GRIP

Prepare Infra

GRIP ON SQL

2024-04-09

Contents

1 Introduction 3

2 System Requirements 3

3 Virus Scan: Exclude QGrip Directories 3

4 QGrip Components 4

5 QGrip DB Host 5

6 New: AD-Domain 6

6.1 Check: KdsRootKey 6

6.2 Create: GSG_QGripServers 7

6.3 Create: gMSA_QGrip$ 7

7 New: QGrip Server 8

7.1 Install: gMSA_QGrip$ 8

7.2 Check/Install: Supporting Software 9

7.2.1 PowerShell 5.1.x (or higher) 9

7.2.2 DOT-net 4.0 (or higher) 9

7.2.3 PowerShell Active Directory Module 10

7.2.4 SQLCmdLine Utils 10

8 New: Backup Share 11

8.1 Create: Share 12

8.2 Authorise: Full control & Share 12

8.3 Backup Share Group 13

8.4 Encryption = member Administrators Group 13

9 New: Instance 14

10 Monitor Mail 15

11 New: FileTransfer Method 16

12 Create: QGrip Users Group 17

13 Distribute Grip-UI (the clients) 17

13.1 Option 1, share 17

13.2 Option 2, local 18

14 Appendix 20

14.1 Add: KdsRootKey 20

14.2 Authorise: ‘Logon as a batch job’ 21

14.3 BackupShare: Authorise and Share 23

14.3.1 Authorise 23

14.3.2 Share 25

1 Introduction

This document describes how to prepare the Infra and create and configure the different components needed for QGrip to work properly.

Hints on how to install missing components can be found in the Appendix of this document.

To make this document easier to read, the following standard values are used throughout this document. These are also used in the script examples where they need to be replaced with your own values before running the piece of code.

Component	Remark	Our notation
AD-Domain		AD
AD-FQN Fully Qualified Name		AD.intra.griponsql.org
QGrip Directory		E:\QGrip
QGrip DBHost Name		VMSQL2019\PRD
QGrip DBHost Port Number		1433
QGrip Database Name		QGrip
QGrip System Account		gMSA_QGrip$
QGrip Servers (AD-Group)		GSG_QGripServers
QGrip Users (AD-Group)		GSG_QGripUsers
QGrip UI Directory		X:\QGrip-UI

gMSA: group Managed Service Account
GSG: Global Security Group

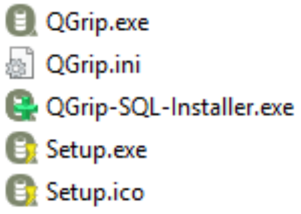
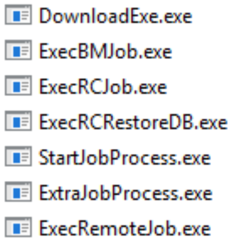
2 System Requirements

Prior to adding new components, you need the check the System Requirements. The Requirements will not be repeated in this document, please use.

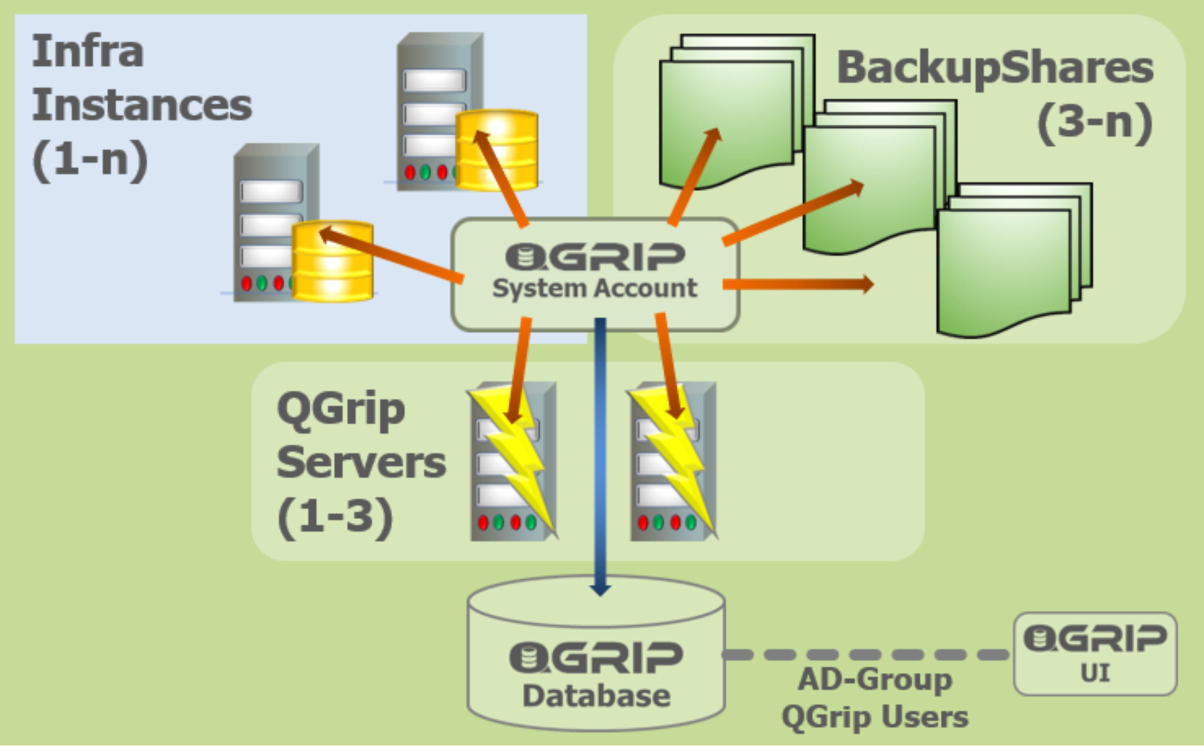
Doc-Tab	Title
Install	System Requirements

3 Virus Scan: Exclude QGrip Directories

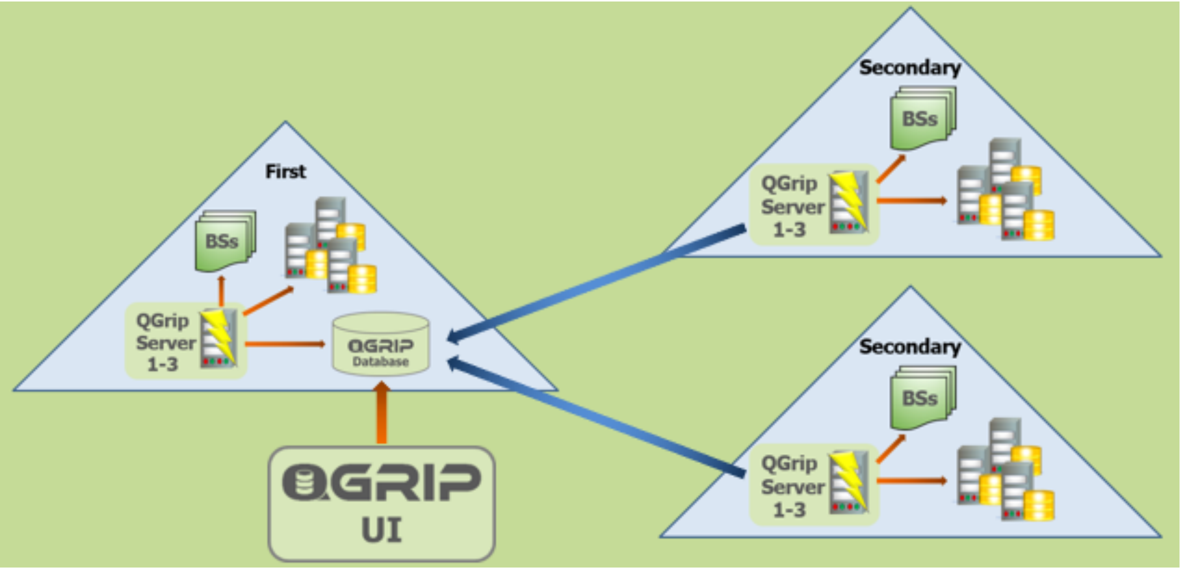
The QGrip directories on each QGrip Server need to be excluded from all virus scan applications. If not, there is a change that the executables are removed by the virus program and QGrip will stop working.

E:\QGrip	E:\QGrip\RemoteJob
 QGrip.exe QGrip.ini QGrip-SQL-Installer.exe Setup.exe Setup.ico	 DownloadExe.exe ExecBMJob.exe ExecRCJob.exe ExecRCRestoreDB.exe StartJobProcess.exe ExtraJobProcess.exe ExecRemoteJob.exe

4 QGrip Components

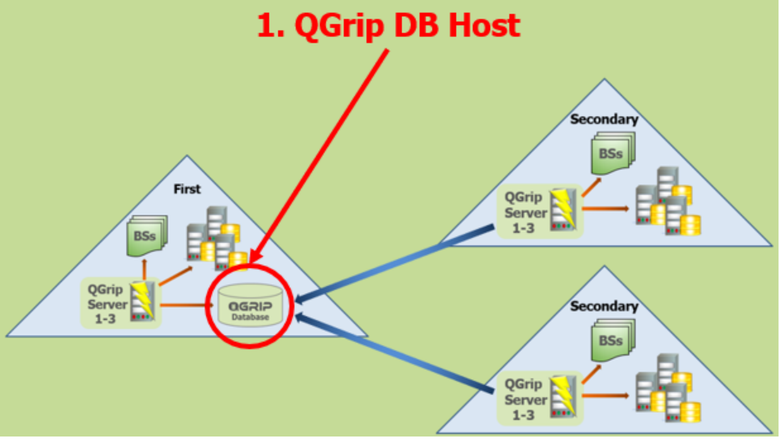


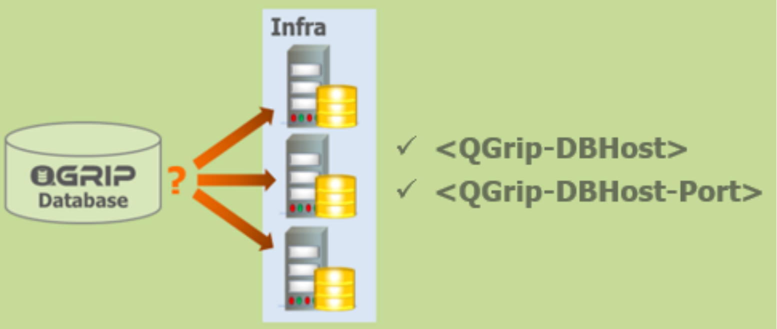
An overview of the QGrip components within one AD-Domain.



Multiple AD-Domain configuration.

5 QGrip DB Host





The QGrip database can be placed on an already existing SQL Server Instance or AlwaysOn Cluster, preferably with High Availability. If the QGrip database is down NO jobs will be started including DBBackup and LogBackup. In QGrip, the DB Host where the QGrip database is running, will be regarded as Production.

Adding the QGrip Database is fully covered in

Doc-Tab	Title
Install	Install QGrip - Setup

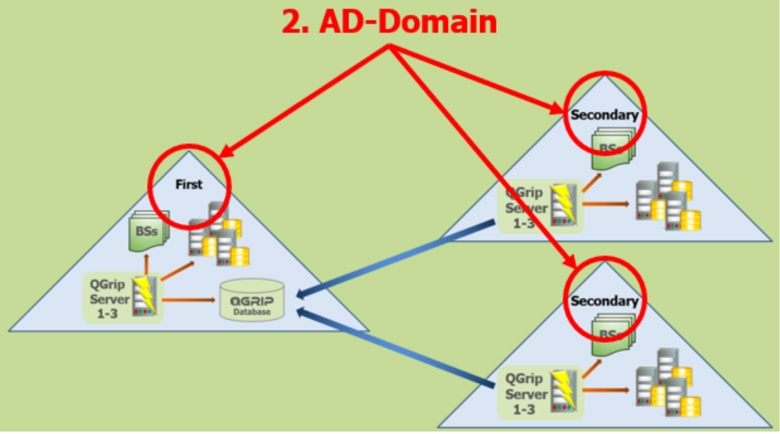
Note

You should read the following before you make a final decision on the location of the QGrip database:

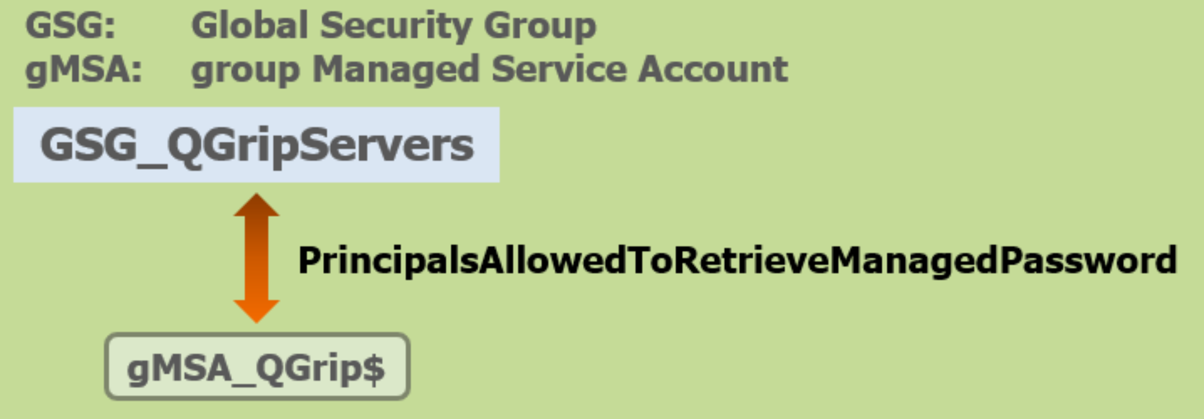
Doc-Tab	Title
Install	Move QGrip Database

This to prevent unnecessary problems in case of a Disaster situation. Be prepared!

6 New: AD-Domain



This section describes the preparations needed before QGrip can be installed and used on an AD-Domain. This is only required once per AD-Domain.



GSG: Global Security Group
gMSA: group Managed Service Account

GSG_QGripServers

PrincipalsAllowedToRetrieveManagedPassword

gMSA_QGrip$

On each AD-Domain, the QGrip System Account needs to be created.
The account must be a group Managed Service Account:

- gMSA_QGrip$

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

- GSG_QGripServers

We advise you to use the same name of the components in every AD-Domain.
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".

6.1 Check: KdsRootKey

On the Domain Controller:

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

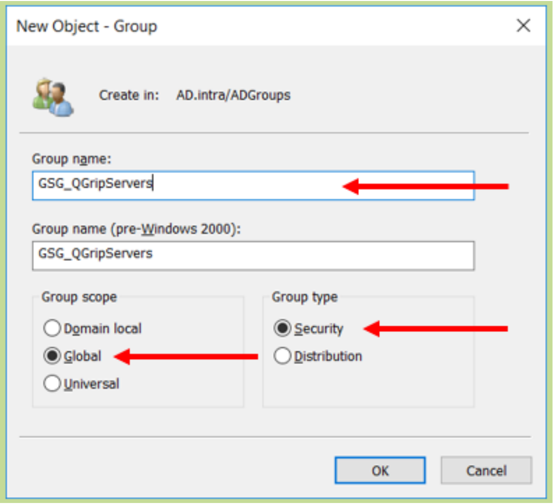
Check existence	PowerShell as Administrator
Get-KdsRootKey	

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

- Add: KdsRootKey.

6.2 Create: GSG_QGripServers

On the Domain Controller or Delegated Server:



New Object - Group

Create in: AD.intra/ADGroups

Group name:
GSG_QGripServers

Group name (pre-Windows 2000):
GSG_QGripServers

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Open the tool ‘Active Directory Users and Computers’ and create the group ‘GSG_QGripServers’ in an appropriate container.

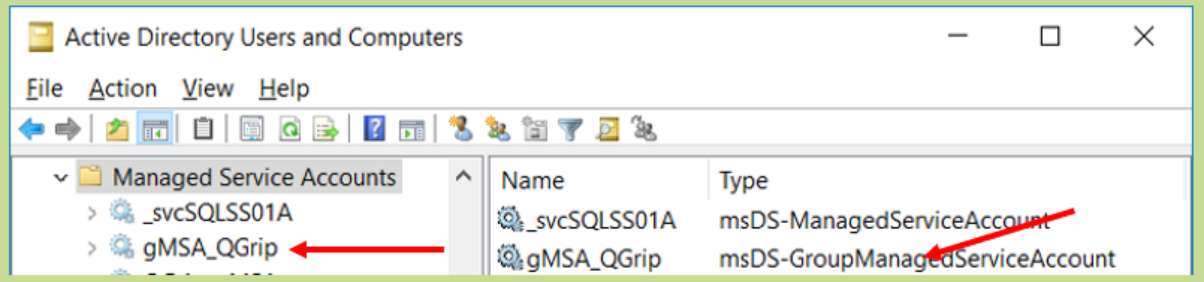
6.3 Create: gMSA_QGrip$

On the Domain Controller:

Create gMSA_QGrip on AD	PowerShell as Administrator
New-ADServiceAccount -name gMSA_QGrip ` **-DNSHostName** gMSA_QGrip.AD.intra.griponsql.org ` **-PrincipalsAllowedToRetrieveManagedPassword** GSG_QGripServers	

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.



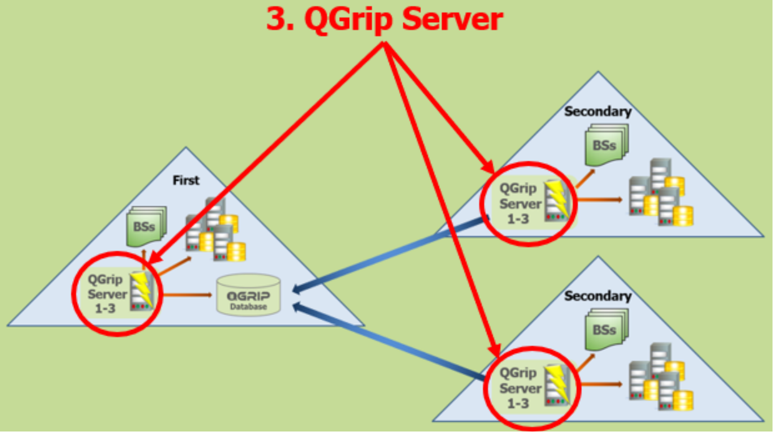
Active Directory Users and Computers

Managed Service Accounts
_svcSQLSS01A
gMSA_QGrip

Name	Type
_svcSQLSS01A	msDS-ManagedServiceAccount
gMSA_QGrip	msDS-GroupManagedServiceAccount

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

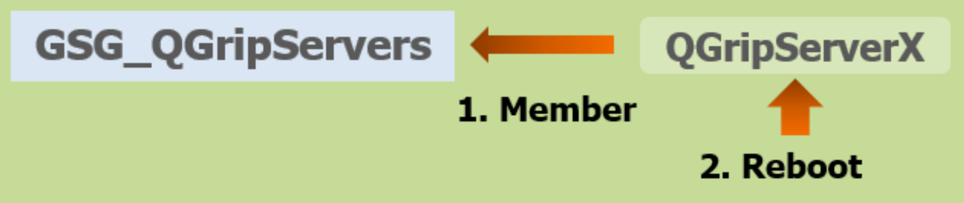
7 New: QGrip Server



This section describes the preparations needed before a QGrip Server can be used.

7.1 Install: gMSA_QGrip$

On the Domain Controller or Delegated Server:



Open the tool 'Active Directory Users and Computers' and add the QGripServerX to the group 'GSG_QGripServers'. The QGripServerX needs to be rebooted before you can continue.

On QGripServerX:

QGripServerX
gMSA_QGrip$
Install

The gMSA_QGrip$ account must be installed locally on the QGripServerX.

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

Install gMSA_QGrip$ on QGripServerX	PowerShell as Administrator
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All **Import-Module ActiveDirectory** **Install-ADServiceAccount** gMSA_QGrip **Test-ADServiceAccount** gMSA_QGrip	

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

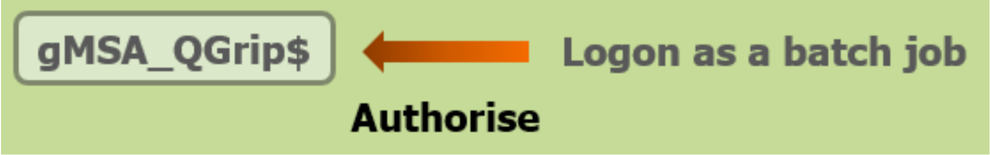
- "$" should be omitted in the statement.

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.

On QGripServerX:

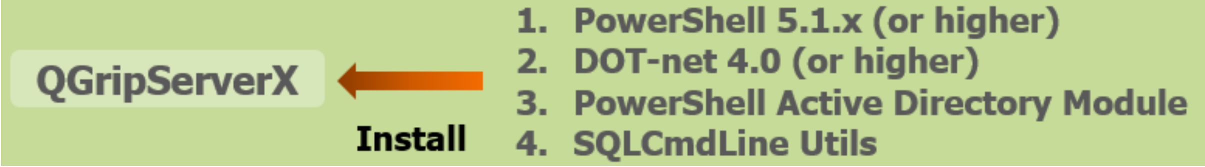


The gMSA_QGrip$ account needs to be member of the local group ‘Logon as a batch job’ on the QGripServer. Detailed description of how it can be implemented can be found in the appendix:

- Authorise: ‘Logon as a batch job’

7.2 Check/Install: Supporting Software

On QGripServerX:


QGripServerX
Install
1. PowerShell 5.1.x (or higher)
2. DOT-net 4.0 (or higher)
3. PowerShell Active Directory Module
4. SQLCmdLine Utils

7.2.1 PowerShell 5.1.x (or higher)

Check PowerShell version on QGripServerX	PowerShell

```
$PSVersionTable.PSVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      14393  1884
```

Install higher version on Windows Server 2012 R2

- Download Win8.1AndW2K12R2-KB3191564-x64.msu
- Copy the msu file to directory on the machine (E:\Software)
- Open a cmd-box as Administrator
- Go to the directory (E:\Software)
- Run this command: Win8.1AndW2K12R2-KB3191564-x64.msu /quiet
- **Wait!** It takes a while before system responds. The machine will be rebooted.

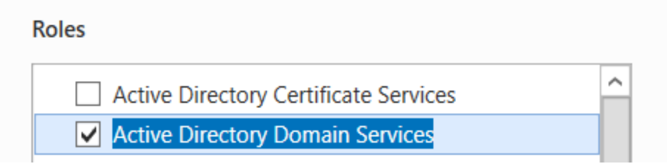
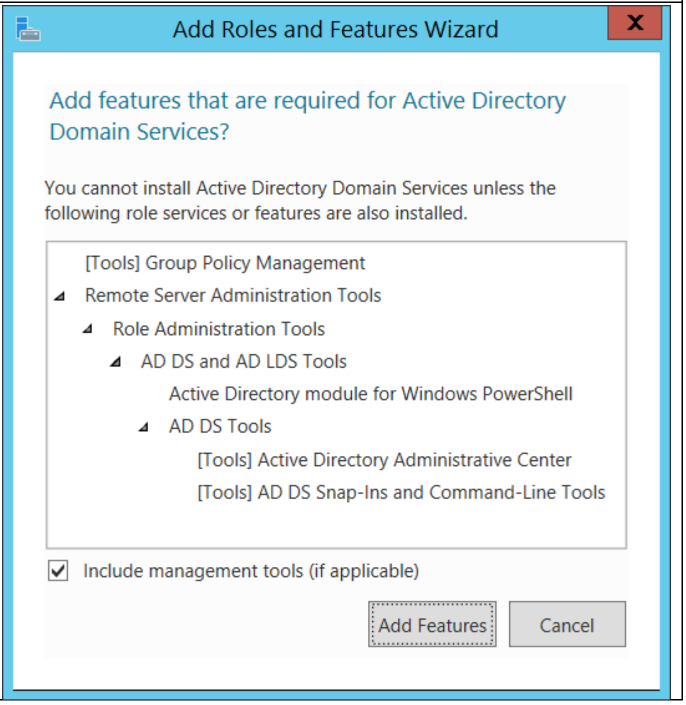
For other Windows versions, you will need to download and install the compliant msu.

7.2.2 DOT-net 4.0 (or higher)

Check DOT-net version on QGripServerX	PowerShell

```
[environment]::Version

Major  Minor  Build  Revision
-----  -----  -----  --------
4      0      30319  42000
```

7.2.3 PowerShell Active Directory Module

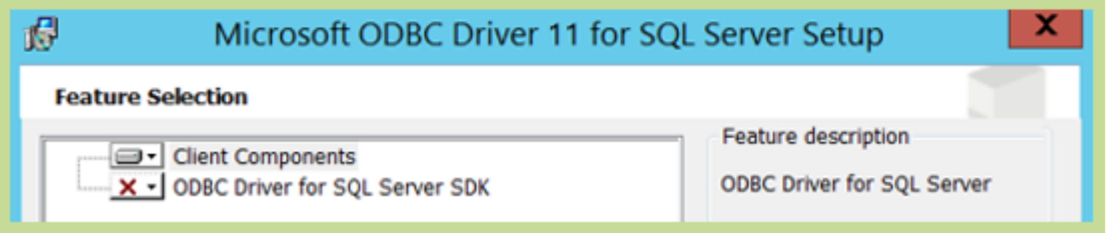
Install PowerShell Active Directory Module on QGripServerX	Server Manager
1. Server Manager -> Dashboard -> Add roles and Features 2. Installation Type: Role-based or Feature-based installation 3. Server Selection: QGripServerX 4. Server Roles: Active Directory Domain Services	 Roles ☐ Active Directory Certificate Services ☑ Active Directory Domain Services
5. Add Features 6. Next, Next, Next, Install	 Add Roles and Features Wizard Add features that are required for Active Directory Domain Services? You cannot install Active Directory Domain Services unless the following role services or features are also installed. [Tools] Group Policy Management ◢ Remote Server Administration Tools ◢ Role Administration Tools ◢ AD DS and AD LDS Tools Active Directory module for Windows PowerShell ◢ AD DS Tools [Tools] Active Directory Administrative Center [Tools] AD DS Snap-Ins and Command-Line Tools ☑ Include management tools (if applicable) Add Features Cancel

7.2.4 SQLCmdLine Utils

Download the highest version you can find of

- msodbcsql.msi
- MsSqlCmdLnUtils.msi

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



Microsoft ODBC Driver 11 for SQL Server Setup

Feature Selection

Client Components

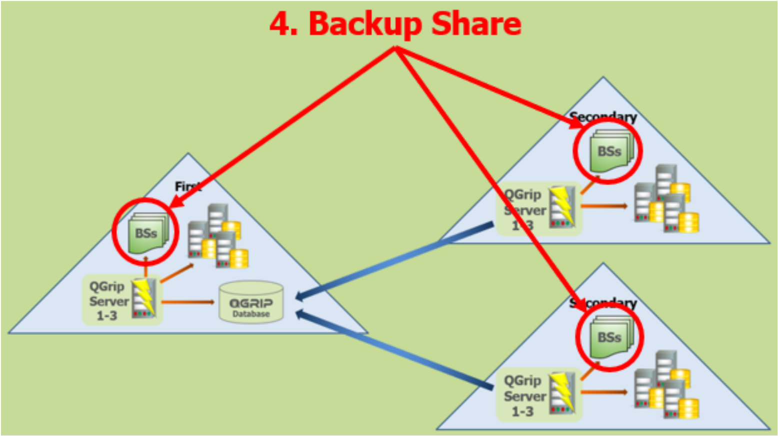
☒ ODBC Driver for SQL Server SDK

Feature description

ODBC Driver for SQL Server

Just select the ODBC driver.

8 New: Backup Share

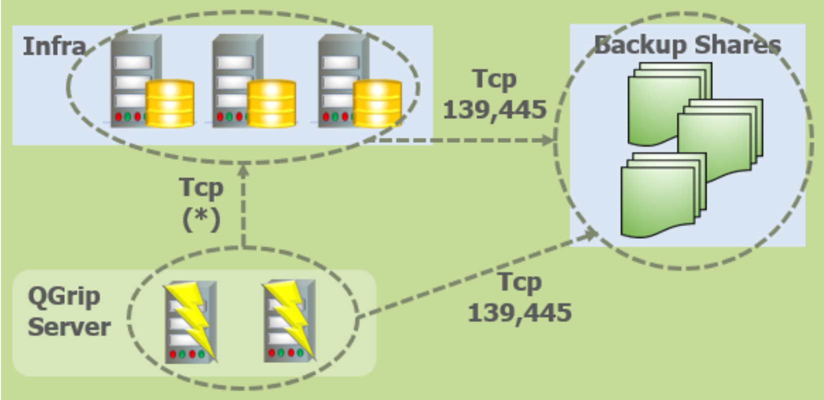


Create backup shares dedicated for the QGrip backups.

The Accessibility module in QGrip will check the backup share when added to QGrip and report errors.

The shares should be on physical (virtual) disk drives and should be empty before added to QGrip. You can define more, see BackupShare Types, but 3 is a minimum for the following (combinations) of Backup Types:

- DBBackup/LogBackup
- CopyOnly/Archive/BaseLine
- Import



The backup shares must be accessible from all SQL Server Instances and all QGrip Servers (ports 139 & 445) within the AD-Domain. Make sure that the backup shares are big enough for your database backup files in combination with retention period. Backup of the backup shares to secondary storage (tape) is highly recommended.

BackupShare Type
When adding a BackupShare in QGrip you will have to choose Share Type, that defines which type of backups will be made to the share.

- DBBackup/LogBackup
  These are the regular backups that are part of the Backup/Restore procedure. The backup files will be kept/removed according to the Clean-up definition you configure.
- CopyOnly/Archive/BaseLine

These are all “extra CopyOnly” backups that do not take part of the normal Backup/Restore procedure. When requesting a backup of one of these types, a “Keep until” date is mandatory. The backup file will stay on the backup share until the “Keep until” date has expired.

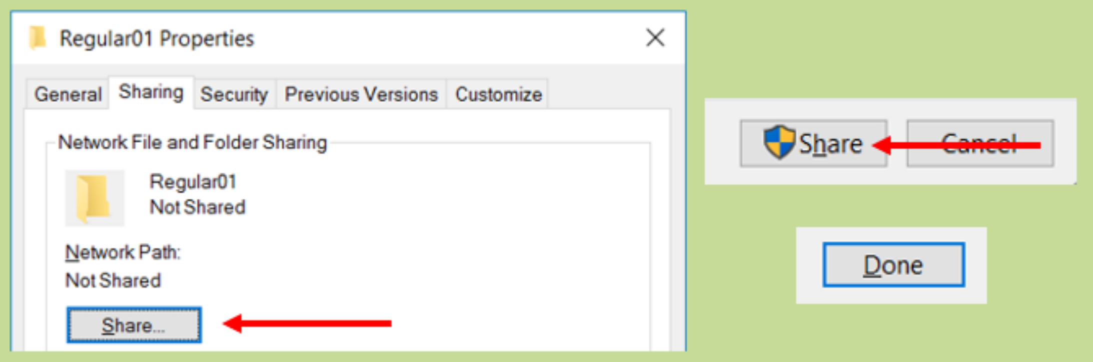
- Import
  The Import backup share will only be used if you need to import databases from backup files from, for instance, a supplier or a DMZ environment. No backups will be made to this share nor will QGrip perform any cleaning. The share will only be scanned on demand via the QGrip UI. Only one Import share is needed even if you have multiple domains.

The total list of Share types:

BackupShare Type	Remark
DBBackup/LogBackup	Mixed (FULL, FULL_COPY_ONLY, DIFF and TRAN).
DBBackup	Only for Database backups (FULL, FULL_COPY_ONLY and DIFF).
LogBackup	Only for Transaction log backups (TRAN).
CopyOnly/Archive/BaseLine	Mixed (COPY, ARCH and BASE).
CopyOnly	Only for CopyOnly backups (COPY).
Archive	Only for Archive backups (ARCH).
BaseLine	Only for BaseLine backups (BASE).
Import	No backups will be made to this share, only for Import-Database process.

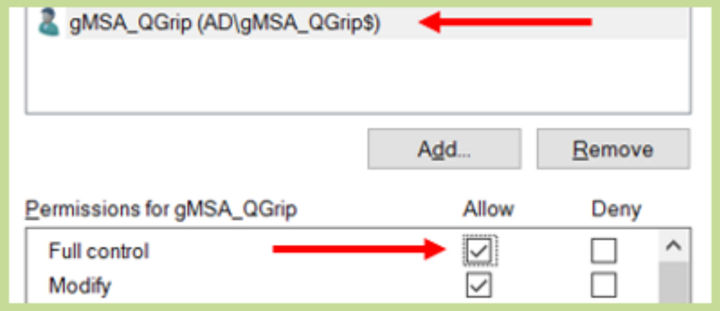
FULL_COPY_ONLY backups are DBBackups made on a SQL Server AlwaysOn cluster.

8.1 Create: Share

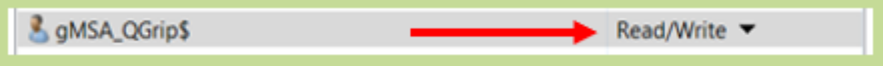


To create a share of the directory created for the backups, right click on the directory and open the properties, in the Sharing tab, click on share and in the next window Share and finally done.

8.2 Authorise: Full control & Share



The gMSA_QGrip$ and all DB Engine accounts need to be authorised Full control on the underlaying directory,



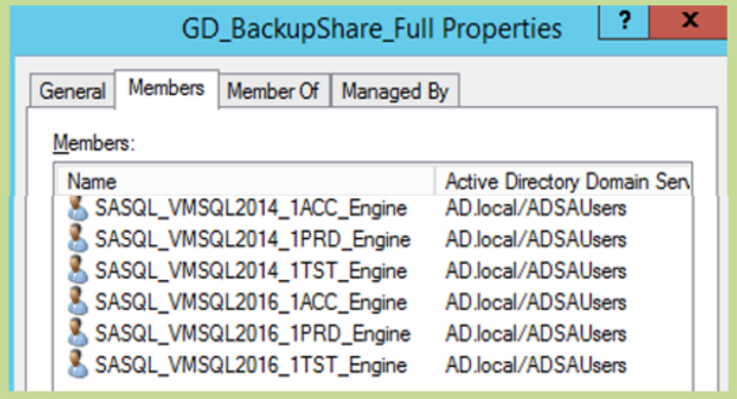
and Read/Write Permissions on the Share.

For a detailed step-by-step description, see Appendix: BackupShare: Authorise and Share

8.3 Backup Share Group

To minimise the number of accounts you need to authorise for each backup share, use an AD group:

1. Create a BackupShare AD-group (AD\GD_BackupShare_Full)
2. Grant full access on all BackupShares to AD-group
3. Add all Instances DB-Engine AD-Accounts to AD-group



Name	Active Directory Domain Serv
SASQL_VMSQL2014_1ACC_Engine	AD.local/ADSAUsers
SASQL_VMSQL2014_1PRD_Engine	AD.local/ADSAUsers
SASQL_VMSQL2014_1TST_Engine	AD.local/ADSAUsers
SASQL_VMSQL2016_1ACC_Engine	AD.local/ADSAUsers
SASQL_VMSQL2016_1PRD_Engine	AD.local/ADSAUsers
SASQL_VMSQL2016_1TST_Engine	AD.local/ADSAUsers

Important Note
Unfortunately, this does not work if the DB-Engine account is (group) Managed Service Account. These accounts will need to be authorised one by one, like the gMSA_QGrip$ account!

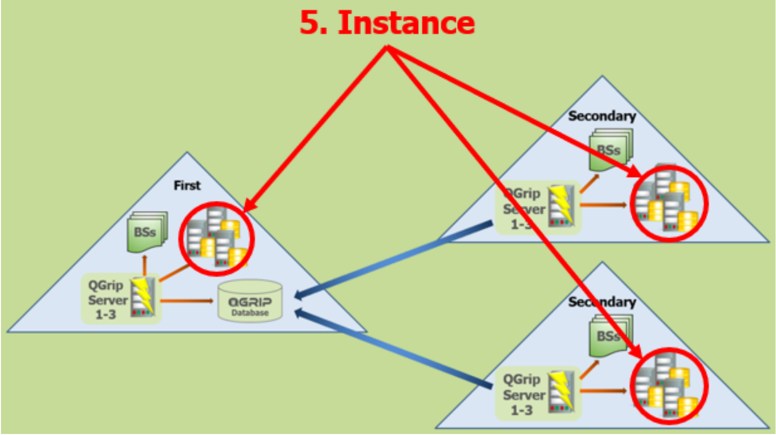
8.4 Encryption = member Administrators Group

If you want QGrip to Discover Symmetric Keys (MASTER KEY) and Certificate and enable TDE or QGrip backup encryption, the QGrip System Account (gMSA_QGrip$) must be added as member of the local Administrators Group on all Backup Share servers.

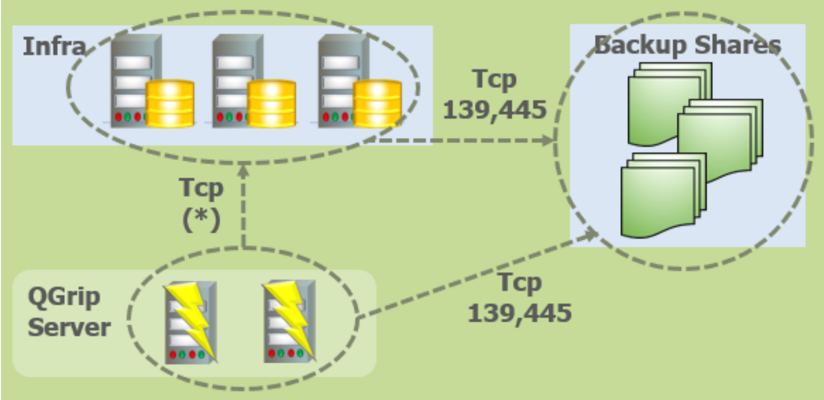
If the backup share is on a cluster, the QGrip System account needs to be member of the local Administrators Group on ALL nodes in the Cluster.

Why?
In order for QGrip to import the Symmetric Keys and Certificates to the QGrip database and make them available on any server, a backup will be made to one of the backup shares. When doing so, SQL Server writes the files to disk with minimal authorisation. In order for QGrip the read these files and import them, the QGrip System account must be member of the Administrators Group, otherwise the read action will fail.

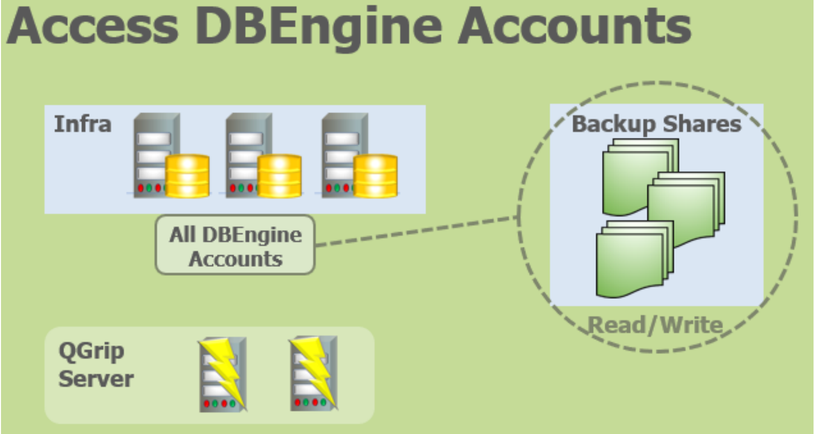
9 New: Instance



This section describes the preparations needed before an Instance can be added to QGrip.
The Accessibility module in QGrip will check everything listed in this section when the Instance is added to QGrip and report errors.

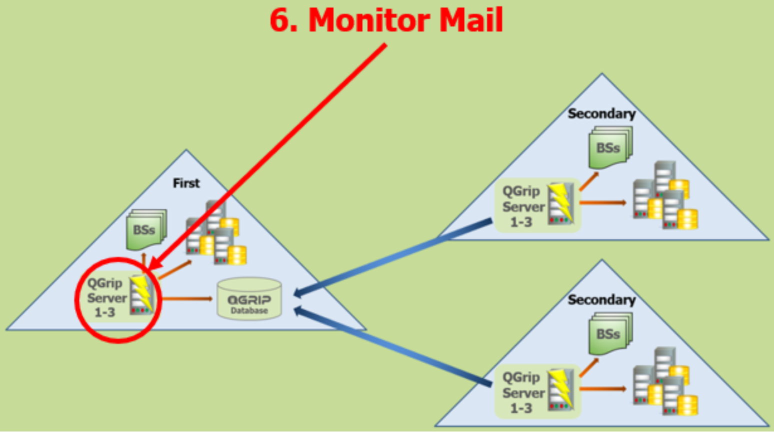


The backup shares within the AD-Domain must be accessible from the Instance (ports 139 & 445).
The Instance must be accessible from all QGrip Server within the AD-Domain.



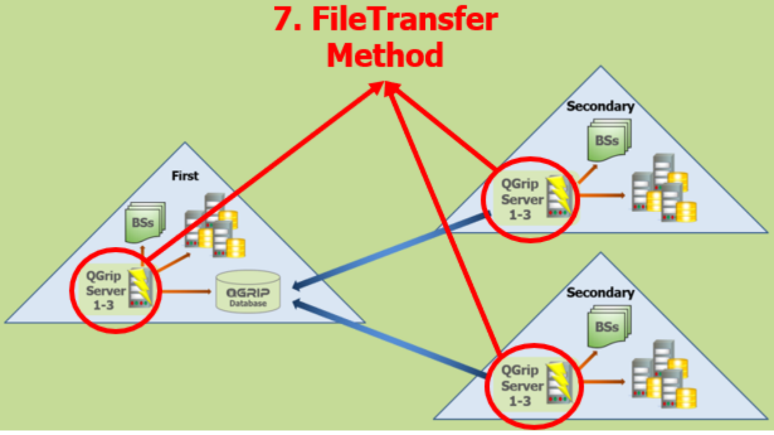
The DB-Engine account needs to be authorised for all Backup Shares within the AD-Domain.
See Appendix: BackupShare: Authorise and Share

10 Monitor Mail

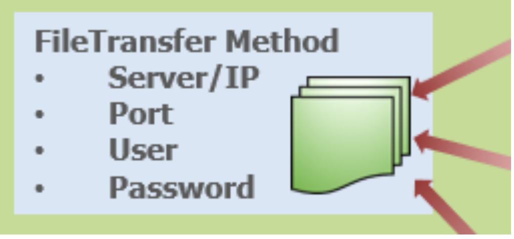


If you want to use the Complementary executable for the external monitoring and/or the backup overview mail, a smtp client must be accessible from the QGrip Server where those components are going to be installed.

11 New: FileTransfer Method



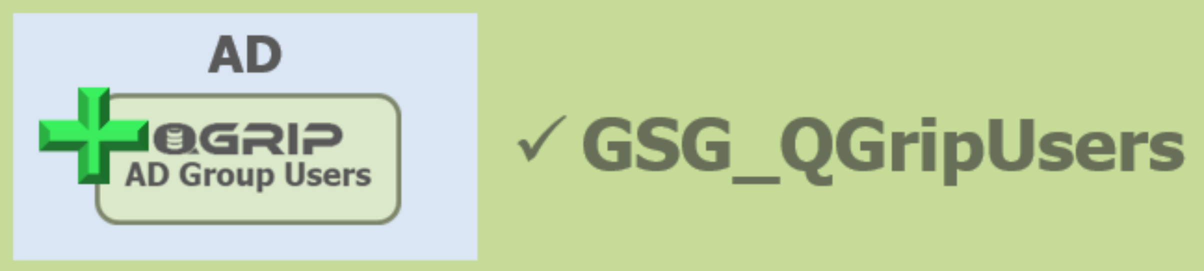
A FileTransfer Method in only needed in a multiple domain configuration. It will be used to exchange backup files between the QGrip Servers in the different AD-Domains to enable clones over the domains.



QGrip currently supports File Copy, FTP and SFTP. File Copy is only possible when there is a certain domain trust.

If you are currently using a method that QGrip does not yet supported, let us know and we will see if it can be added to QGrip.

12 Create: QGrip Users Group

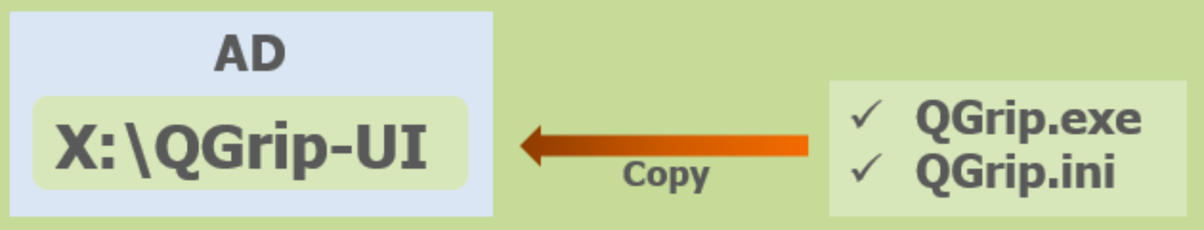


Create the QGrip Users Group on Active Directory.

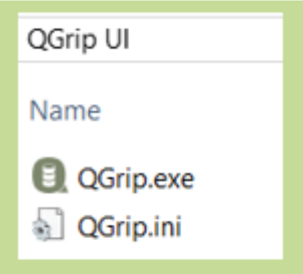
The GSG_QGripUsers is needed for the communication between the Grip-UI and the QGrip Database. The actual QGrip users should be added to this group.

13 Distribute Grip-UI (the clients)

13.1 Option 1, share



The GSG_QGripUsers should have been added as QGrip login during the Initial Configuration.



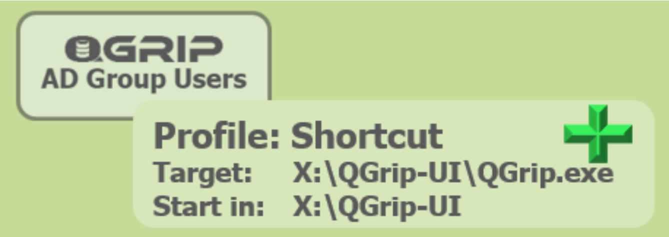
QGrip UI

Name

QGrip.exe

QGrip.ini

Download the QGrip.exe file using the Setup on one of the QGrip Servers. Place the QGrip.exe file together with the QGrip.ini file on the Grip-UI directory/share.

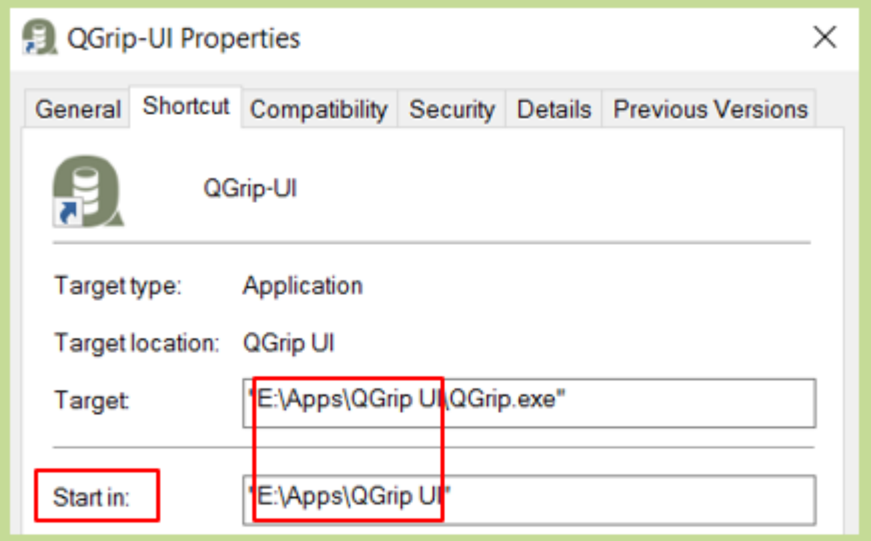


Profile: Shortcut

Target: X:\QGrip-UI\QGrip.exe

Start in: X:\QGrip-UI

In the profile of the members of GSG_QGripUsers, add a shortcut with the following properties:



QGrip-UI Properties

QGrip-UI

Target type: Application

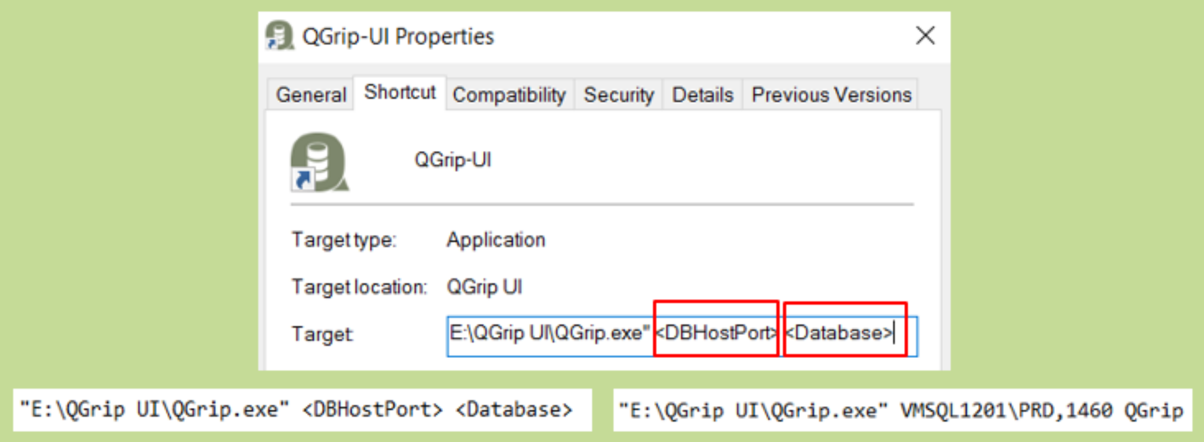
Target location: QGrip UI

Target: "E:\Apps\QGrip UI\QGrip.exe"

Start in: "E:\Apps\QGrip UI"

It is important that the “Start in:” property is equal to the “Target:” directory otherwise the QGrip.ini file will not be found.

The QGrip.exe can work also without the QGrip.ini by adding arguments to the target in a shortcut.



QGrip-UI Properties

QGrip-UI

Target type: Application

Target location: QGrip UI

Target: E:\QGrip UI\QGrip.exe" <DBHostPort> <Database>

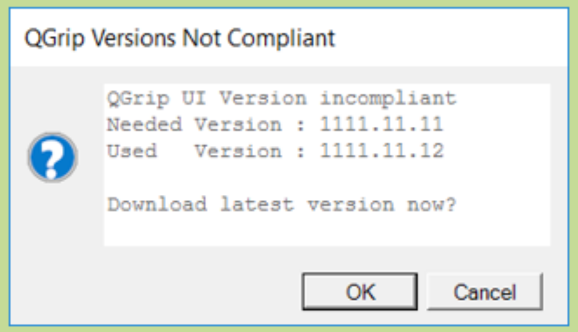
```
"E:\QGrip UI\QGrip.exe" <DBHostPort> <Database>
```

```
"E:\QGrip UI\QGrip.exe" VMSQL1201\PRD,1460 QGrip
```

The first argument is the DBHostPort and the second the Database, separated by spaces.
Both values can be found in the QGrip.ini

13.2 Option 2, local

Distribute the QGrip.exe together with the QGrip.ini to the users and let them place the files locally.



QGrip Versions Not Compliant

```
QGrip UI Version incompliant
Needed Version : 1111.11.11
Used   Version : 1111.11.12

Download latest version now?
```

This option is almost easier as the users can download the latest version themselves in case there is a new version of the Grip-UI after a new release.

14 Appendix

14.1 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:

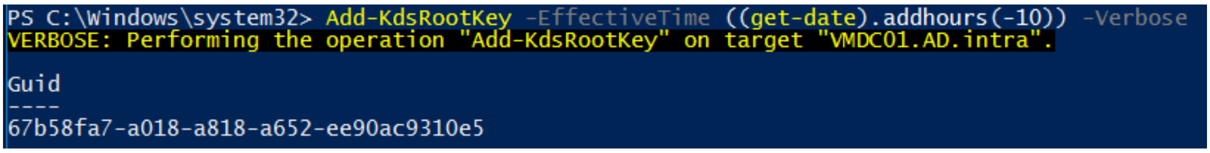
```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
```

On the Domain Controller:

Check existence KdsRootKey	PowerShell as Administrator
Get-KdsRootKey	

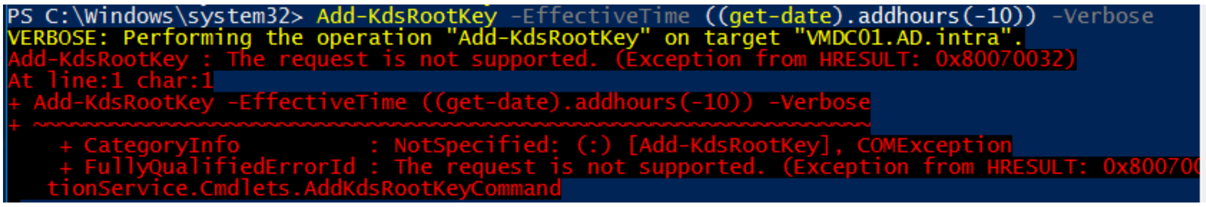
If no key is returned, you will need to create one.

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: 0x80070
   tionService.Cmdlets.AddKdsRootKeyCommand
```

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

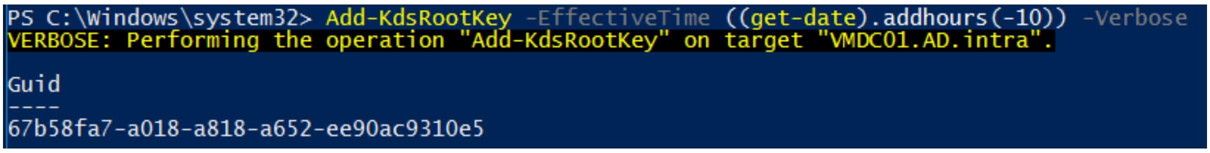
On another server:

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	



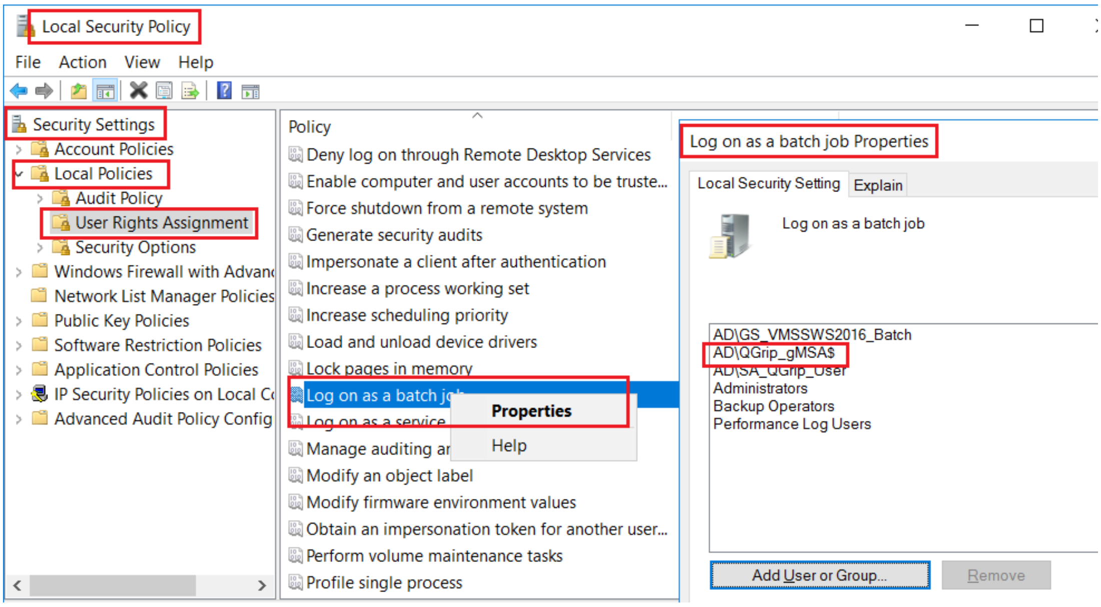
```
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "VMDC01.AD.intra".

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.

14.2 Authorise: ‘Logon as a batch job’

This section contains a detailed description of how ‘Logon as a batch job’ can be authorised on the local machine.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanc
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Co
Advanced Audit Policy Config
Policy
Deny log on through Remote Desktop Services
Enable computer and user accounts to be truste...
Force shutdown from a remote system
Generate security audits
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch jo
Log on as a service
Manage auditing ar
Modify an object label
Modify firmware environment values
Obtain an impersonation token for another user...
Perform volume maintenance tasks
Profile single process
Properties
Help
Log on as a batch job Properties
Local Security Setting
Explain
Log on as a batch job
Add User or Group...
Remove

AD\GS_VMSSWS2016_Batch
AD\QGrip_gMSA$
AD\SA_QGrip_User
Administrators
Backup Operators
Performance Log Users

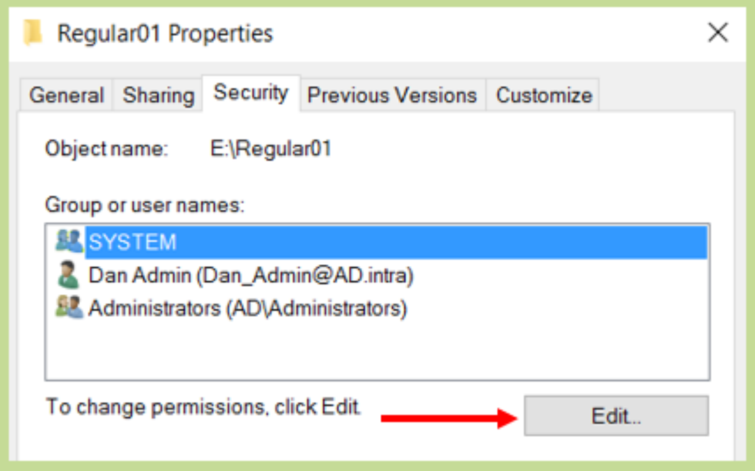
Start ‘Local Security Policy’ locally
Browse -> Security Settings
-> Local Policies
-> User Rights Assignment
-> Log on as a batch job
-> Properties (Right-Click)
The ‘Log on as a batch job properties’ windows will open.

In the tab ‘Local Security Section’, click [Add User of Group] to select the System account from the AD (not local). You might need to add ‘Service Accounts’ as Object Types if your gMSA_QGrip$ is not found when searching on AD.

Click [Apply].

14.3 BackupShare: Authorise and Share

14.3.1 Authorise



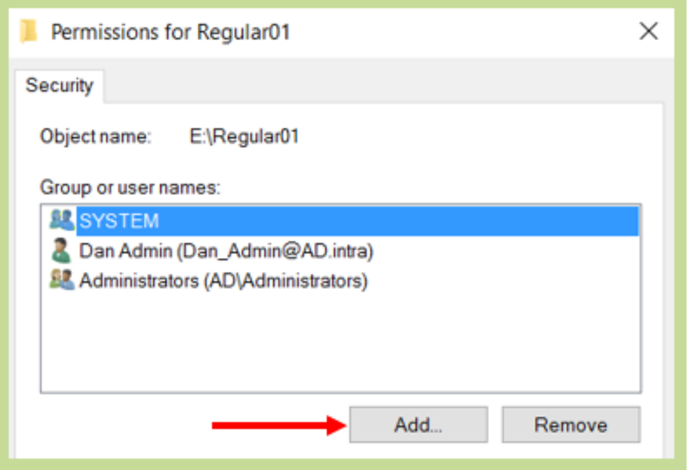
Object name: E:\Regular01

Group or user names:

- SYSTEM
- Dan Admin (Dan_Admin@AD.intra)
- Administrators (AD\Administrators)

To change permissions, click Edit.

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

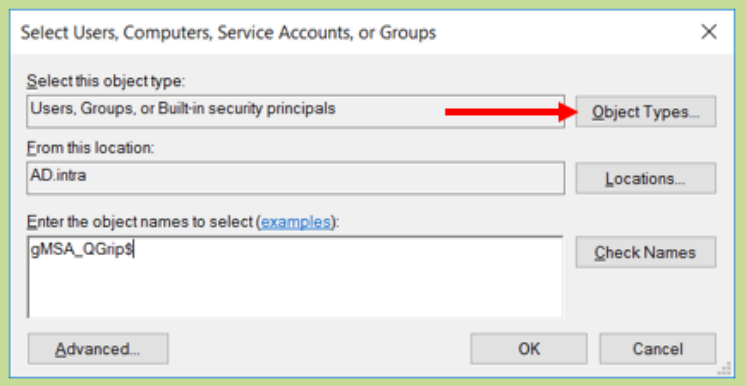


Object name: E:\Regular01

Group or user names:

- SYSTEM
- Dan Admin (Dan_Admin@AD.intra)
- Administrators (AD\Administrators)

In the Permissions window, click Add.

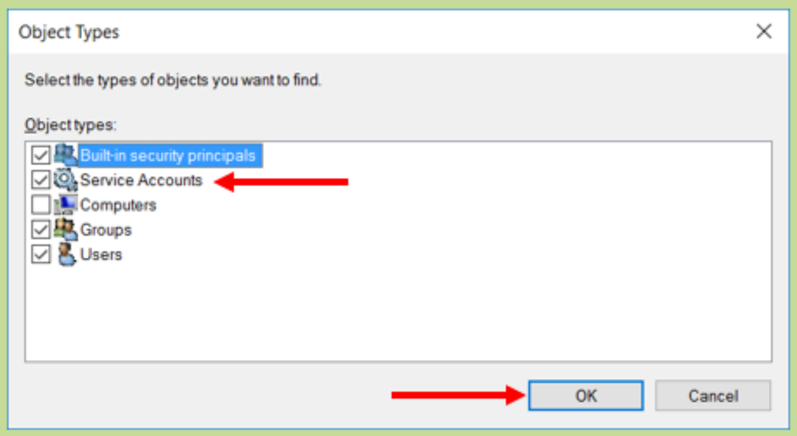


Select this object type: Users, Groups, or Built-in security principals

From this location: AD.intra

Enter the object names to select (examples): gMSA_QGrip$

If the account you want to authorise is a (group) Managed Service Account, click on Object Types.



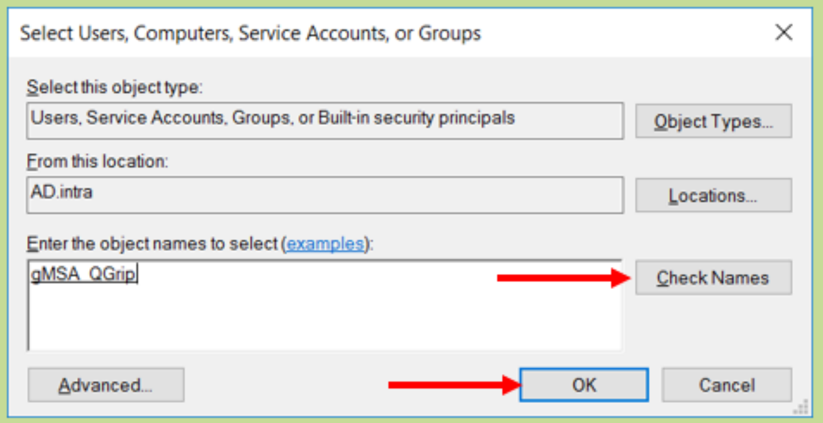
Object Types

Select the types of objects you want to find.

Object types:

☑ Built-in security principals
☑ Service Accounts
☐ Computers
☑ Groups
☑ Users

Check the Service Accounts checkbox and click OK.



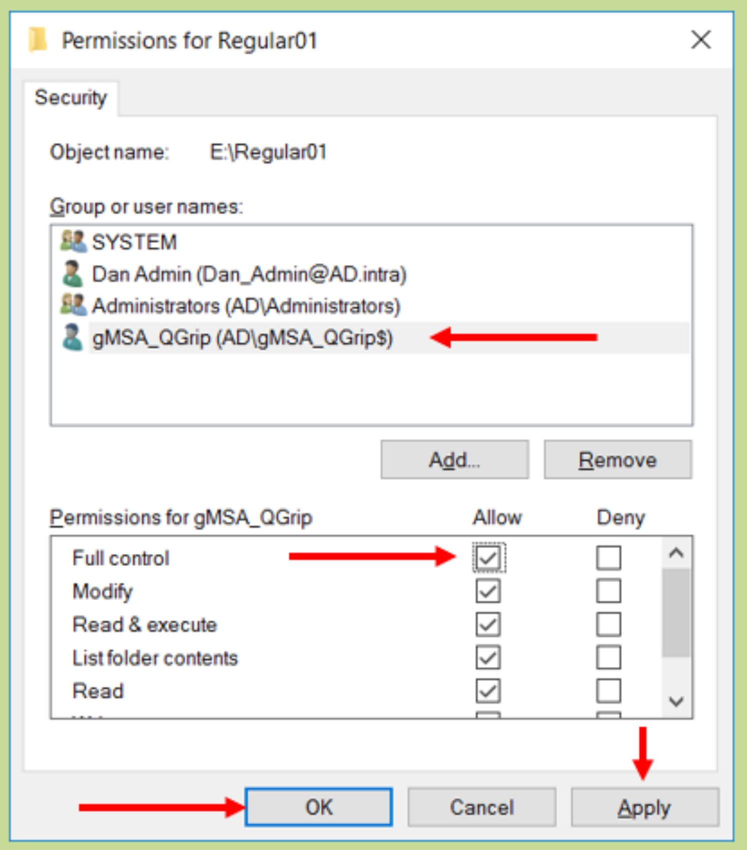
Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
AD.intra

Enter the object names to select (examples):
gMSA_QGrip

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



Permissions for Regular01

Security

Object name: E:\Regular01

Group or user names:

- SYSTEM
- Dan Admin (Dan_Admin@AD.intra)
- Administrators (AD\Administrators)
- gMSA_QGrip (AD\gMSA_QGrip$)

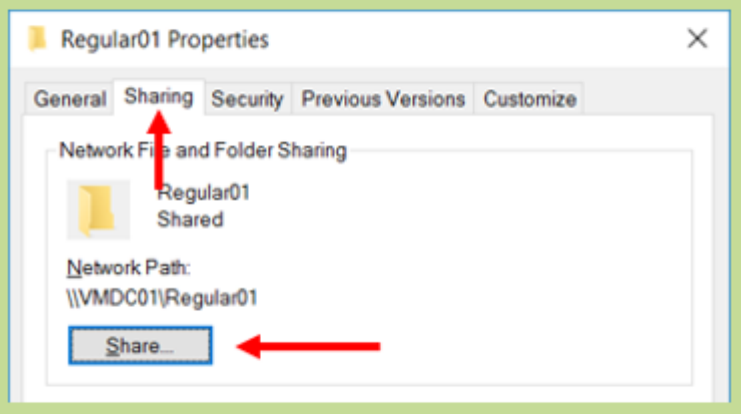
Add... Remove

Permissions for gMSA_QGrip	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

OK Cancel Apply

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

14.3.2 Share



Regular01 Properties

General Sharing Security Previous Versions Customize

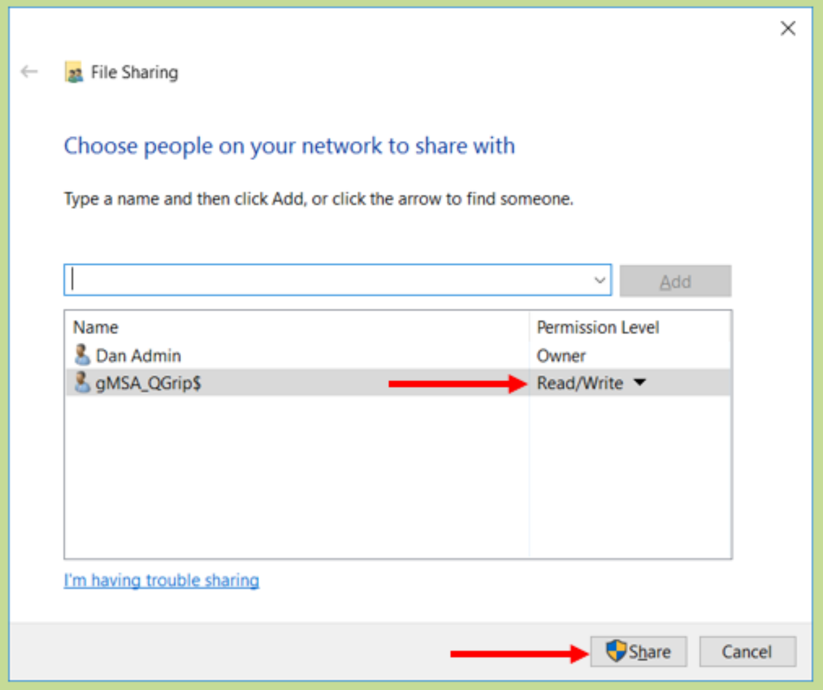
Network File and Folder Sharing

Regular01
Shared

Network Path:
\\VMDC01\Regular01

Share...

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



File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Dan Admin	Owner
gMSA_QGrip$	Read/Write

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