Required account information - <HOSTING COMPANY>

Details of the STMP server to configure Database mail set up

- Account to connect to SMTP server
- Recommend set up of email group that email alerts are set to. This method means that a group of people are informed of alerts

Account name and password of the AD account that will be set as the SQL Admin of the SQL server. In some other installations this is the administrator of the local machine. If this is the case want to ensure this has been documented and agreed.

AD Accounts details for the three SQL services (See other document attached for server info)

Server – (See other document attached for server info)

Pre-Installation set up checks – <HOSTING COMPANY>

BOIS settings to check

Intel hyper-threading has been enabled
Intel Turbo Boost is enabled
Check Power management setting in BIOS / UEFI is set to use OS or disabled
Node Interleaving has been disabled (NUMA) – this is recommended for best performance
If using virtualization, ensure virtualization support is enabled

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

OS Configuration – completed prior to installation of SQL server
Reason – ensure best performance

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Hard drive partitioning is the NTFS Allocation unit size hosting SQL database files (Including tempdb files) should be 64K
Reason - SQL server stores data in extents which are groups of eight 8kb pages these are physically contiguous to each other for a total of 64 KB

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Install and patch Windows Software

The infrastructure hosting company should address this.

Make sure there no pending reboots for Windows.

Reason – ensure the most up to date version of the OS has been installed

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Check the Power Management settings

Windows power plan should be set to High Performance

Confirm that this setting is not overridden by hypervisor settings

Reason – ensure best performance from SQL server

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Grant Windows Rights to SQL Server Account (See Local Group Policy Editor)

Reason – The SQL server account that is used to manage the database should be allocated to an AD group. This group should be granted sysadmin permissions on the database. So the AD accounts for individuals can be added to the specific group. They then have admin permissions to the database(s)

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Is Instant file initialization – turned on?

Set up - https://www.brentozar.com/blitz/instant-file-initialization/

Also, IFI will not happen if *Transparent Data Encryption (TDE) is in use*.

Reason – This will improve the speed of backups creating/restoring a database or growing data/log files.

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Grant – Perform volume maintenance tasks to the SQL Server Service Account

This will be requested as part of the SQL server installation, best to ensure this is reviewed and granted at this stage.

Reason – This will improve the speed of backups creating/restoring a database or growing data/log files.

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Grant – Lock pages in memory

How - https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-the-lock-pages-in-memory-option-windows?view=sql-server-2017

Reference - https://www.red-gate.com/simple-talk/sql/database-administration/great-sql-server-debates-lock-pages-in-memory/

Reason – Improve performance of SQL server

Action	Confirmed by	Date

<HOSTING COMPANY>	Support Person	25/11

Enable Remote Desktop – via OS

Reason – enable remote access to the server

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Anti-virus software settings

Configure antivirus software to skip. certain types of files

- SQL Server data files (.mdf, .ndf, .ldf files)
- SQL Server backup files (.bak, .trn files)
- Full-Text catalog files
- Trace files (.trc files)
- SQL audit files (.sqlaudit files)
- SQL query files (.sql files)

The following file directory
- %ProgramFiles%\Microsoft SQL Server\MSSQL13.<Instance Name>\MSSQL\Binn\SQLServr.exe

Reference - https://support.microsoft.com/en-us/help/309422/choosing-antivirus-software-for-computers-that-run-sql-server

https://blogs.msdn.microsoft.com/docast/2018/02/01/operating-system-best-practice-configurations-for-sql-server/

Reason – do not want anti-virus software scanning files which are used by SQL server

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Confirm how the many cores and sockets are available for the VM -
https://www.mssqltips.com/sqlservertip/4801/sql-server-does-not-use-all-assigned-cpus-on-vm/

4 sockets will be allocated to each VM when initially installed

NB This will inform the number of TempDB files installed

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Confirm and review the drive and directory structure across all three environments see Disk and Directory Names

Reason – when moving solutions from one environment to another, consistent settings will make this process much quicker and simpler.

Action	Confirmed by	Date
<HOSTING COMPANY>	Support Person	25/11

Information required for installation of SQL server environment - Eyecademy

Features to be installed

Database engine
Enable Always on Availability Groups
SSMS – separate download recommends this is not installed on the server. It is recommended that if administrating the SQL Server instance, then administrating the instance is done from a remote PC.

Action	Confirmed by	Date
Eyecademy		

Authentication mode

Set SA Password – question for the client should disable the SA account. Best practice suggests that only Windows Authentication is used to connect to SQL server. As using SQL authentication to connect is not as secure.

Action	Confirmed by	Date
Eyecademy	Robert French	25/11/2019

AD accounts

Account for each SQL Server Service, these should be regular Domain User Accounts. Or alternatively Group Managed Service Accounts (gMSA) could be used. Note there can be issues with gMSA - https://blog.waynesheffield.com/wayne/archive/2018/02/using-gmsa-sql-server/

For each service account listed below a separate account should be created for each environment. This is so that if one account is breached for any reason, then only one environment is comprised.

Database Engine (SQLServerService)

Server Name	See other doc for server info
User name	
Password	

SQL Server Service Account agent (SQLAgentService)

Server Name	See other doc for server info
User name	
Password	

Admin AD account

Server Name	See other doc for server info
User name	
Password	

Action	Confirmed by	Date
Eyecademy / <HOSTING COMPANY>	Support Person	25/11

Disk and Directory Names

Best practice recommends that have separate drives for each of the following types of file. These should be **consistent between environments** this means that when databases are moved between environments this can be done with minimal disruption.

Drive letter and directory (examples)	Purpose
C:\SQLServer	SQL Server Application Files
D:\Data	SQL Server data files
E:\Log	SQL Server log files
F:\TempDB	SQL Server tempdb files
G:\Backup	SQL Server backup files – this ideally should be a completely different location if possible offsite

Reference - https://www.varonis.com/blog/sql-server-best-practices-in-virtualized-environments/
Reason -

Action	Confirmed by	Date
Eyecademy /<HOSTING COMPANY>	Support Person	25/11
Eyecademy	Robert French	25/11 (added drive letters)

Post installation tasks

Set recovery model for system databases
Master – Simple recovery model – Confirmed
Model – Full recovery model - Confirmed
Tempdb - Simple recovery model – Confirmed
MSDB - Simple recovery model – Confirmed
Reason – they should be backed up, although most do not change significantly

```sql
SELECT @@SERVERNAME

SELECT
name,
recovery_model,
recovery_model_desc
FROM sys.databases
GO
```

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2016

SQL server agent should be set to automatic start up. This should have been set as part of the installation process for SQL server. Hence this task is a confirmation that the agent is set as expected.

Reason- this is used to schedule a wide variety of tasks automatically, so should restart automatically when SQL server restarts

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Check firewall rules are in place for SQL Server

Reason – the SQL Server will not be accessible if network traffic is not allowed through the firewall.

Action	Confirmed by	Date
Eyecademy		

Backup checksum default from zero to one

Reference - https://www.sqlskills.com/blogs/glenn/sqlskills-sql101-how-you-can-make-your-database-backups-more-reliable/

https://www.sqlskills.com/blogs/erin/backup-checksum-default-option-in-sql-server-2014/

Reason – best practice ensures SQL server is checking the backup when it is creating it.

```
EXEC sp_configure 'BACKUP CHECKSUM DEFAULT', 1;
RECONFIGURE WITH OVERRIDE;

SELECT *
FROM [sys].[configurations]
WHERE name LIKE 'Backup%'
ORDER BY [name];
```


Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Backup compression

Reference - https://blog.sqlauthority.com/2017/09/30/sql-server-enable-backup-compression-default/

Reason – makes backups smaller and quicker
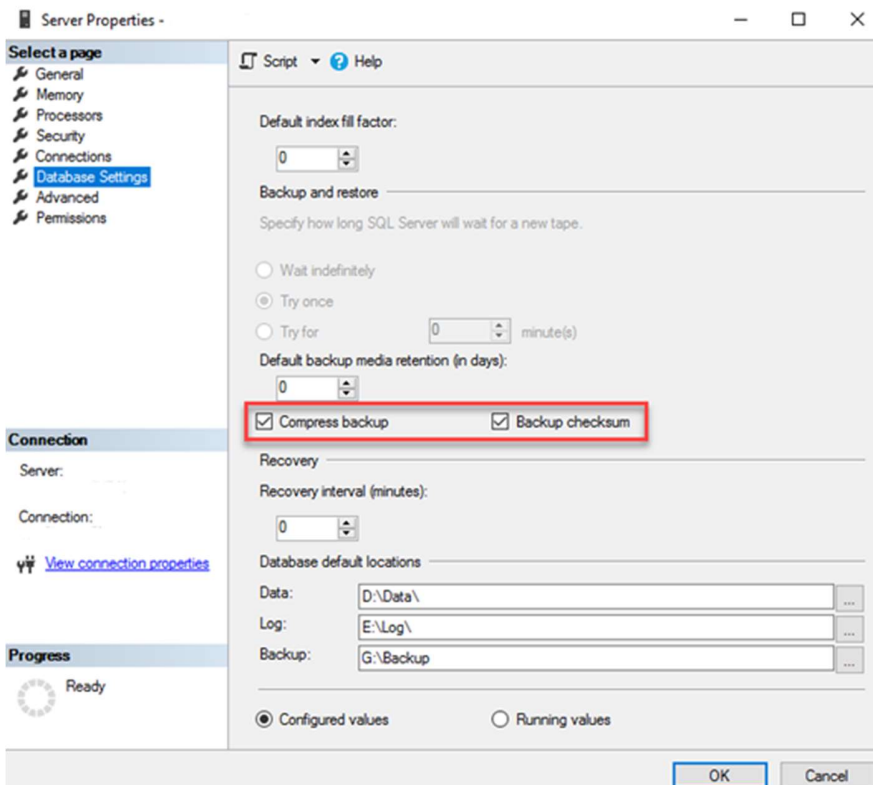
Action	Confirmed by	Date
Eyecademy		

Cost threshold for parallelism

Suggested value is currently 50

References - https://www.brentozar.com/archive/2017/03/why-cost-threshold-for-parallelism-shouldnt-be-set-to-5/

http://www.dbafire.com/2016/10/07/cost-threshold-parallelism-best-practice-recommendations/

Reason – optimal query performance.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Max degree of parallelism

Reference - https://support.microsoft.com/en-us/help/2806535/recommendations-and-guidelines-for-the-max-degree-of-parallelism-confi

https://www.mssqltips.com/sqlservertip/2650/what-maxdop-setting-should-be-used-for-sql-server/

Four cores with initial installation so set to **Four**

Reason – best query performance.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Set the Max server memory

Reference - https://www.brentozar.com/archive/2011/09/sysadmins-guide-microsoft-sql-server-memory/
https://www.sqlskills.com/blogs/jonathan/how-much-memory-does-my-sql-server-actually-need/

Reason – SQL server will take as much memory as it requires to run the workload and will manage the memory internally. This value should be (check) 80% of the overall memory available for the system the instance is installed on.

8GB - Total System memory (8192mb)
80% of 8GB = 6554mb

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Optimize for ad hoc workloads

Reference - https://www.red-gate.com/simple-talk/blogs/using-optimize-for-ad-hoc-workloads/

Reason – Query execution plans which are not reused are not kept, can improve performance
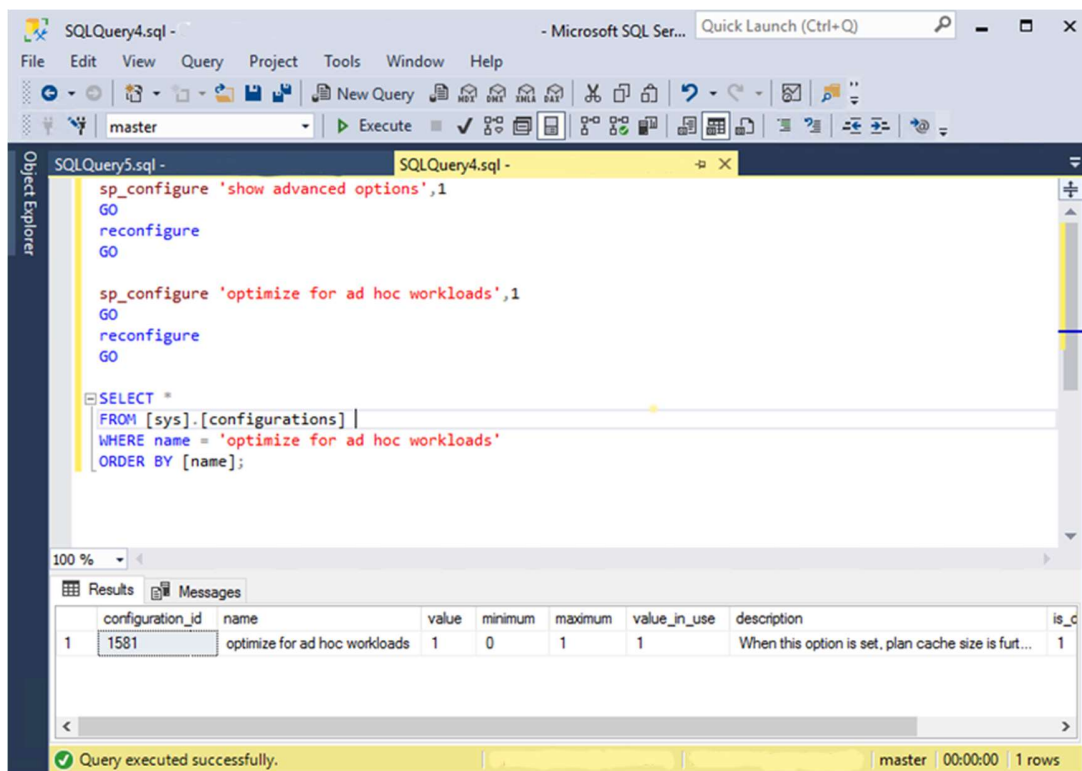
```
sp_configure 'show advanced options',1
GO
reconfigure
GO

sp_configure 'optimize for ad hoc workloads',1
GO
reconfigure
GO

SELECT *
FROM [sys].[configurations]
WHERE name = 'optimize for ad hoc workloads'
ORDER BY [name];
```

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Set Tempdb for configuration – these should be on the fastest disks available. This can share the same drive as the log files see Disk and Directory Names
Reference - https://johnmccormack.it/2016/12/configuring-tempdb-sql-server-2016-instances/
Recommendation is one tempdb per core, since four cores initially only **four tempdbs** will be set up
Reason – the temp db is accessed by SQL server a great deal, the faster the data access to these files the faster internal processes run. This can also be a performance bottle neck which is not easy to diagnose.

Action	Confirmed by	Date
Eyecademy		

Check and review the data base default file locations – this would to the drives that have been specified in the Disk and Directory Names section. See Disk and Directory Names
Reason – If the drive which holds the OS fails, that same drive should not hold the database files. So, if lose the OS files then still have the database.   Same with separate drive for backups which should be placed on a completely different server.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Set up database mail – this will require connection to SMTP server and distribution groups set up.
Reason – this will allow sending of automated messages should there be an issue with the SQL server. Using a distribution group means that a group of people are informed of the issue rather than a single person which could be a single point of failure.

AD Account	Password
See other doc	

Action	Confirmed by	Date
Eyecademy /<HOSTING COMPANY>	Support Person	25/11

Revoke access to Extended stored procedures for Public role.

xp_availablemedia, xp_dirtree, xp_enumgroups, xp_fixeddrives, xp_regaddmultistring, xp_regdeletekey, xp_regdeletevalue, xp_regenumvalues, xp_regremovemultistring, xp_regwrite, xp_regread, xp_servicecontrol, xp_subdirs.

Do not grant server permissions to the server public role for these extended stored procedure.

Review permissions granted to Public database role.

https://basitaalishan.com/2013/04/04/the-public-role-do-not-use-it-for-database-access/

Reason – minimize the surface area for attack.

```sql
WITH [PublicRoleDBPermissions]
AS (
    SELECT p.[state_desc] AS [PermissionType]
        ,p.[permission_name] AS [PermissionName]
        ,USER_NAME(p.[grantee_principal_id]) AS [DatabaseRole]
        ,CASE p.[class]
            WHEN 0
                THEN 'Database::' + DB_NAME()
            WHEN 1
                THEN OBJECT_NAME(major_id)
            WHEN 3
                THEN 'Schema::' + SCHEMA_NAME(p.[major_id])
            END AS [ObjectName]
    FROM [sys].[database_permissions] p
    WHERE p.[class] IN (0, 1, 3)
        AND p.[minor_id] = 0
    )
SELECT [PermissionType]
    ,[PermissionName]
    ,[DatabaseRole]
    ,SCHEMA_NAME(o.[schema_id]) AS [ObjectSchema]
    ,[ObjectName]
    ,o.[type_desc] AS [ObjectType]
    ,[PermissionType] + ' ' + [PermissionName] + ' ON ' + QUOTENAME(SCHEMA_NAME(o.[schema_id])) + '.' +
QUOTENAME([ObjectName]) + ' TO ' + QUOTENAME([DatabaseRole]) AS [GrantPermissionTSQL]
    ,'REVOKE' + ' ' + [PermissionName] + ' ON ' + QUOTENAME(SCHEMA_NAME(o.[schema_id])) + '.' +
QUOTENAME([ObjectName]) + ' TO ' + QUOTENAME([DatabaseRole]) AS [RevokePermissionTSQL]
FROM [PublicRoleDBPermissions] p
INNER JOIN [sys].[objects] o
    ON o.[name] = p.[ObjectName]
        AND OBJECTPROPERTY(o.object_id, 'IsMSShipped') = 0
WHERE [DatabaseRole] = 'Public'
ORDER BY [DatabaseRole]
    ,[ObjectName]
    ,[ObjectType]
```

Zero record returned

This will need to be run for each database created to confirm there is no access granted for Public Role.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Ensure DAC is enabled (this is not the same as RDP access)

Reference - https://www.sqlshack.com/sql-server-dedicated-admin-connection-dac-how-to-enable-connect-and-use/

Reason – allow dedicated admin access to the server using SQLCMD to diagnosis and resolve an unresponsive SQL server

```
sp_configure 'remote admin connections', 1;
reconfigure;

SELECT *
FROM [sys].[configurations]
WHERE name = 'remote admin connections'
```
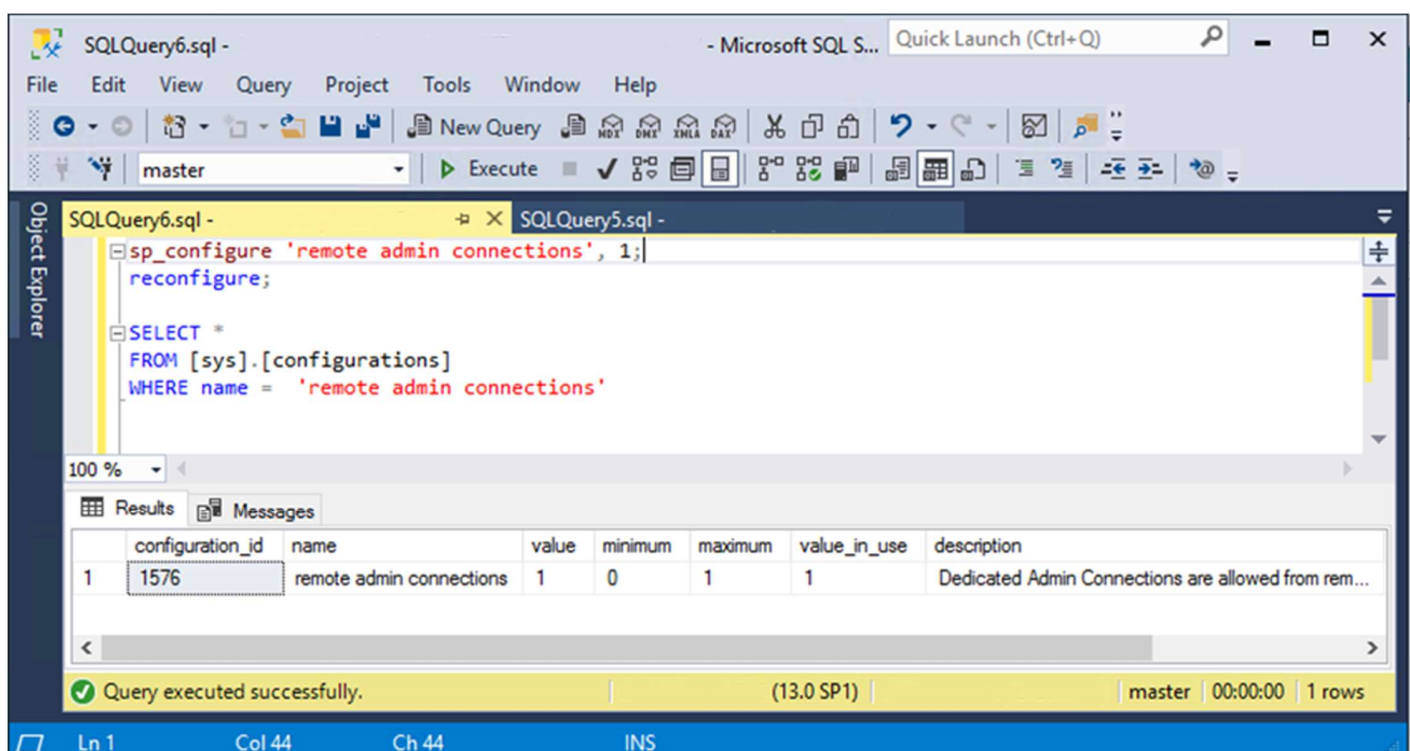

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Install First Responder Kit from Brent Ozar Unlimited (https://www.brentozar.com/archive/category/first-responder-kit/)

NB this is updated on a regular basis, so will require to be updated

Reason – these are open source and free tools which are used by many database professionals to diagnosis performance issues.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Install Ola Hallengren maintenance scripts (https://ola.hallengren.com)

Reason – these scripts are open source and free scripts and are used in many production SQL server environments. They can be used to configure, set up and run many maintenance tasks.

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Enable query store

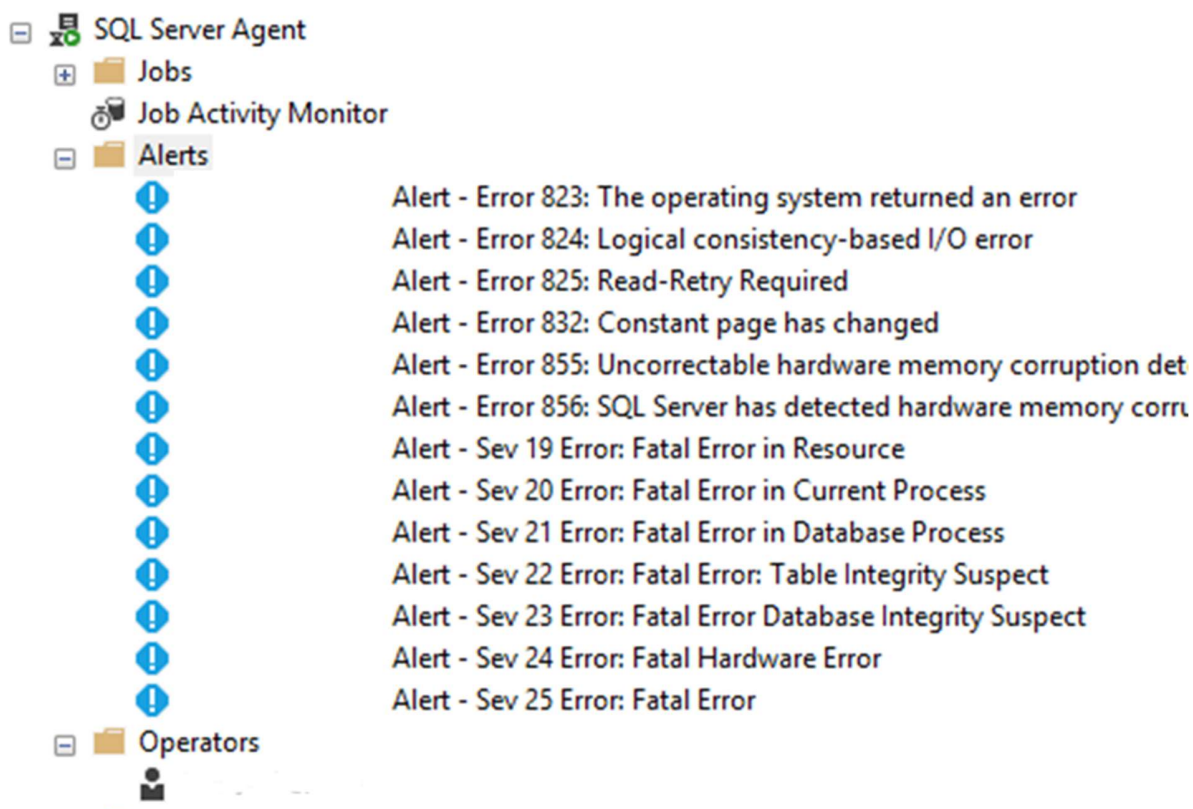**Reason** -this is a monitoring tool built into SQL server this can be used to diagnosis performance issues.

This requires to be enabled for each database there is no server instance setting

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019

Add SQL server agent alerts as recommend by Glenn Berry

Reference - https://www.sqlskills.com/blogs/glenn/creating-sql-server-agent-alerts-for-critical-errors/

Reason – these should alert the monitoring group of issues so that can look at what is causing the underlying issue.
https://www.red-gate.com/simple-talk/sql/database-administration/provisioning-a-new-sql-server-instance-part-three/

SQL Server Agent
  Jobs
  Job Activity Monitor
  Alerts
    Alert - Error 823: The operating system returned an error
    Alert - Error 824: Logical consistency-based I/O error
    Alert - Error 825: Read-Retry Required
    Alert - Error 832: Constant page has changed
    Alert - Error 855: Uncorrectable hardware memory corruption det
    Alert - Error 856: SQL Server has detected hardware memory corru
    Alert - Sev 19 Error: Fatal Error in Resource
    Alert - Sev 20 Error: Fatal Error in Current Process
    Alert - Sev 21 Error: Fatal Error in Database Process
    Alert - Sev 22 Error: Fatal Error: Table Integrity Suspect
    Alert - Sev 23 Error: Fatal Error Database Integrity Suspect
    Alert - Sev 24 Error: Fatal Hardware Error
    Alert - Sev 25 Error: Fatal Error
  Operators

Action	Confirmed by	Date
Eyecademy	Robert French	26/11/2019