QGrip-UI
Admin Menu
Infra

GRIP ON SQL

2024-04-15

Contents

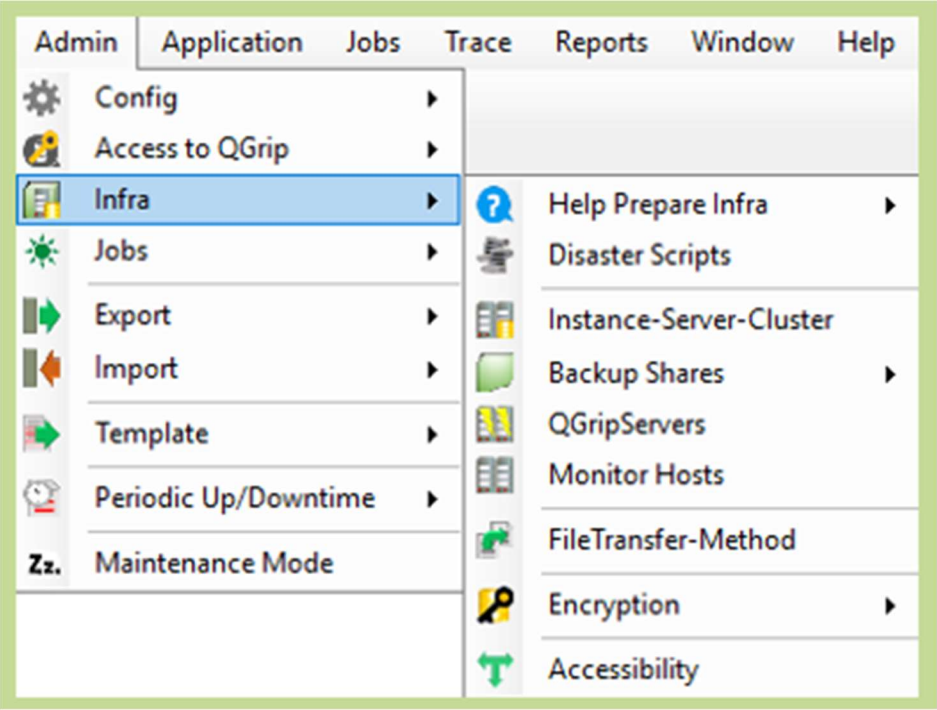
1 Introduction 4
2 Help Prepare Infra 5
2.1 Prepare for Instance 5
2.2 Prepare for Backup Share 6
2.3 Prepare for QGrip Server 7
2.4 Prepare for Move QGrip Database 8
3 Disaster Scripts 9
4 Instance-Server-Cluster 10
4.1 Instance 10
4.2 Server 11
4.3 Clusters 11
5 Backup Shares 13
5.1 Backup Share: Servers 13
5.2 Backup Shares: Edit 13
5.3 Backup Shares: Inconsistencies 15
5.3.1 Identification of BackupShare Inconsistencies 15
5.3.2 Resolution of BackupShare Inconsistencies 15
5.3.3 Delete Alien Files 15
5.3.4 Delete Restored Files 16
5.3.5 Register Restored Files 16
5.3.6 Delete Missing Files 16
5.4 Backup Shares: Keep Until Files 17
6 QGrip Servers 18
7 Monitor Hosts 18
8 FileTransfer-Method 19
9 Encryption 19
9.1 Symmetric Keys 20
9.1.1 Symmetric Key: Refresh 21
9.1.2 Symmetric Key: Details 21
9.1.3 Symmetric Key: Create 22
9.1.4 Symmetric Key: CopyTo 23
9.1.5 Symmetric Key: Drop 23
9.1.6 Symmetric Key: ExpBackup 24
9.1.7 Symmetric Key: Exp2File 25

9.1.8 Symmetric Key: Delete 26
9.2 Certificates 26
9.2.1 Certificate: Refresh 27
9.2.2 Certificate: Details 27
9.2.3 Certificate: Create 28
9.2.4 Certificate: CopyTo 28
9.2.5 Certificate: Drop 29
9.2.6 Certificate: ExpBackup 29
9.2.7 Certificate: Delete 30
9.3 Always On: Symmetric Keys & Certificates 31
10 Accessibility 32

1 Introduction

This document describes the items in the Admin Menu -> Infra of the QGrip-UI.

Required QGrip Role	Menu
QGrip-Admin	Admin -> Infra



Note that the Admin menu will only be visible for QGrip-Admin users and all Menu-Items will be enabled.

The FileTransfer-Method will only be visible in a Multiple Domain Configuration.

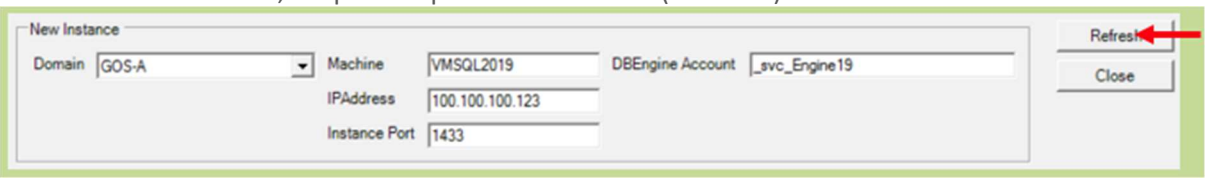
2 Help Prepare Infra

Planning to add a new Instance, Backup Share (Server) or QGrip Server to the QGrip configuration?
Or do you need to Move the QGrip Database?
This module can help you speed it up. Not only listing the information you need but also generate PowerShell statements that you need to check connectivity and create accounts.

Fill the upper part of the windows and hit the refresh button to fill the different tab pages.

2.1 Prepare for Instance

This window is intended for adding an existing SQL Server Instance to QGrip.
If you want to install SQL Server on a new machine, use the plugin QGrip-SQL-Installer documentation instead, chapter Prepare Instance Host (Machine).



Select domain and fill the rest of the fields and hit Refresh.

Firewall Rules

Description	SourceName	DestName	SourceIP	DestIP	DestPort
SQL Server Host -> Backup Share	VMSQL2019	ASHARE01	100.100.100.123	10.10.10.10	139,445
QGrip Server -> SQL Server Instance	ADEVQS01	VMSQL2019	10.10.20.41	100.100.100.123	1433

Use info to request firewall change whenever needed.

Firewall Checks

Description	CheckOnName	CheckOnIP
	Run on SQL Server Host : VMSQL2019	Run on SQL Server Host : VMSQL2019
SQL Server Host -> Backup Share	Test-NetConnection -Computer ASHARE01 -Port 139	Test-NetConnection -Computer 10.10.10.10 -Port 139
SQL Server Host -> Backup Share	Test-NetConnection -Computer ASHARE01 -Port 445	Test-NetConnection -Computer 10.10.10.10 -Port 445
	Run on QGrip Servers : ADEVQS01	Run on QGrip Servers : ADEVQS01
QGrip Server -> SQL Server Host	Test-NetConnection -Computer VMSQL2019 -Port 1433	Test-NetConnection -Computer 100.100.100.123 -Port 1433

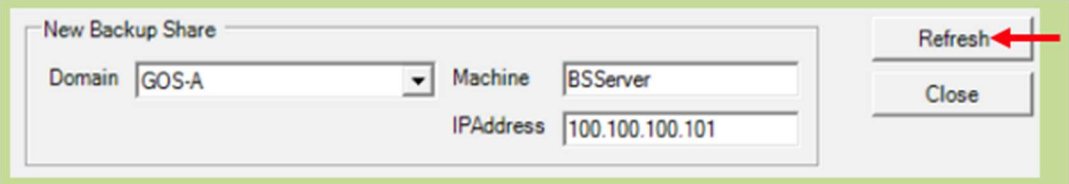
Use the statements to check if required connectivity is possible.

Authorisation Backup Shares

Instruction
On each Backup Share below
Add the account : _svc_Engine19
1. At disk level, with Full control.
2. Share the Folders with Read/Write.
Shares on Backup Share Server: ASHARE01
\\ASHARE01\DEV-CopyOnly
\\ASHARE01\DEV-Import
\\ASHARE01\DEV-Regular

Use the info to authorise the DB Engine account on existing Backup Shares.

2.2 Prepare for Backup Share



Select domain and fill the rest of the fields and hit Refresh.

Firewall Rules

Description	SourceName	DestName	SourceIP	DestIP	DestPort
SQL Server Host -> Backup Share	ADEVSQL12	BSServer	10.10.20.51	100.100.100.101	139,445
SQL Server Host -> Backup Share	ADEVSQL16	BSServer	10.10.20.52	100.100.100.101	139,445
QGrip Server -> Backup Share	ADEVQS01	BSServer	10.10.20.41	100.100.100.101	139,445

Use info to request firewall change whenever needed.

Firewall Checks

Description	CheckOnName	CheckOnIP
	Run on SQL Server Host : ADEVSQL12	Run on SQL Server Host : ADEVSQL12
SQL Server Host -> Backup Share	Test-NetConnection -Computer BSServer -Port 139	Test-NetConnection -Computer 100.100.100.101 -Port 139
SQL Server Host -> Backup Share	Test-NetConnection -Computer BSServer -Port 445	Test-NetConnection -Computer 100.100.100.101 -Port 445
	Run on SQL Server Host : ADEVSQL16	Run on SQL Server Host : ADEVSQL16
SQL Server Host -> Backup Share	Test-NetConnection -Computer BSServer -Port 139	Test-NetConnection -Computer 100.100.100.101 -Port 139
SQL Server Host -> Backup Share	Test-NetConnection -Computer BSServer -Port 445	Test-NetConnection -Computer 100.100.100.101 -Port 445

Use the statements to check if required connectivity is possible.

Authorisation Backup Shares

Instruction
On Backup Share Server : BSServer
Domain: GOS-A
1. Create Folders (Suggestion: Regular, CopyOnly, Import)
2. At disk level, add following accounts with Full control:
GOS-A\DEV_gMSA_QGrip$
GOS-A\DEV12A_M_DBEng$
GOS-A\DEV12P_M_DBEng$
GOS-A\DEV12T_M_DBEng$
GOS-A\DEV16A_M_DBEng$
GOS-A\DEV16P_M_DBEng$
GOS-A\DEV16T_M_DBEng$
3. Share the Folders with Read/Write to accounts above.
4. On Backup Share Server : BSServer
Add [GOS-A\DEV_gMSA_QGrip$] as member of local Administrators group

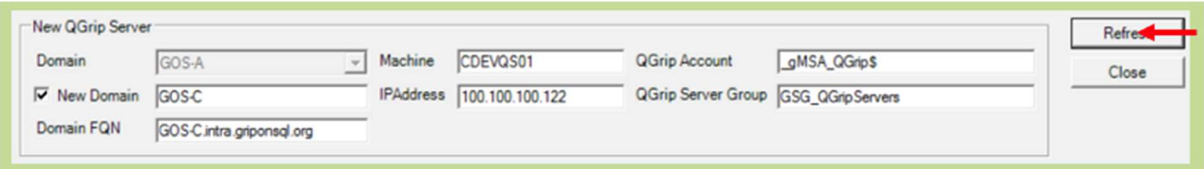
Use the info to create the backup shares and authorise the existing DB Engine accounts and the QGrip System Account.

Disk Space Estimate

Description	InstanceName	Domain	Environment	SpaceUsed(GB)
Per Instance	ADEVSQL12\TST	GOS-A	Test	0,51
Per Instance	ADEVSQL16\TST	GOS-A	Test	0,11
Per Instance	ADEVSQL12\ACC	GOS-A	Acceptance	0,25
Per Instance	ADEVSQL16\ACC	GOS-A	Acceptance	0,16
Per Instance	ADEVSQL12\PRD	GOS-A	Production	1,41
Per Instance	ADEVSQL16\PRD	GOS-A	Production	0,30
Per Instance	BDEVSQL1601\B16AOPRD1	GOS-B	Production	0,05
Per Instance	BDEVSQL1602\B16AOPRD2	GOS-B	Production	0,07

Gives an overview of how much disk space is currently used by each Instance and subtotals by different combination. Can be used for sizing of the new backup share or help when determining which Instances should use the new backup shares.

2.3 Prepare for QGrip Server



Select domain or check new domain if applicable and fill the rest of the fields and hit Refresh.

Firewall Rules

Description	SourceName	DestName	SourceIP	DestIP	DestPort
QGrip Server -> QGrip Database Host	CDEVQS01	ADEVSQL12	100.100.100.122	10.10.20.51	1460

Use info to request firewall change whenever needed.

Firewall Checks

Description	CheckOnName	CheckOnIP
	Run on QGrip Server : CDEVQS01	Run on QGrip Server : CDEVQS01
QGrip Server -> QGrip Database Host	Test-NetConnection -Computer ADEVSQL12 -Port 1460	Test-NetConnection -Computer 10.10.20.51 -Port 1460

Use the statements to check if required connectivity is possible.

Create QGrip Account

```
---- On Domain Controller or Delegated server, Domain: GOS-C
---- Active Directory Users and Computers Tool:
-- Create Security Group: GSG_QGripServers
-- Add as Members of group: GSG_QGripServers
-- Server: CDEVQS01

---- On Domain Controller, Domain: GOS-C
---- PowerShell as Administrator (Member Domain/Enterprise Admin group)
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All

New-ADServiceAccount -name _gMSA_QGrip `
-DNSHostName _gMSA_QGrip.GOS-C.intra.griponsql.org `
-PrincipalsAllowedToRetrieveManagedPassword GSG_QGripServers

-- Reboot Server: CDEVQS01

---- Locally, on Server : CDEVQS01
---- PowerShell as Administrator (Member Domain/Enterprise Admin group)
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-PowerShell -Online -All
Import-Module ActiveDirectory

Install-ADServiceAccount _gMSA_QGrip
Test-ADServiceAccount _gMSA_QGrip
```

Contains instructions and PowerShell commands to create the (gMSA) QGrip System Account.

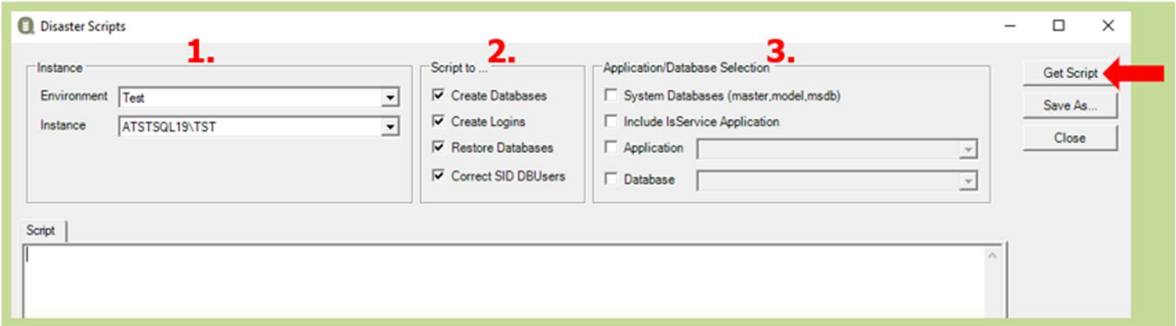
2.4 Prepare for Move QGrip Database

Doc-Tab	Title
Install	Move QGrip Database

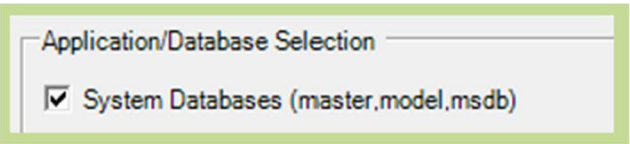
This part has been described in a separate document.

3 Disaster Scripts

Whenever needed, you can use the Disaster Scripts to restore (part of) a SQL Server Instance. The scripts are based on the information in the QGrip database and depend on the Discover job for creating Databases, Logins and Database Users. The generated restore script will be until the latest backup files.



1. Select the Instance
2. Select the Script type
3. Narrow down your selection (Optional)
4. Hit the [Get Script] button



System Databases (master, model, msdb)
The scripts generated for the system databases CANNOT be used without further modification. However, they can assist you with the latest backup files.

4 Instance-Server-Cluster

Recommended documentation

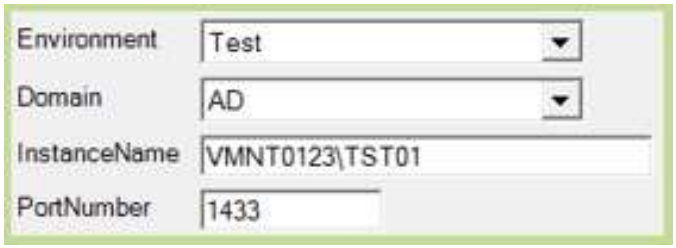
Doc-Tab	Title
Infra	Instance-Server-Cluster

4.1 Instance

Possible actions: View, New, Edit and Delete

You can add new Instances to QGrip and edit/delete existing ones. Immediately after adding an Instance, the Accessibility check will start running to make sure that the Instance is approachable and that backups can be made to all backup shares.

Note
When adding more instances, make sure you press the New button. Otherwise, you will just be editing the current Instance.

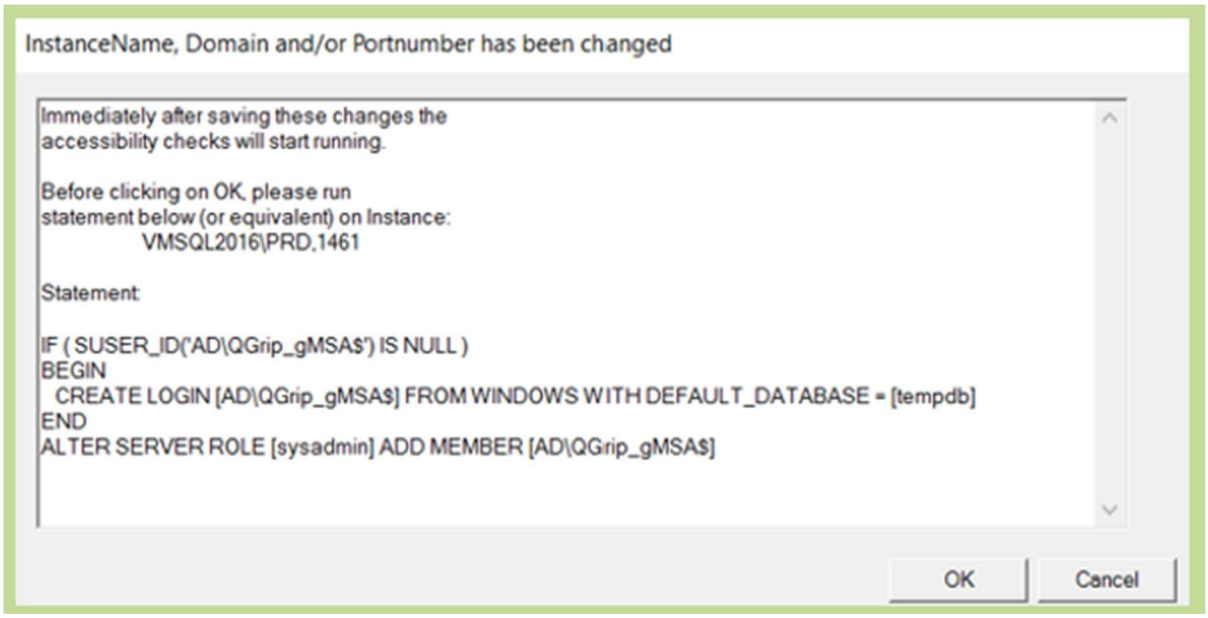


When adding or editing an Instance you only need to enter:

Field	Description
Environment	For which Environment is the Instance intended.
Domain	On which AD-Domain is the Instance running.
InstanceName	The actual name of the Instance, must be the same as @@SERVERNAME.
PortNumber	Even if the Port Number is default, 1433, we recommend that you always enter it.

The rest of the fields will be filled during the Discover process.

Instance Name	Remark
Named Instance	Use the full name including the “Instance”: VMSQL2014\DEV
Default Instance	Do not add the MSSQLSERVER “Instance”: ~~VMSQL2014\MSSQLSERVER~~ Use VMSQL2014 instead.



When the Save button is pushed for a new/edited Instance, you will receive a Popup concerning the QGrip System Account that needs to be created on the new instance in order to enable access for QGrip. Ignoring this message will result in Accessibility problems.

Do not forget to check the Accessibility after adding new or changing existing Instances.

The Discover job of the Instance will automatically be triggered when the Instance has successfully been added. The job will not start running if there are Accessibility issues.

Job Schedules
When an Instance has been saved and the discover job has run once on the Instance, you can edit the Instance's Job Schedule.
This can be done in the Schedules Window (Menu: Admin -> Jobs -> Schedules)

4.2 Server

Possible actions: View, Edit and Delete

During the Discover of an Instance, it will be determined which Server (Host) the Instance is running on. If the host is a Server that does not yet exist in QGrip, it will be added automatically.

Only the field Licensed Cores can be edited.

Field	Description
Licensed Cores (*)	For SQL Server license.

(*) Number of Licensed Cores (For SQL Server) will be used in License Compliancy Report and during the Charges (Split Cost) module.

Delete
A server that does not contain any Instances and is not Cluster Node in a Cluster can be deleted.

4.3 Clusters

Possible actions: View and Delete

If the Discover process detects that an Instance is running on a Cluster, the Cluster will be added to QGrip. The Cluster information cannot be edited in QGrip.

Delete
A Cluster that does not contain any Instances or Cluster Nodes can be deleted.

5 Backup Shares

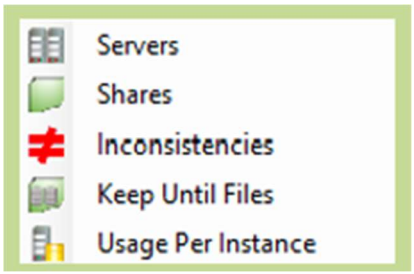
Recommended documentation

Doc-Tab	Title
Infra	Backup Share

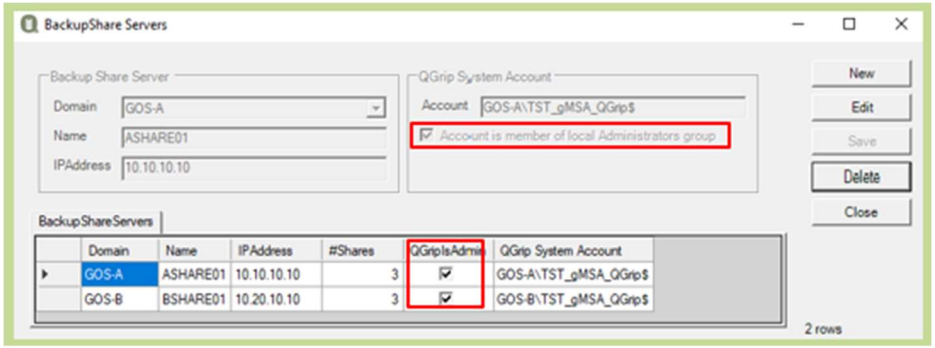
All backups within QGrip will be made to shares. The Backup Shares added to QGrip must already exist on your infra structure. The QGrip document

Install: Prepare Infra

contains a section suggesting how you should configure the permissions on the Backup Share to make the integration with QGrip smooth.



5.1 Backup Share: Servers



Before you can add Backup Shares, you need to add the Server that will host the Shares. You only need to select the Domain and enter server name and IP address.

If you have enabled Encryption, Symmetric Keys and Certificates, you can see if the QGrip System Account is Local Administrator on the Backup Share Servers, marked Red in picture above.

5.2 Backup Shares: Edit

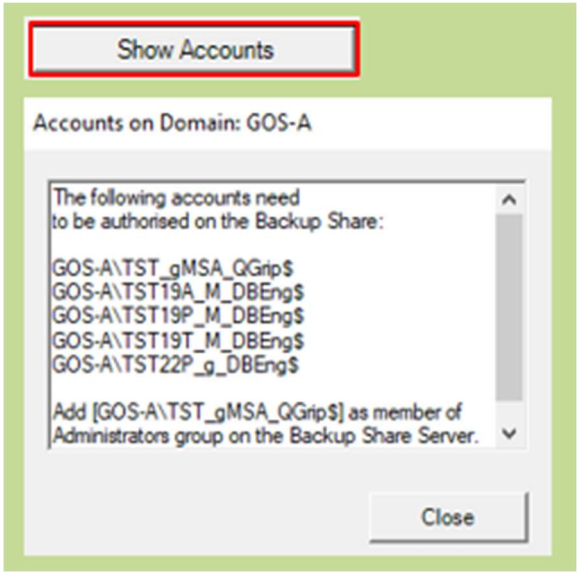
Click on New to define a new Backup Share or Edit to change an existing one. It is only possible to delete a BackupShare if it is no longer being used and there are no registered backup files left on it.

Name	Description	Remark
Share Name	The visible name of the share.	Can be changed at all times.
Share Type	Choose the type of backup files that will be stored on the Share	As soon as one Schedule is using the share, no alteration is possible.
Max Parallel	The max number of processes that are allowed to write to the share	Can be changed at all times.

	simultaneously. If the Max is reached, other processes have to wait until one of the busy processes has finished.	
Share Path	The UNC path to the share.	Can be changed until one backup has been written to the share. Changing the path will trigger the Accessibility Check.
Capacity Used Space Free Space	These fields will be filled by the system.	Not editable.
Max Used	High Water Mark The maximum of used space (between backup and delete files)	This value can be reset by using button: Reset Max Used

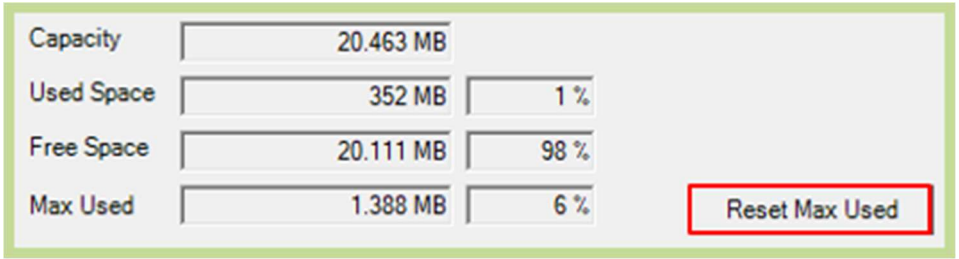
Note:
Accessibility check will run after adding or modifying Backup Shares. Do not forget to check the status of the Accessibility checks.

Show Accounts:



Push this button to see all Accounts (QGrip + DBEngine) that need to be authorised for a Backup Share.

Reset Max Used



QGrip is continuously monitoring the Used Space on the Backup Shares. During a backup window, the Used Space will increase as backup files are added before old files can be deleted. The Max Used is the High Watermark and will show the Max Used up until now, even if it was a year ago. Use the Reset Max Used button to reset the value and start all over again.

5.3 Backup Shares: Inconsistencies

5.3.1 Identification of BackupShare Inconsistencies

QGrip fully maintains the backup shares (except Import backup share) and the files on the shares must be consistent with the backup files registered in the QGrip database. The following Jobs will check for Inconsistencies:

- DomainJob: DeleteCheck-BackupFiles
- DomainJob: Check-BackupShares

Fixing any Inconsistencies should be done in the QGrip-UI except putting Missing files back on the backup share.

Inconsistency Types:

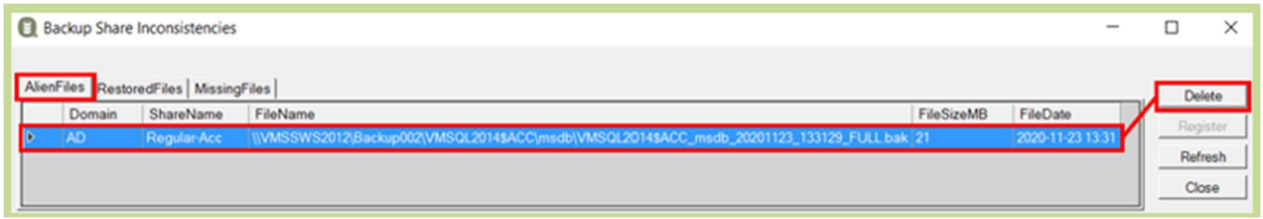
Inconsistency Type	Description
Alien Files	Files are unknown to QGrip. It is possible that the files have been restored from Tape but the files are so old that the Job History for that file has been deleted.
Restored Files	Files can be found in QGrip but are marked as Deleted. This happens when a deleted file has been restored from Tape.
Missing Files	According to the QGrip administration the files should be on the Backup Share but they are not.

5.3.2 Resolution of BackupShare Inconsistencies

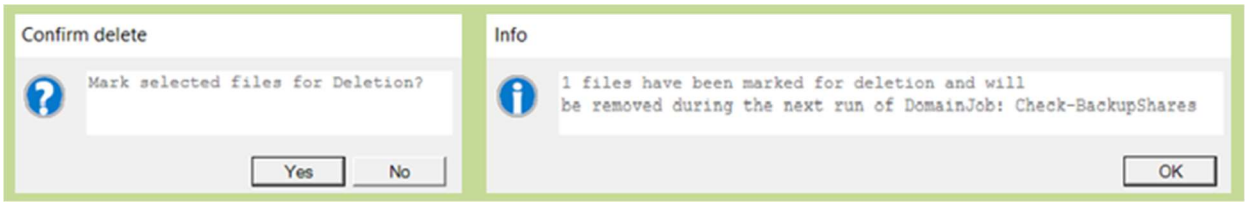
Possible Actions

Inconsistency Type	Possible Action
Alien Files	Let QGrip remove the files from the Backup Share
Restored Files	Let QGrip remove the files from the Backup Share if they are not needed or Register the files in QGrip with a keep until date.
Missing Files	Let QGrip remove the files from the QGrip administration or Manually find the files and put them back on the Backup Share

5.3.3 Delete Alien Files

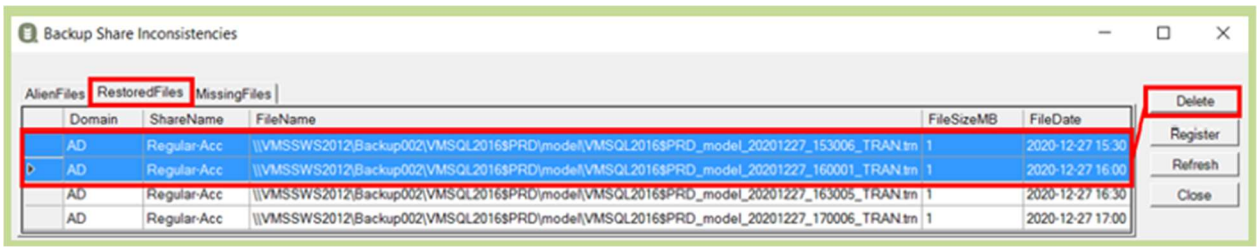


In the Tab Alien Files select the files you want to delete and press Delete.

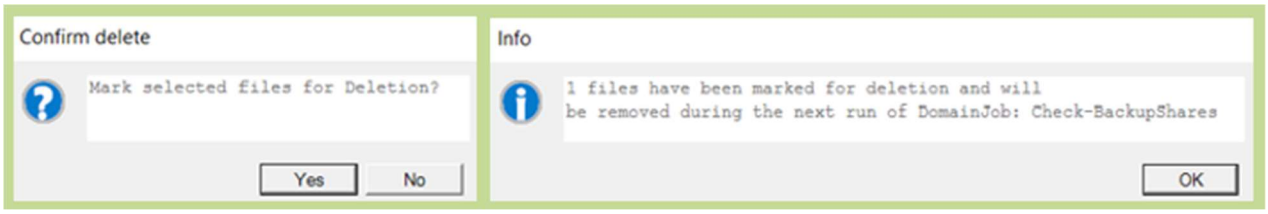


The files will be deleted during the next run of job: DomainJob – Check-BackupShares

5.3.4 Delete Restored Files

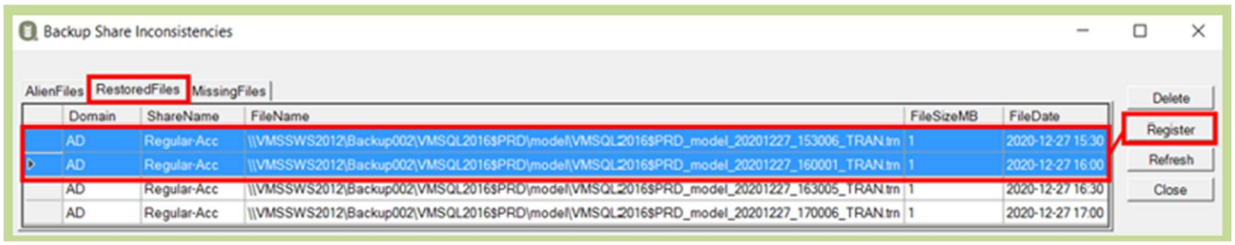


In the Tab RestoredFiles, select the files you want to delete and press Delete.

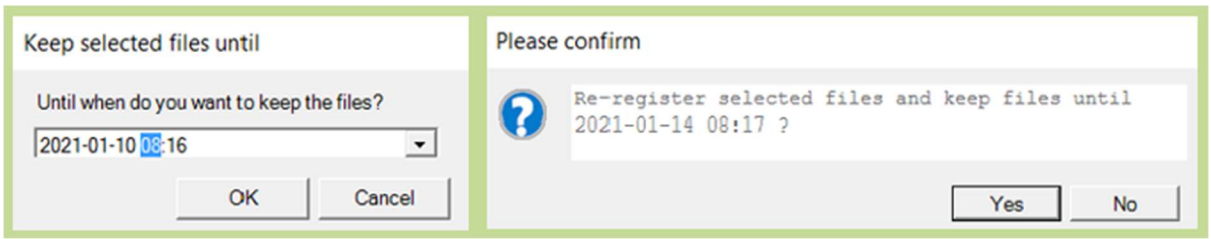


The files will be deleted during the next run of job: DomainJob – Check-BackupShares

5.3.5 Register Restored Files

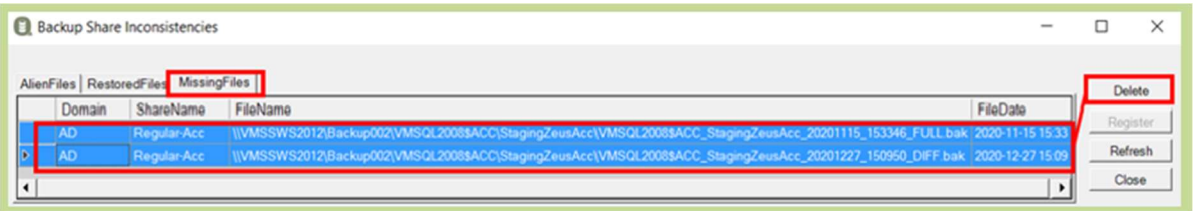


In the Tab RestoredFiles, select the files you want to Register and press Register.

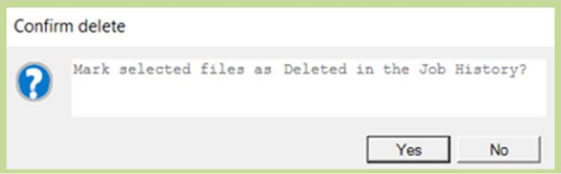


Enter the date until when you want to keep the files and confirm your choice.

5.3.6 Delete Missing Files



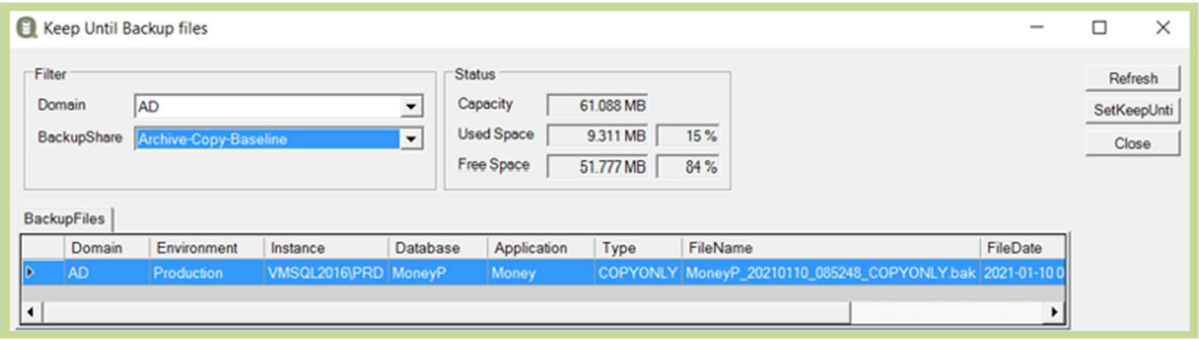
In the Tab MissingFiles, select the files you want to mark as deleted and press Delete.



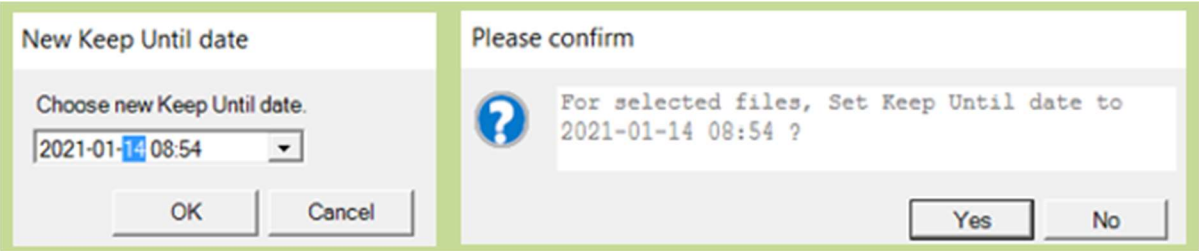
Confirm your choice.

5.4 Backup Shares: Keep Until Files

This window shows the Backup Files for which the “Keep Until” date has been set. Normally, that are CopyOnly, Archive and BaseLine backups but it can also be Restored Files that have been “Re-Registered”.



You can change the Keep Until date by selecting backup files in the overview and press [SetKeepUntil]:



Set the date in the past if you want the files to be deleted as soon as possible.

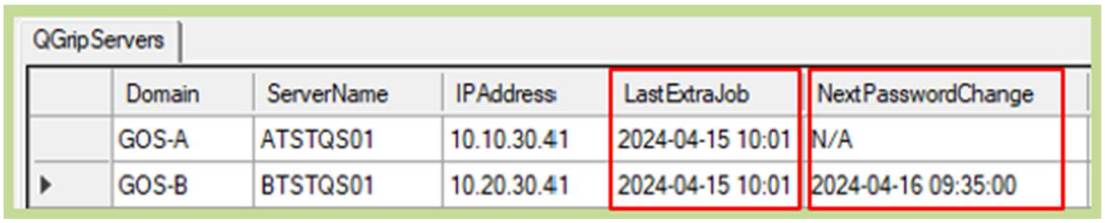
6 QGrip Servers

Recommended documentation

Doc-Tab	Title
Infra	QGripServer

You can view all QGrip Servers but you can only Edit the Remark and IP Address if it is missing.

If a QGrip Server is part of a Multiple Domain Configuration and is using a QGripMSA to communicate with the QGrip Database, you can also change the change password frequency and time.

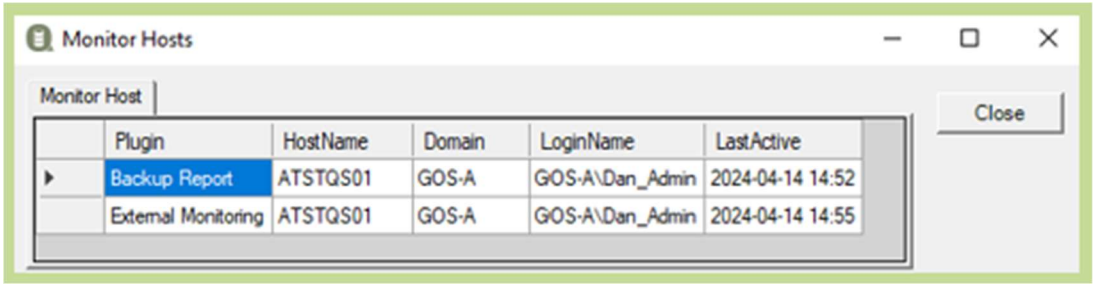


The Extra Job should run every minute on all QGrip Servers. If you suspect that a QGrip Server is not working properly, check the time of LastExtraJob. If it is more that 3 minutes ago, login on the QGrip Server and check the Logfiles for errors.

7 Monitor Hosts

Recommended documentation

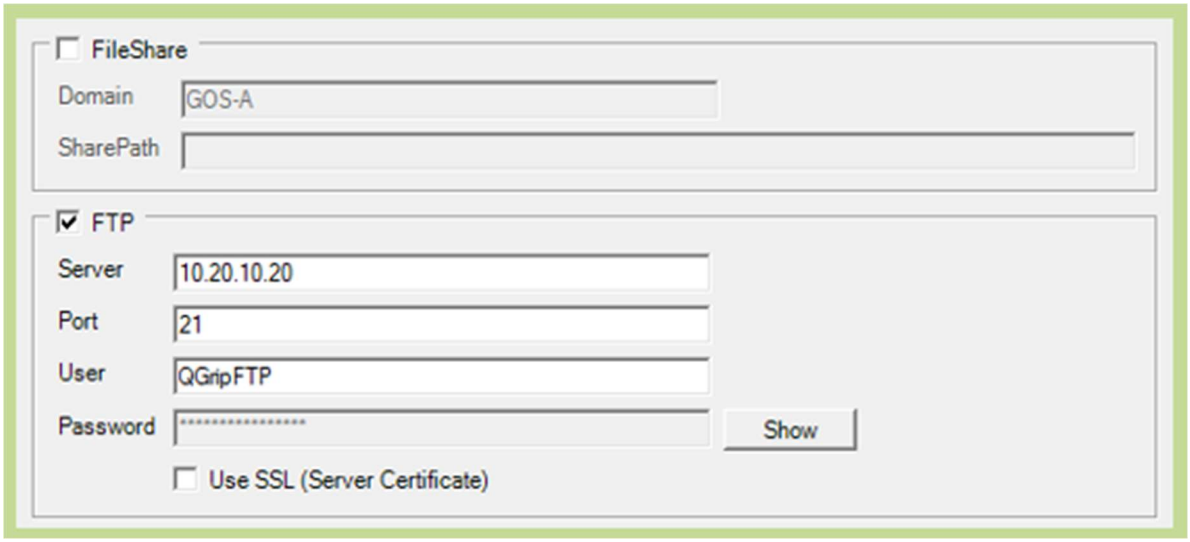
Doc-Tab	Title
Plugins	Mail Backup Report
Plugins	External Monitoring



If you are using the Plugins Backup Report and/or External Monitoring, you can see from which host they are initiated, the Login Name and when it was Last Active.

8 FileTransfer-Method

The FileTransfer-Method menu item will only be visible in a Multiple Domain Configuration (more than 1 AD-Domain).



Select the protocol/option you want to use and fill the parameters.

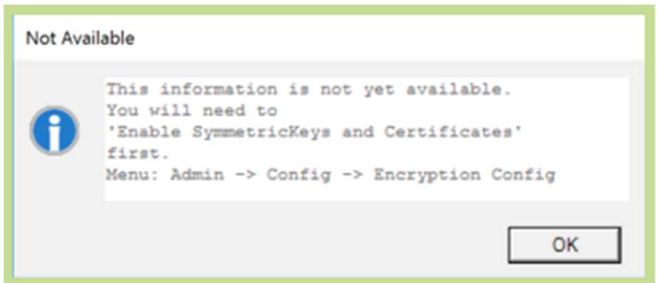
The accessibility check QGripServer-TransferMethod will start running for all QGripServers immediately after saving changes.

If QGrip does not yet support the method you want to use, please let us know and we will see if we can add it.

9 Encryption

Recommended documentation

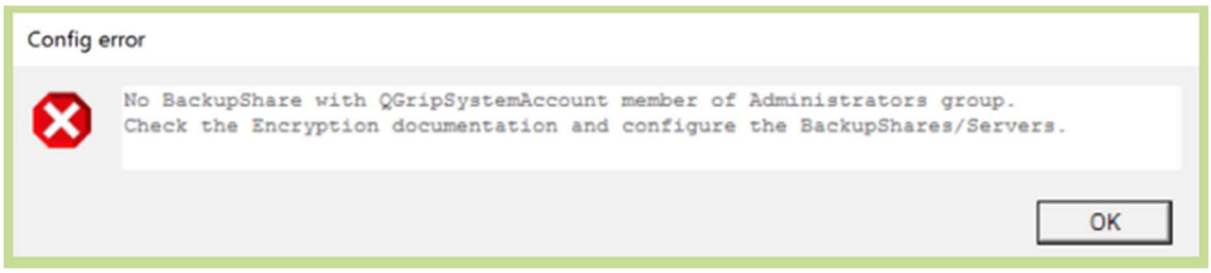
Doc-Tab	Title
Infra	Encryption (Keys and Certificates)
Jobs	QGrip Backup Encryption



The Symmetric Keys and Certificate module will not be available as long as it has not yet been enabled.

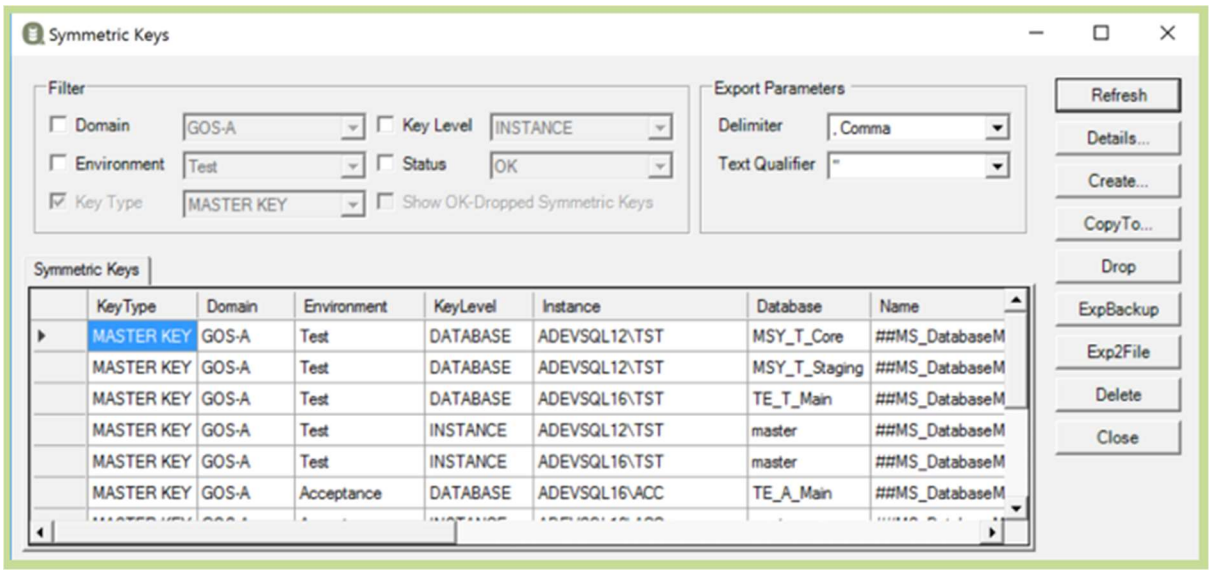
Temporary Status:
Queued For CopyTo
Queued For Create
Queued For Drop
Queued For Backup
Queued For Verify-Password

All actions done on Symmetric Keys and Certificates are done via the RemoteJob Queue with as Job Type 'SymmetricKey' or 'Certificate'. When a request has been placed on the Queue to be executed, the object will get a Temporary Status. As long as it has that status, the object cannot be changed in the QGrip-UI. When your request, let say Create Symmetric Key has been processed, you will receive a personal message.



If you try to start an action and there is no Backup Share available for Backup/Import, you will receive the error message above.

9.1 Symmetric Keys

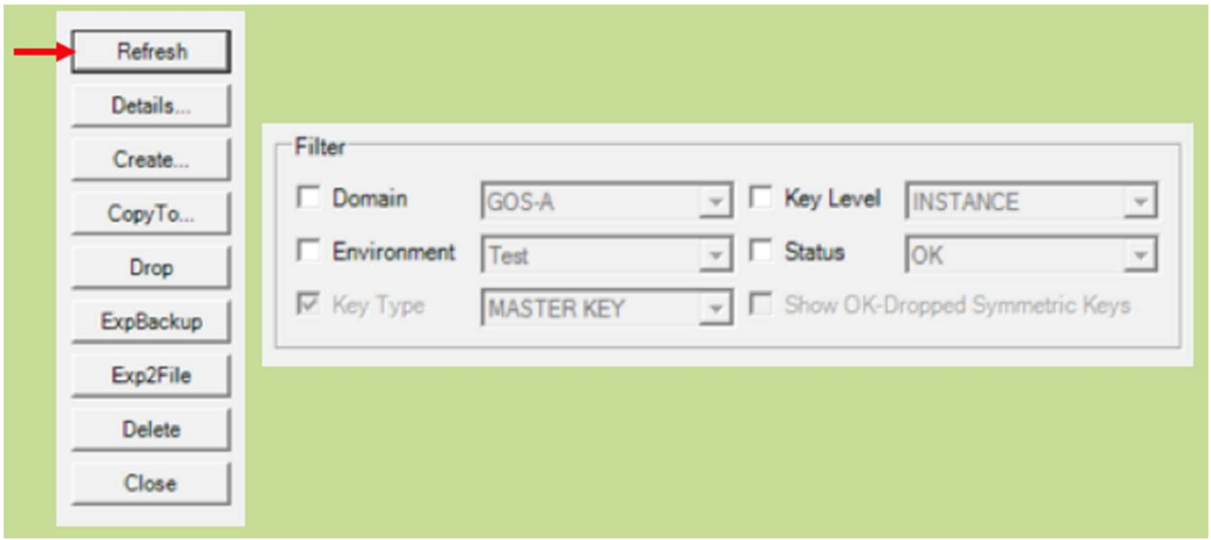


The Symmetric Keys main window is compact with a lot of different buttons that will be explained here below.

The status of a Symmetric Key depends on the availability of information and if QGrip is able to backup and import the Key to QGrip.

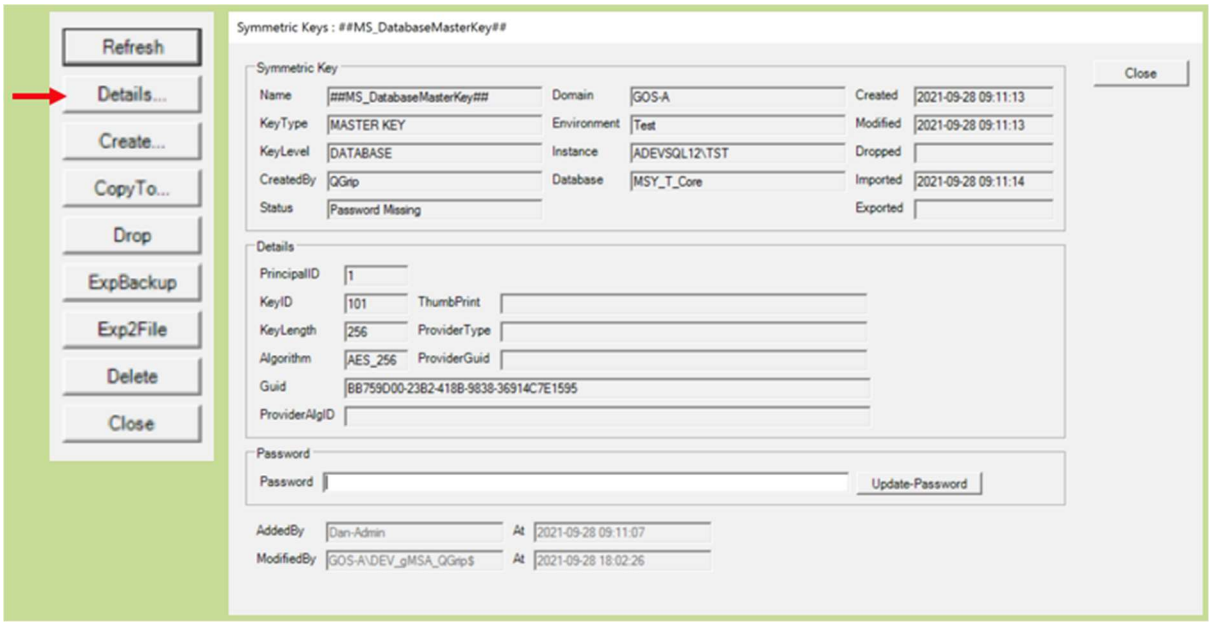
Status	Remark
Password Missing	As long as the password is missing, QGrip will not be able to backup and import the Symmetric Key (file) to QGrip.
Import Missing	Password is available but Backup/Import fails because of missing Authorisation on the Backup Share server (QGrip System Account member of Administrators group)
OK	Password is available and import to QGrip completed.
OK-Dropped	Password is available and import to QGrip completed but the Symmetric Key has been dropped on the Instance.

9.1.1 Symmetric Key: Refresh



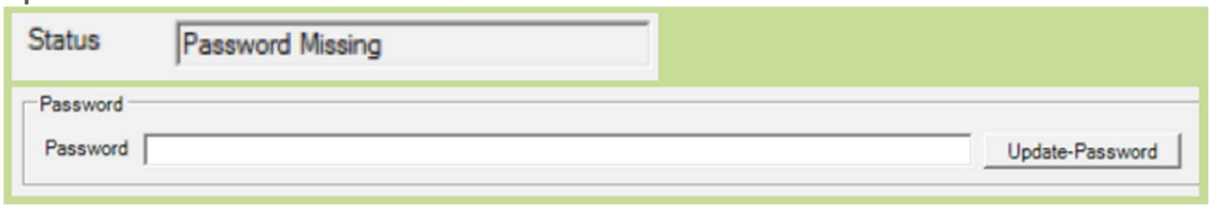
When the Refresh button is pushed, the data in the tab page will be refreshed according to the setting in the Filter.

9.1.2 Symmetric Key: Details



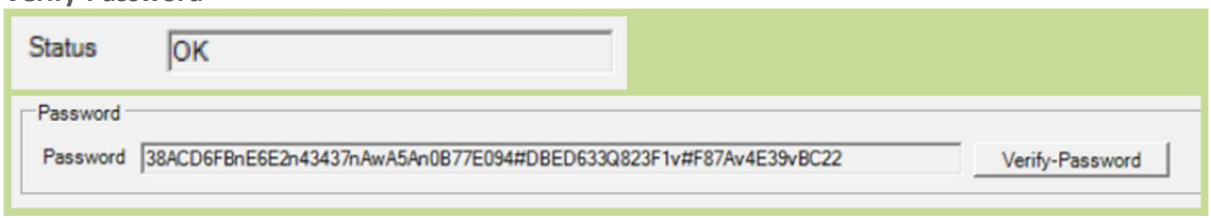
When the Details button is pushed, the details of the current row in the tab page will be shown.

Update-Password



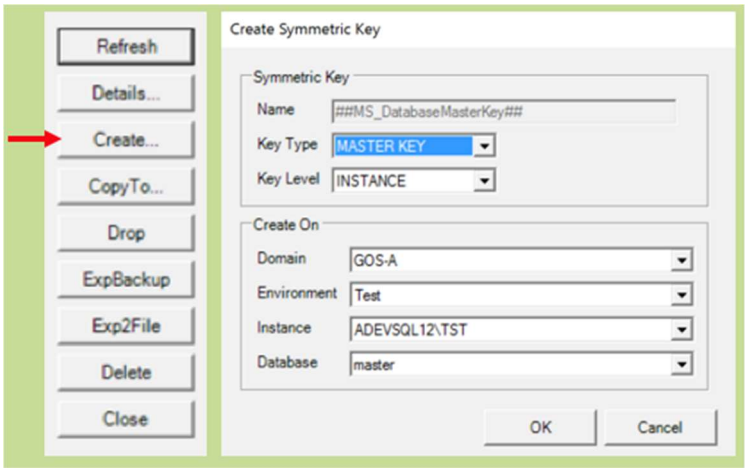
If the status of the Symmetric Key is 'Password Missing' you can add the password if you have it and hit the 'Update-Password' button. QGrip will save the password its database and push a 'Verify-Password' job on the Queue. If the password you entered is incorrect, the status will go back to 'Password Missing'. If it is correct, a backup and import of the Symmetric Key will be done and the status changed to 'OK'.

Verify-Password



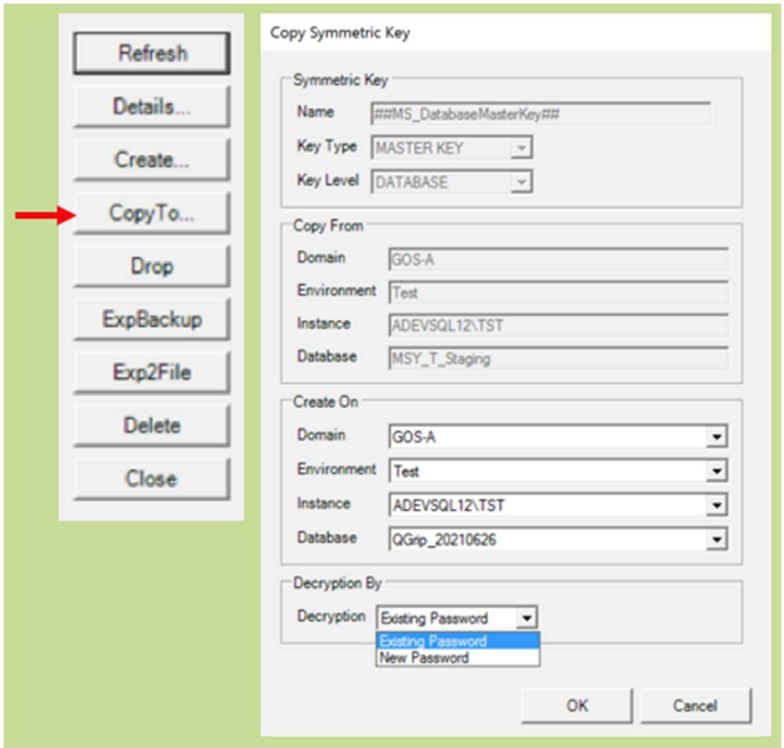
If the status of the Symmetric Key is 'OK' you can hit the 'Verify-Password' button to check that the password is still correct. If the password is incorrect, the Symmetric Key will get the status 'Password Missing'. The backup/import of the key have now also been removed as they are no longer valid and the backup/import useless.

9.1.3 Symmetric Key: Create



With the Create button, you can create a new Symmetric Key (of type MASTER KEY). Depending on the Key Level (INSTANCE/DATABASE) it can be created on a user database or in the master. A password of length 64 will be generated for the key and saved in the QGrip database.

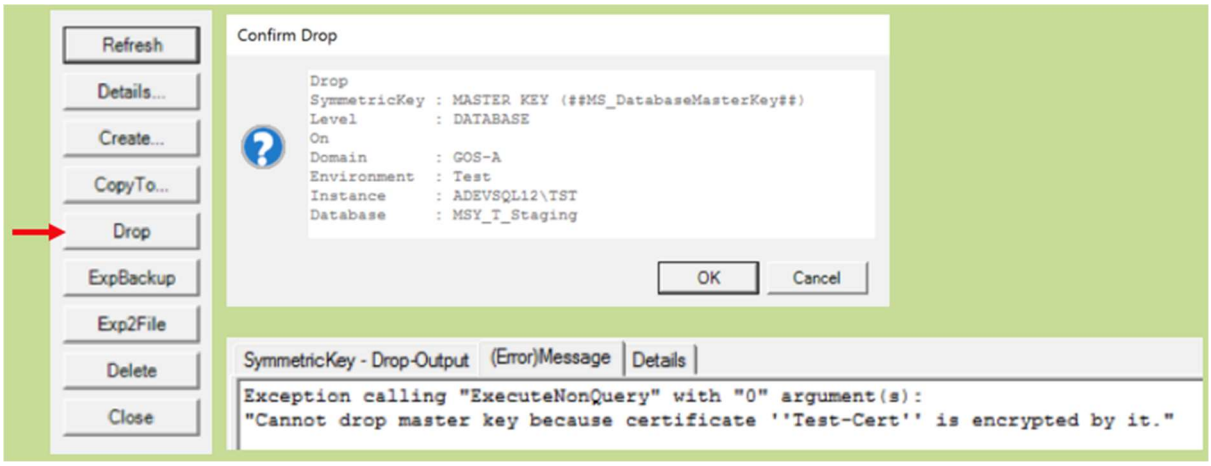
9.1.4 Symmetric Key: CopyTo



With the CopyTo button, you can copy an existing Symmetric Key to another database. You will only be able to copy Key Level to the same Key Level (master -> master or user database -> user database). You have the option to choose Decryption by Existing or New Password. If New Password is chosen, a password of length 64 will be generated.

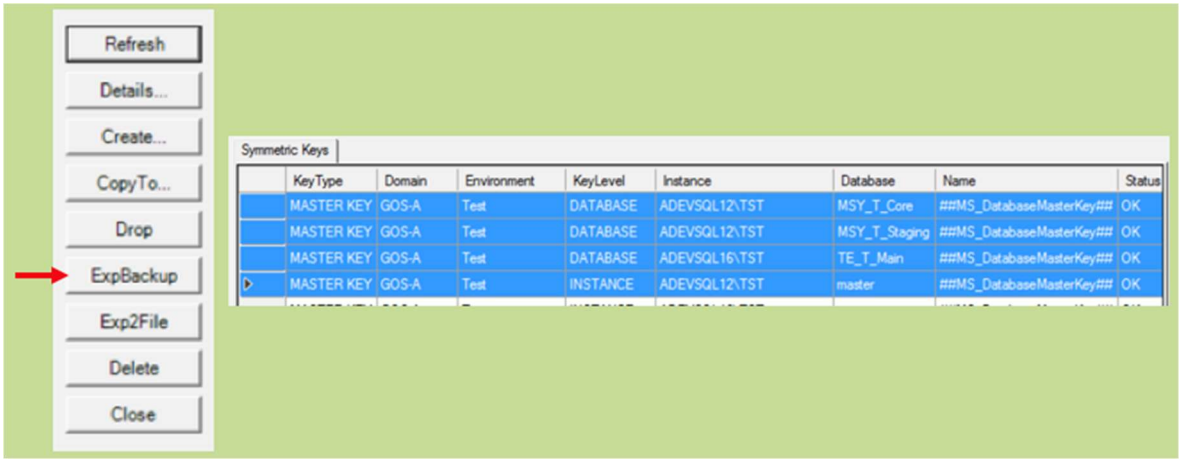
9.1.5 Symmetric Key: Drop

The difference between Drop and Delete is that Drop will drop the Symmetric Key on the Instance. The Symmetric Key info, including Backup/Import will still remain in the QGrip database.

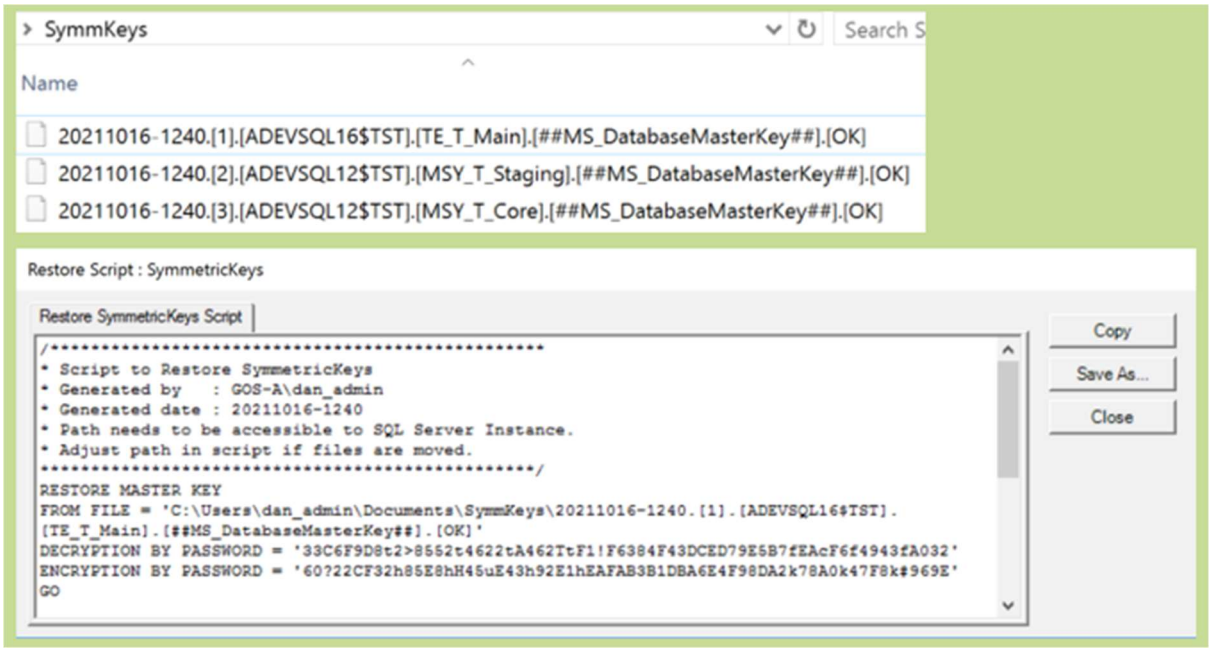


Drop the Symmetric Key related to the current row in the tab-page on the remote Instance. The information in QGrip will remain but the Symmetric Key will get the status: OK-Dropped
It is possible that the drop fails if the Symmetric Key has been used for encryption of other objects. In that case, the status will not change and no alterations will be made to the Symmetric Key.

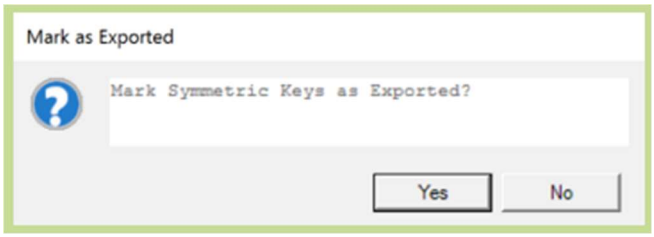
9.1.6 Symmetric Key: ExpBackup



To export Backups Imported to QGrip, select the Symmetric Keys in the tab-page and hit the ExpBackup button. The status of the Symmetric Keys must be ‘OK’ or OK-Dropped’. You will be asked to select to save a file. We advise you to create a new directory because as all the files will be saved there.

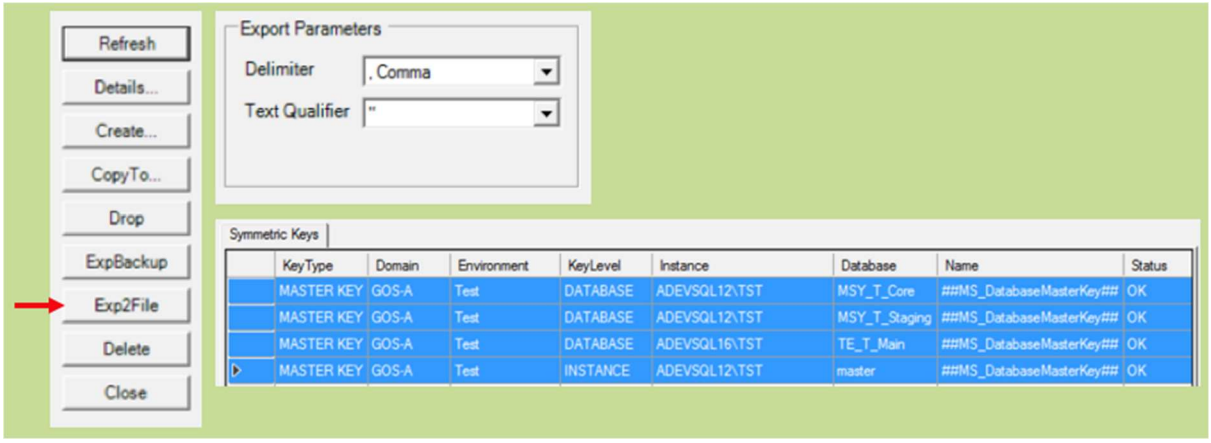


The files to (re-)create the Symmetric Keys have been placed in the directory. A popup with a script to create the objects will be shown. This popup will contain passwords and you should pay attention to where you save it.



You will receive a question if you want to mark the Symmetric Keys as exported or not. This is important for the delete that will be explained in one of the following sections. Only records with status 'OK-Dropped' and 'Marked as Exported' can be deleted from the QGrip administration.

9.1.7 Symmetric Key: Exp2File

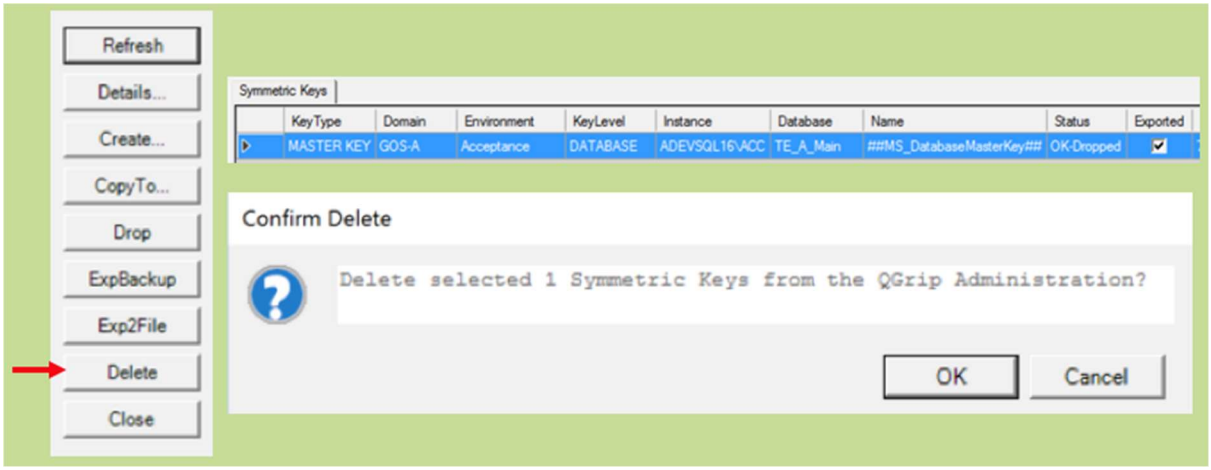


The difference between 'ExpBackup' and 'Exp2File' is that 'Exp2File' saves the selected rows in the tab-page to a csv-file, including the Symmetric Key passwords. The 'Export Parameters' will be used

to configure the file. The file will contain passwords and you should pay attention to where you save it.

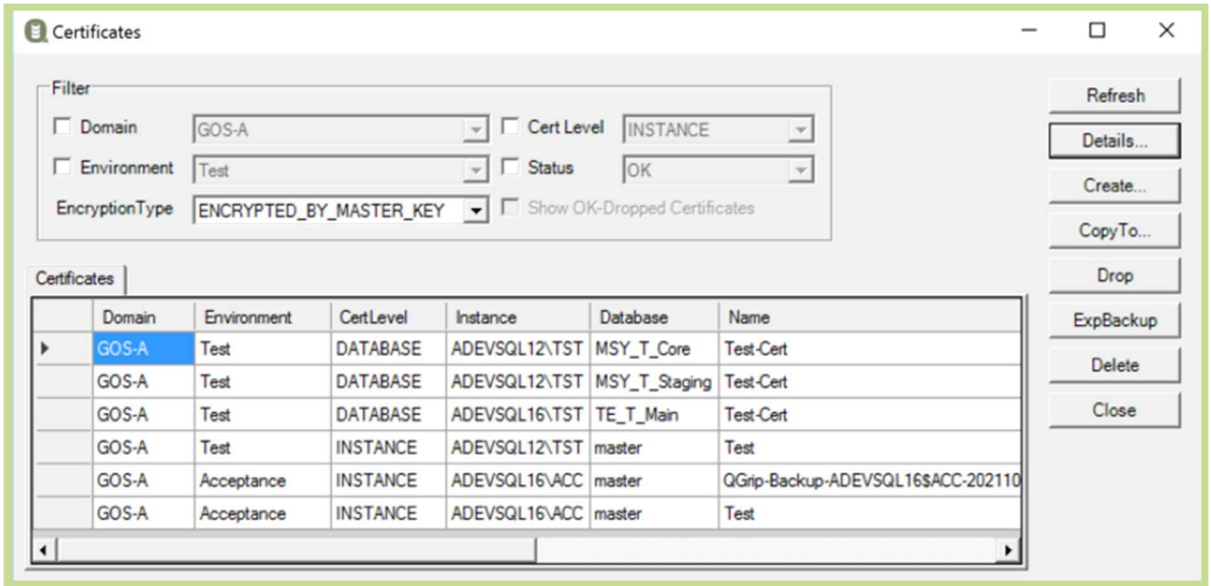
9.1.8 Symmetric Key: Delete

The difference between Delete and Drop is that Delete will delete the Symmetric Key from the QGrip administration. Delete is only possible if the Symmetric Key has status 'OK-Dropped' and has been marked as 'Exported'.

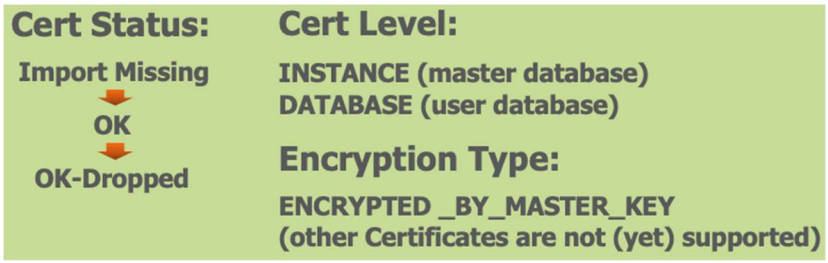


Select the Symmetric Keys you want to delete from the QGrip administration and hit Delete. QGrip will check that the records have the right status and that they have been marked as 'Exported'.

9.2 Certificates



The Certificates main window is compact with a lot of different buttons that will be explained here below.

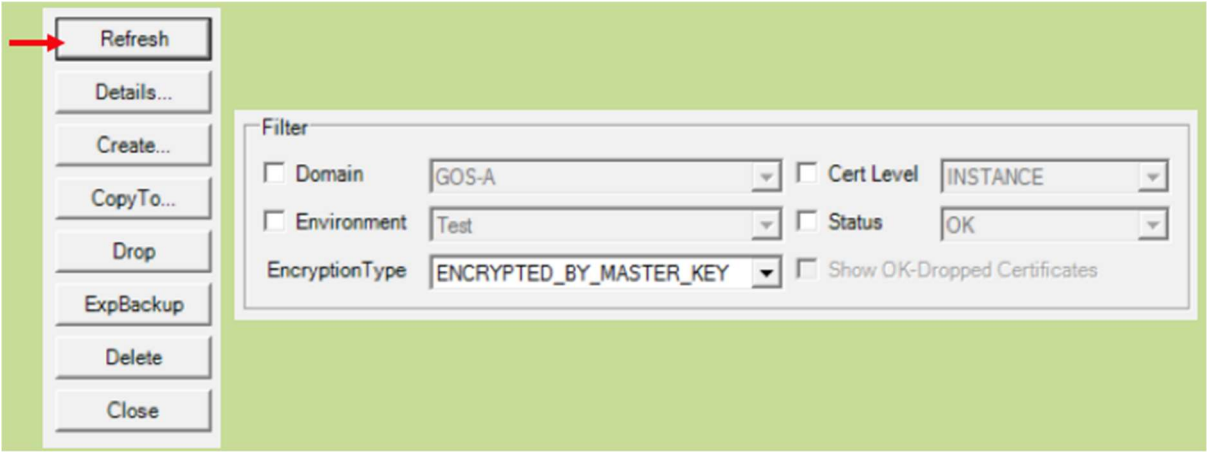


The status of a Certificate depends on the availability of information and if QGrip is able to backup and import the Certificate to QGrip. QGrip will only allow 'Actions' on Certificates that have encryption type 'ENCRYPTED_BY_MASTER_KEY'. If another Encryption type is selected in the filter, the action buttons will be disabled.

Status	Remark
Import Missing	Certificate is available but Backup/Import fails because of missing Authorisation on the Backup Share server (QGrip System Account member of Administrators group). If the Cert Level is DATABASE and the Password of the Symmetric Key (MASTER KEY) is not in QGrip, the status will also be Import Missing.
OK	Password is available and import to QGrip completed.
OK-Dropped	Import to QGrip completed but the Certificate has been dropped on the Instance.

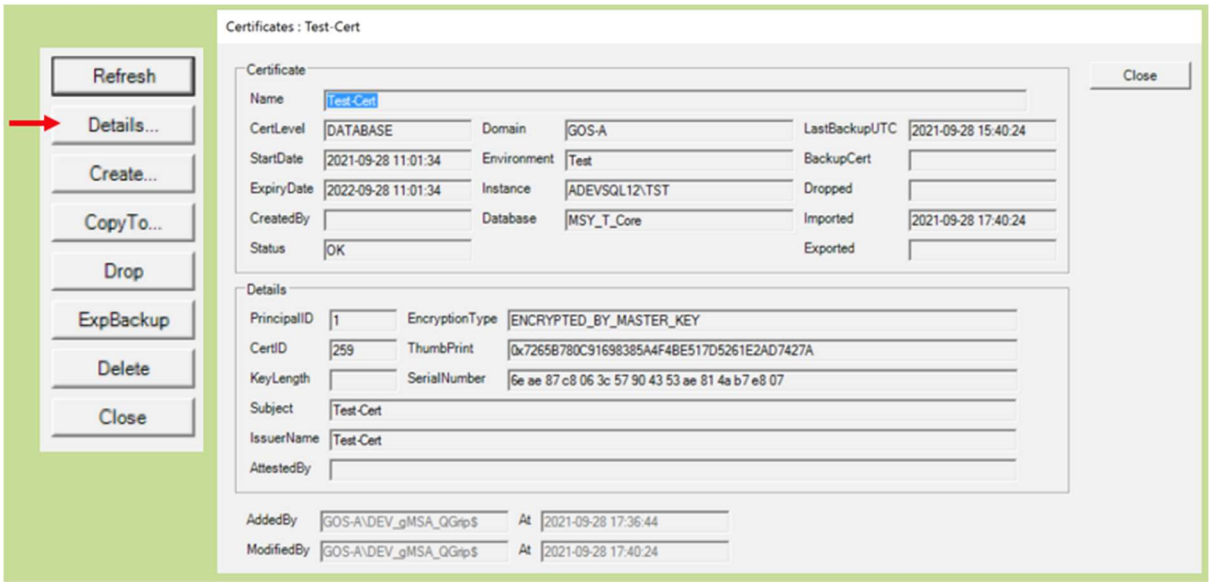
Symmetric Key Automatically created
Whenever needed, if a certificate is created or copied to a new Instance/Database, QGrip will automatically create the needed Symmetric Key (MASTER KEY) to complete the request.

9.2.1 Certificate: Refresh



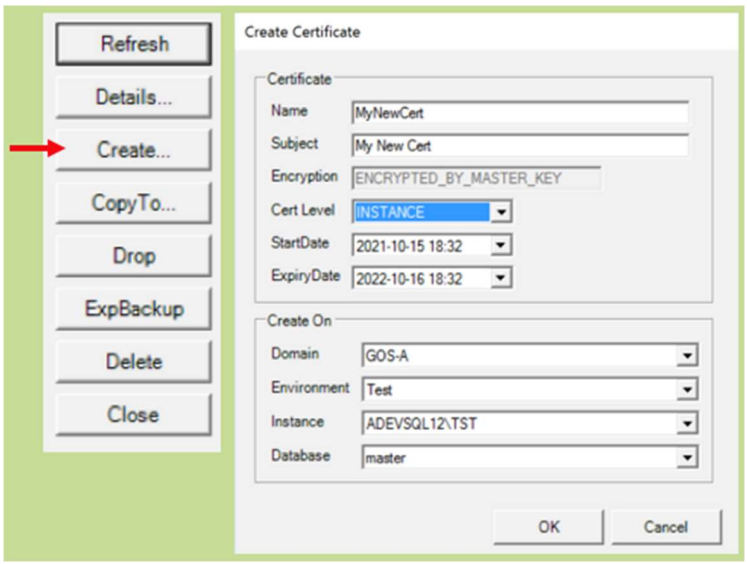
When the Refresh button is pushed, the data in the tab page will be refreshed according to the setting in the Filter.

9.2.2 Certificate: Details



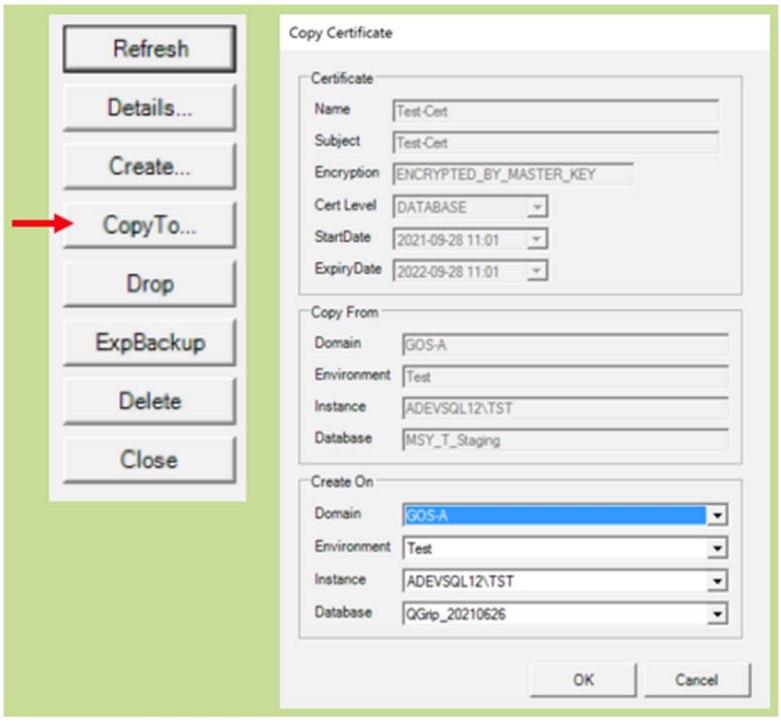
When the Details button is pushed, the details of the current row in the tab page will be shown.

9.2.3 Certificate: Create



With the Create button, you can create a new Certificate. Depending on the Key Level (INSTANCE/DATABASE) it can be created on a user database or in the master. You will need to enter a name and subject. The Start Date is automatically set to yesterday. This is to prevent warnings as certificates are using UTC time.

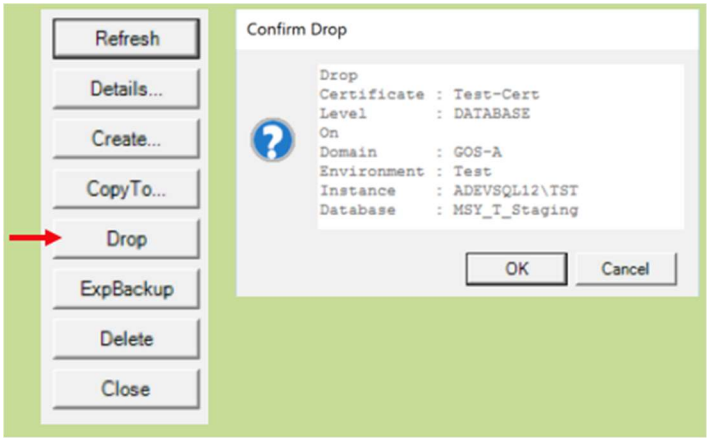
9.2.4 Certificate: CopyTo



With the CopyTo button, you can copy an existing Certificate to another database. You will only be able to copy Cert Level to the same Cert Level (master -> master or user database -> user database).

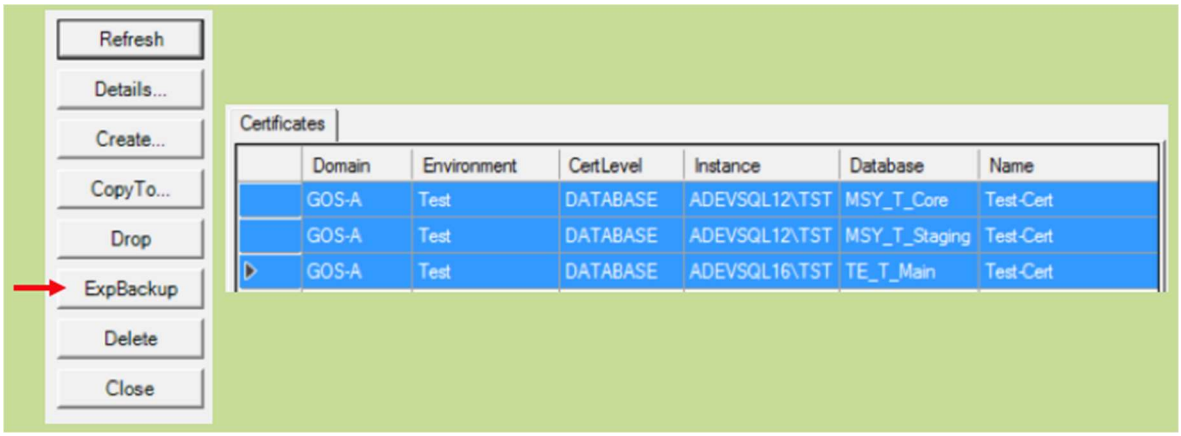
9.2.5 Certificate: Drop

The difference between Drop and Delete is that Drop will drop the Certificate on the remote Instance. The Certificate info, including Backup/Import will still remain in the QGrip database.



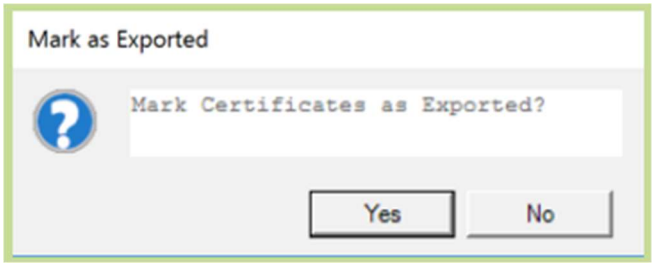
Drop the Certificate related to the current row in the tab-page on the remote Instance. The information in QGrip will remain but the Certificate will get the status: OK-Dropped
It is possible that the drop fails if the Certificate has been used for encryption of other objects. In that case, the status will not change and no alterations will be made to the Certificate.

9.2.6 Certificate: ExpBackup



To export Backups Imported to QGrip, select the Certificates in the tab-page and hit the ExpBackup button. The status of the Certificates must be 'OK' or OK-Dropped'. You will be asked to select to save a file. We advise you to create a new directory because as all the files will be saved there.

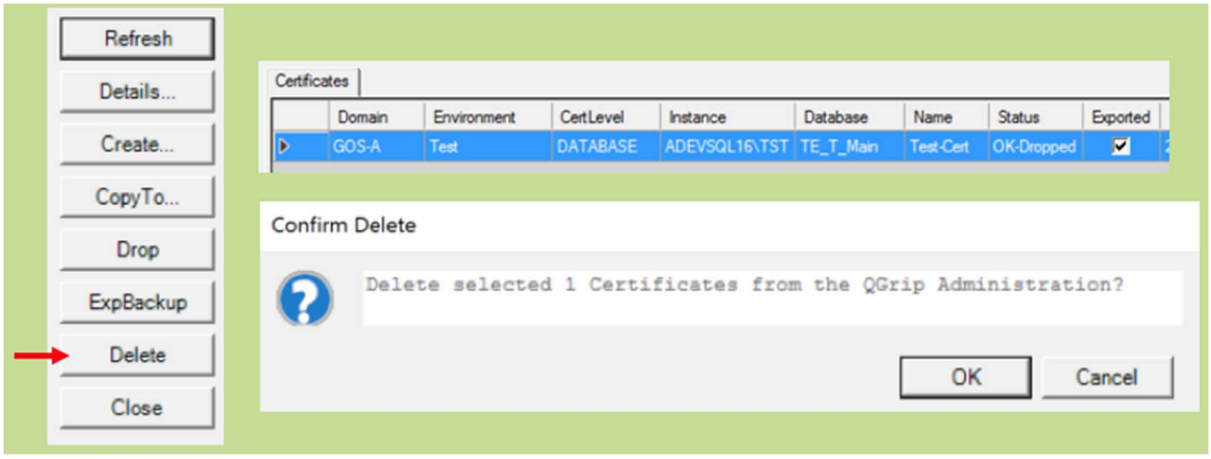
The files to (re-)create the Certificates have been placed in the directory. A popup with a script to create the objects will be shown. This popup will contain passwords and you should pay attention to where you save it.



You will receive a question if you want to mark the Certificates as exported or not. This is important for the delete that will be explained in the following sections. Only records with status 'OK-Dropped' and 'Marked as Exported' can be deleted from the QGrip administration.

9.2.7 Certificate: Delete

The difference between Delete and Drop is that Delete will delete the Certificate from the QGrip administration. Delete is only possible if the Certificate has status 'OK-Dropped' and has been marked as 'Exported'.



Select the Certificates you want to delete from the QGrip administration and hit Delete. QGrip will check that the records have the right status and that they have been marked as 'Exported'.

9.3 Always On: Symmetric Keys & Certificates

You might have noticed that there is no distinction made with DB Host type Instance/Listener in the Symmetric Keys and Certificates windows above and that is on purpose. Whenever you manipulate (Create, CopyTo, Drop or Backup) a Symmetric Key or Certificate of a database being part of an availability group on an Always On cluster, the action will automatically be performed for the databases in all replicas.

Passwords used for Symmetric Keys as well as File Passwords and Import files will be identical.

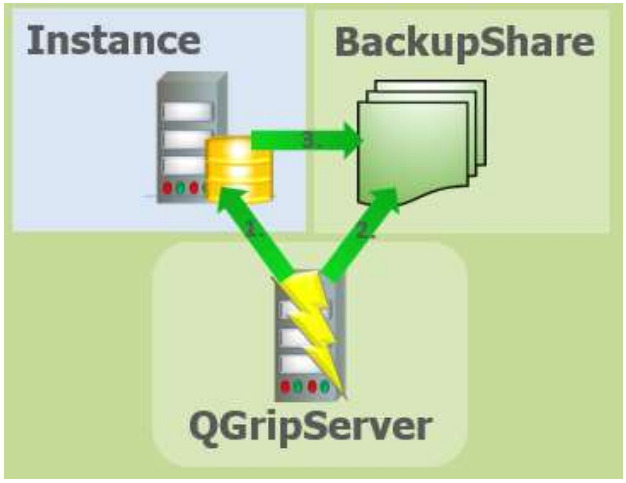
10 Accessibility

Recommended documentation

Doc-Tab	Title
Infra	Accessibility

In order for QGrip to work properly the Accessibility triangle needs to be in order at all times.

1. Every QGripServer -> Every Instances
2. Every QGripServer -> Every BackupShares
3. Every Instances -> Every BackupShares



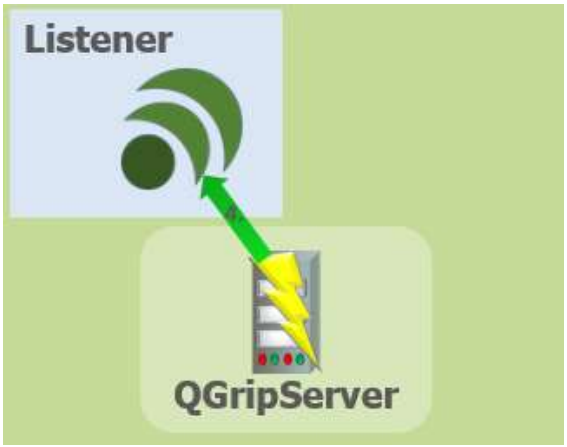
The check (1 and 2) will be triggered and start running immediately after one of these actions:

- New QGripServer
- New BackupShare
- BackupShare path changed
- New Instance
- Instance Name or Port Number changed

Check 3 will only start when check 1 and 2 have been successful for Instance/BackupShare combination.
All QGrip processes on all QGripServers run under one account (QGrip System Account). That account must have full rights on all BackupShares and be SYSADMIN (directly) on all Instances. The DBEngine account of all Instances must also have full rights on all BackupShares to be able to backup and restore/clone databases.

Additional Accessibility check for Always On Cluster.

4. Every QGripServer -> Every Listener



The check 4 will be triggered and start running immediately after one of these actions:

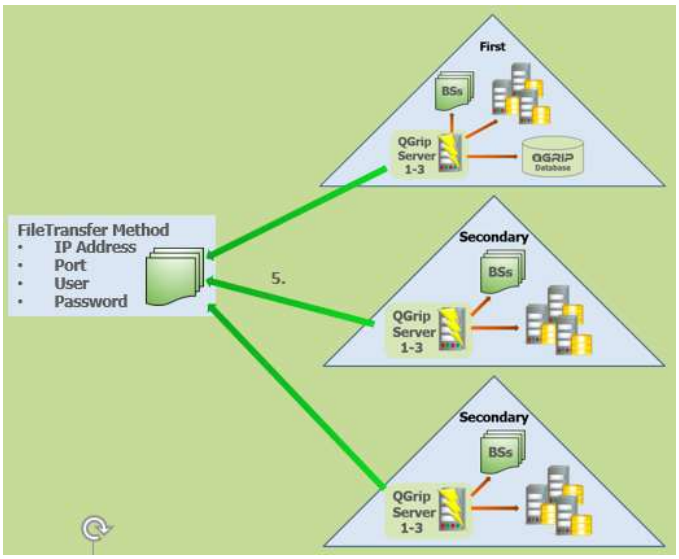
- New QGripServer
- New Listener
- Listener IP Address or Port Number changed

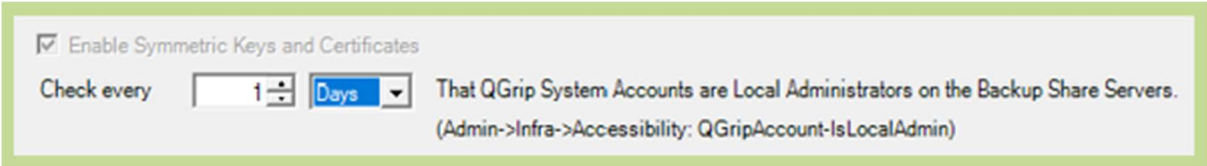
Additional Accessibility check for FileTransfer Method

5. Every QGripServer -> FileTransfer Method

The check 5 will be triggered and start running immediately after one of these actions:

- New QGripServer
- New FileTransfer Method
- Parameters FileTransfer Method Changed

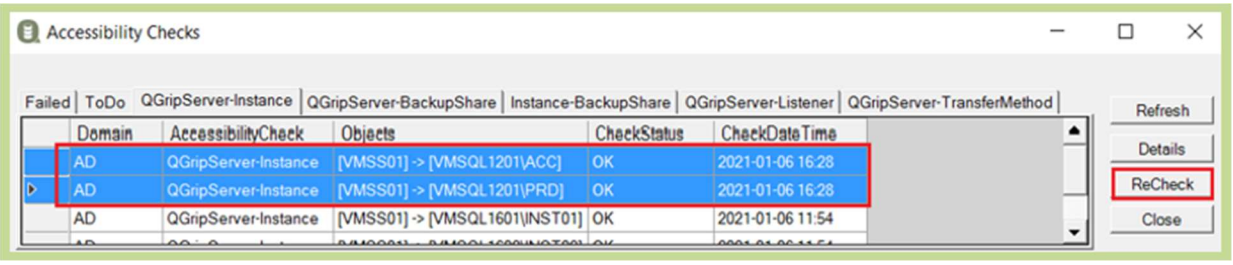




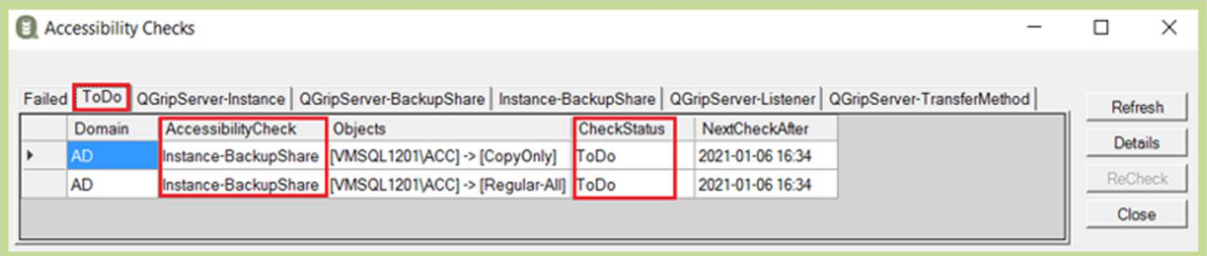
Additional Accessibility check for QGripAccount-IsLocalAdmin on Backup Share server. This check, number 6, is the only check that is repeatable.

Tab	Check	Description
Failed	1,2,3,4,5,6	Open the details to see hints on what might cause failure.
ToDo	1,2,3,4,5,6	Waiting to start, remember that 3 will only start if 1-2 are ok.
QGripServer-Instance	1	Successful checks.
QGripServer-BackupShare	2	Successful checks.
Instance-BackupShare	3	Successful checks.
QGripServer-Listener	4	Successful checks, only for Always On.
QGripServer-TransferMethod	5	Successful checks, only in Multiple AD-Domain Configuration.
QGripAccount-IsLocalAdmin	6	Successful checks, only if Symmetric Keys and Certificates have been enabled.

The Accessibility window has 8 tabs.



ReCheck by selecting rows and press ReCheck button. Works for all Tabs except for ToDo.



If checks are not being picked up from the ToDo tab-page, it will probably be check type 3 and check type 1 and/or 2 have failed for the combination.