QGRIP

Add Instance to QGrip

GRIP ON SQL

2024-04-16

Contents

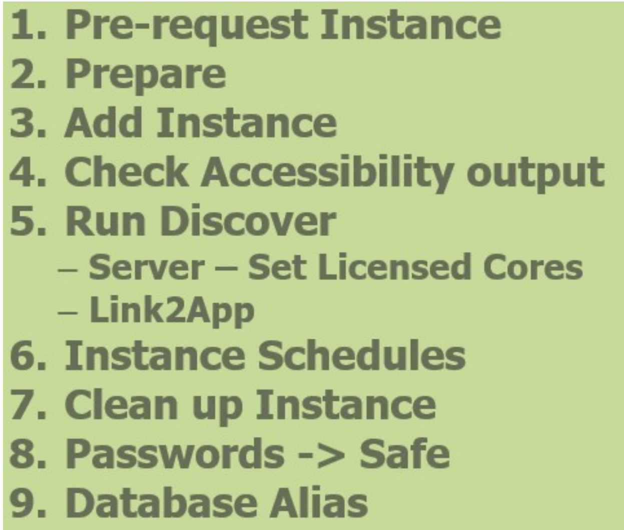
1 Introduction

This document contains a checklist of the steps that are needed when adding an Instance to QGrip. It might look like a lot but should not take longer than a few minutes unless there are Firewall issues that need to be solved.

Errors
Adding an Instance will activate the Accessibility checks. If these checks fail, Errors will be issued. These errors need to be solved.

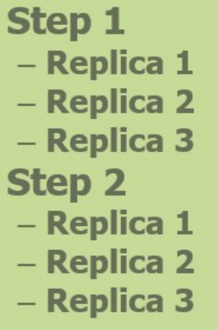
Warnings
QGrip will issue warning if something is not activated, Inconsistent or Incomplete. You are advised to solve *all* these warnings!

2 Checklist



1. Pre-request Instance
2. Prepare
3. Add Instance
4. Check Accessibility output
5. Run Discover
   - Server – Set Licensed Cores
   - Link2App
6. Instance Schedules
7. Clean up Instance
8. Passwords -> Safe
9. Database Alias

Instance part of Always On?



Step 1
- Replica 1
- Replica 2
- Replica 3

Step 2
- Replica 1
- Replica 2
- Replica 3

If the instance you are about to add is part of an SQL Server Always On cluster, you should do each step for all Instances/Replicas on the cluster before continuing with the next step.

2.1 Pre-request Instance

Requirement	Remark
SQL Server 2012 or Higher	

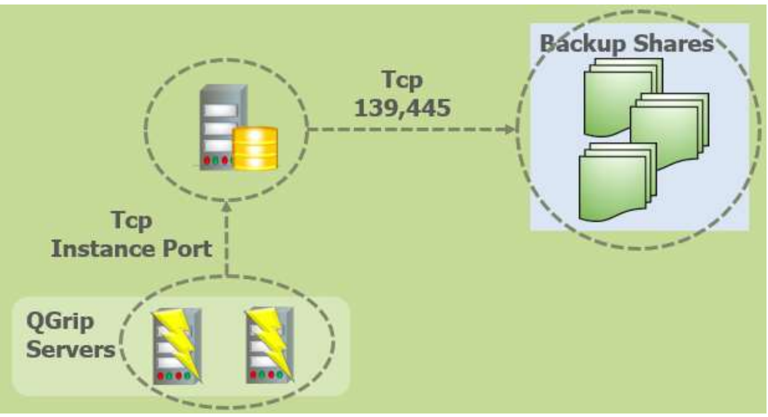
DB Engine service must run as an AD-account	Needed for access to all BackupShares within its own AD-Domain.
TCP-IP enabled	The TCP IP protocol needs to be enabled.
IP-All TCP Port	Fixed port needs to be set, not dynamic port.
One DTAP environment	QGrip considers all Databases on an Instance to belong to the same DTAP environment.

Additional requirements for Instances in a SQL Server Always On configuration:

Requirement	Remark
Databases Readable on all Replicas	Thus, also on Secondary Replicas

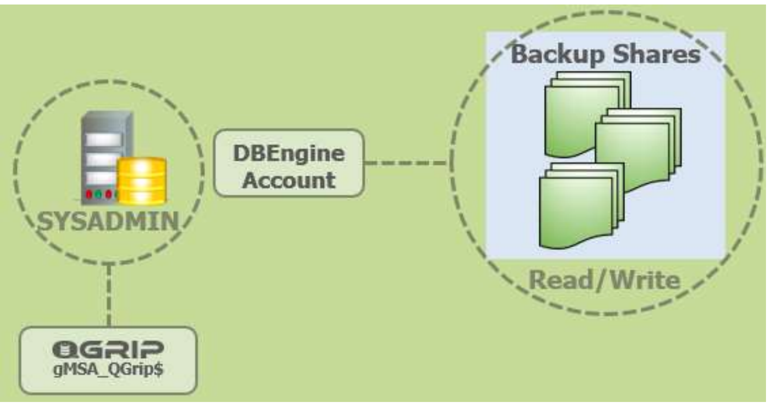
2.2 Prepare

Firewalls



Firewall between the QGrip Servers and the Instance need to be open on the Instance Port.
Firewall between the Instance and all Backup Shares within the domain need to be open on port 139 and 445.

Access & Authorisation

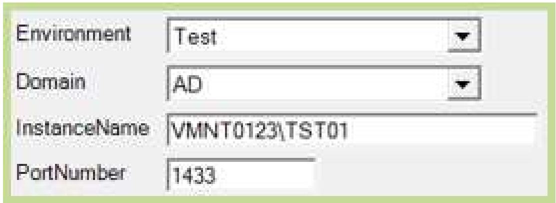


The DB Engine account of the Instance must have read/write authorisation on the backup shares and Full rights on the underlaying disks.

The QGrip System account (gMSA_QGrip$) needs to be added as SYSADMIN on the Instance. You will receive a popup in the QGrip-UI when the Instance is added so it can wait.

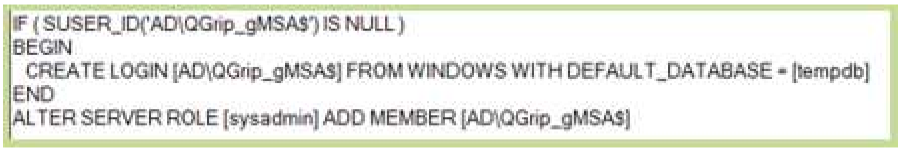
2.3 Add Instance

In the QGrip-UI, Admin->Infra->Instance-Server-Cluster, click on New to add a new Instance:



Environment	Test
Domain	AD
InstanceName	VMNT0123\TST01
PortNumber	1433

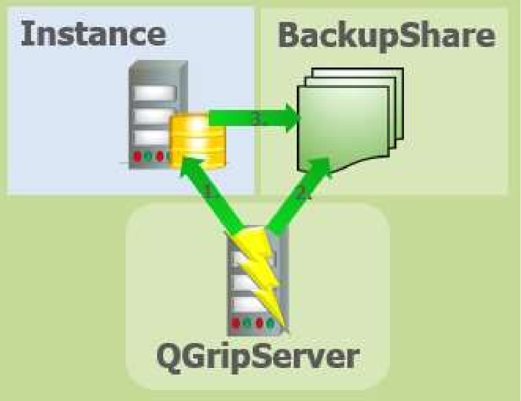
Remember that the Instance Name should be the same as @@SERVERNAME on the Instance.



```
IF ( SUSER_ID('AD\QGrip_gMSA$') IS NULL )
BEGIN
  CREATE LOGIN [AD\QGrip_gMSA$] FROM WINDOWS WITH DEFAULT_DATABASE = [tempdb]
END
ALTER SERVER ROLE [sysadmin] ADD MEMBER [AD\QGrip_gMSA$]
```

When you save the Instance, you will receive a popup concerning creating the QGrip System Account. If not done in advance, copy the statement and execute it on the Instance before continuing.

2.4 Check Accessibility output



When saving the new instance, the accessibility check will start running for the object. You will receive a personal message for each check. Make sure that none of the Checks failed.

Do not proceed before solving all Accessibility issues. If you have changed parameters, you can rerun the Accessibility check from the Failed tab.

2.5 Run Discover

In the QGrip-UI, request a Discover job of the new instance.

New Server?
If the Instance is on a Server that is new to QGrip, you should check and change the Licensed cores.

Link2App
Link new Instance objects to Applications.
If there are unknown objects, consider cleaning up the instance.

2.6 Instance Schedules

Activate job schedules for the Instance. The Discover job should always be scheduled 1-2 daily.

Activate

- **Discover**
- **System Usage**

Before activating Backup & Maintenance Job Schedules, be sure to disable them where they are currently starting.

Activate

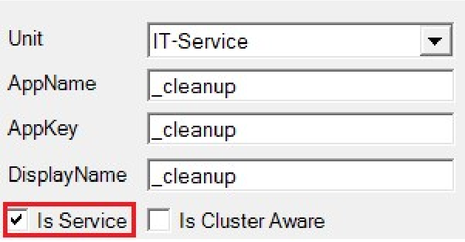
- **DBBackup**
- **LogBackup**
- **(CheckDB)**
- **(Optimise)**

2.7 Clean up Instance

If the Discover process has found objects that you know for sure are not used, consider dropping them and clean up the Instance.
If you are not sure, use the tip here below and wait a few weeks. The LoginLastActive and SystemUsage might help the investigation if the objects are used.

2.7.1 TIP: _Cleanup Application

When you first start using QGrip, you will probably be confronted with objects of which the owner and status is unknown. A possible temporary solution is creating a fake Application and link the unclear objects to that Application and sort them out later. Make sure to define the Application as ‘Is Service’ to avoid confusion as the objects will probably be spread out over several Instances.



Unit	IT-Service
AppName	_cleanup
AppKey	_cleanup
DisplayName	_cleanup
☑ Is Service	☐ Is Cluster Aware

2.8 Passwords -> Safe

If the Instance you just added, supports SQL Server authentication, you should add the passwords of all SQL Logins to the QGrip password safe. If it is just a few, do it one-by-one otherwise, use the Import module.

Tip Import

1. Export
2. Complete with passwords
3. Import

2.9 Database Alias

Add and Link Database aliases for the Application/Databases that are not complete. There will be a warning for each application.