imagicle

Create a SQL user for IAS database

Applies to:

Imagicle UC Suite (any version).

Description

Use this procedure if you need to create a SQL user to be used by Imagicle UC Suite to connect to a Microsoft SQL Server instance other than the default one, or if you want to leverage Windows integrated authentication
For example, you need to host Imagicle UC Suite's database on an external SQL Server instance and you want UCS to connect using a SQL account other than *sa*.

Note: If you plan to use your own MS-SQL Server installation and license, co-located inside Imagicle UC Suite VM, please make sure to install it BEFORE running Imagicle UC Suite setup package.

How-to create a new user

The main steps are:

1. Create a SQL user according to this procedure on the target SQL Server instance. Don't create any database, the database must be automatically created by the Imagicle DB configuration tool.
2. Run "Imagicle AS Database Configuration" tool to configure the desired SQL Server instance and SQL user credentials. This will create the Imagicle database.

To create a SQL user with sample username ***imagicleUser*** and sample password ***imagiclePassword***, run the following SQL script (according to UC Suite version) on the target SQL Server instance:

On 2019.Winter.1 or newer

```
USE [master]
CREATE LOGIN [imagicleUser] WITH PASSWORD=N'imagiclePassword',DEFAULT_LANGUAGE=[us_english],CHECK_EXPIRATION=OFF,CHE
GRANT CONNECT SQL TO [imagicleUser]
GRANT CREATE ANY DATABASE TO [imagicleUser]
GRANT VIEW ANY DATABASE TO [imagicleUser]
```

On 2018.Summer.1

```
USE [master]
CREATE LOGIN [imagicleUser] WITH PASSWORD=N'imagiclePassword',DEFAULT_LANGUAGE=[us_english],CHECK_EXPIRATION=OFF,CHE
GRANT CONNECT SQL TO [imagicleUser]
GRANT CREATE ANY DATABASE TO [imagicleUser]
GRANT VIEW ANY DATABASE TO [imagicleUser]
â  GRANT VIEW ANY DEFINITION TO [imagicleUser]
```

From 2017.Spring.2 to 2018.Spring.1

```
USE [master]
CREATE LOGIN [imagicleUser] WITH PASSWORD=N'imagiclePassword', DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_englis
GRANT CONNECT SQL TO [imagicleUser]
GRANT CREATE ANY DATABASE TO [imagicleUser]
â  GRANT VIEW ANY DATABASE TO [imagicleUser]
GRANT VIEW ANY DEFINITION TO [imagicleUser]
```

Up to 2017.Spring.1

```
USE [master]
CREATE LOGIN [imagicleUser] WITH PASSWORD=N'imagiclePassword', DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_engli
GRANT CONNECT SQL TO [imagicleUser]
GRANT CREATE ANY DATABASE TO [imagicleUser]
â  GRANT VIEW ANY DATABASE TO [imagicleUser]
GRANT VIEW ANY DEFINITION TO [imagicleUser]
GRANT CONTROL SERVER TO [imagicleUser]
```

If database already exists

If the target database already exists before creating the SQL user (for example, because it has been restored or moved from another SQL server), follow these steps:

1. create the desired SQL user according to previous section
2. run the following SQL script to make the slected user db owner of the existing database:

```
use [BluesPro]
exec sp_changedbowner [imagicleUser]
```

If user already exists

If the SQL user already exists, you can verify if all requirements are satisfied by following these steps:

1. Log in to SQL Server with the user that will be used by the Imagicle Application Suite
2. Download this SQL script
3. If needed, on the first line change 'BluesPro' with the correct database name that will be used by the Imagicle Application Suite
4. Run the script
5. Verify on the resulting table that the status of all requirements is 'OK'

MS-SQL Server Password Policy

Please mind current MS-SQL password guidelines, to avoid entering a weak password:

- At least eight characters long, up to max 128.
- Combines letters, numbers, and symbol characters within the password.
- Is not found in a dictionary.
- Is not the name of a command.
- Is not the name of a person.
- Is not the name of a user.
- Is not the name of a computer.
- Is changed regularly.
- Is different from previous passwords.

Moreover, certain symbols must be avoided in SQL Server login and/or password: [] {}() , ; ? * ! @ ' ^

How-to leverage Windows integrated authentication

Introduction

Starting from version **2019.Winter.1**, UC Suite can connect to a local or remote SQL server using the Windows integrated authentication, instead of the traditional SQL authentication (connection via username and password).

This authentication method introduces some new constraints and configuration steps that must be performed manually on the SQL Server. Please, read the following paragraph for the configuration and constraint details of such authentication method.

Requirements

- Every **UC Suite server** that needs to be configured to use integrated authentication **must belong to a domain**. This constrain is strengthened by the database configuration wizard that will fail throwing and error if an integrated authentication connection is going to be configured on a machine that does not belong to any domain.
- If an external **SQL server** is being used (as it normally is), the SQL server **must belong to the same Windows domain** of the Imagicle server(s).
- A domain user enabled to access the SQL server with the rights indicated in the next paragraph. This is needed for the following operations:
    - First Imagicle Suite setup or DB reconfiguration
    - Imagicle backup (run in interactive mode)
    - Restore of an Imagicle backup
- Local system accounts enabled on SQL server as described in the paragraph "UC Suite local SYSTEM account SQL credentials" below.

Domain user executing UC Suite tools

The logged user that needs to run the UC Suite tools connecting to the database (backup/restore, node removal tool, DB configuration wizard, etc.) **must be a domain user** that has the required privileges to log into and possibly modify the SQL Server using integrated authentication. In particular the domain user used to configure the DB must be defined as Login in the SQL server instance and must be assigned the following SQL privileges:

- VIEW ANY DATABASE
- CREATE ANY DATABASE

These requirements are strengthened by the database connection configuration wizard that will fail throwing and error if the executing user cannot authenticate to the SQL Server.

UC Suite local SYSTEM account SQL credentials

To enable SQL Windows integrated authentication, the local system computer account of each UC Suite must be provided with proper SQL logins. Generally speaking each SQL server used by the UC Suite must contain a SQL login for every UC Suite server that needs to log in to it and each UC Suite database must contain a SQL user for every UC Suite server using it.

The login will be used every time a UC Suite service needs to authenticate to SQL and needs to be granted with the same privileges usually required by the UC Suite for the simple SQL Server account. If both the UC Suite server and the SQL server belong to the same domain, but the UC Suite is not provided with a proper SQL login, the configuration wizard will fail showing an error message reporting the missing login or the missing grants. The UC Suite will therefore not be able to use integrated authentication. Each SQL server must contain the logins of all of the UC Suite servers that needs to log in to it via integrated authentication. The creation of a system login has to be performed manually following the procedure described in the "Creation of a Computer Account login in the SQL Server" section of this article.

On the other hand, the database user will be used by the just created login to be able to access the UC Suite database and must be granted the db_owner role. This procedure has to be manually performed only in the case of a replicated database cluster following the procedure described in the "Creation of a Computer Account user in the SQL Server Database" section of this article and must be executed on each SQL database for all the non local nodes.

To summarize, the following actions must be performed to use SQL Windows integrated authentication:

- **Single installation** â Before running the database configuration wizard, add to SQL Server:
    - a login for the computer account of the UC Suite, as described in details in section "Creation of a Computer Account login in the SQL Server" of this article
    - a login for the regular domain user used during the installation/configuration operations.
- **Cluster, shared database** â Before running the database configuration wizard on each cluster node, add to the shared SQL Server:
    - a login for the computer account of every node of the cluster, as described in details in section "Creation of a Computer Account login in the SQL Server" of this article
    - a login for the regular domain user used during the installation/configuration operations.
- **Cluster, replicated database**
    - **â** Before running the database configuration wizard on the cluster nodes, add to every SQL server:
        - a login for the computer account of each node as described, as described in details in section "Creation of a Computer Account login in the SQL Server" of this article

◊ a login for the regular domain user used during the installation/configuration operations.

- Upon completing the configuration wizard add to every UC Suite database a user for every non local node as described, as described in details in section "Creation of a Computer Account user in the SQL Server Database" of this article.

Getting the NETBIOS name of an Imagicle server

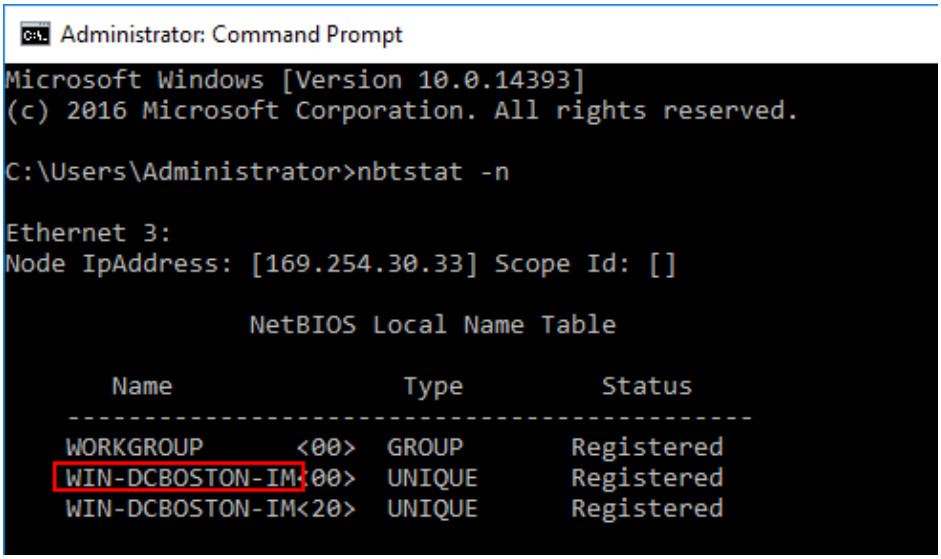
In the following steps you'll need to know the NETBIOS name of each Imagicle server. Here the instructions to get it:

1) Run a command shell (CMD.EXE) with local Administrator rights.

2) Within the command shell execute the command:

```
nbtstat -n
```

3) Take note of the NETBIOS server name from the command output ('WIN-DCBOSTON-IM' in the exampe below):



Please, notice that the NETBIOS server name maybe different (actually shorter) than the computer name you can see in the Computer properties form of Windows.

Creation of a Computer Account login in the SQL Server - Remote SQL Server

The following T-SQL script is used to create a SQL Windows login associated to a domain machine account and grant it with the mandatory privileges requested by the UC Suite installation. This login will be used by the LOCAL SYSTEM account to authenticate to the SQL Server.

The script must be executed manually on each SQL server instance for each **remote** UC Suite server (domain\hostname$) that needs to authenticate to SQL. Therefore:

- if you are running a cluster of 2 Imagicle servers with a single remote SQL server instance and a shared DB cluster mode, you'll need to run the script 2 times (one for each Imagicle hostname).
- if you are running a cluster of 2 Imagicle servers with 2 remote SQL server instances and a replicated DB cluster mode, you'll need to run the script 4 times (2 times on each SQL server instance).

```
DECLARE @MACHINE_NAME  nvarchar(100)

SET @MACHINE_NAME = 'domain\hostname$'        -- replace domain and hostname$ with the NetBIOS domain \ hostname of

--Do not edit below this line--
USE [master]
IF NOT EXISTS(SELECT * FROM sys.server_principals WHERE name = @MACHINE_NAME)
```

```
BEGIN
    EXEC('CREATE LOGIN [' + @MACHINE_NAME + '] FROM WINDOWS WITH DEFAULT_LANGUAGE=[us_english]')
END
EXEC('GRANT CONNECT SQL TO [' + @MACHINE_NAME + ']')
EXEC('GRANT CREATE ANY DATABASE TO [' + @MACHINE_NAME + ']')
EXEC('GRANT VIEW ANY DATABASE TO [' + @MACHINE_NAME + ']')
```

@MACHINE_NAME variable must be set using the NetBIOS domain name and the hostname of the machine that needs to log in to SQL Server, followed by a final '$' character.

Creation of a Computer Account login in the SQL Server - Local SQL Server

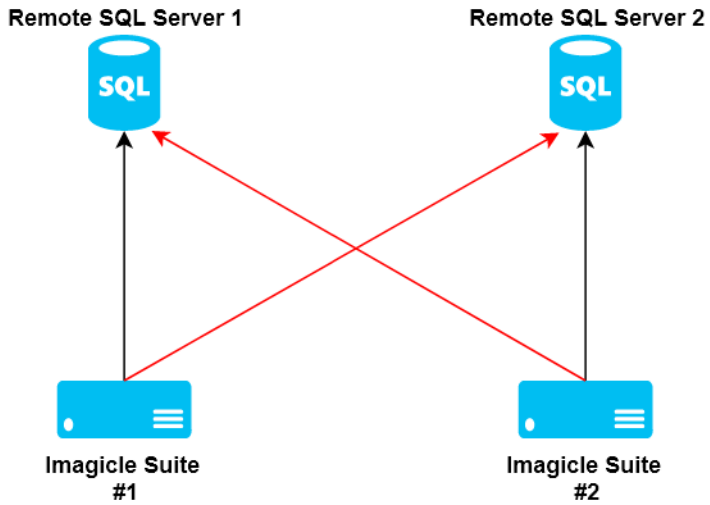
If the SQL server is running on the same UC Suite server (co-resident SQL), on each UC Suite server you need to execute the following T-SQL script:

```
DECLARE @MACHINE_NAME  nvarchar(100)

SET @MACHINE_NAME = 'NT AUTHORITY\SYSTEM'

--Do not edit below this line--
USE [master]
IF NOT EXISTS(SELECT * FROM sys.server_principals WHERE name = @MACHINE_NAME)
BEGIN
    EXEC('CREATE LOGIN [' + @MACHINE_NAME + '] FROM WINDOWS WITH DEFAULT_LANGUAGE=[us_english]')
END
EXEC('GRANT CONNECT SQL TO [' + @MACHINE_NAME + ']')
EXEC('GRANT CREATE ANY DATABASE TO [' + @MACHINE_NAME + ']')
EXEC('GRANT VIEW ANY DATABASE TO [' + @MACHINE_NAME + ']')
```

This must be done even for stand-alone installations that needs to leverage the Windows integrated authentication.

Creation of a Computer Account user in the SQL Server Database

This step is required only if you need to manage an application suite **cluster** running a **replicated** database model. It is necessary to enable each Imagicle suite server to read/write the content of remote nodes databases, in a crossed mode (red lines in the schema above).



The UC Suite database is supposed to be already existing on each SQL server, previously created by the UC Suite DB configuration wizard tool.
The following T-SQL script is used to create a DB user associated to the previously created login and grant it with the db_owner role. This user will be used by the LOCAL SYSTEM account to authenticate to the UC Suite database.

```
DECLARE @MACHINE_NAME  nvarchar(100)
SET @MACHINE_NAME = 'domain\hostname$' -- NetBIOS domain \ hostname of the machine (with final $)
USE [<DB_NAME>] -- UC Suite DB

--Do not edit below this line--
IF NOT EXISTS(SELECT * FROM sys.server_principals WHERE name = @MACHINE_NAME)
BEGIN
    RAISERROR ('The server login %s was not found. Aborting operation.',16,2,@MACHINE_NAME);
END
ELSE
BEGIN
    IF NOT EXISTS(SELECT * FROM sys.database_principals WHERE name = @MACHINE_NAME)
    BEGIN
        EXEC('CREATE USER [' + @MACHINE_NAME + '] FOR LOGIN [' + @MACHINE_NAME + ']')
    END
    EXEC sp_addrolemember N'db_owner', @MACHINE_NAME
END
```

@MACHINE_NAME variable must be set using the NetBIOS domain name and the hostname of the machine followed by a '$' character, while **<DB_NAME>** must be replaced with the database name used by the UC Suite installation.

This query is needed only in a replicated database cluster scenario and must be executed on every database of the cluster **for all the non local nodes** (domain\hostname$).

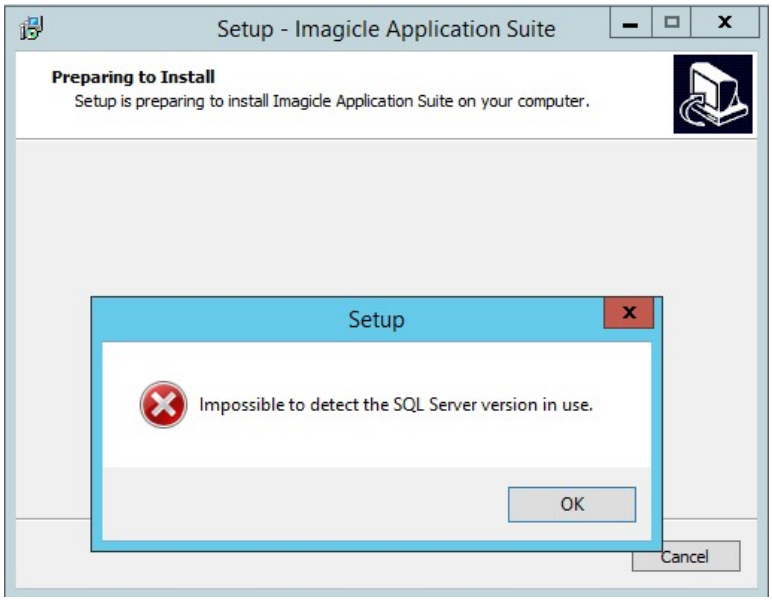
Hostname update

UC Suite hostname is used to provide the UC Suite server with the required credentials to log into the SQL Server via integrated authentication. Thus, if the hostname must be changed, the SQL logins and users manually created in the previous steps must be updated accordingly.

Troubleshooting Most Common Issues

Setup

Updating a UC Suite where Windows integrated authentication was already configured could result in the following error. IN the following picture Windows user cannot access SQL Server through integrated authentication during UC Suite setup.



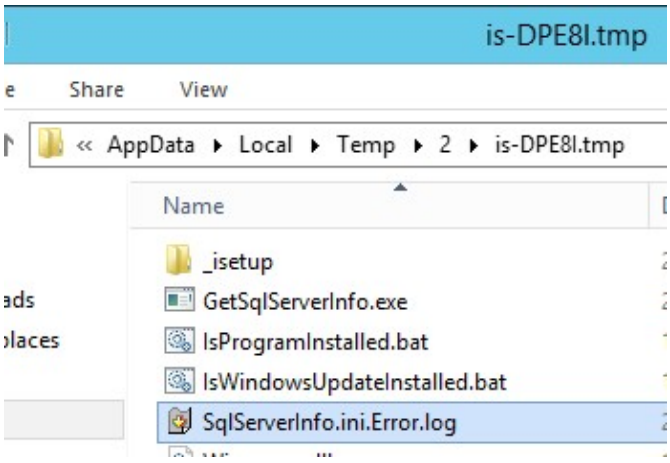
This means that the Windows account used to log into the UC Suite that is performing the update operation cannot access SQL Server through integrated authentication (for instance because it is not a domain account, but rather a local one).

The setup log (%TEMP%\Setup Lo....txt) shows something like

```
2018-08-24 09:17:45.998   Executing: "C:\Users\ADMINI~1\AppData\Local\Temp\2\is-DPE8I.tmp\GetSqlServerInfo.exe" "C:\
2018-08-24 09:17:46.889   Execution completed with return code: 18452
2018-08-24 09:17:46.889   GetSqlServerInfo failed, result 18452
```

The first row of this example (highlighted) points to a folder

(C:\Users\ADMINI~1\AppData\Local\Temp\2\is-DPE8I.tmp) that can be opened in file explorer and contains a file named SqlServerInfo.ini.Error.log on which the error details are logged.



For example:

```
System.Data.SqlClient.SqlException: Login failed. The login is from an untrusted domain and cannot be used with Windo
```

DB configuration wizard

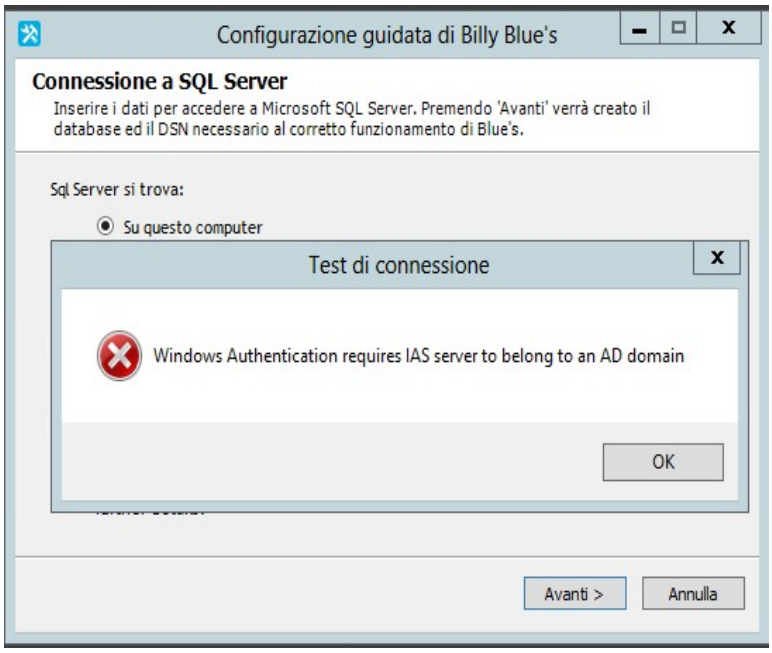
Configuration wizard run without Administrative privilege

The following error can happen when the DB configuration wizard is not run "As Administrator"

In order to be able to proceed just run again the wizard selecting the "Run as Administrator" option.

UC Suite not belonging to a domain

This occurs when the UC Suite does not belong to a domain.

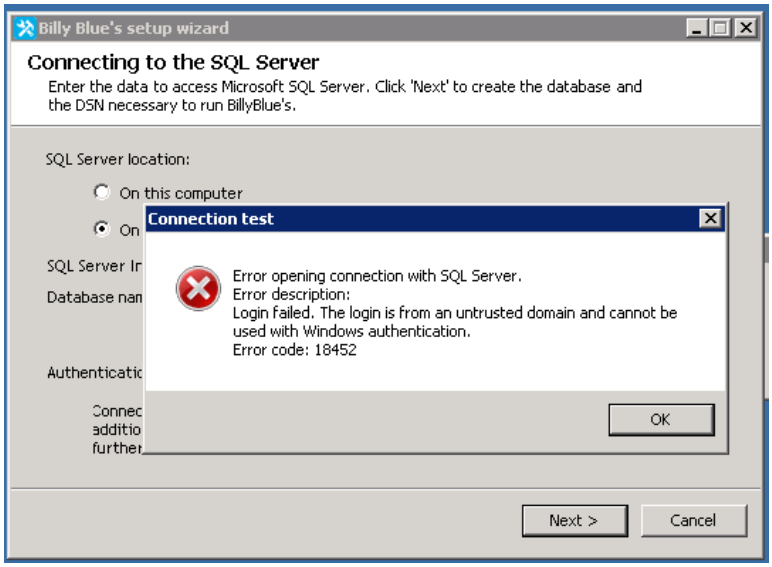


In picture above the user is trying to use Windows integrated authentication from a UC Suite not belonging to any domain.

Windows integrated SQL authentication failure

Tjis error could be caused by the following reasons:

1. The UC Suite and the remote SQL Server belong to different domains
2. The UC Suite and the remote SQL Server belong to the same domain, but the Windows account executing the operation doesn't (for instance because it is local machine administrator)
3. The UC Suite and the executing Windows user belong to the same domain, but the SQL Server does not

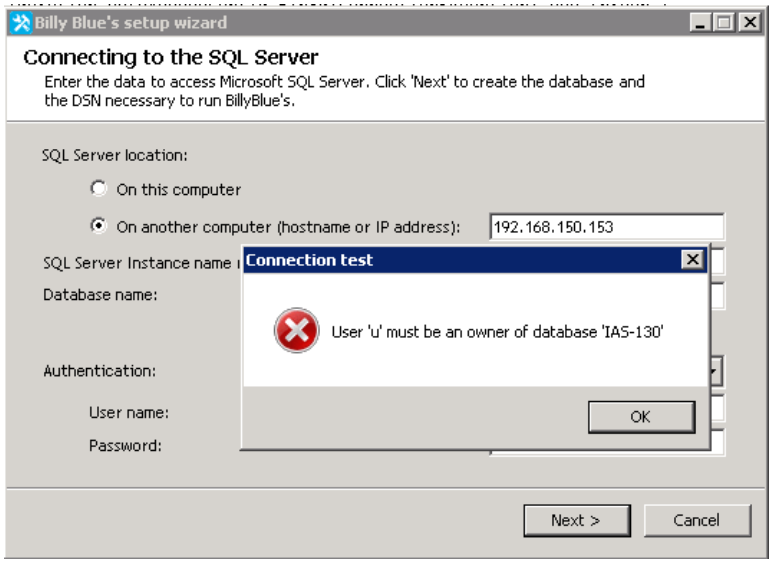


In picture above a user performing the database configuration wizard cannot log into SQL Server using integrated authentication.

SQL account not meeting the minimum privileges to access the UC Suite DB

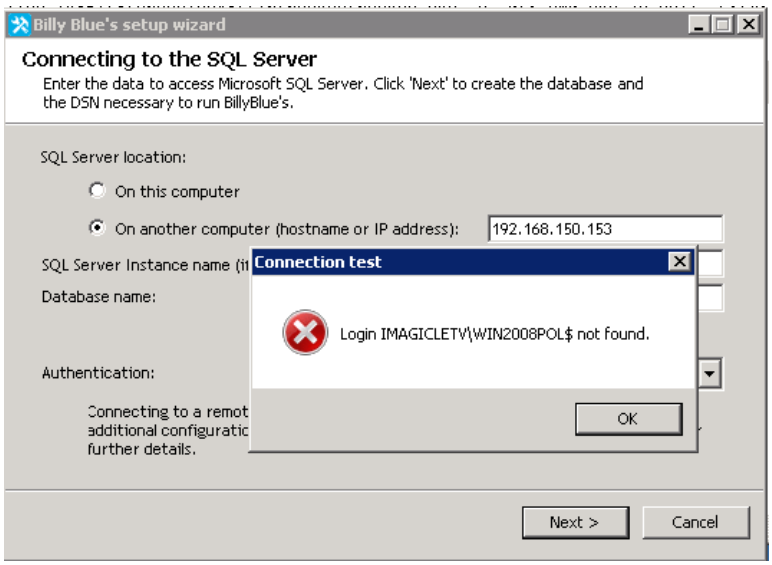
This error can occur when the user is trying to configure the DB using a SQL account that does not comply with the guidelines

Note: this error cannot occur if Windows integrated authentication is selected and the executing user is a domain account



Computer account login not found in the SQL Server

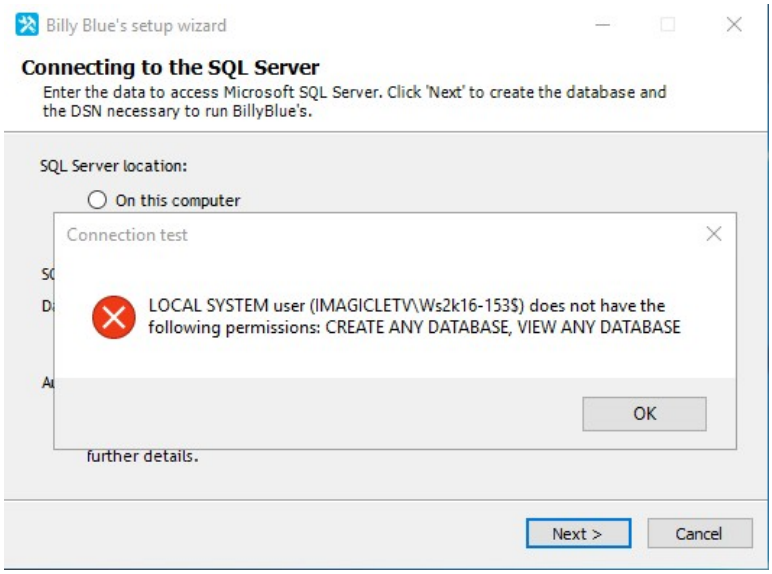
This error occurs when using integrated authentication and the local computer account (domain/hostname$) has not been added to the SQL server following the procedure explained in the section "Creation of a Computer Account login in the SQL Server" of this article.



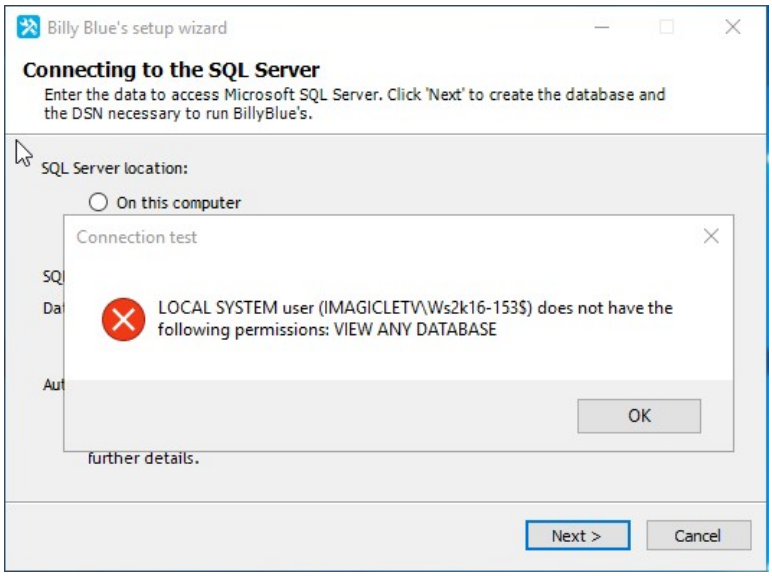
In picture above local computer account cannot into SQL Server via integrated authentication because it was not added to the SQL Server logins.

Computer account login on SQL Server does not meet the minimum grants required

This error occurs when the configuration described in section "Creation of a Computer Account login in the SQL Server" of this article has not been properly done. The popup error message reports the missing grants that needs to be added (using the query described in the above mentioned section of the article).

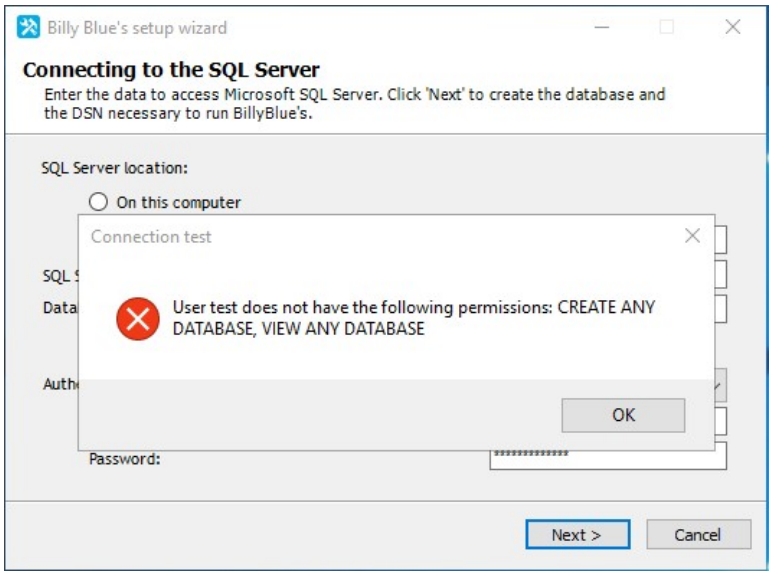


In picture above the user is configuring the database connection via integrated authentication method, but the CREATE ANY DATABASE and VIEW ANY DATABASE grants are missing for the local computer account.



In picture above the user is configuring the database connection via integrated authentication method, but the VIEW ANY DATABASE grant is missing for the local computer account.

The same error can also occurs using usual SQL authentication when the SQL user used to configure the connection is not granted with the minimum privileges described in this support page.



In picture above the user is configuring the database connection via SQL authentication method, but the CREATE ANY DATABASE and VIEW ANY DATABASE grants are missing for the SQL account used in the configuration.

Advanced Troubleshooting Hints

Useful log are placed in: <install dir>\Apps\BillyBlues\Engine\guidedconfiguration.log

Diagnostic tool is placed in: StonevoiceAS\System\GetSqlServerInfo.exe -c "<connection string>" -o c:\out.txt

If a connection is correctly established this tool produces an output file out.txt (given the last parameter of the command line provided in this example)

```
[SqlServerInfo]
IsLocal=0
InstanceName=IMAGICLE
ProductVersion=10.50
Edition=Express Edition
EngineEdition=4
DbName=master
[LoginInfo]
SystemUser=u
LoginExists=False
[ServerPrivileges]
ConnectSql=True
CreateAnyDatabase=False
ViewAnyDatabase=False
[DatabasePrivileges]
UserIsOwner=False
```

On the other hand, upon failing in logging into the SQL Server specified by the connection string, the tool generates an error file out.txt.error.log that shows the both the error message and stack

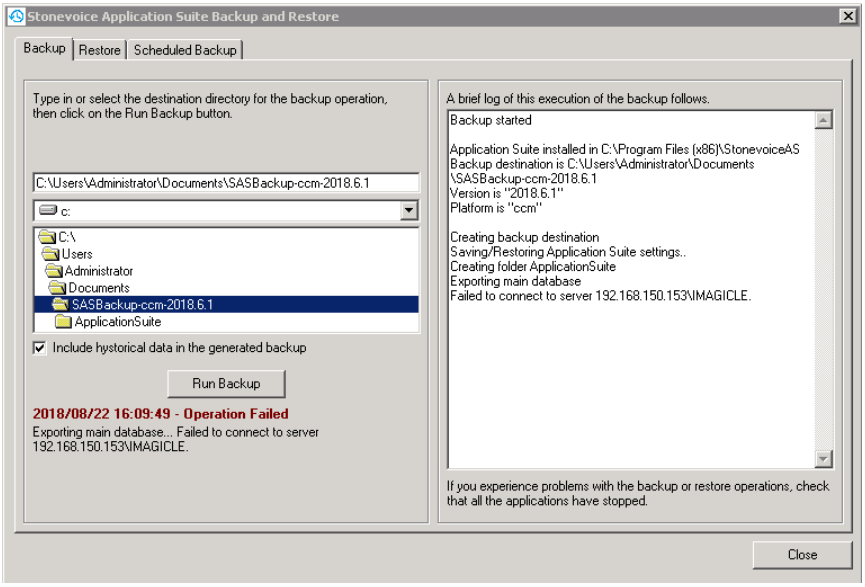
```
System.Data.SqlClient.SqlException: Login failed. The login is from an untrusted domain and cannot be used with Windo
   at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection)
   at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj)
   at System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, B
   at System.Data.SqlClient.SqlInternalConnectionTds.CompleteLogin(Boolean enlistOK)
   at System.Data.SqlClient.SqlInternalConnectionTds.AttemptOneLogin(ServerInfo serverInfo, String newPassword, Boole
   at System.Data.SqlClient.SqlInternalConnectionTds.LoginNoFailover(String host, String newPassword, Boolean redirec
   at System.Data.SqlClient.SqlInternalConnectionTds.OpenLoginEnlist(SqlConnection owningObject, SqlConnectionString
   at System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString con
   at System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, Object poolGroupProvid
   at System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnection owningConnection, DbConnectio
   at System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject)
   at System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject)
   at System.Data.ProviderBase.DbConnectionPool.GetConnection(DbConnection owningObject)
   at System.Data.ProviderBase.DbConnectionFactory.GetConnection(DbConnection owningConnection)
```

```
   at System.Data.ProviderBase.DbConnectionClosed.OpenConnection(DbConnection outerConnection, DbConnectionFactory co
   at System.Data.SqlClient.SqlConnection.Open()
   at GetSqlServerInfo.Program.Main(String[] args
```

Backup & Restore

The backup fails with error "Failed to connect to server ..."

backup fails showing the following screen (backup failed because the executing user cannot connect to SQL Serve via integrated authentication):



and the log Var\Log\BackupRestore\ApplicationSuite.log.txt shows:

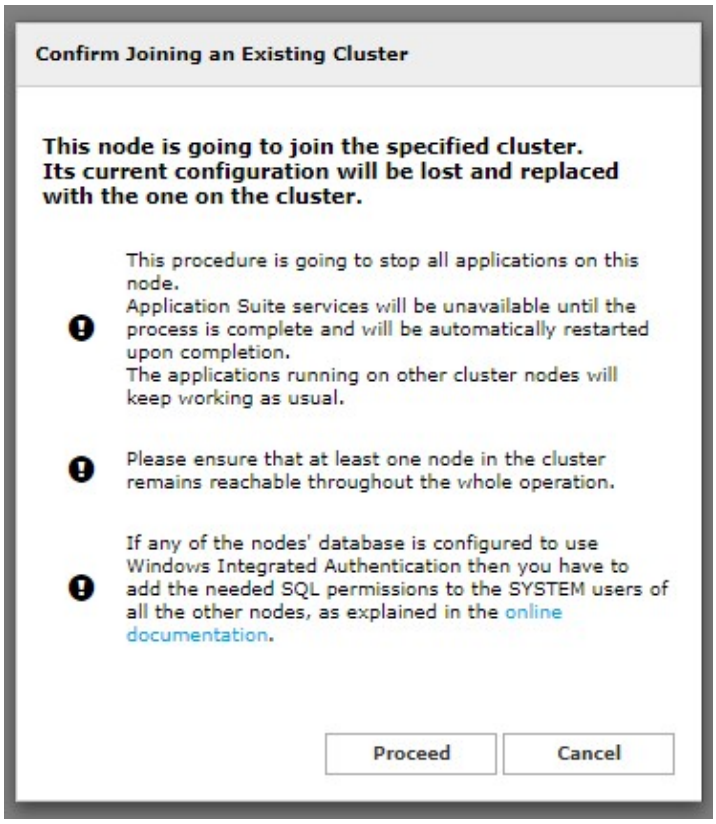
```
...

0822 16:09:51.935 ERROR {  1} [ApplicationSuite] [SvDataComUtils] An error occurred: Function {ExportDatabase}, {
Exception Type {Microsoft.SqlServer.Management.Common.ConnectionFailureException}
Message {Failed to connect to server 192.168.150.153\IMAGICLE.}
...InnerException {
Exception Type {System.Data.SqlClient.SqlException}
Message {Login failed. The login is from an untrusted domain and cannot be used with Windows authentication.}
```

This occurs when the Windows user that is performing the backup cannot access the DB via integrated authentication

WorkAround: a possible workaround consists in executing the database backup tool as a local system account

New machine joining a UC Suite cluster

When a new machine is joining a cluster, a new message is shown as follows



Even if the database configuration is not carried out correctly as described in this document, the cluster joining will be successful, but the databases won't be able to synchronize with each other:

22/08/2018 18.03.22	Replication Service	Cluster Data Synchronisation	⚠	206	This IAS Cluster node failed to synchronise its data (Task FaxDB) with current remote node: WS2K16-153:192.168.150.153. The reason of the synchronisation failure is: failed to synchronise database (Cannot open database "IAS" requested by the login. The login failed. Login failed for user 'IMAGICLETV\WINDOWS2012POL$'.)	☑	☑