

QGRIP

Plugin

QGrip SQL Installer

GRIP ON SOL

2024-04-16

Contents

1	Introduction	4
2	Getting Started.....	5
2.1	Prepare	5
2.2	Start QGrip-SQL-Installer	5
2.3	Main Buttons	6
3	Install SQL Instance	8
3.1	Install Tab: General.....	8
3.2	Install Tab: Services	9
3.3	Install Tab: Instance.....	9
3.4	Install Tab: Directories.....	10
3.5	Install Tab: TempDB.....	11
3.6	Install Tab: Software + Scripts	12
3.7	Install Tab: Install + Configure	12
4	Templates and Post Install scripts.....	15
4.1	Edit Template.....	16
4.2	Export Template	19
5	Post Install Scripts	20
5.1	Edit Script.....	21
5.2	Check Substitutions	22
6	Prepare Instance Host (Machine)	23
6.1	Firewalls.....	23
6.2	Managed Service Accounts (Stand Alone Instance)	24
6.2.1	Check: KdsRootKey.....	24
6.2.2	Create: MSA accounts on AD	25
6.2.3	Install: MSA accounts on New Instance Host.....	26
6.3	group Managed Service Accounts (Always on Cluster)	27
6.3.1	Check: KdsRootKey.....	27
6.3.2	Create: GSG_AOCluster01.....	27
6.3.3	Create: gMSA accounts on AD	28
6.3.4	Install: gMSA accounts on New Instance Hosts	29
7	Offline-Install.....	30
8	New Instance Host Help.....	32
9	Prepare QGrip-ToolShare.....	35
10	Install Failed: Known Errors	37

10.1	The credentials for SQL Server Agent service are invalid.....	37
11	Appendix	38
11.1	Install: SQLCmdLine Utils.....	38
11.2	Create: QGripSQLInstall.....	38
11.2.1	Find Password: QGripSQLInstall	38
11.3	Add: KdsRootKey	39
11.4	QGrip-ToolShare: Authorise and Share	41
11.4.1	Authorise.....	41
11.4.2	Share	42

1 Introduction

The QGrip-SQL-Installer is a separate executable that can be used to quickly install and configure new SQL Server Instances. Templates are used to ensure uniformity and save time. The QGrip-SQL-Installer does only support (group) Managed Service Accounts (MSA, gMSA) for the SQL Server Agent and DBEngine services which is much better from a security point of view. The Templates and Post Install (hardening and standards) scripts are edited in the QGrip-SQL-Installer.exe and saved in the QGrip Database.

When the machine, where the SQL Server Instance will run, has been delivered and prepared and all necessary firewalls are open, you will only need +/- 10 minutes before the SQL Server Instance is up-and-running. Once running, the Instance has been added to QGrip and authorisation for the Backup Shares have been set. Only the Instance Schedules need to be activated in QGrip.

The following will be done by the QGrip-SQL-Installer:

- Set block size disks.
- Generate Config file.
- Run the setup.
- Run all available CU's and service packs.
- Set TCP port number.
- Add local firewall rules (Instance port, UDP 1434 and 5022 in case of Always on Instance).
- Move System DB Data/Log files (optional).
- Adjust start-up parameters.
- Add retry start-up services.
- Set SPN if needed.
- Set Max Size Tempdb files.
- Set Instance Max/Min Memory.
- Enable AlwaysOn (only AlwaysOn Instance, manual action).
- Run Hardening & Standards Scripts.
- Add gMSA_QGrip\$ as SYSADMIN on the Instance.
- Authorise DBEngine account for QGrip Backup Shares.
- Add the Instance to QGrip.
- Set sa (or equivalent) password and save password in QGrip (only mixed mode).
- Trigger Discover of the Instance.

The only manual action is enabling AlwaysOn in SQL Server Configuration Manager when applicable. A popup will appear when this action is needed.

The QGrip-SQL-Installer should be used to install mainstream SQL Server Instances and will only install the database engine. If you need to install other options, like SSIS, SSAS and Reporting Service, you will need to add these options after the install or do the whole install manually.

2 Getting Started

2.1 Prepare

Before you can start installing new SQL Server Instances using the QGrip-SQL-Installer, some preparation is needed:

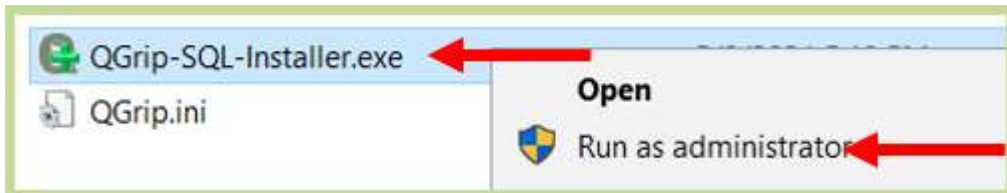
1. Prepare QGrip-ToolShare.
2. Create Templates and Post Install scripts (hardening/standards script).
3. Prepare the machine (Instance Host), see section

2.2 Start QGrip-SQL-Installer

The QGrip-SQL-Installer can be downloaded from the QGrip database using the QGrip-Setup. It contains version control and you will be asked to download the correct version if needed when starting the executable. The QGrip.ini with the connection string to the QGrip database is needed in the same directory as the executable.

If you only want to edit Templates and/or Post Install scripts, you can start QGrip-SQL-Installer.exe from anywhere (QGrip Server?) but if you want to Install a new SQL Server Instance, the executable needs to be started from new Instance host. If the latter, you can choose to start it directly from the QGrip-ToolShare or copy the exe- and ini-files to a local directory on the machine and start it from there.

Run as Administrator



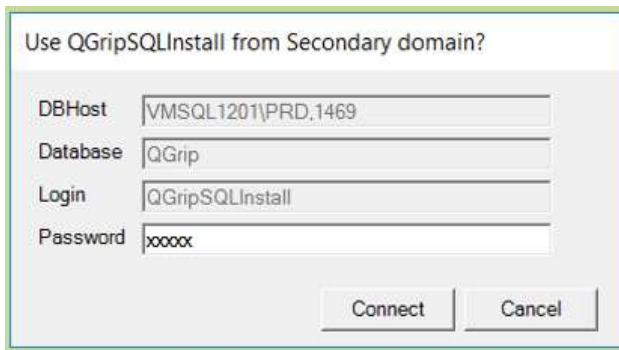
The QGrip-SQL-Installer needs to be started as Administrator. Your AD account needs to be QGrip-Admin and you must also be Local Admin on the machine.

Error: SQLCmd not available



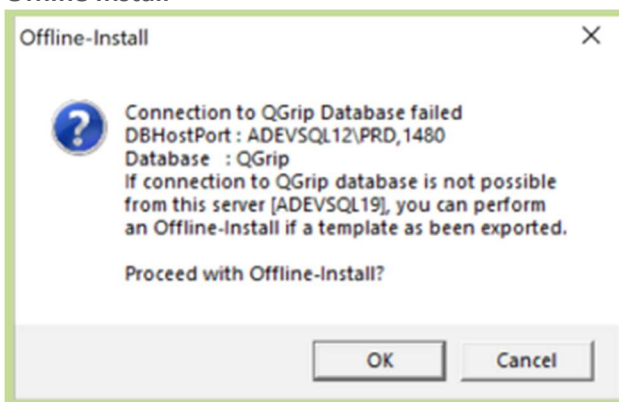
If you get this error message you need to install the SQLCmdLineUtils, see appendix.

Started on Secondary Domain



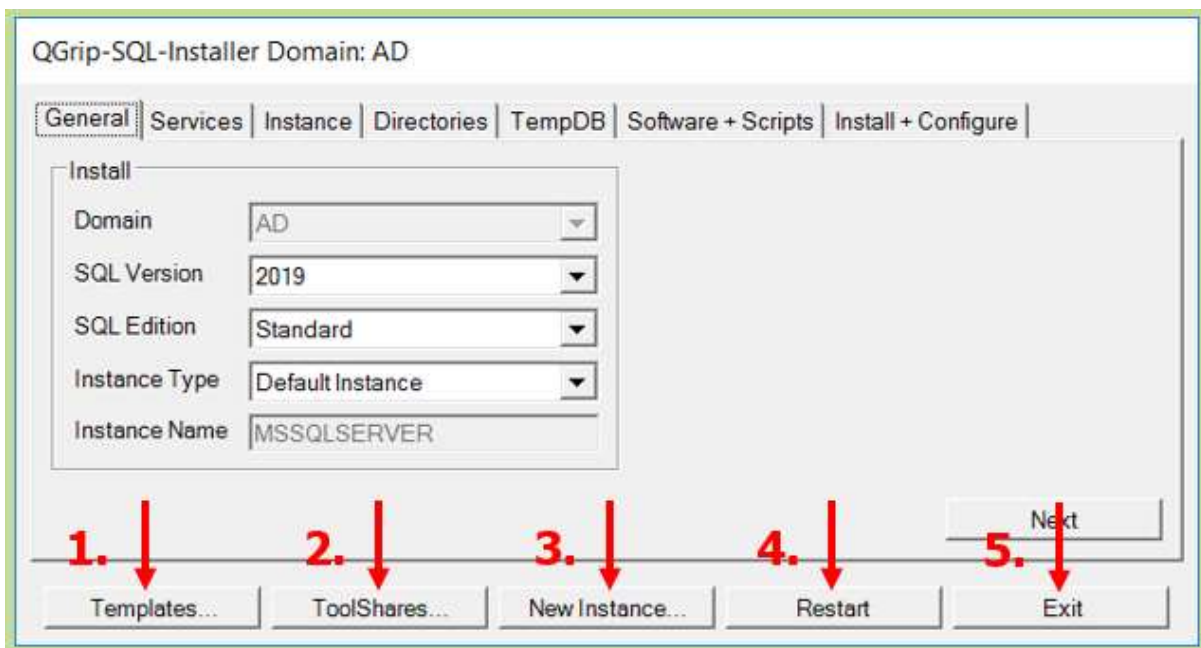
If you run QGrip-SQL-Installer on a secondary domain, you need to create and use the QGripSQLInstall account, see appendix.

Offline Install



If it is impossible to connect to the QGrip database from the Machine where you want to install SQL Server, you can do an 'Offline-Install'. It will take 5 seconds before you see the message above (connection timeout is set to 5 seconds). See section Offline-Install below.

2.3 Main Buttons

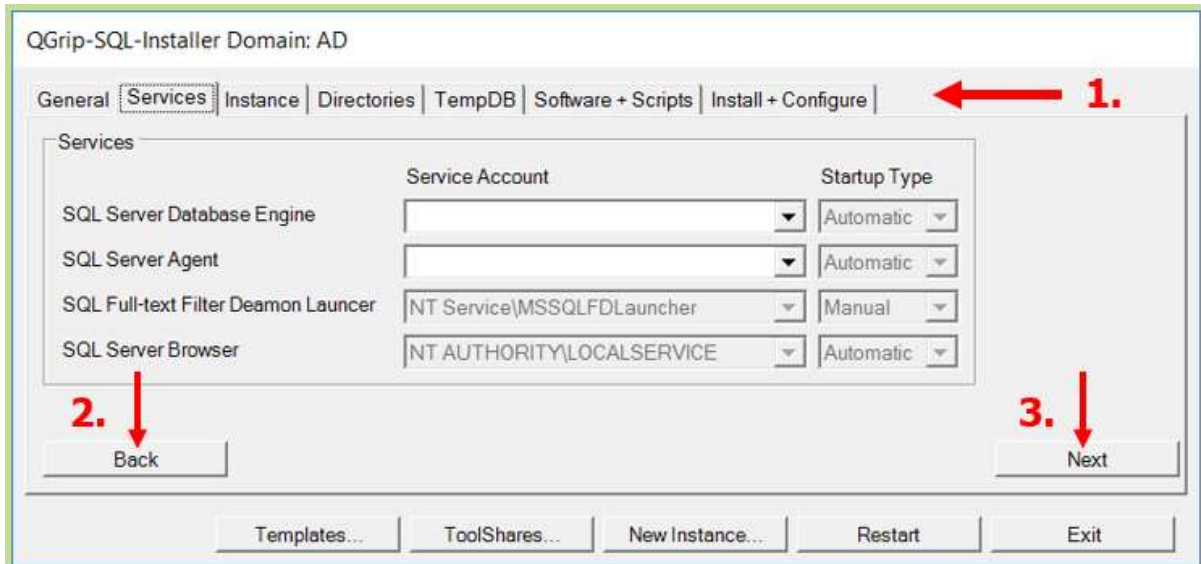


The main buttons can be found at the bottom of the main window.

1. **[Templates...]** to open the Templates window to edit Templates and Post Install Scripts.
2. **[ToolShares...]** to open the ToolShares window where the UNC path to the shares can be set and found.
3. **[New Instance...]** to open the New Instance Host Help window where information needed for a new Instance Host can be generated like Disk requests according to Template, Firewall Rules/Checks and Scripts/Instruction to create the DBEngine and Agent accounts.
4. **[Restart]** will reset all parameters in the Install window and allow you to start from scratch again.
5. **[Exit]** to close QGrip-SQL-Installer.

3 Install SQL Instance

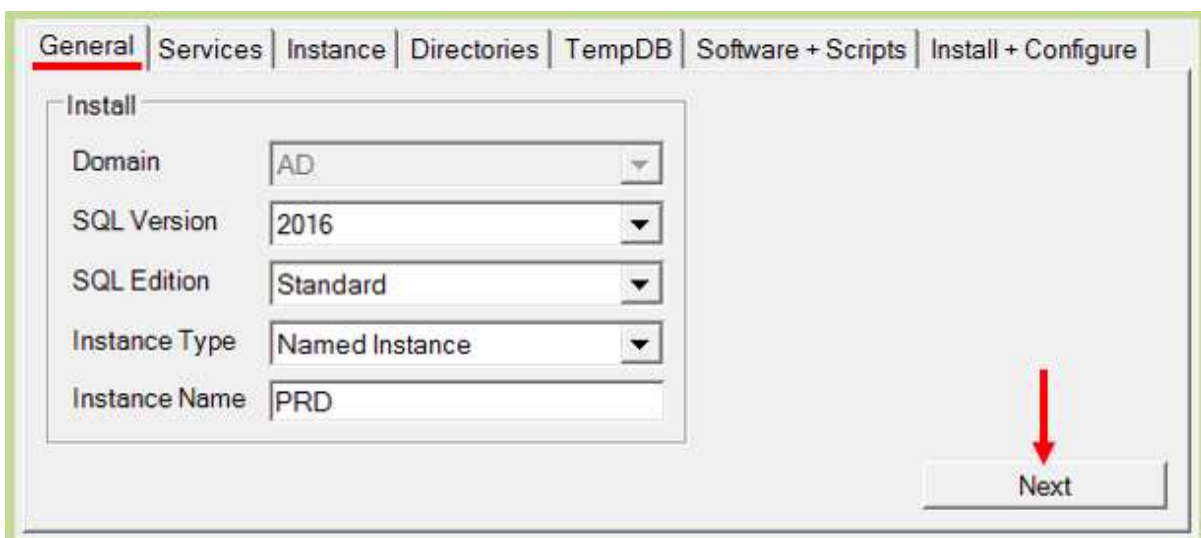
Take a snapshot/backup of the new Instance Host/Machine before you start and make sure that you can revert to the snapshot in case the Install fails.



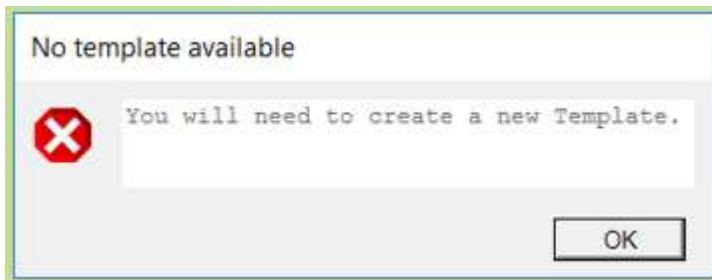
1. The tabs represent the steps that need to be completed. Tab page can only be switched with the **2. Back** and **3. Next** buttons. When switching to the next tab, the input is checked and verified.

If you need to adjust the Template you are using, press Templates and adjust the Template. When you are ready, you will need to push Restart to load the adjusted Template and start all over again.

3.1 Install Tab: General

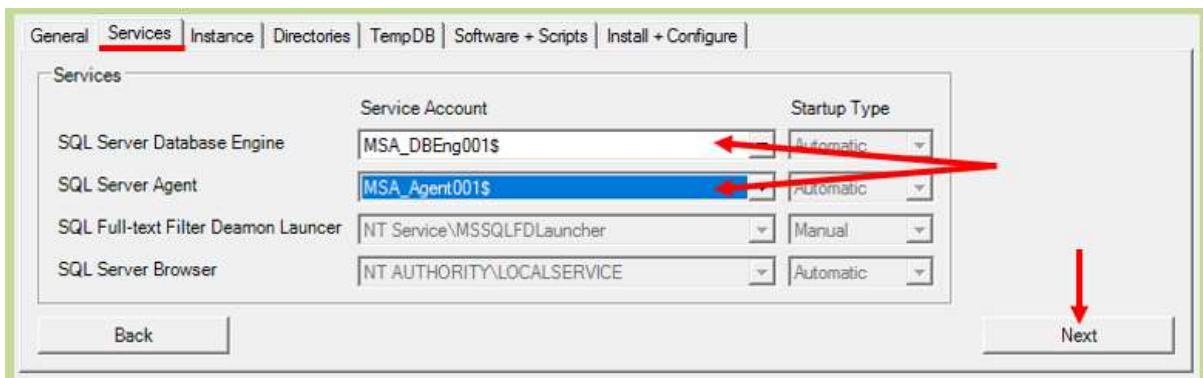


Choose the type of SQL Server Instance you want to Install and press Next.
Instance name is only required for Instance Type 'Named Instance' and 'Always On Instance'.



If there is no template for chosen combination, you will need to create it.

3.2 Install Tab: Services



The 'Startup Type' is greyed out and the setting in the Template cannot be overruled. Choose Service Account for the Database Engine and Agent services and press **Next**.

Service Accounts (MSA, gMSA) will only be shown here if they have been

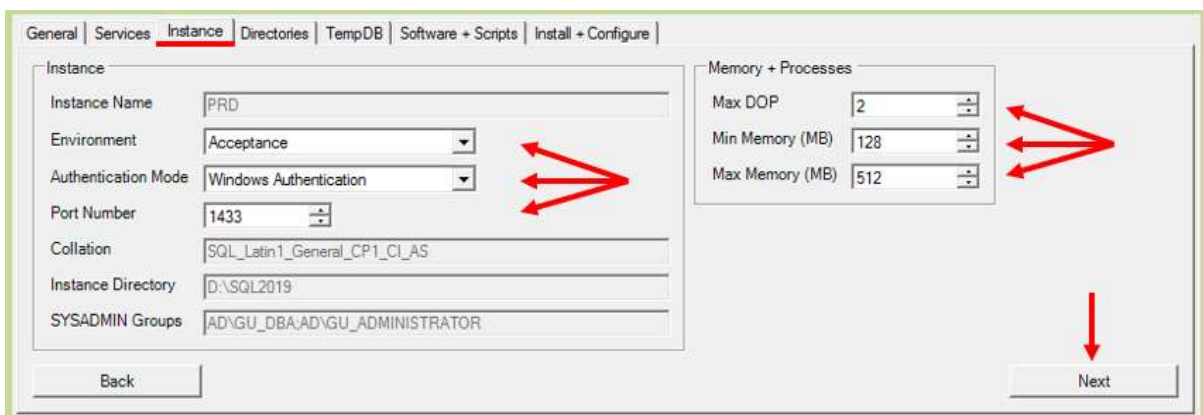
- created on the AD for this particular Machine and
- have been installed on this Machine

as described in the Prepare Instance Host (Machine) section.

The type of Account shown (MSA, gMSA) depend on the Instance Type chosen in the General tab:

- Default Instance: MSA + gMSA
- Named Instance: MSA + gMSA
- Always On Instance: gMSA

3.3 Install Tab: Instance



Choose and check the parameters and press **Next**.

Instance

Select (DTAP) Environment, Authentication Mode and Port Number.

Instance Name has been set from tab General and cannot be changed here.

Collation, Instance Directory and SYSADMIN Group are greyed out and the setting in the Template cannot be overruled.

Memory + Processes

QGrip default **Max DOP** = number of available processors. Set it to 0 to use all available processors.

QGrip default **Min Memory (MB)** = 128

QGrip default **Max Memory (MB)** = MAX (512, Available Memory – Instance Type Factor)

Instance Type Factor: Default Instance, Named Instance: 2.048 MB

Always On Instance: 3.072 MB

Next: Input Check

When Next is pressed, the following will be checked and errors shown:

Port Number: Already in use on Machine

Instance Directory: The Drive exists on the Machine and is not used as DVD drive.

SYSADMIN Groups: Current account (yours) is member of (at least one) SYSADMIN groups.

Memory: Min Memory > Max Memory

Min Memory: Exceeds (Available Memory - 512 MB).

Max Memory: Exceeds (Available Memory - 512 MB).

3.4 Install Tab: Directories

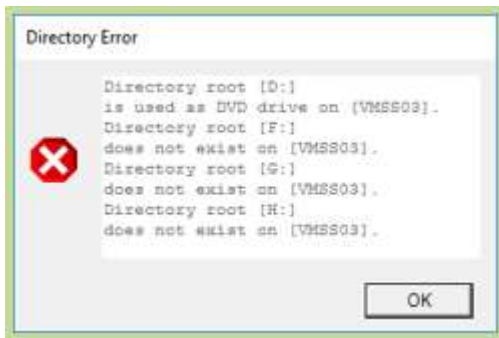
The screenshot shows the 'Directories' tab of the QGRIP SQL Installer. The 'Install Directories' section contains the following fields:

- Shared Features: D:\SQL2019
- Shared Features(x86): D:\SQL2019\{x86}
- User Database Data: E:\SQL2019\PRD\DATA
- User Database Log: F:\SQL2019\PRD\LOG
- Tempdb Data: G:\SQL2019\PRD\TEMPDBDATA
- Tempdb Log: G:\SQL2019\PRD\TEMPDBLOG
- Backup Directory: H:\SQL2019\PRD\BACKUP

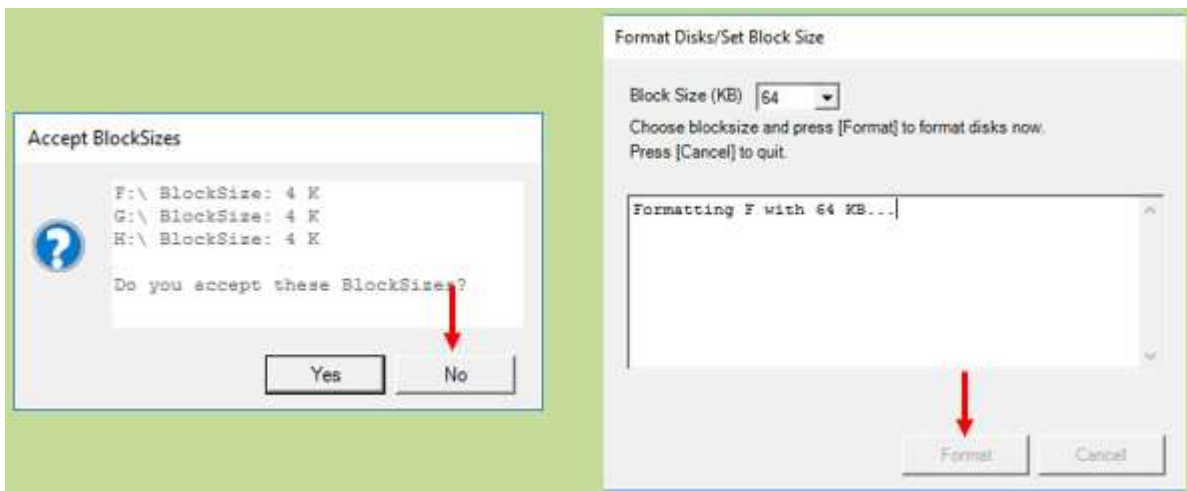
Below this section, there is a checkbox for 'Move System Databases (master,model,msdb)' which is checked. Underneath, there are fields for 'System Database Data' (E:\SQL2019\PRD\DATA) and 'System Database Log' (F:\SQL2019\PRD\LOG). At the bottom of the window, there are 'Back' and 'Next' buttons. Red arrows in the image point to the 'User Database Data', 'User Database Log', and 'Tempdb Data' fields, and another red arrow points to the 'Next' button.

The Directories are greyed out and the setting in the Template cannot be overruled. If the {InstanceName} variable has been used in the Template, it has now been replaced with the actual Instance Name that was set in Tab General.

Check the parameters and press **Next**.

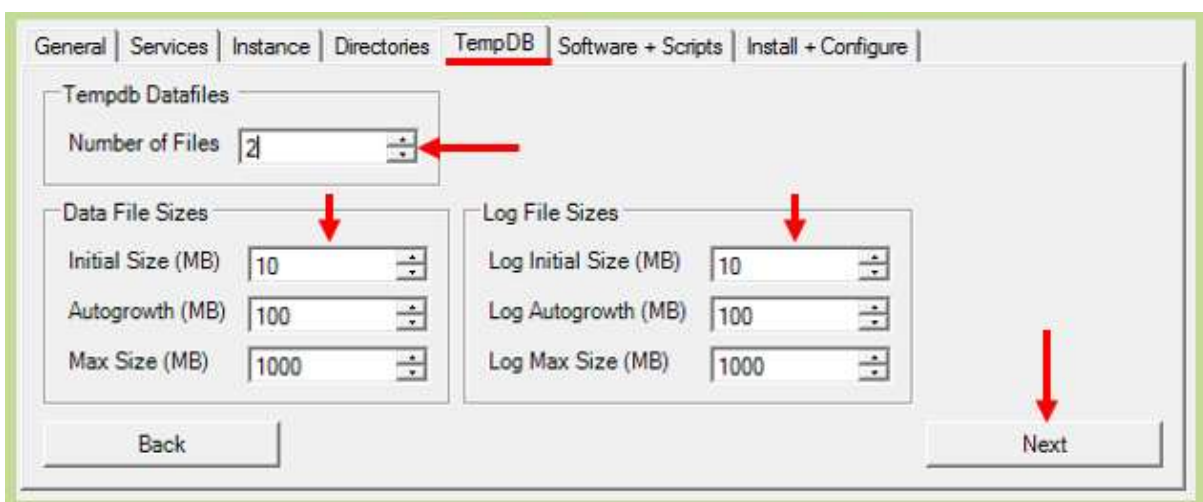


If the Directory Drive does not exist on the machine or is used as DVD drive, you will receive an Error.



If the Drives for User Data/Log, Tempdb Data/Log or System DB Data/Log are empty, you will be asked to accept the Block Sizes. Choose no if you want to change, choose the preferred Block Size and Click Format. If the disks are large, setting the block size might take a few minutes.

3.5 Install Tab: TempDB

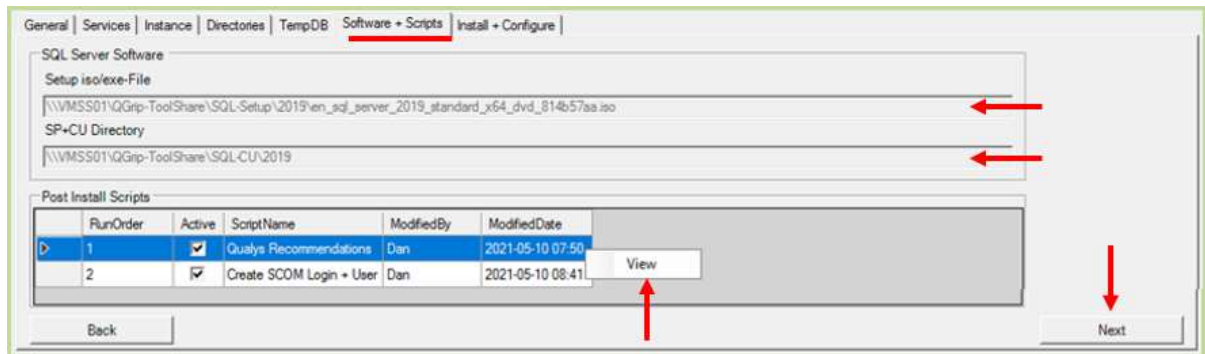


Choose and check the parameters and press **Next**.

Number of Datafiles will be set to the number of available processors on the Machine but with a max of 8.

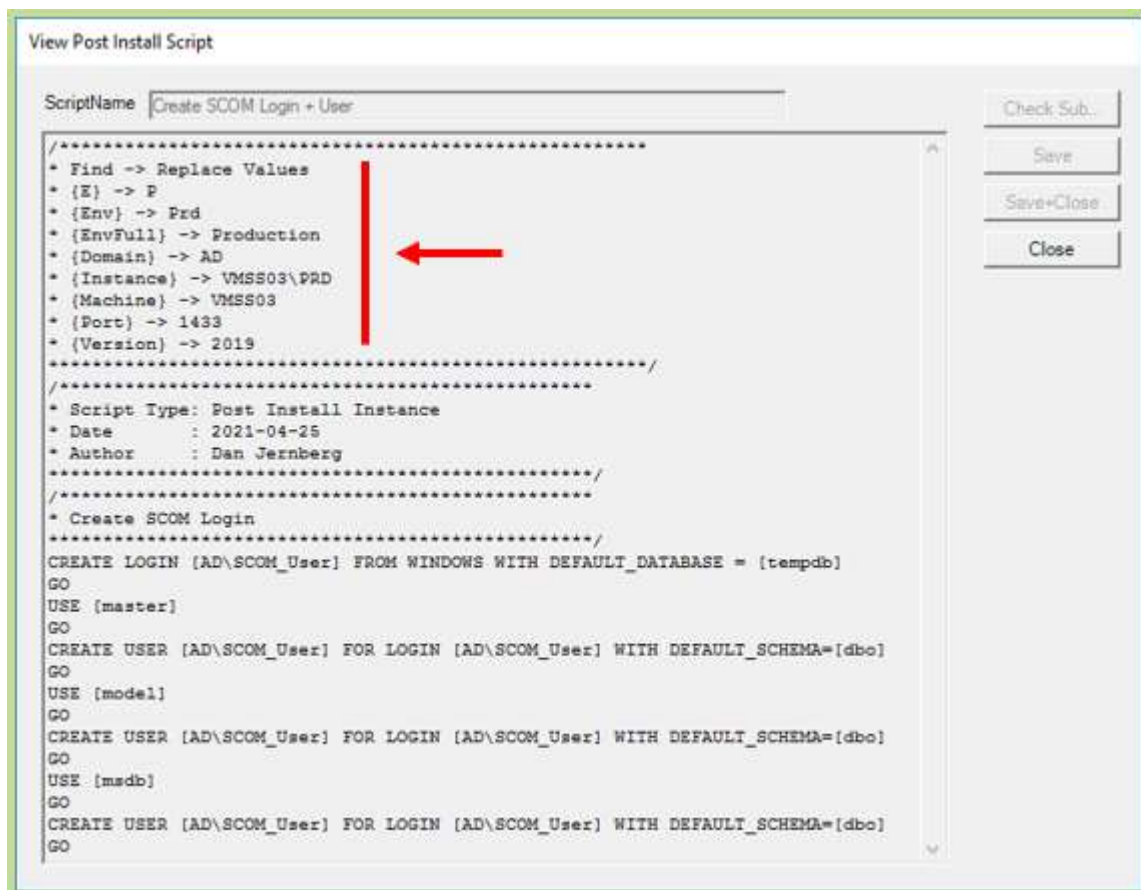
The Sizes are per file, have been copied from the Template and all values can be adjusted for the Install. By keeping the Initial Sizes small, the Instance will start more quickly.

3.6 Install Tab: Software + Scripts



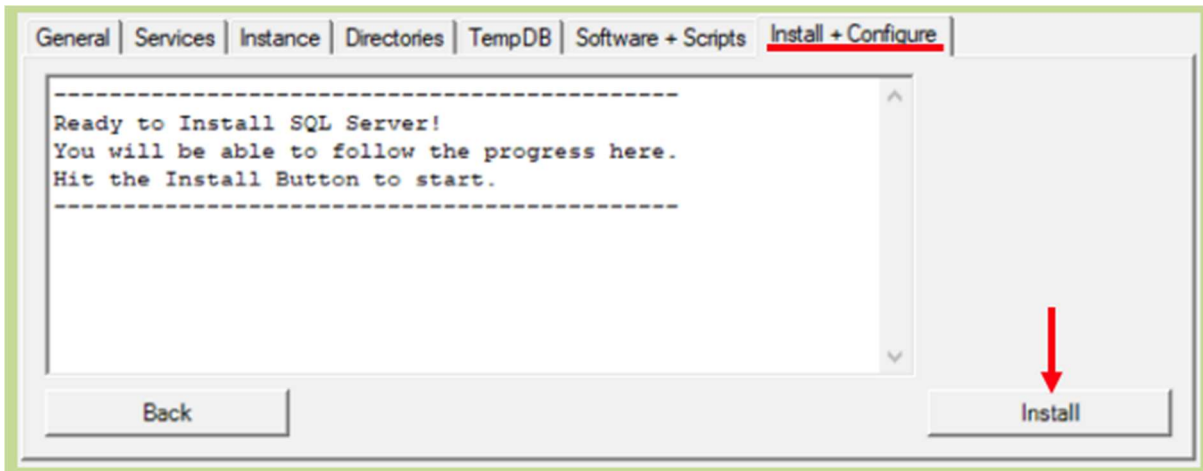
The setting in the Template cannot be overruled. Check the parameters and press **Next**.

By selecting and right clicking on a Post Install Script, it can be viewed.



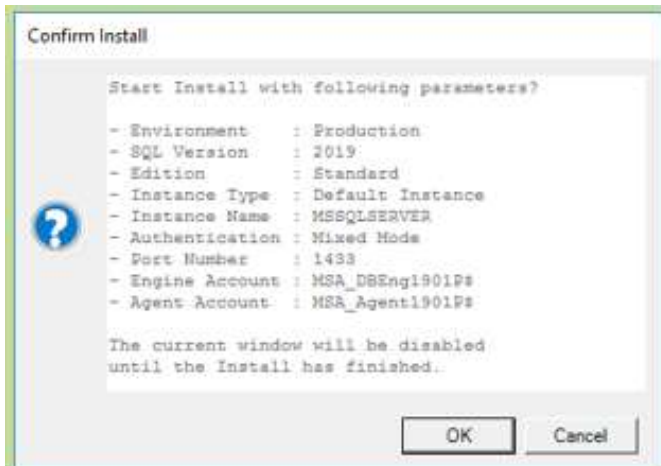
The substitutions have been applied to the script and is shown how it will run during the Post Install. A section with the Find->Replace values has been added at the very beginning of the script.

3.7 Install Tab: Install + Configure



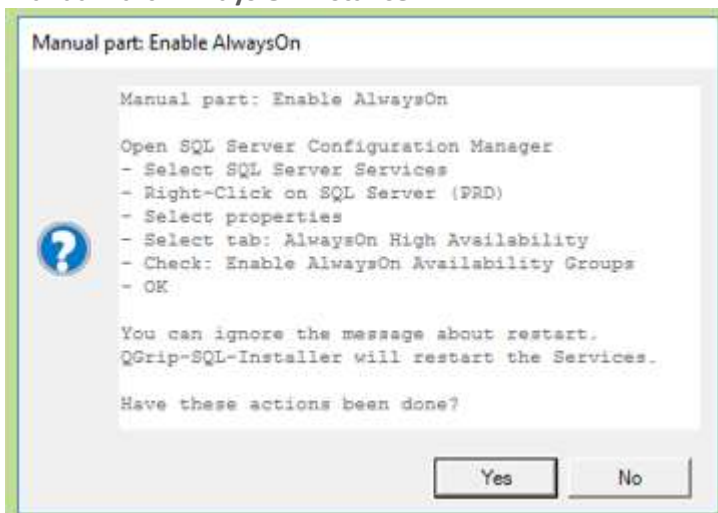
To start the Install, press **Install**.

Confirm Install



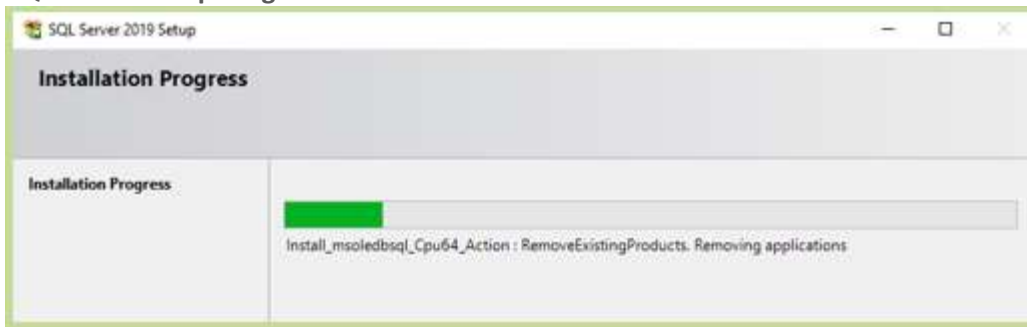
Check the parameters and press OK to start the Install. The Install will take 3 – 10 minutes.

Manual Part: Always On Instance



There is one manual part that needs to be done during the Install of an Always On Instance. The popup above will appear when the step should be executed. You must do these steps before you click Yes, otherwise in install will fail!

SQL Server Setup Progress

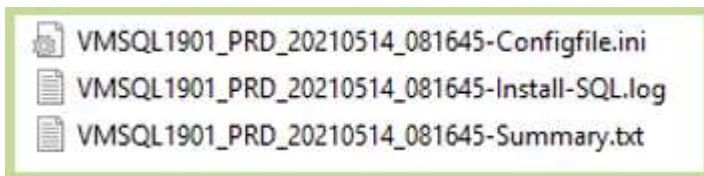


During parts of the install, the SQL Server Setup progress will be visible. Just wait!

Install Status



When the Install has finished, a popup is shown with the Status and the location of the Logfile.



These 3 files will be available in the directory where QGrip-SQL-Installer was started.

If the Install fails with an error, please check section

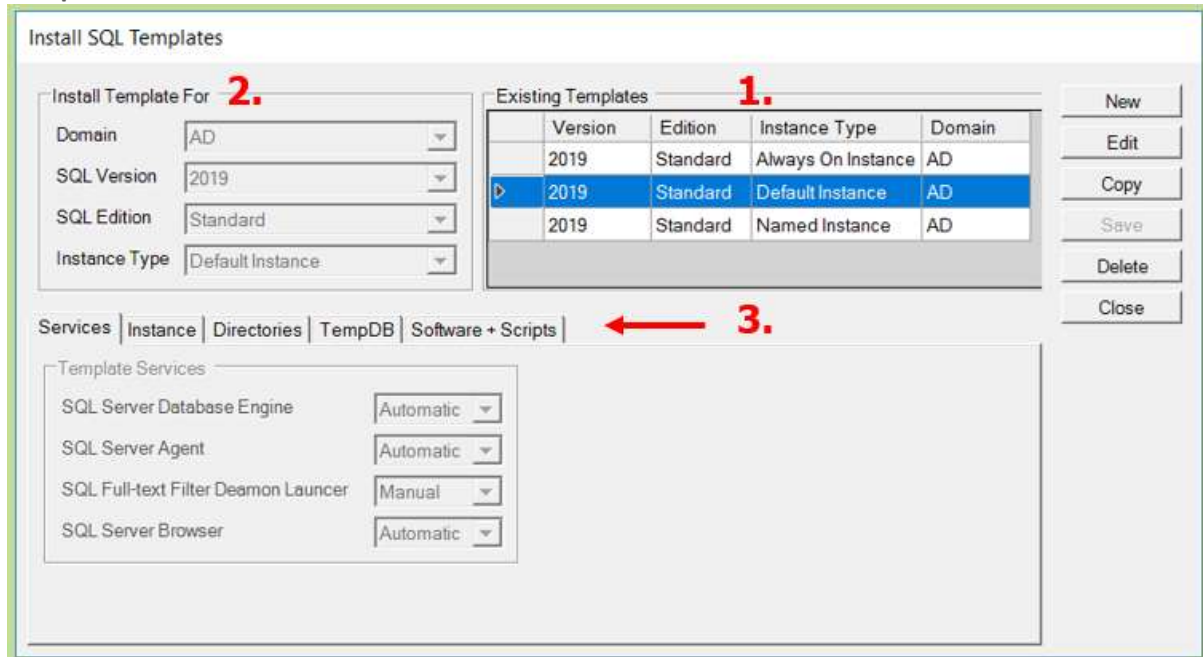
- Install Failed: Known Errors

at the end of this document. If your error is not listed there, please contact Grip on SQL.

4 Templates and Post Install scripts

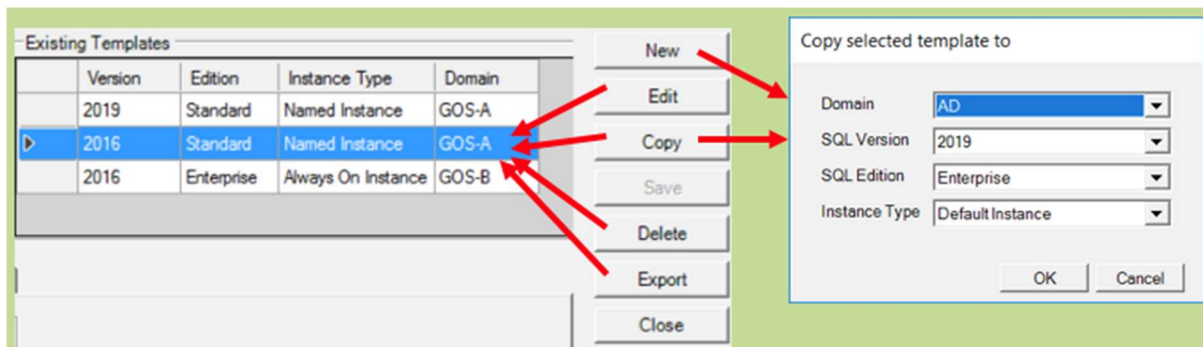
The Templates are used as a 'suggestion' during the actual Install of the SQL Server Instances and almost all values can be adjusted during the actual Install. We advise you, however, to correct the Template instead of changing the values again and again during the Install.

Templates Window



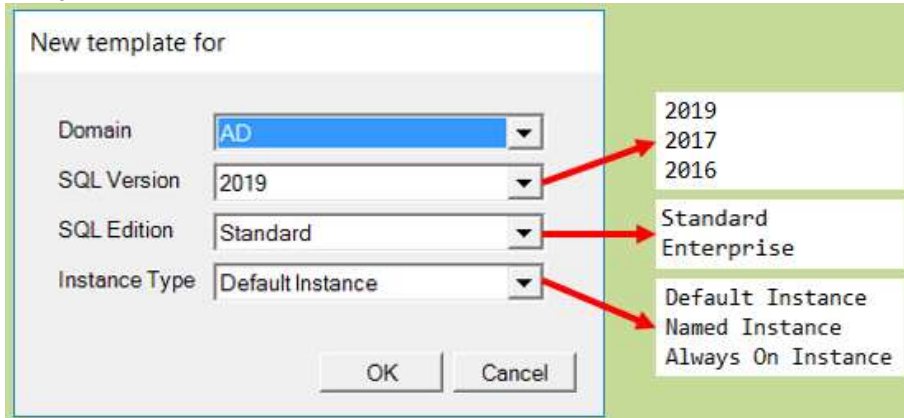
1. Listing of all available Templates. When a row is selected, the details of the Template will be shown in 2. and in the different tabs in 3.

Buttons



- New** Define a New Template from scratch.
- Edit** Press to Edit the selected Template.
- Copy** Press to Copy selected Template to a New Template.
- Save** Save the current Template, only enabled in edit mode.
- Delete** Press to Delete the selected Template.
- Export** Press to Export the selected Template to be for an Offline-Install.
- Close** Press to Close the Templates Window.
- Cancel** Press Cancel to exit edit mode without saving changes. Only visible in Edit mode.

Template for Selection



When a new template is created (new and copy), you will need to select for which type of install the template is and on which AD Domain. These parameters cannot be changed later.

4.1 Edit Template

New Template

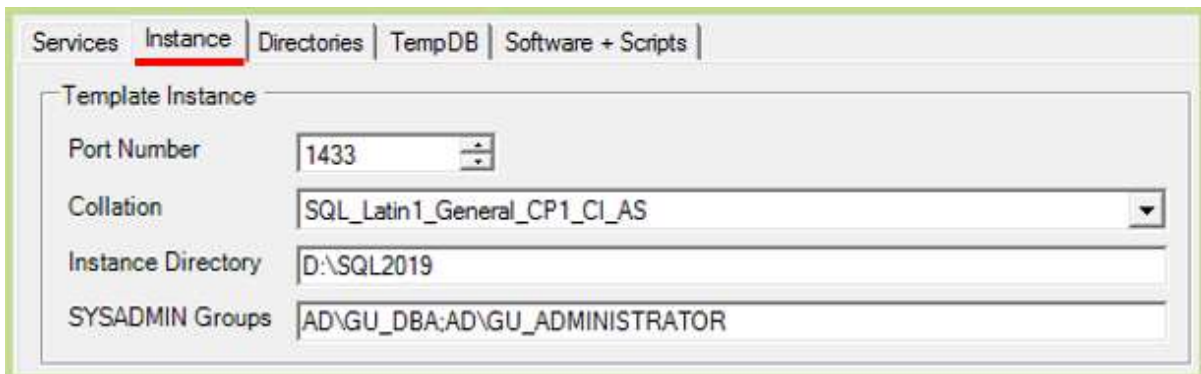
If the Template has been created from scratch (New), QGrip will fill the template with default values. You will need to check the template thoroughly, especially the directories and the location of the software (Setup iso and SP+CU).

Services



Define the Services start mode. DB Engine and Agent cannot be changed and are always Automatic.

Instance



Default Port Number, Collation and Instance Directory. At least one SYSADMIN group needs to be listed. In case of multiple groups, separate with comma or semicolon.

Directories

The screenshot shows the 'Directories' tab of the QGRIP SQL Installer. The 'Template Directories' section includes the following fields:

- Shared Features: D:\SQL2019
- Shared Features(x86): D:\SQL2019\x86
- User Database Data: E:\SQL2019\{InstanceName}\DATA
- User Database Log: F:\SQL2019\{InstanceName}\LOG
- Tempdb Data: H:\SQL2019\{InstanceName}\TEMPDBDATA (with an 'Insert' button and a text box containing 'InstanceName')
- Tempdb Log: H:\SQL2019\{InstanceName}\TEMPDBLOG
- Backup Directory: G:\SQL2019\{InstanceName}\BACKUP

The 'Move System Databases (master,model,msdb)' checkbox is checked. The 'System Database Data' field is E:\SQL2019\{InstanceName}\DATA and the 'System Database Log' field is F:\SQL2019\{InstanceName}\LOG.

Define the default directories.

The substitution variable {InstanceName} will be replaced with the actual Instance Name during the Install and should only be used for Named Instances. You can right click in the text box to paste the variable.

Check Move System Databases if requested. The default destination will be set to same directory as User Database Data/Log but a separate Disk/Directory can be used.

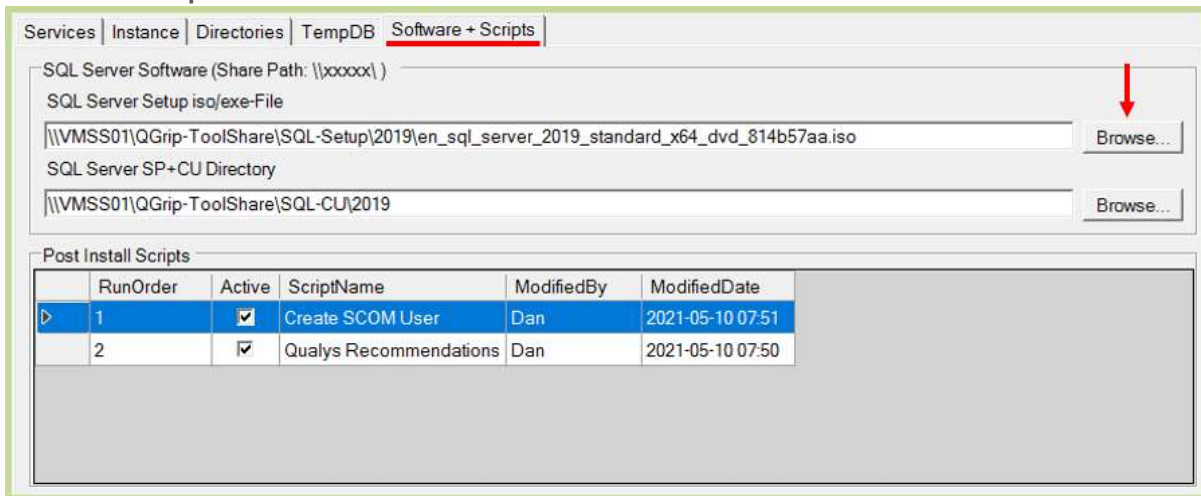
TempDB

The screenshot shows the 'TempDB' tab of the QGRIP SQL Installer. It is divided into two sections:

- Data File Sizes:**
 - Initial Size (MB): 10
 - Autogrowth (MB): 100
 - Max Size (MB): 1000
- Log File Sizes:**
 - Log Initial Size (MB): 10
 - Log Autogrowth (MB): 100
 - Log Max Size (MB): 1000

This is the definition for one data file. During the Install, data files will be created for each available processor, to a max of 8.

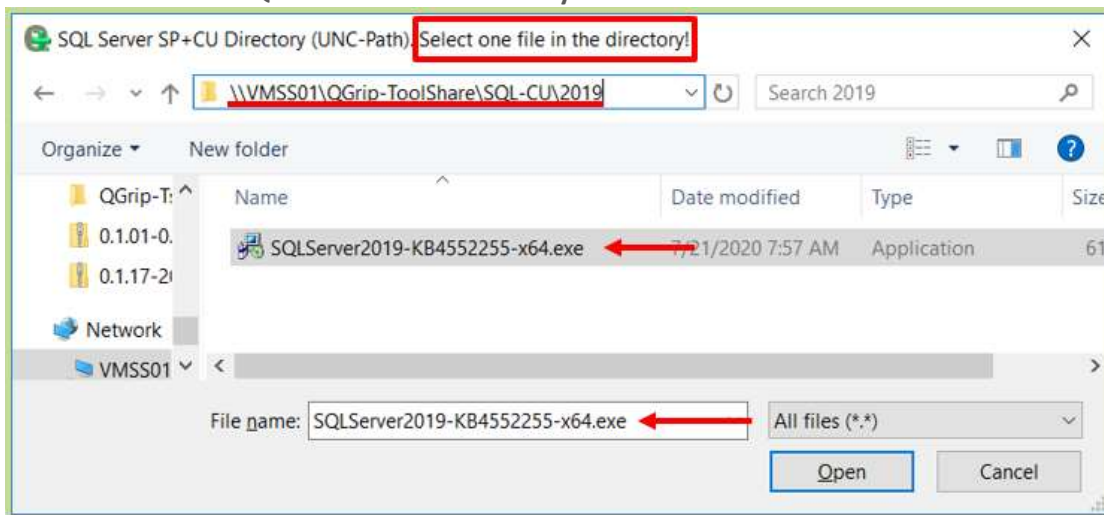
Software + Scripts



The Post Install Scripts are described in the next section.

The location of Setup file and the SP+CU directory. The Browse buttons will only be enabled if the QGrip-SQL-Installer is started in the AD Domain that the Template is intended for but can always be edited manually.

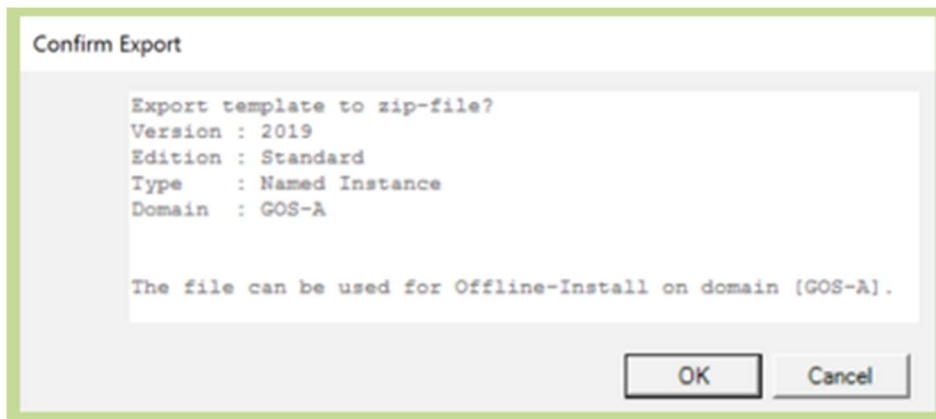
Attention Browse: SQL Server SP+CU Directory



Minor flaw. QGrip does not support the selection of just a directory. To select the SP+CU directory, you must select one of the files in the directory and then push [Open]!

4.2 Export Template

Select the Template that you want to use during an Offline-Install. Make sure that it is for the correct Domain, Version, Edition and Instance type.



Confirm that it is the right template.



The zip-file will be created on the QGrip-ToolShare (Offline-Install directory) in the current domain. If needed, copy the zip-file to the QGrip-ToolShare in the domain where you need it.

5 Post Install Scripts

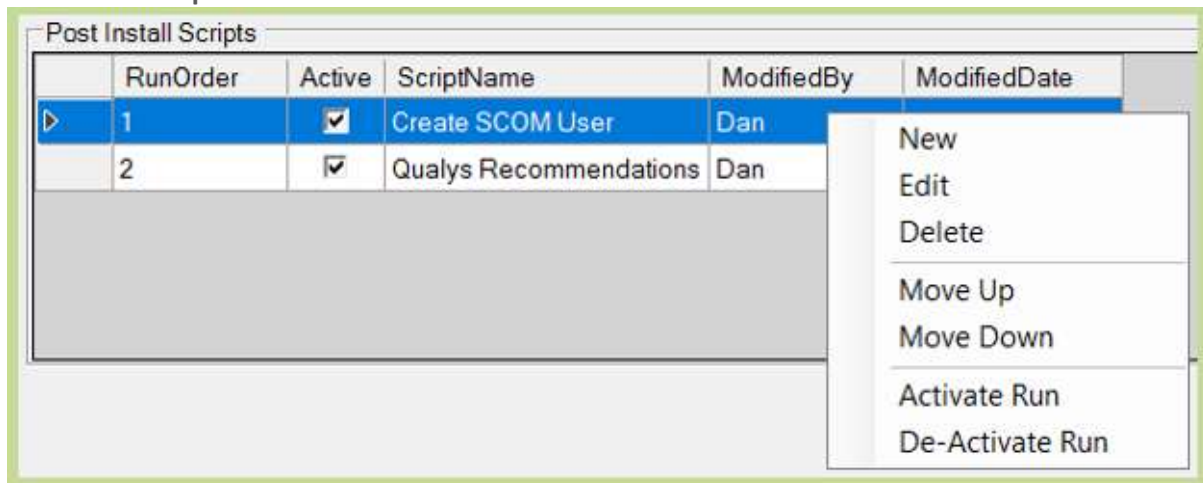
Post Install Scripts can be created to apply your own Hardening and Standards to the SQL Server Instance after it has been installed. A problem when creating the scripts is that it is hard to test them in advance.

The set of Post Install scripts is global and are the same for all Templates.

The 'Run Order' indicates in which order the scripts should run. If the Run Order is changed, the change will apply to all Templates!

Per Template you can only define if the script should run (Activate Run) or not (De-Activate Run).

Post Install Scripts



RunOrder	Active	ScriptName	ModifiedBy	ModifiedDate
1	<input checked="" type="checkbox"/>	Create SCOM User	Dan	
2	<input checked="" type="checkbox"/>	Qualys Recommendations	Dan	

Select the script row and right-click to open the context menu:

New Create a new Script.

Edit Edit the selected Script.

Delete Delete the selected Script.

Move Up Change the Run Order of selected script.

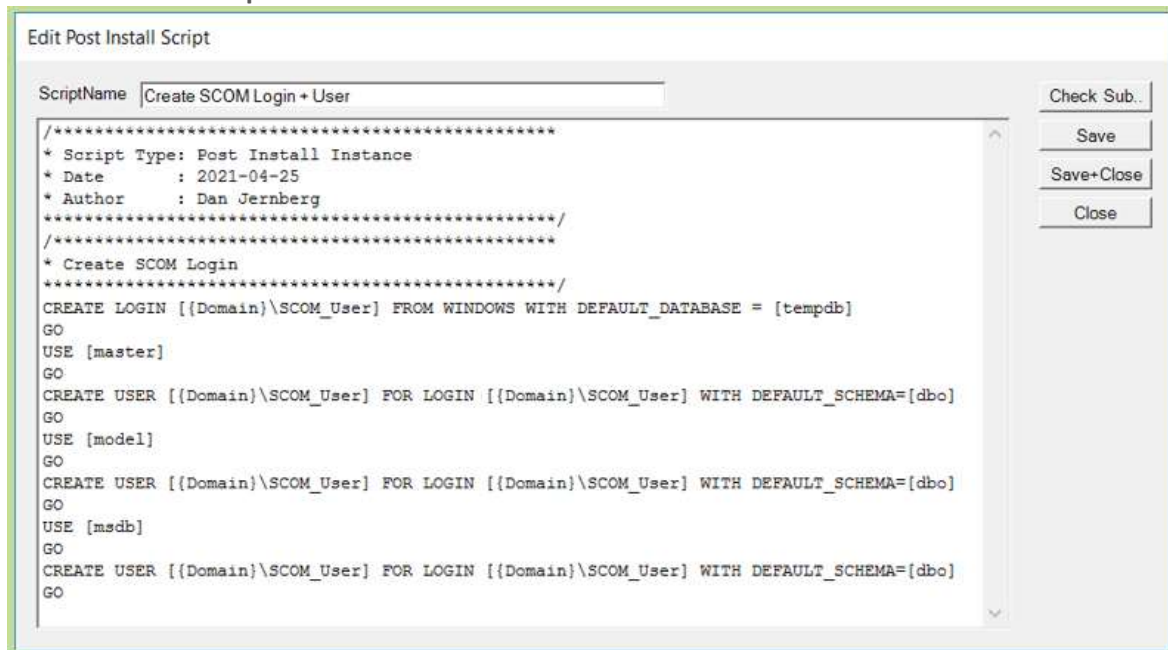
Move Down Change the Run Order of selected script.

Activate Run Indicate that the selected script should run when this Template is used.

De-Activate Run Indicate that the selected script should not run when this Template is used.

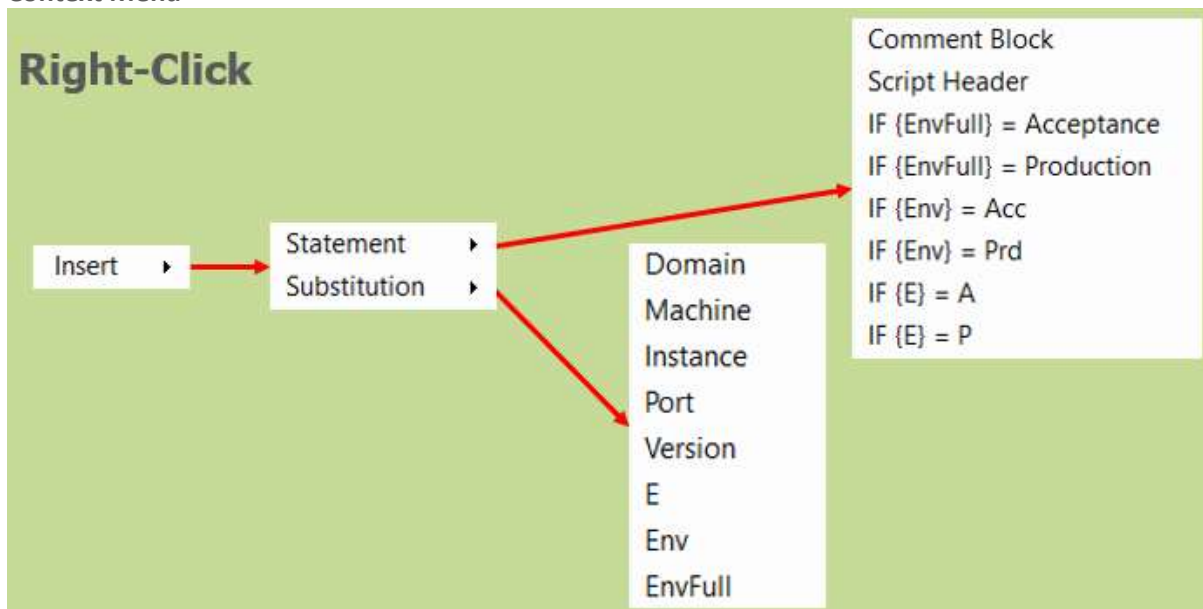
5.1 Edit Script

Edit Post Install Script



The Post Install Script is a normal T-SQL script. You should create the scripts in such a fashion that they can run without errors on all combination of Instances, (DTAP) environments, versions and AD Domains. This can be accomplished by using the predefined substitution variables in the scripts. These variables will be substituted with the actual values before the script is run.

Context Menu



When editing a script, set the cursor where you want to insert a statement or a variable, right-click and choose statement/variable.

Substitution Variables

Variable	Example after sub.	Description
{Domain}	AD	AD Domain where Instance is Running.
{Machine}	VMSQL16	The machine/host of the Instance.
{Instance}	VMSQL16\PRD	The full Instance name.
{Port}	1433	The port the instance is listening to.
{Version}	2019	The SQL Server version (2016,2017,2019).
{E}	P	(*) The Environment EnvChar
{Env}	Prd	(*) The Environment ShortName
{EnvFull}	Production	(*) The Environment FullName

(*) Value depend on the names you have given the Environment in your configuration.

Environments				
	InUse	FullName	ShortName	EnvChar
▶	<input type="checkbox"/>	Develop	Dev	D
	<input type="checkbox"/>	UnitTest	Uni	U
	<input type="checkbox"/>	Test	Tst	T
	<input checked="" type="checkbox"/>	Acceptance	Acc	A
	<input type="checkbox"/>	Integration	Int	I
	<input checked="" type="checkbox"/>	Production	Prd	P

5.2 Check Substitutions

It is tricky to test the Post Install Scripts in advance but you can use the [Check-Sub...] button in the edit window to see what the script looks like after the substitutions have been applied to the script. And if you have a SQL Server Instance where you can run the scripts after substitution, even better.

Check Script Substitutions Close

Substitutions

Domain: Machine:

Environment: Instance:

Version: Port:

Substitute Back to Original

Post Install Script

```

/*****
* Script Type: Post Install Instance
* Date       : 2021-04-25
* Author    : Dan Jernberg
*****/
/*****
* Create SCOM Login
*****/
CREATE LOGIN [{{Domain}}\SCOM_User] FROM WINDOWS WITH DEFAULT_DATABASE = [tempdb]
GO
USE [master]
GO
CREATE USER [{{Domain}}\SCOM_User] FOR LOGIN [{{Domain}}\SCOM_User] WITH DEFAULT_SCHEMA=
[dbo]

```

Fill the Substitutions with the values you want to test and press [Substitute].
To go back to the original script, press [Back to Original].

6 Prepare Instance Host (Machine)

Before the QGrip-SQL-Installer can be used to install a new SQL Server Instance on a host/machine, the following needs to be finished.

1. OS, Windows Server 2012R2, 2016 or 2019.
2. Disks need to be added (should match the Template).
3. Windows Failover Cluster needs to be ready (only for SQL Server Always On).
4. Firewall Rules.
5. Create (group) Managed Service Accounts (gMSA, MSA).

Step 4 and 5 are described in the following sub sections.

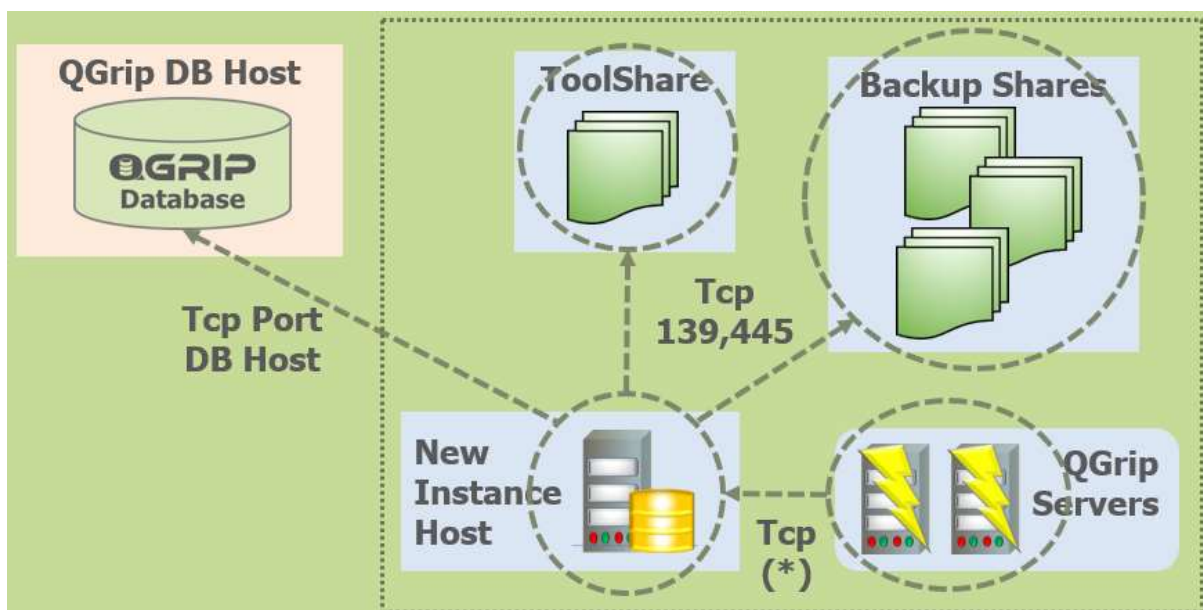
Pay attention to the type of Managed Service Account needed:

- gMSA Always on Cluster
- MSA Stand Alone instances (not Always on)

Use the **'New Instance Host Help'** described in the next section to

- Request Disks according to Template,
- Define Firewall rules needed for the new Instance Host,
- Check/Test Firewall connectivity after implementation Firewall rules,
- Generate Semi-automatic scripts for creation of (group) Managed Service Accounts.

6.1 Firewalls



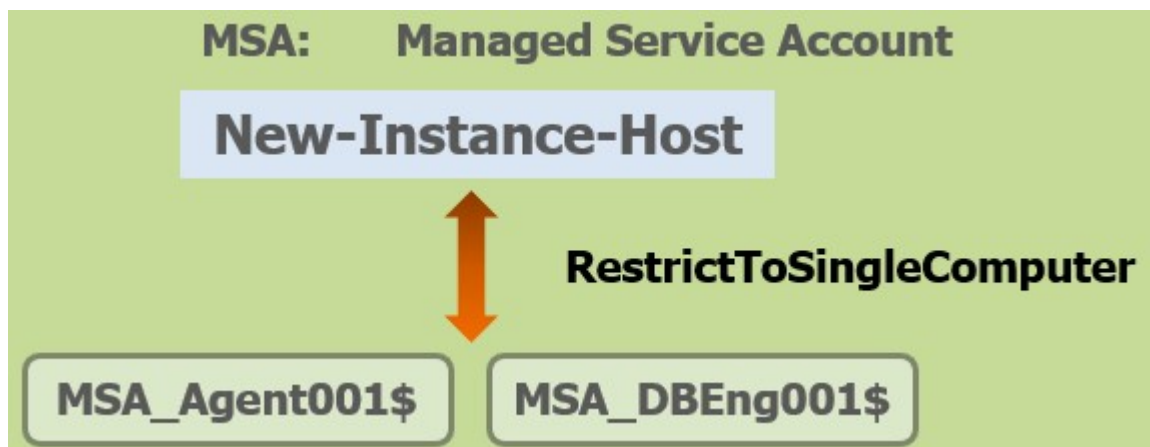
The following firewalls need to be open in order to perform the Install with QGrip-SQL-Installer. (*) is the port number that the new Instance will be listening to.

Only the firewalls to the ToolShare, Backup Shares and from the QGrip Servers within the same AD Domain as the New Instance Host need to be open.

QGrip-SQL-Installer needs to connect to the QGrip database during the Install. When the Install is ready, the firewall rule can be removed again. If it is not possible to connect to the QGrip database, you can do an 'Offline-Install', see section 'Offline-Install' below.

6.2 Managed Service Accounts (Stand Alone Instance)

This section describes how the Managed Service Accounts (MSA) for the Agent and DBEngine services should be created before a new Instance can be installed. The Instance is Stand Alone and will not participate in an Always on Cluster. The names used in this section are only examples and should be replaced with the names according to your own standards.



For each new Instance Host, the Agent and DBEngine accounts need to be created once. The accounts must be Managed Service Accounts:

- MSA_Agent001\$
- MSA_DBEng001\$

The principal allowed to retrieve the MSA passwords is Restricted to Single Computer:

- New-Instance-Host

The max length of a MSA is 15 including the '\$'.

Required Authorisation

Member of Domain Admins / Enterprise Admin group on the AD-Domain

All actions below should be executed in a PowerShell window opened "as Administrator".

6.2.1 Check: KdsRootKey

On the Domain Controller:

A KdsRootKey is needed to create group Managed Service accounts (gMSA).

Check existence	PowerShell as Administrator
Get-KdsRootKey	

If no key is returned, you will need to create one as described in the Appendix:

- Add: KdsRootKey.

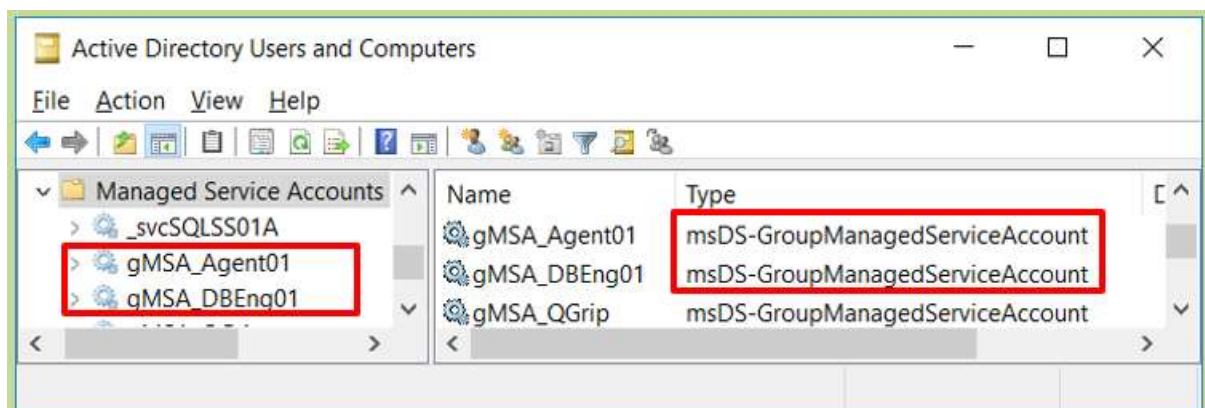
6.2.2 Create: MSA accounts on AD

On the Domain Controller:

Create MSA_Agent001\$ and MSA_DBEng001\$ on AD	PowerShell as Administrator
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All	
New-ADServiceAccount -name MSA_Agent001 ` -RestrictToSingleComputer -Enabled \$True Add-ADComputerServiceAccount -Identity New-Instance-Host ` -ServiceAccount MSA_Agent001	
New-ADServiceAccount -name MSA_DBEng001 ` -RestrictToSingleComputer -Enabled \$True Add-ADComputerServiceAccount -Identity New-Instance-Host ` -ServiceAccount MSA_DBEng001	

Replace with your own values before running the statement and note the following:

- “\$” should be omitted in the statement,
- “`” indicates that the statement continues on the next line.



The MSA account should be visible in the ‘Managed Service Accounts’ container in the ‘Active Directory Users and Computers’ tool.

The New-Instance-Host needs to be rebooted otherwise the following step will fail.

6.2.3 Install: MSA accounts on New Instance Host

On New Instance Host:



Make sure the machine was rebooted in the last step!

The MSA accounts must be installed locally on the New Instance Host.

Required Authorisation

Member of Domain Admins / Enterprise Admin group on the AD-Domain

Install gMSA on New Instance Host	PowerShell as Administrator
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All Import-Module ActiveDirectory	
Install-ADServiceAccount MSA_Agent001 Test-ADServiceAccount MSA_Agent001	
Install-ADServiceAccount MSA_DBEng001 Test-ADServiceAccount MSA_DBEng001	

Replace with your own values before running the statement and note the following:

- “\$” should be omitted in the statement.

The test statement should return True.

Possible problems

If executing the statements take long and fail, check that the firewall to the Domain Controller on port 9389 is open.

6.3 group Managed Service Accounts (Always on Cluster)

This section describes how the group Managed Service Accounts (gMSA) for the Agent and DBEngine services should be created before a new Instance can be installed that will be part of an Always on Cluster. The names used in this section are only examples and should be replaced with the names according to your own standards.



For each new Always on Cluster, the Agent and DBEngine accounts need to be created once. The accounts must be group Managed Service Accounts:

- gMSA_Agent01\$
- gMSA_DBEng01\$

The principal allowed to retrieve the gMSA passwords is a Global Security Group:

- GSG_AOCluster01

The max length of a gMSA is 15 including the '\$'.

Required Authorisation

Member of Domain Admins / Enterprise Admin group on the AD-Domain

All actions below should be executed in a PowerShell window opened "as Administrator".

6.3.1 Check: KdsRootKey

On the Domain Controller:

A KdsRootKey is needed to create group Managed Service accounts (gMSA).

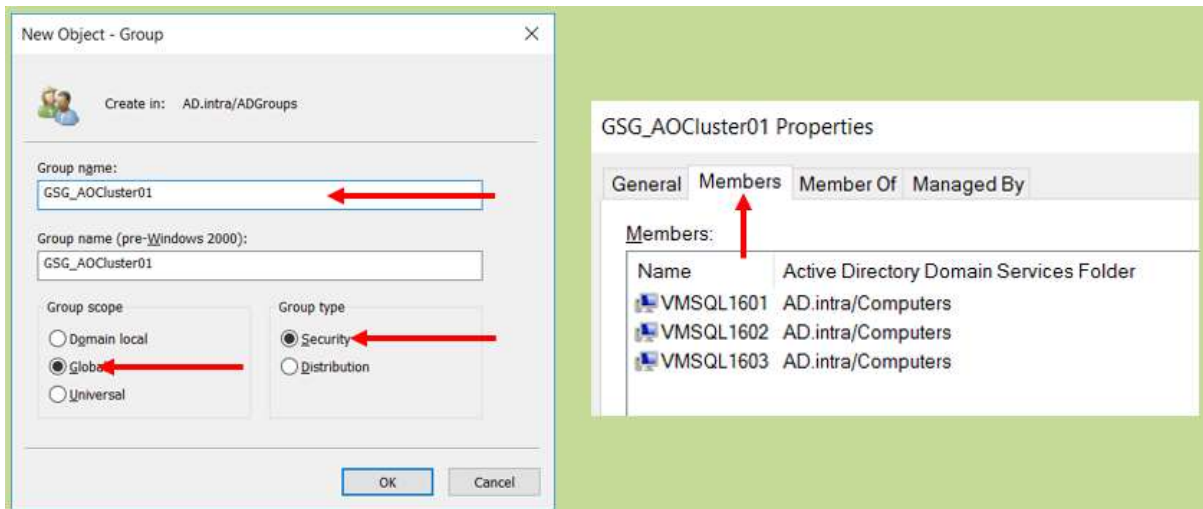
Check existence	PowerShell as Administrator
Get-KdsRootKey	

If no key is returned, you will need to create one as described in the Appendix:

- Add: KdsRootKey.

6.3.2 Create: GSG_AOCluster01

On the Domain Controller or Delegated Server:



Open the tool 'Active Directory Users and Computers' and create the group 'GSG_AOCluster01' in an appropriate container. Add all machines/nodes in the cluster to the group.

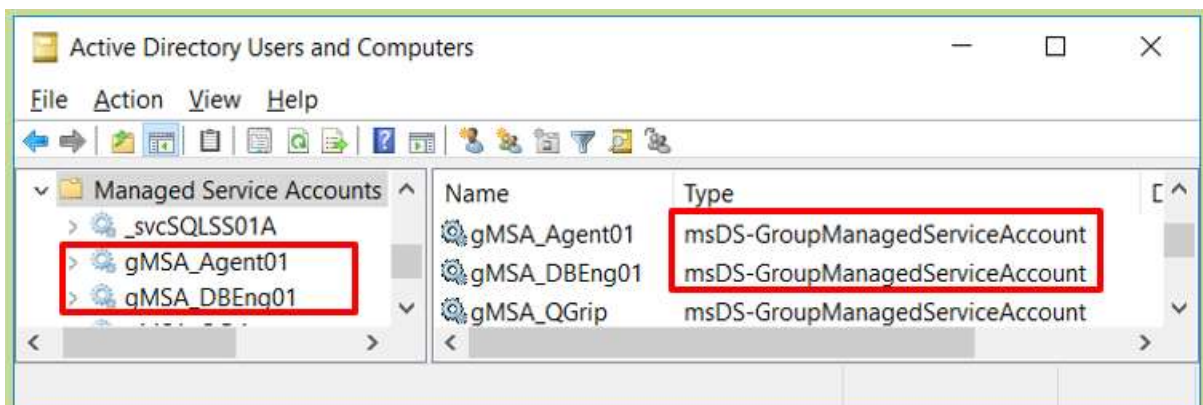
6.3.3 Create: gMSA accounts on AD

On the Domain Controller:

Create gMSA_Agent01\$ and gMSA_DBEng01\$ on AD	PowerShell as Administrator
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All	
New-ADServiceAccount -name gMSA_Agent01 ` -DNSHostName gMSA_Agent01.AD.intra.griponsql.org ` -PrincipalsAllowedToRetrieveManagedPassword GSG_AOCluster01	
New-ADServiceAccount -name gMSA_DBEng01 ` -DNSHostName gMSA_DBEng01.AD.intra.griponsql.org ` -PrincipalsAllowedToRetrieveManagedPassword GSG_AOCluster01	

Replace with your own values before running the statement and note the following:

- "\$" should be omitted in the statement,
- "`" indicates that the statement continues on the next line,
- "DNSHostName" is confusing and is not a regular hostname. It's the account name with the qualified domain.



The gMSA account should be visible in the 'Managed Service Accounts' container in the 'Active Directory Users and Computers' tool.

All Servers that are member of the group GSG_AOCluster01 must be **rebooted**, otherwise the next step will fail.

6.3.4 Install: gMSA accounts on New Instance Hosts

On each New Instance Host in GSG_AOCluster01:



Make sure the machine was rebooted in the last step!

The gMSA accounts must be installed locally on each New Instance Host.

Required Authorisation

Member of Domain Admins / Enterprise Admin group on the AD-Domain

Install gMSA on New Instance Host	PowerShell as Administrator
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All Import-Module ActiveDirectory	
Install-ADServiceAccount gMSA_Agent01 Test-ADServiceAccount gMSA_Agent01	
Install-ADServiceAccount gMSA_DBEng01 Test-ADServiceAccount gMSA_DBEng01	

Replace with your own values before running the statement and note the following:

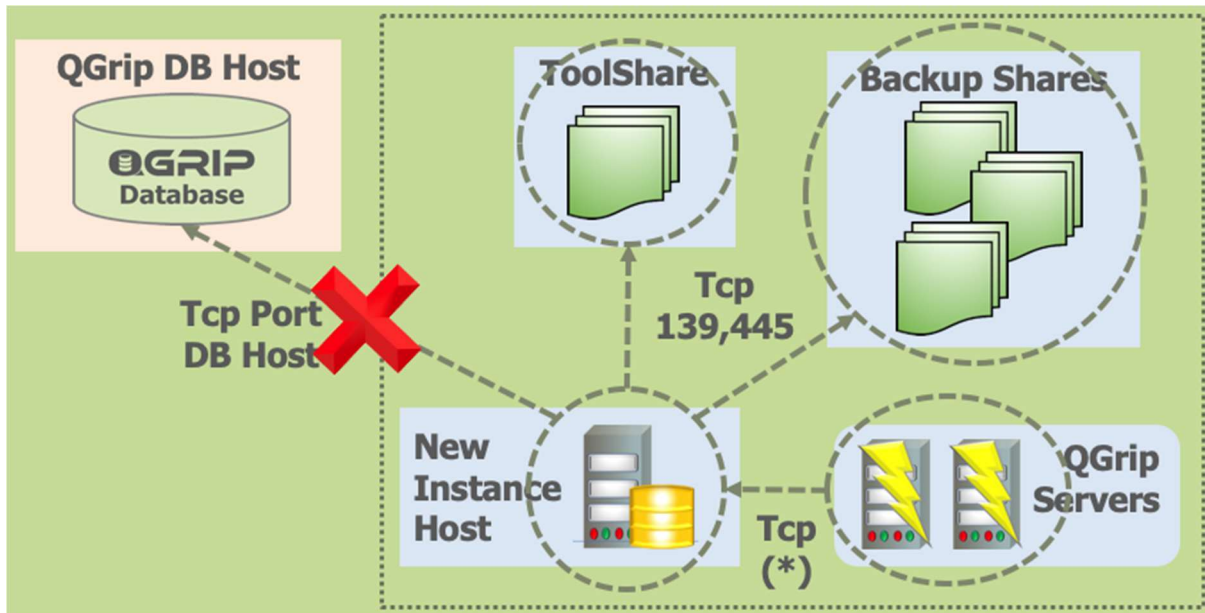
- "\$" should be omitted in the statement.

The test statement should return True.

Possible problems

If executing the statements take long and fail, check that the firewall to the Domain Controller on port 9389 is open.

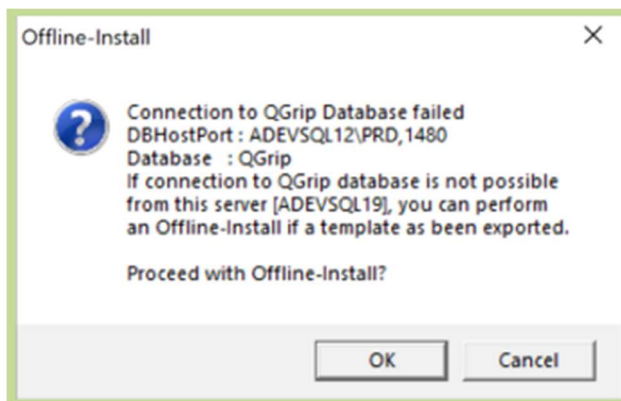
7 Offline-Install



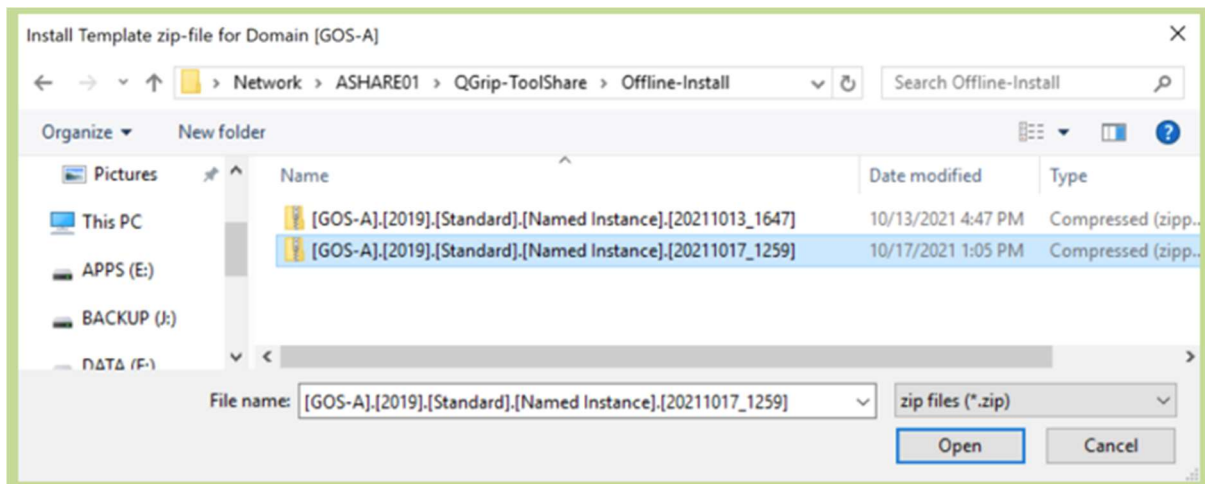
If it is not possible to connect to the QGrip database from the Machine where you want to Install SQL Server, you can use QGrip-SQL-Installer and do an Offline-Install.

Before you can perform an Offline-Install, you must make an export of the template you want to use for the Install, see section Export template here above.

Make sure you are using the latest version of QGrip-SQL-Installer. Normally this is checked against the QGrip database but that is not possible during the Offline-Install.

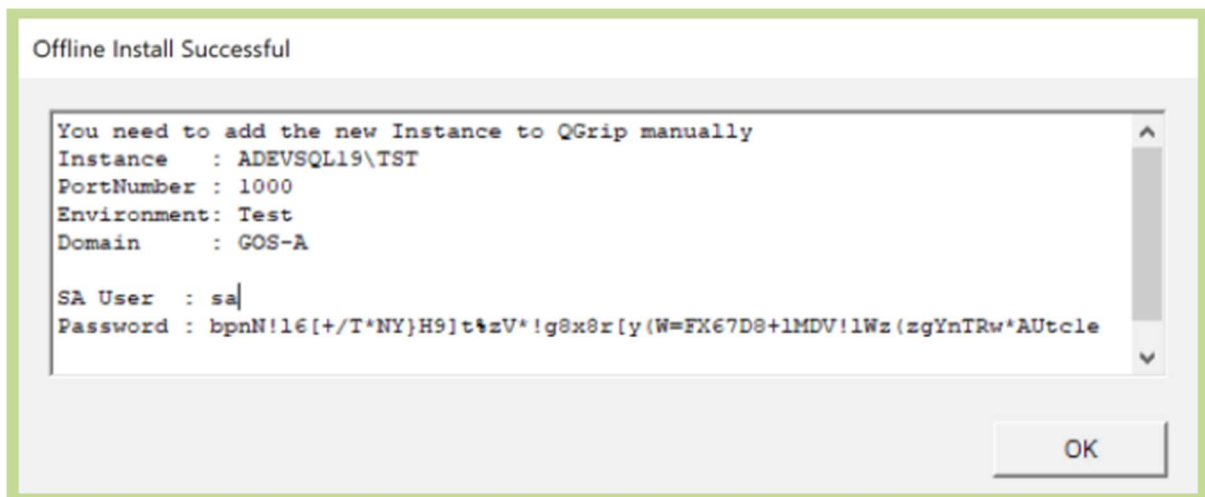


When you start QGrip-SQL-Installer from a machine with no connection to the QGrip database the message above will appear.



You will immediately be asked to select the exported zip-file you want to use for the install. QGrip will check that the Domain of the file is correct for the current Machine.

The rest of the install is the same as a normal install, some buttons in the Interface are missing due to the missing connection with the QGrip database.



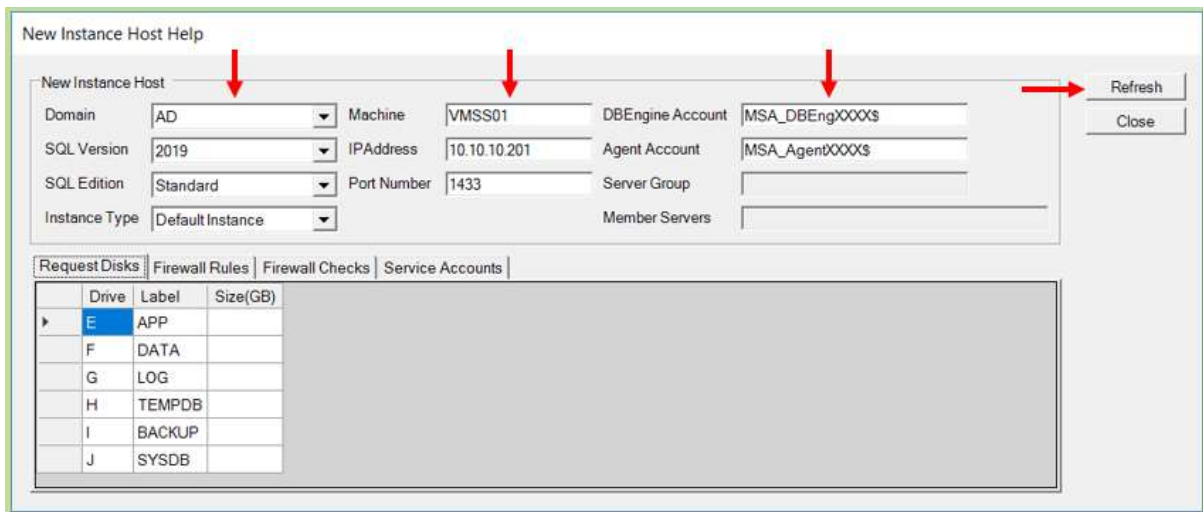
At the end, you will receive a popup with the [sa] user (or equivalent) and the generated password and information you need to manually add the Instance to QGrip.

8 New Instance Host Help

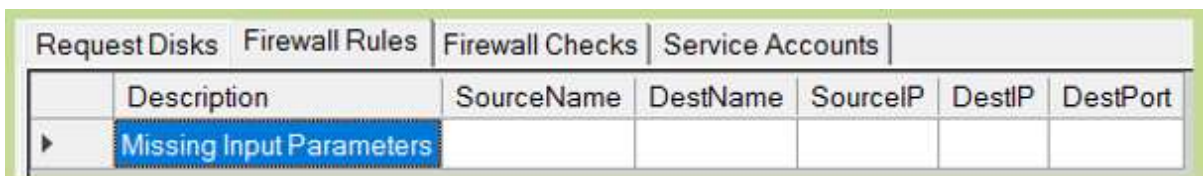
The New Instance Host Help is very useful at different stages when it comes to a New Instance Host and will spare you from manual editing.



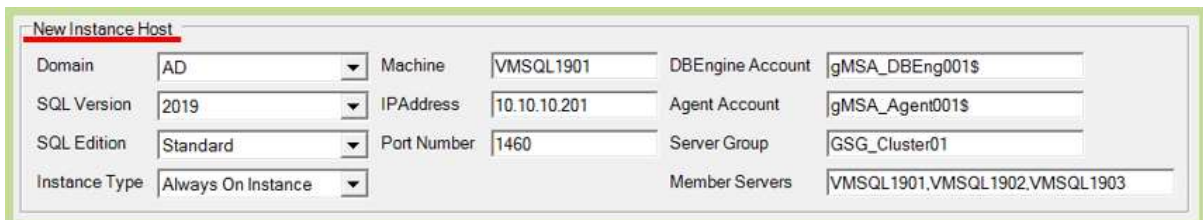
The window can be opened from the button panel in the main Install window.



Fill in the different parameters for the New Instance Host and press **Refresh**.



It does not matter if you don't have all parameters, the different tabs will still be filled but with 'Missing Input Parameters'. It's logical that you don't know for instance the IPAddress of a server that has not yet been created.



The input parameters are straight forward. The Server Group and Member Servers will only be enabled if the Instance Type is 'Always On Instance'. The Server Group should be filled with a value that is name that is unique and not yet present on the AD-Domain. The Member servers is a list of all servers (nodes) in the Always On Cluster.

Tab: Request Disks

Request Disks	Firewall Rules	Firewall Checks	Service Accounts
▶	D	APP	
	E	DATA	
	F	LOG	
	G	BACKUP	
	H	TEMPDB	

To use before the New Instance Host has been requested. The needed directories/drives are derived from the Template that will be use according to the selected Domain, Version, Edition and Instance Type.

Request Disks	Firewall Rules	Firewall Checks	Service Accounts			
	Description	SourceName	DestName	SourceIP	DestIP	DestPort
	SQL Server Instance -> QGrip DB Host	VMSQL1901	VMSQL1201	10.10.10.201	10.10.10.110	1460
▶	SQL Server Instance -> QGrip-ToolShare	VMSQL1901	VMSS01	10.10.10.201	10.10.10.201	139.445
	SQL Server Instance -> Backup Share	VMSQL1901	VMDC01	10.1		
	QGrip Server -> SQL Server Instance	VMSS01	VMSQL1901	10.10.10.201	10.10.10.2	

Use to request Firewall rules changes. The New Instance Host name and IP address together with the port number will be needed to produce accurate output.

Request Disks	Firewall Rules	Firewall Checks	Service Accounts
	CheckOnName	CheckOnIP	
▶	Run on : VMSQL1901	Run on : VMSQL1901	
	Test-NetConnection -Computer VMSQL1201 -Port 1460	Test-NetConnection -Computer 10.10.10.110 -Port 1460	
	Test-NetConnection -Computer VMDC01 -Port 139	Test-NetConnection -Computer 10.10.10.1 -Port 139	
	Test-NetConnection -Computer VMDC01 -Port 445	Test-NetConnection -Computer 10.10.10.1 -Port 445	
	Test-NetConnection -Computer VMSS01 -Port 139	Test-NetConnection -Computer 10.10.10.201 -Port 139	
	Test-NetConnection -Computer VMSS01 -Port 445	Test-NetConnection -Computer 10.10.10.201 -Port 445	
	Run on QGrip Servers : VMSS01	Run on QGrip Servers : VMSS01	
	Test-NetConnection -Computer VMSQL1901 -Port 1460	Test-NetConnection -Computer 10.10.10.201 -Port 1460	

Use to check that Firewall rules have been implemented correctly. The New Instance Host name and IP address together with the port number will be needed to produce accurate output.

Request Disks	Firewall Rules	Firewall Checks	Service Accounts
Command			
---- On Domain Controller, Domain: AD			
---- PowerShell as Administrator (Member Domain/Enterprise Admin group)			
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All			
New-ADServiceAccount -name gMSA_Agent001 *			
-DNSHostName gMSA_Agent001.AD.intra *			
-PrincipalsAllowedToRetrieveManagedPassword GSG_Cluster01			
New-ADServiceAccount -name gMSA_DBEng001 *			
-DNSHostName gMSA_DBEng001.AD.intra *			

Use as instruction and command statements. The statements will contain the Service account and machine/Server Group and Member Server, provided as input. The lines starting with

- ---- are only instructive
- -- are instruction for actions that need to take place in another tool.

The other lines are statements that should be executed in the tool defined in the proceeding instruction (----) line.

9 Prepare QGrip-ToolShare

A QGrip-ToolShare is needed in every AD Domain where you want to use the QGrip-SQL-Installer. To avoid connectivity problems (firewalls) you are advised to place the share on the same server as the QGrip Backup Share.

Suggested layout directories

QGrip-SQL-Installer

With the executable and the QGrip.ini. The QGrip.ini should always be copied from a QGrip Server within the same AD Domain as the QGrip-ToolShare.

SQL-CMDLineUtils

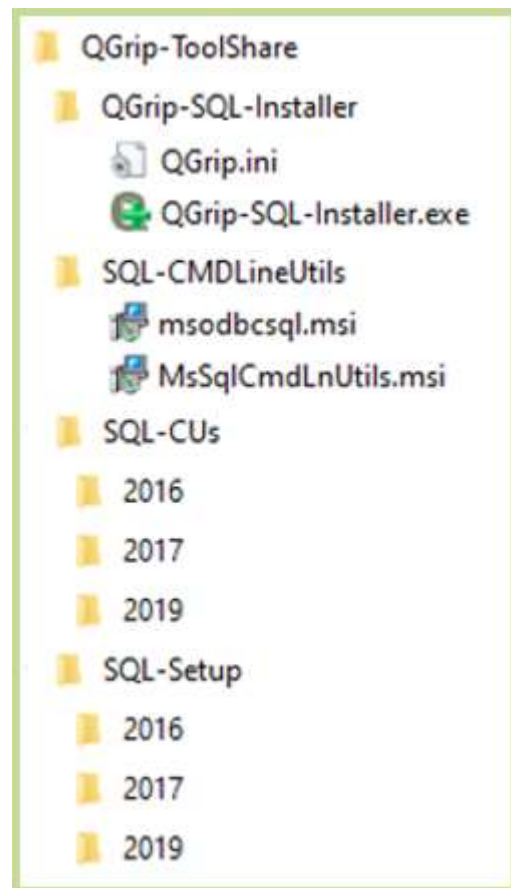
ODBC + CMDLineUtils have to be installed on every machine prior to starting QGrip-SQL-Installer and should be easy to access.

SQL-CUs

With subdirectories for each SQL Version. All Service packs and CUs should be placed in these directories.

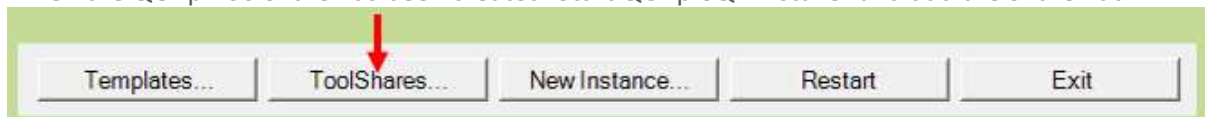
SQL-Setup

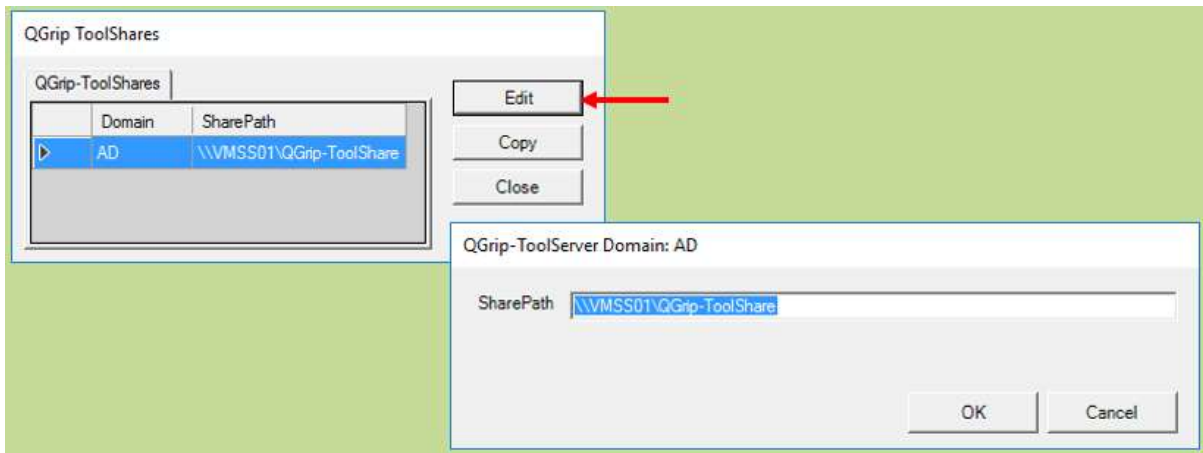
With subdirectories for each SQL Version. The SQL Setup iso/exe files, should be placed in these directories.



Only the accounts that are going to use QGrip-SQL-Installer to perform the install need to be authorised for the QGrip-ToolShare.

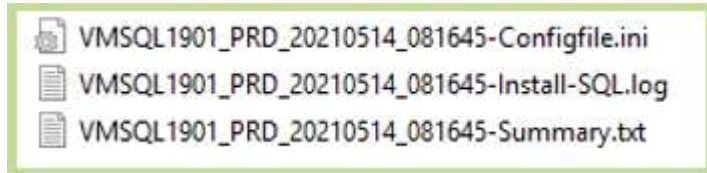
When the QGrip-ToolShare has been created. Start QGrip-SQL-Installer and add the Share Path.





10 Install Failed: Known Errors

10.1 The credentials for SQL Server Agent service are invalid.



The error can be found in the Summary.txt file.

Complete Error Message:

The credentials you provided for the SQL Server Agent service are invalid. To continue, provide a valid account and password for the SQL Server Agent service.

Situation:

The MSA/gMSA account has been installed locally on the machine before a snapshot was taken so it is available, otherwise you would not be able to select it at all. But if you have been reverting back to the snapshot a couple of times, this error might occur.

Solution:

When you have reverted back to the snapshot, reboot the machine and this problem will go away.

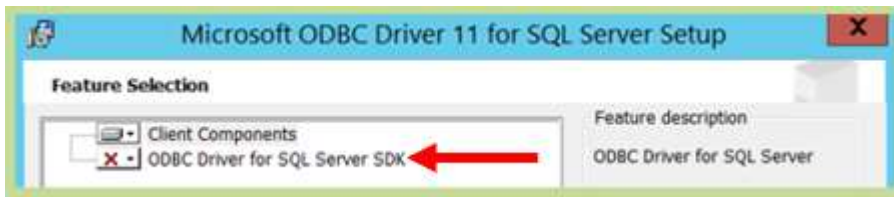
11 Appendix

11.1 Install: SQLCmdLine Utils

Copy the following files from the QGrip-ToolShare to local temp directory on the current server (you might also be able to start them directly from the ToolShare):

1. msodbcsql.msi
2. MsSqlCmdLnUtils.msi

Start the msi-files in the order as here above.



Just select the ODBC driver.

11.2 Create: QGripSQLInstall

If the current domain is not trusted, you will not be able to connect to the QGrip database using your own AD account. You will need to create the temporary QGripSQLInstall account. When you have finished the install/uninstall, remove the login as soon as possible. QGrip will remind you with a Warning as long as the account has not been removed.

QGrip-UI:

Required QGrip Role	Menu
QGrip Admin	Admin -> Access to QGrip -> QGrip Logins Tab: QGripSQLInstall

Press [New], choose Password Length and Press [Save].

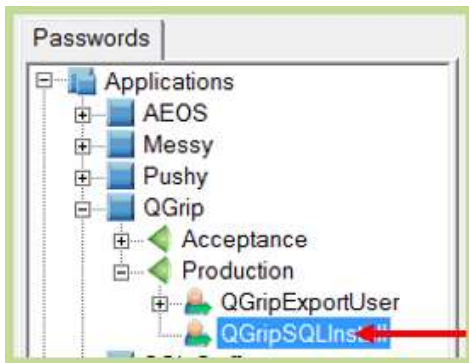
Use [Refresh] button to see when account has been created.

11.2.1 Find Password: QGripSQLInstall

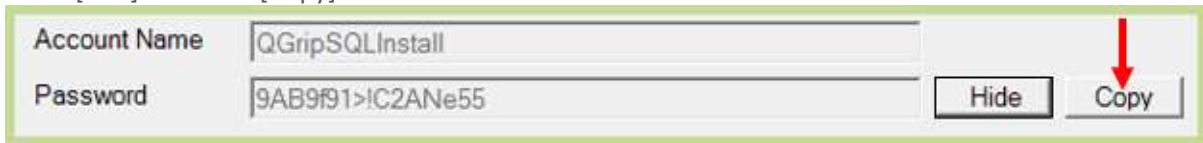
QGrip-UI:

Required QGrip Role	Menu
QGrip Admin	Application -> Password Safe

Locate and select the Account under
Applications->QGrip->QGripSQLInstall



Press [Edit] and then [Copy].



11.3 Add: KdsRootKey

Required Authorisation

Member of Domain Admins / Enterprise Admin group on the AD-Domain

A KdsRootKey is needed in order to add (group) Managed Service Accounts. If it is not yet available, you will need to create one.

Informational only, DO NOT EXECUTE statements:

The statements below should be used in a production environment:

```
Add-KdsRootKey -EffectiveImmediately
```

Even if it says EffectiveImmediately, you will need to wait for up to 10 hours before proceeding. This is a safety measure to make sure all Domain Controllers have replicated and are able to respond to gMSA requests.

In a test lab you can use the following statement instead:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
```

On the Domain Controller:

Check existence KdsRootKey	PowerShell as Administrator
Get-KdsRootKey	

If no key is returned, you will need to create one.

Create KdsRootKey	PowerShell as Administrator
Add-KdsRootKey -EffectiveImmediately	

```
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "VMDC01.AD.intra".

Guid
----
67b58fa7-a018-a818-a652-ee90ac9310e5
```

The output should look something like above. Remember EffectiveImmediately = +/- 10 hours!

```
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "VMDC01.AD.intra".
Add-KdsRootKey : The request is not supported. (Exception from HRESULT: 0x80070032)
At line:1 char:1
+ Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Add-KdsRootKey], COMException
+ FullyQualifiedErrorId : The request is not supported. (Exception from HRESULT: 0x80070032)
tionService.Cmdlets.AddKdsRootKeyCommand
```

If the statement results in a “The request is not supported” error. Try on another server.

On another server:

Try installing Remote Server Admin Tools (RSAT) on another server in the AD-Domain, and try the same statements from there.

Check existence KdsRootKey	PowerShell as Administrator
Get-KdsRootKey	

If no key is returned, you will need to create one.

Create KdsRootKey	PowerShell as Administrator
Add-KdsRootKey -EffectiveImmediately	

```
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "VMDC01.AD.intra".

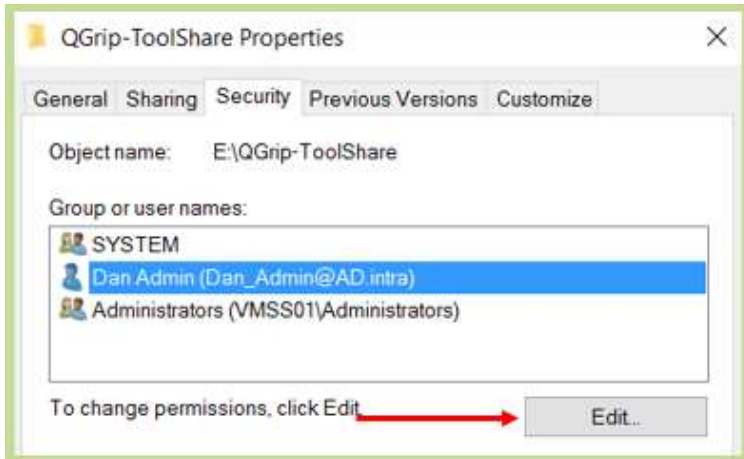
Guid
----
67b58fa7-a018-a818-a652-ee90ac9310e5
```

The output should look something like above.

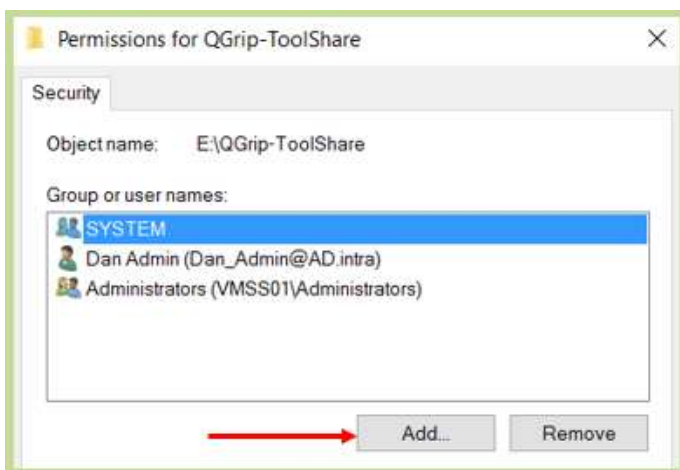
In this case, the statement “Get-KdsRootKey” will NOT return the key when executed on the domain controller.

11.4 QGrip-ToolShare: Authorise and Share

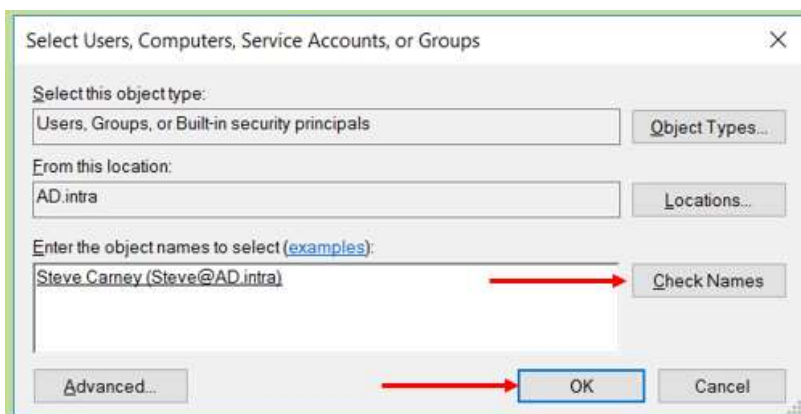
11.4.1 Authorise



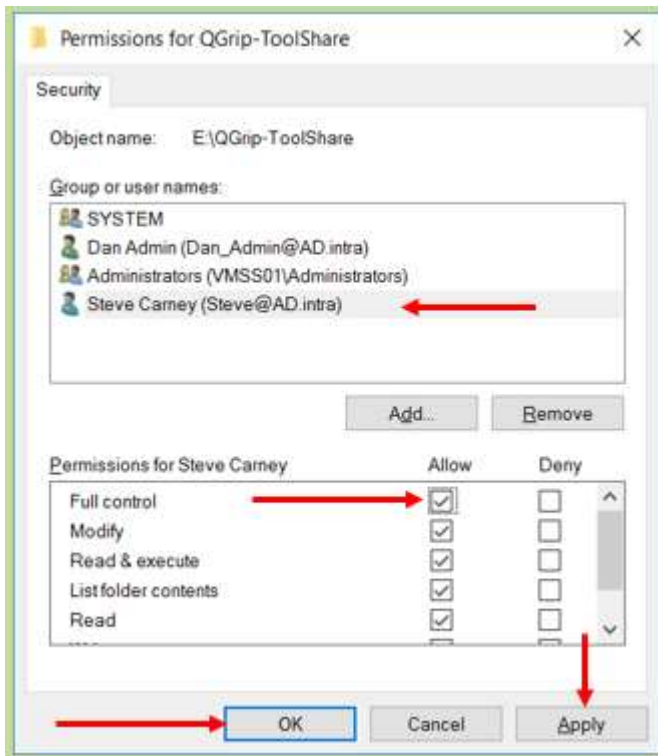
To authorise account on the underlying directory, right click on the directory and open the properties. In the Security tab, click Edit.



In the Permissions window, click Add.



When clicking on Check Names, the account should now be found and you can click OK.

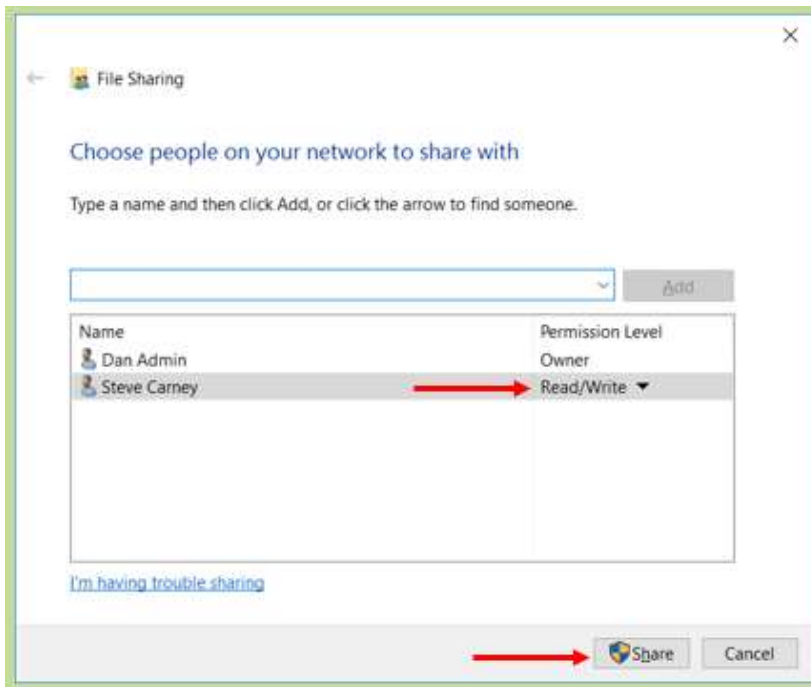


Select the account just added and check allow Full Control followed by Apply and OK.

11.4.2 Share



Click on the directory and open the properties. In the Sharing tab, click Share.



Verify that the user has Read/Write permission and press Share.