher
- Search Host

- Service Host
 - Workflow Agent
 - Translation Manager
2. Logon to these services is SYSTEM account as in screenshot



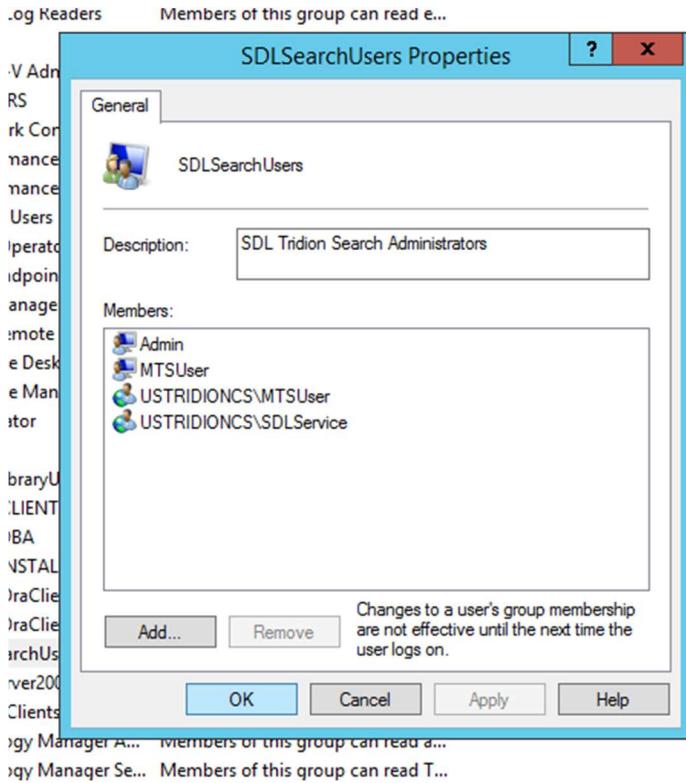
- a. Search Indexer
- b. Monitoring service

4. IIS config

1. All CM endpoints including Topology Manager are using the SDLService application pool

Virtual Path	Physical Path	Site	Application Pool
/hubs/backplaneHub	D:\SDL_Web\hubs\backplaneHub	SDL Web	SDLService (v4.0)
/hubs/notificationHub	D:\SDL_Web\hubs\NotificationHub	SDL Web	SDLService (v4.0)
/TemplateBuilder	D:\SDL_Web\web\TemplateBuilder	SDL Web	SDLService (v4.0)
/templating	D:\SDL_Web\templating	SDL Web	SDLService (v4.0)
/webdav	D:\SDL_Web\webdav	SDL Web	SDLService (v4.0)
/webservices	D:\SDL_Web\web\webservices	SDL Web	SDLService (v4.0)
/WebUI	D:\SDL_Web\web\WebUI\WebRoot	SDL Web	SDLService (v4.0)
/WFListener	D:\SDL_Web\workflow	SDL Web	SDLService (v4.0)
Root Application	D:\SDL_Web\TopologyManager\web	SDL Web Topolog...	SDLService (v4.0)
Root Application	D:\SDL_Web\web	SDL Web	SDLService (v4.0)

5. Add service user account to the SDLSearchUsers group

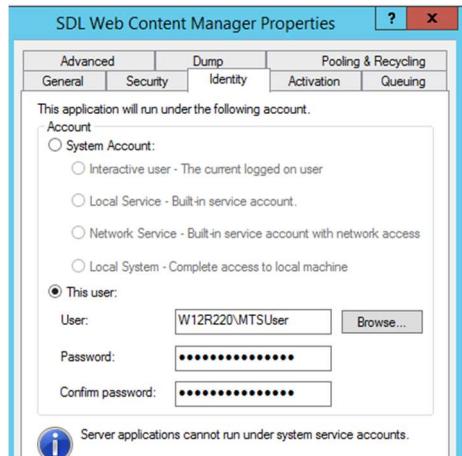


6. Other CM functionality tested

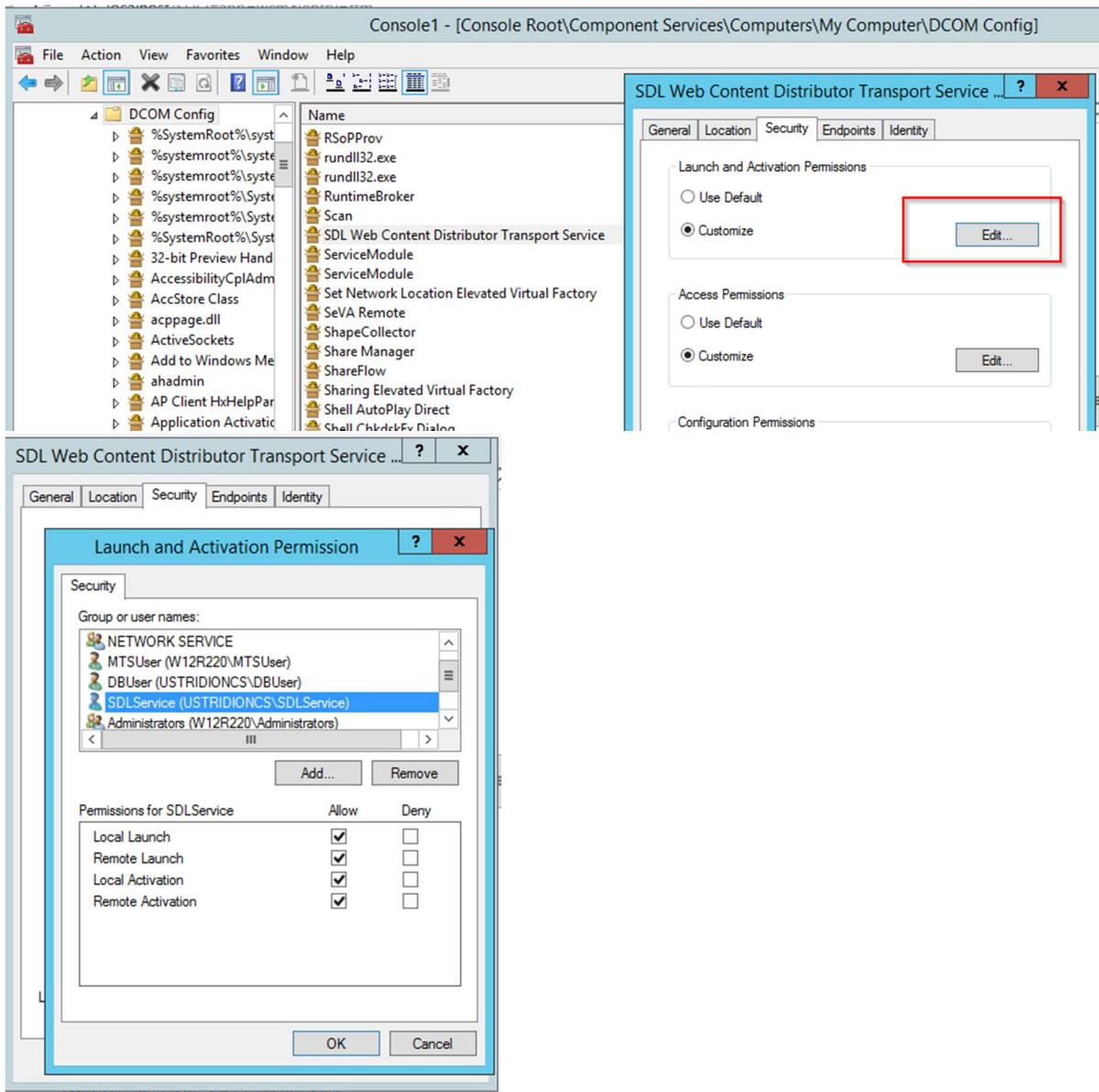
1. Publishing
2. Content Porter
3. Template Builder
4. Event system (by customer)

7. Component service configuration

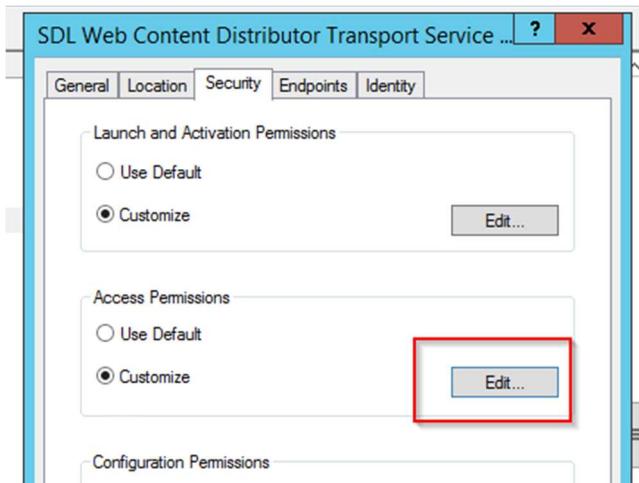
1. COM+ SDL Web Content Manager identity is machine name\MTSUSER

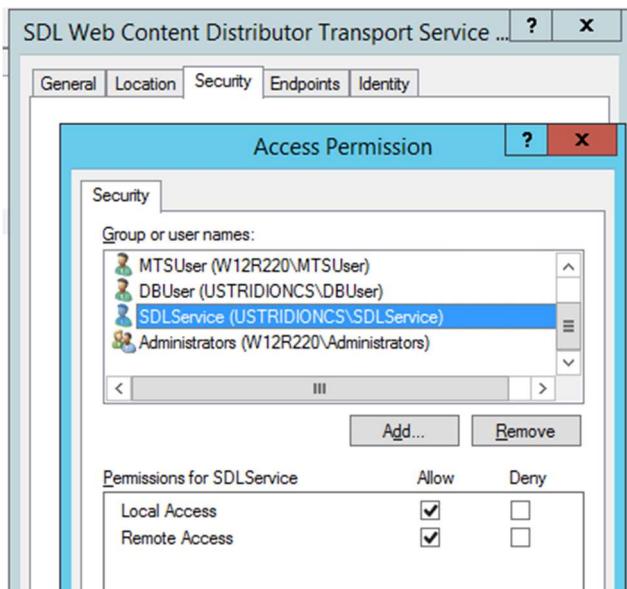


2. Navigate to MMC > Components Services > Computers > My Computers > DCOM Config > SDL Web Content Distributor Transport Service
 - a. Edit Launch and Activation Permissions. Add SDLService as user and grant permissions.

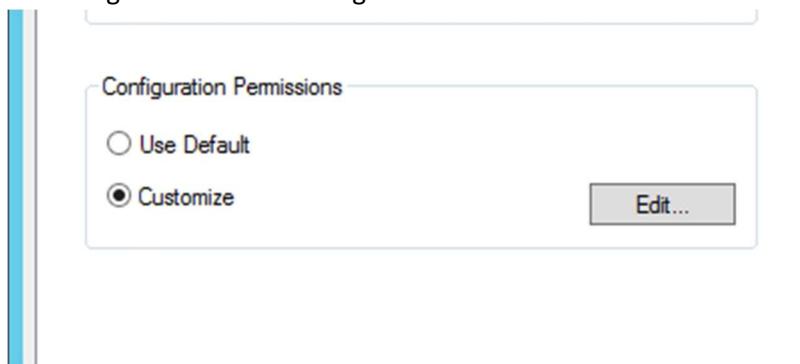


b. Also add service account for “Access Permissions”





- c. No changes needed for Configuration Permissions.



8. Topology Manager configuration

As noted in the Web 8.5 documentation, it is necessary to modify the Topology Manager Web.config to use integrated authentication.

<https://docs.sdl.com/LiveContent/content/en-US/SDL%20Web-v5/GUID-A7B26918-1A7B-4AE8-A6A6-16B82C893CC0>

C. CD configuration

Documentation page on configuring CD databases for integrated authentication

<https://docs.sdl.com/LiveContent/content/en-US/SDL%20Web-v5/GUID-975723FD-3A94-40F6-BBC7-82571A851488>

For SQL Server 2014, MS JDBC driver 7.2 was downloaded from page

<https://docs.microsoft.com/en-us/sql/connect/jdbc/download-microsoft-jdbc-driver-for-sql-server-2017>

sqljdbc_auth.dll was placed at C:\Program Files\Java\jre1.8.0_172\bin on test server, but can be put in other location as desired.

1. Microservice configuration

1. Database configured as per documentation

Map	Database	User	Default Schema
<input type="checkbox"/>	REPLICAS		
<input type="checkbox"/>	ReportServer		
<input type="checkbox"/>	ReportServerTempDB		
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input checked="" type="checkbox"/>	TCB_WEB85_W12R220	SDLService	dbo
<input type="checkbox"/>	tempdb		
<input type="checkbox"/>	TridionContent		
<input type="checkbox"/>	TridionCore		
<input checked="" type="checkbox"/>	TCM_WEB85_W12R220	USTRIDIONCS\SDLService	dbo

Guest account enabled for: TCB_WEB85_W12R220

Database role membership for: TCB_WEB85_W12R220

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input checked="" type="checkbox"/>	db_datareader
<input checked="" type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input checked="" type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input checked="" type="checkbox"/>	public

2. \$jvmoptions in .\installService.ps1 script of Microservice bin folder was modified to include reference to java.library.path param, ie

```
$jvmoptions = "-Xrs", "-Xms128m", "-Xmx128m", "-Djava.library.path=C:/Program Files/Java/jre1.8.0_172/"  
Microservice was then reinstalled.
```

3. cd_storage_conf.xml of microservice edited as below

```
<Property Name="databaseName" Value="DATABASE_NAME"/>  
<!-- <Property Name="user" Value="USERNAME"/>  
<Property Name="password" Value="PASSWORD"/> -->  
<Property Name="integratedSecurity" Value="true"/>
```

4. After service startup, fails with error

```
2019-05-14 19:17:39,667 ERROR RetryPoolingDataSource - Passing exception to the caller. Attempt:0
```

```
Message:Integrated authentication failed. ClientConnectionId:9dff118a-e5be-4a98-9f04-a0ec11187ab8
```

```
2019-05-14 19:17:59,462 ERROR SQLExceptionHelper - Integrated authentication failed.
```

```
ClientConnectionId:62865e3e-93a1-4771-8493-6184dfb96032
```

```
...
```

```
2019-05-14 19:17:59,586 ERROR SpringApplication - Application startup failed
```

```
org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name  
'dataSourceFactoryImpl': Unsatisfied dependency expressed through field 'dataSourceProviders'; nested  
exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with  
name 'tridionConfigDataSourceProvider': Unsatisfied dependency expressed through field 'dataSource';  
nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with  
name 'tridionConfigDataSource': Invocation of init method failed; nested exception is  
javax.persistence.PersistenceException: org.hibernate.exception.JDBCConnectionException: Unable to
```

acquire JDBC Connection

...

Caused by: org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'tridionConfigDataSourceProvider': Unsatisfied dependency expressed through field 'dataSource'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'tridionConfigDataSource': Invocation of init method failed; nested exception is javax.persistence.PersistenceException: org.hibernate.exception.JDBCConnectionException: Unable to acquire JDBC Connection

...

Caused by: javax.persistence.PersistenceException: org.hibernate.exception.JDBCConnectionException: Unable to acquire JDBC Connection

at org.hibernate.internal.ExceptionConverterImpl.convert(ExceptionConverterImpl.java:147)
at org.hibernate.internal.ExceptionConverterImpl.convert(ExceptionConverterImpl.java:155)

...

Caused by: org.hibernate.exception.JDBCConnectionException: Unable to acquire JDBC Connection

at

org.hibernate.exception.internal.SQLStateConversionDelegate.convert(SQLStateConversionDelegate.java:115)

at

org.hibernate.exception.internal.StandardSQLExceptionConverter.convert(StandardSQLExceptionConverter.java:42)

at org.hibernate.engine.jdbc.spi.SqlExceptionHelper.convert(SqlExceptionHelper.java:111)

at org.hibernate.engine.jdbc.spi.SqlExceptionHelper.convert(SqlExceptionHelper.java:97)

...

Caused by: com.microsoft.sqlserver.jdbc.SQLServerException: Integrated authentication failed.

ClientConnectionId:62865e3e-93a1-4771-8493-6184dfb96032

D. Addendum

9. CM and DB must be hosted on separate machines.
10. Both servers must be added to the same domain.
11. NT AUTHORITY\NETWORK SERVICE user does not need to be added as a SQL Server Login, or as a DB user, or to the TRUSTEES table. It had previously been added but functionality is not disrupted when it is disabled as in screenshot.

The screenshot shows the SSMS interface with the 'Results' tab selected. In the results pane, there is a table named 'Logins' with the following data:

ID	NAME	ENABLED	IS_PREDEFINED	ITEM_TYPE	PRIVILEGE	IS_DEFAULT_GROUP	DELETED	DESCRIPTION	L...
1	USTRIDIONCS\Administrator	1	0	65552	1	0	0	SDL Web Content Management Administrator	10...
2	USTRIDIONCS\MTSUser	1	1	65552	1	0	0	System Account	NU...
3	USTRIDIONCS\SDLService	1	1	65552	1	0	0	SDLService account	NU...
4	W12R220\Admin	1	0	65552	1	0	0	Admin	10...
5	W12R220\MTSUSER	1	1	65552	1	0	0	MTSUSER	NU...
6	NT AUTHORITY\NETWORK SERVICE	0	1	65552	1	0	0	NULL	NU...
7	someuser	1	1	65552	1	0	0	NULL	NU...

In the object browser pane, under the 'Security' folder, the 'Logins' node is expanded, showing the following logins:

- ##MS_PolicyEventProcessingLogin##
- ##MS_PolicyTsqlExecutionLogin##
- NT AUTHORITY\LOCAL SERVICE
- NT AUTHORITY\SYSTEM
- NT SERVICE\MSSQLSERVER
- NT SERVICE\SQLSERVERAGENT
- NT SERVICE\SQLWAN

12. If below error (the target principal is incorrect. Cannot generate SSPI context) is seen, this is likely due to an application pool or logon account being designated to an account other than the service account.

