|  |
| --- |
| Norfolk & Suffolk Constabulary  ICT Infrastructure Technical Design |
| SQL AlwaysOn Availability Group v0.d– DRAFT |
| 16 May 2016 |

# Document Data

## Change History

The following Change History log contains a record of changes made to this document:

|  |  |  |  |
| --- | --- | --- | --- |
| Published / Revised | Version # | Author | Section / Nature of Change |
| 16 May 2016 | v0.d | Paul Maxfield | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Document Distribution List

This document has been issued to the following people for sign off (SO), review (R) or information (I).

|  |  |  |
| --- | --- | --- |
| Name | Role/Representing | Action Required |
|  | Database Services Peer Reviewer | SO |
|  | CTO Design Manager | SO |
|  | ICT Servers & Data Management | R |
|  |  | R |
|  |  | R |
|  |  | R |
|  |  | R |
|  |  | R |
|  |  | I |
|  |  |  |
|  |  |  |

# Contents

[Document Data i](#_Toc452464920)

[1.1 Change History i](#_Toc452464921)

[1.2 Document Distribution List i](#_Toc452464922)

[2 Contents ii](#_Toc452464923)

[3 Introduction 4](#_Toc452464924)

[3.1 Purpose and Scope of Document 4](#_Toc452464925)

[3.2 Intended Audience 4](#_Toc452464926)

[3.3 Acceptance Criteria 4](#_Toc452464927)

[3.4 Related Documentation 4](#_Toc452464928)

[3.5 Terminology and Acronyms 4](#_Toc452464929)

[4 Infrastructure Design 5](#_Toc452464930)

[4.1 Infrastructure Overview 5](#_Toc452464931)

[4.2 Licence 6](#_Toc452464932)

[5 Server Configuration 6](#_Toc452464933)

[5.1 Virtual Machine Configuration 6](#_Toc452464934)

[5.1.1 Operating System Configuration 7](#_Toc452464935)

[5.1.2 Operating System and SQL Disk Configuration 7](#_Toc452464936)

[5.1.3 Operating System Required Updates 8](#_Toc452464937)

[5.2 Network Configuration 8](#_Toc452464938)

[5.2.1 Subnets 8](#_Toc452464939)

[5.2.2 TCP IP Configuration 8](#_Toc452464940)

[5.2.3 Adapter Configuration 9](#_Toc452464941)

[5.2.4 Routes 9](#_Toc452464942)

[5.2.5 Name Resolution 9](#_Toc452464943)

[5.3 Windows Server Failover Clustering 9](#_Toc452464944)

[5.3.1 Cluster Name 9](#_Toc452464945)

[5.4 SQL Server configuration 10](#_Toc452464946)

[5.4.1 SQL Install File Locations 10](#_Toc452464947)

[5.4.2 SQL Service Accounts 11](#_Toc452464948)

[5.4.3 Memory Settings 11](#_Toc452464949)

[5.4.4 Database Mail 11](#_Toc452464950)

[5.4.5 Temporary database configuration (tempdb) 12](#_Toc452464951)

[5.4.6 SQL Server Settings 12](#_Toc452464952)

[5.4.7 Database Directory Structure 12](#_Toc452464953)

[5.4.8 Database Maintenance Plans 13](#_Toc452464954)

[5.5 Availability Groups Configuration 13](#_Toc452464955)

[5.5.1 Availability Replicas Configuration 14](#_Toc452464956)

[5.5.2 Endpoints Configuration 15](#_Toc452464957)

[5.5.3 Availability Group Service Principal Name 15](#_Toc452464958)

[5.6 Server access 15](#_Toc452464959)

[5.7 Oracle client 15](#_Toc452464960)

[6 Backup 16](#_Toc452464961)

[6.1 Backup and Recovery Architecture 16](#_Toc452464962)

[6.1.1 Tivoli Storage Management client 16](#_Toc452464963)

[6.1.2 Recovery Mechanism 16](#_Toc452464964)

[7 Monitoring 17](#_Toc452464965)

[7.1 Monitoring Tools 17](#_Toc452464966)

[8 Security 18](#_Toc452464967)

[8.1 Firewall 18](#_Toc452464968)

[8.2 Anti-Virus Exclusions 18](#_Toc452464969)

[References 19](#_Toc452464970)

[Appendix A 20](#_Toc452464971)

# Introduction

## Purpose and Scope of Document

The purpose of this document is to specify detailed configuration guidance in the build of a Microsoft SQL Server AlwaysOn Availability Group. This includes the physical infrastructure design decisions, infrastructure components configuration, and implementation tasks.

## Intended Audience

The design document is intended for ICT personnel working on IT Operations, Licensing and Service Management, as well as relevant Constabulary stakeholders who need to view the detail behind the design.

## Acceptance Criteria

The following criteria should be used when reviewing and approving this proposal:

* Does the design comply with existing security standards?
* Does the design meet Service Continuity guidelines and comply with DR and Service Continuity standards?
* Does the design follow the architectural and design principles?
* Does the design meet operational technical governance?
* Does the design adequately document the licenses required to deliver the solution?

## Related Documentation

|  |  |  |
| --- | --- | --- |
| Document | Location | Version |
| Hyper-V 2012 R2 Detailed Design |  |  |
| Microsoft SQL Server Database Strategy |  | TBD |
| Technical Design SQL Server |  | TBD |
| SQL Server Operations Guide |  | TBD |
|  |  |  |

## Terminology and Acronyms

This table defines the client-specific terminology and acronyms used in this document

|  |  |
| --- | --- |
| Term / Acronym | Definition |
| SQL | Structured Query Language |
| AAG | AlwaysOn Availability Group |
| WSFC | Windows Server Failover Clustering |
| FCI | Failover Cluster Instance |
| DB | Database |
| DTS | Data Transformation Services |
| SSIS | SQL Server Integration Services |
| CLR | Common Language Runtime |
| OU | Organisational Unit |
| SAN | Storage Area Network |
| DNS | Domain Name System |
| DHCP | Dynamic Host Configuration Protocol |
| VM | Virtual Machine |
| TSM | Tivoli Storage Manager |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| DR | Disaster Recovery |

# Infrastructure Design

## Infrastructure Overview

The AlwaysOn Availability Group (AAG) feature is a mix of SQL Clustering and SQL Mirroring with the goal to minimize Recovery Point Objective (RPO) and Recovery Time Objective (RTO). This feature is presented by Microsoft as an alternative to SQL Mirroring which is deprecated since SQL Server 2012, providing a Disaster Recovery (DR) option for those systems on DB-OCC04 (Cluster 4) that require a failover replica.

In addition the AAG feature offers a number of service improvements over its predecessor with the following capabilities:

* More than one mirror, multiple DR sites
* Ability to read real-time from the mirrors
* Ability to execute backups from the mirror
* Include multiple user databases within one mirroring relationship
* Mixture of synchronous and asynchronous data replication between primary and multiple mirrors
* Extend scalability of the data replication
* Accelerate failover
* Multi-subnet failover and reconnects

Each node that participate within an AAG is an active instance of SQL and can host database locally, thus the AAG feature can be implemented only where the application requires and supports the feature.

The solution is to be hosted in the Hyper-V 2012 R2 environment, following the current virtualisation strategy, with 3 VMs within MER1 and MER2 at the OCC and a VM at the Dereham DR site. This offers sufficient capacity for the migration of existing systems off of Cluster 4 with some scope to grow.  
  


## Licence

The AlwaysOn Availability Group (AAG) feature is an Enterprise feature and as such will require the appropriate licence model, this is consistent with the current Cluster 4 build which offers other Enterprise feature to the hosted databases, such as data compression. The licencing requirements of this solution will be satisfied from the existing pool of Enterprise licences and the decommissioning of Cluster 4 post migration.

The following table summarises the HA and DR features supported by SQL Server 2014[[1]](#footnote-1)

**High Availability features for SQL Server 2014 Licenses:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature Name** | **Enterprise** | **Business Intelligence** | **Standard** |
| Server Core support | Yes | Yes | Yes |
| Log Shipping | Yes | Yes | Yes |
| Database mirroring | Yes | Yes (Safety Full Only) | Yes (Safety Full Only) |
| Backup compression | Yes | Yes | Yes |
| AlwaysOn Failover Cluster Instances | Yes (Node support: Operating system maximum) | Yes (Node support: 2) | Yes (Node support: 2) |
| **AlwaysOn Availability Groups** | **Yes (up to 8 secondary replicas,**  **including 2 synchronous secondary replicas)** |  |  |

For more information on Features/Licenses:

* SQL Server 2014 Features:

<http://msdn.microsoft.com/en-us/library/cc645993%28v=sql.120%29.aspx#High_availability>

# Server Configuration

All nodes are to be built with the same VM configuration standard, using 8 virtual CPUs with 16GB. Where larger workloads are anticipated this can be flexed up as required.

## Virtual Machine Configuration

See the virtual machine specification table below:

|  |  |
| --- | --- |
| **Feature** | **Specification** |
| Generation | 2 |
| Memory (fixed) | 16384 MB |
| Processor | 8 vCPU |
| NUMA | 1 |
| SCSI Controller | 4 |
| Network Adapter | 2 |

### Operating System Configuration

All nodes are to be provisioned with the same Operating System (OS) configuration standard, using Microsoft Windows Server 2012 R2. Operating system configuration requirement specific to the hosting of SQL services are specified below:

|  |  |
| --- | --- |
| **Feature** | **Specification** |
| Windows Edition | Windows Server 2012 R2 Standard |
| Architecture | 64-bit |
| Domain | norfolk.police.uk |
| System Locale | en-GB |
| Processor scheduling | Background Services |
| Page File (fixed) | 2 GB |
| Power Options | High Performance |
| Additional Features | .Net 3.5 Framework, Failover Clustering |

*Review* *Appendix for script to test and configure necessary options and install additional features.*

### Operating System and SQL Disk Configuration

All instances of SQL use a standard disk layout, utilising windows mount points to optimize the adding and extending of disk storage. With the SQL service separate disks are provided for System, data, transaction logs, backups and temporary database. The table below illustrates a typical specification for each SQL node:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Function** | **SCSI Controller** | **Size (GB)** | **Block Size (k)** | **Mount Path** |
| Operating System | 0 | 60 | Default | C: |
| SQL System | 0 | 10 | 64 | T: |
| Backup | 1 | 250 | 64 | T:\Data\_X\backup\_01 |
| Data | 1 | 251 | 64 | T:\Data\_X\data\_01 |
| Data | 1 | 252 | 64 | T:\Data\_X\data\_02 |
| Transaction Log | 2 | 91 | 64 | T:\Data\_X\tLog\_01 |
| Transaction Log | 2 | 92 | 64 | T:\Data\_X\tLog\_02 |
| Temporary Database | 3 | 50 | 64 | T:\Data\_X\tempdb\_01 |

*Review Appendix for script to setup disk configuration.*

Caution: disks sizes shouldn’t exceed 300GB, this is due to how the storage is configured within the Hyper-V environment. With an initial disk size threshold, we have some flexibility to increase the disks where demand requires. For larger disk requirements its recommend that the database Primary file be split to span multiple disks as illustrated in the example below with the i2\_Live database:

|  |
| --- |
|  |

### Operating System Required Updates

With Windows Server Failover Clustering (WSFC) and AlwaysOn Availability Group (AAG) there are a number of recommended hotfixes see

* Recommended hotfixes and updates for Windows Server 2012 R2-based failover clusters:

<https://support.microsoft.com/en-gb/kb/2920151>

See the windows hotfix specification table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date that update was added** | **Related KB article** | **Title** | **Component** |
| March 23, 2016 | [3130944](https://support.microsoft.com/en-gb/kb/3123593) | DPM filter driver can't track changes on CSV or VM setting files can't be online in Windows Server 2012 R2 | Clussvc.exe Csvfs.sys |
| March 23, 2016 | [3137691](https://support.microsoft.com/en-gb/kb/3137691) | LBFO Dynamic Teaming mode may drop packets in Windows Server 2012 R2 | mslbfoprovider.sys |
| March 23, 2016 | [3130939](https://support.microsoft.com/en-gb/kb/3130939) | Nonpaged pool memory leak occurs in a Windows Server 2012 R2-based failover cluster | Svhdxflt.sys |
| October 28, 2015 | [3091057](https://support.microsoft.com/en-gb/kb/3091057) | Cluster validation fails in the "Validate Simultaneous Failover" test in a Windows Server 2012 R2-based failover cluster | Cprepsrv |
| December 18, 2014 | [3013769](https://support.microsoft.com/en-gb/kb/3013769) | December 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 | Multiple |
| November 18, 2014 | [3000850](https://support.microsoft.com/en-gb/kb/3000850) | November 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 | Multiple |
| April 8, 2014 | [2919355](https://support.microsoft.com/en-gb/kb/2919355) | Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update April, 2014 | Multiple |

*It is essential that updates on all nodes are kept in sync, review Appendix for script to apply updates.*

## Network Configuration

Communication between Server Cluster nodes is critical for smooth cluster operations. For networking configuration, two or more independent networks must connect the nodes of a cluster to avoid a single point of failure. The Windows Server Failover Clustering (WSFC) is stretched across three sites MER1 and MER2 at the OCC and the Dereham DR site, and the use of two local area networks (LANs) is typical for public and heartbeat communications.

### Subnets

The following subnets have been provisioned for the cluster configuration:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **Public LAN** | **Public Subnet** | **Heartbeat LAN** | **Heartbeat Subnet** |
| DER | v-lan-102 | 10.129.82.0/24 | v-lan-101-hb | 10.129.81.0/24 |
| MER1 | v-lan-111 | 10.34.81.0/24 | v-lan-113-hb | 10.34.83.0/24 |
| MER2 | v-lan-122 | 10.34.82.0/24 | v-lan-124-hb | 10.34.84.0/24 |

To aid in the identification of each LAN adapter these should be renamed during the build to ‘LAN’ for Public LAN and ‘Heartbeat’ for Heartbeat LAN.

### TCP IP Configuration

The following IP have been provisioned for each nodes public and heartbeat LAN, in addition a cluster resource IP has also been provisioned for each of the three subnets.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hostname** | **VLAN** | **IP Public** | **IP Cluster** | **VLAN** | **IP Heartbeat** | **Note** |
| DB-DE45 | v-lan-102 | 10.129.82.25 | 10.129.82.200 | v-lan-101-hb | 10.129.81.25 |  |
| DB-OC45 | v-lan-122 | 10.34.82.30 | 10.34.82.200 | v-lan-124-hb | 10.34.84.30 |  |
| DB-OC46 | v-lan-122 | 10.34.82.25 | 10.34.82.200 | v-lan-124-hb | 10.34.84.25 | Cluster resource  shared with DB-OC45 |
| DB-OC47 | v-lan-111 | 10.34.81.40 | 10.34.81.200 | v-lan-113-hb | 10.34.83.40 |  |

### Adapter Configuration

To eliminate possible communication issues, remove all unnecessary network traffic from the network adapter that is set to heartbeat adapter. Clustering communicates by using Remote Procedure Call (RPC) calls on IP sockets with User Datagram Protocol (UDP) packets, apply the follow measures to ensure appropriate communication:

* Remove NetBIOS from the adapter.
* Set the proper adapter binding order.

*The network binding order rule for SQL server cluster must be set up in this order:*

1. *Public network: teamed adaptor(s)*
2. *Private (Heart beat) network*

* Set the proper Cluster Network Roles.

### Routes

Configure TCP/IP and routes correctly. See the following table for route configuration of the heartbeat adapters, this illustrates the route for each node’s heartbeat adapter, e.g. for DB-OC46 to reach Destination Prefix 10.34.83.40/32 a route through 10.34.84.1 must be generated.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Destination | 10.34.84.30/32 | 10.34.84.25/32 | 10.34.83.40/32 | 10.129.81.25/32 |
| DB-OC45 | n/a | 10.34.84.1 | 10.34.84.1 | 10.34.84.1 |
| DB-OC46 | 10.34.84.1 | n/a | 10.34.84.1 | 10.34.84.1 |
| DB-OC47 | 10.34.83.1 | 10.34.83.1 | n/a | 10.34.83.1 |
| DB-DE45 | 10.129.81.1 | 10.129.81.1 | 10.129.81.1 | n/a |

*Review Appendix for script to configure network adapters and apply routes.*

### Name Resolution

Standard dynamic DNS registration will be used for servers, with a Host Record TTL of 300 seconds set on the cluster resource. All servers will be members of the *norfolk.police.uk* domain.

Change the HostRecordTTL (Using Windows PowerShell)

1. Open PowerShell window via **Run as Administrator**.
2. Import the FailoverClusters module.
3. Use the **Get-ClusterResource** cmdlet to find the Network Name resource, then use **Set-ClusterParameter** cmdlet to set the **HostRecordTTL** value.

The following PowerShell example sets the HostRecordTTL to 300 seconds for all Network Named resources on the Cluster.

|  |
| --- |
| Import-Module FailoverClusters  Get-ClusterResource | Where-Object {$\_.ResourceType -eq 'Network Name'} |  Set-ClusterParameter HostRecordTTL 300 |

## Windows Server Failover Clustering

Unlike other cluster setups, The AlwaysOn Availability Group (AAG) feature does not depend on any form of shared storage. AAG relies on the Windows Failover Clustering (WSFC) cluster to monitor and manage the current roles of the availability replicas that belong to a given availability group and to determine how a failover event affects the availability replicas. A WSFC resource group is created for every availability group that you create. The WSFC cluster monitors this resource group to evaluate the health of the primary replica.

### Cluster Name

The following Network Name has been provisioned, additional AAG Clusters can be incrementally added:

* SQL-AAG01

## SQL Server configuration

Each SQL node is to be built with the same set of features and configuration standard, using Microsoft SQL Server 2014 Enterprise Edition. The configuration requirement are specified below:

|  |  |
| --- | --- |
| **Feature** | **Specification** |
| SQL Server Edition | Microsoft SQL Server 2014 Enterprise Edition |
| Architecture | 64-bit |
| Build | Latest Supported Service Pack with security updates |
| Server Collation | Latin1\_General\_CI\_AS |
| Instance | Default (MSSQLSERVER) |
| Instance Directory | T:\Data\_X\SQL2014 |
| Port | Default (1433) |
| Security Mode | Mixed |
| SQL Browser Service | Disabled |
| SQL Features | To replicate the current Cluster 4 build the following features will be installed as standard:   * SQL Database Engine * Reporting Services[[2]](#footnote-2) * Database replication * Full text Search * Integration Services * SQL Server Management Studio |
| Network Protocols Settings | Enabled Network Protocols:   1. TCP and named pipes 2. Shared Memory |

*Review Appendix for script to test and configure necessary options and install additional features.*

### SQL Install File Locations

An installation of SQL Server, whether default or named, has its own set of program and data files, as well as a set of common files on the computer. The directory path for these components are listed in the table below:

|  |  |
| --- | --- |
| **Feature** | **Specification** |
| Instance Directory | T:\Data\_X\SQL2014 |
| Common files | C:\Program Files\Microsoft SQL Server |
| 32-bit Common files | C:\Program Files (x86)\Microsoft SQL Server |
| System Databases | T:\Data\_X\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\DATA |
| User Databases Data | T:\Data\_X\data\_01\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Data |
| User Databases Transaction Log | T:\Data\_X\tlog\_01\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Data |
| Backup Directory | T:\Data\_X\backup\_01\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Backup |
| Temporary Data Directory | T:\Data\_X\tempdb\_01\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Data |
| Temporary Transaction Log Directory | T:\Data\_X\tlog\_01\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Data |

### SQL Service Accounts

For an availability group to work with Kerberos, all server instances that host an availability replica for the availability group must use the same SQL Server service account, be a Domain User in the OU=SQL, OU=SERVICE ACCOUNTS Organisational Unit. Additionally the following special permissions are also required:

|  |  |  |
| --- | --- | --- |
| **Permissions** | **Justification** | **Location** |
| Read servicePrincipalName Write servicePrincipalName | When the SQL service starts, it attempts to register its Service Principal Name (SPN) with Active Directory, this can be done manually via ‘ADSI Edit’, however human error will result in authentication failure. | Active Directory |
| TrustedForDelegation | Required for delegation, use in linked servers for double hop authentication. | Active Directory |
| Lock pages in memory | The SQL Server 64-bit version uses "locked pages" to prevent the process working set (committed memory) from being paged out or trimmed by the operating system. | Server Node |
| Perform volume maintenance tasks | The SQL Server uses SE\_MANAGE\_VOLUME\_NAME a.k.a. "Perform volume maintenance tasks" to allow for Instant file initialization, enabling creating of large files instantly. | Server Node |

*Review Appendix for script to test and configure necessary permissions.*

Change the TrustedForDelegation (Using Windows PowerShell)

1. Open PowerShell window via **Run as Administrator**.
2. Import the ActiveDirectory module.
3. Use the **Get-ADUser** cmdlet to find the DistinguishedName of the account, then use **Set-ADAccountControl** cmdlet to set the **TrustedForDelegation** value.

The following PowerShell example will set the TrustedForDelegation to true for SQL Service Account  
SA-DBAG4X-SQLServer.

|  |
| --- |
| Import-Module ActiveDirectory  Get-ADUser -Filter 'Name -eq "SA-DBAG4X-SQLServer"' | Set-ADAccountControl -TrustedForDelegation $true |

The following service accounts have been provisioned for the SQL AAG:

|  |  |
| --- | --- |
| **Account** | **Function** |
| SA-DBAG4X-SQLServer | SQL DB Engine |
| SA-DBAG4X-SQLAgent | SQL Agent Service |

### Memory Settings

To improve performance, SQL Server caches data in memory, to ensure this performance is uniform across each node of the AAG the following min and max memory settings have been defined:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Minimum server memory | 0 |
| Maximum server memory | 13500 MB |

*Review Appendix for script to configure minimum and maximum memory settings.*

### Database Mail

Database Mail is an enterprise solution for sending e-mail messages from the SQL Server Database Engine, database mail is configured to use [dbaalerts@norfolk.pnn.police.uk](mailto:dbaalerts@norfolk.pnn.police.uk) for the function of sending alert on the status of the SQL service. *Review Appendix for script to configure and test dbmail.*

### Temporary database configuration (tempdb)

The **tempdb** system database is a global resource that is available to all users connected to the instance of SQL Server and is used to hold the following: temporary user objects, internal objects, and row versions. Configuration of the tempdb is vital to smooth SQL Server performance, the following specifications have been defined to establish a standard configuration:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Number of files | 1 file per logical core, up to a maximum of 8 files. |
| Data File Size | (Disk.Capacity x 0.7)/(No CPU’s <= 8) |
| Autogrowth / Maxsize | None |
| Log File Size | equal Individual Data File Size |

*Review Appendix for script to configure tempdb.*

### SQL Server Settings

The following lists, post SQL install configuration options not covered above:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Database Setting. Compress backup | enabled |
| Connections. Remote query timeout | 60 |
| Advanced. Optimize for an ad hoc workloads | True |
| sp\_configure. xp\_cmdshell | 1 |
| sp\_configure. clr enabled | 1 |
| sp\_configure. remote admin connections | 1 |

*Review Appendix for script to configure additional options.*

### Database Directory Structure

Further to Section [6.4.1 SQL Install File Locations](#_SQL_Install_File) the following table specifies the file-systems to be created for all SQL instances.

|  |  |
| --- | --- |
| **Directory Path** | **Contents** |
| T:\Data\_X\backup\_0x | Additional Backup Directory(s), incremented by 1, e.g. 02, 03…etc. |
| T:\Data\_X\data\_0x | Additional Data Directory(s), incremented by 1, e.g. 02, 03…etc. |
| T:\Data\_X\diag\_01 | sqldiag and server side trace data |
| T:\Data\_X\FTData | Full text search data files |
| T:\Data\_X\oracle | Oracle client install |
| T:\Data\_X\Packages | Directory for SSIS packages and configuration files |
| T:\Data\_X\PoSh | PowerShell scripts |
| T:\Data\_X\tempdb\_0x | Additional Temporary Data Directory(s), incremented by 1, e.g. 02, 03…etc. |
| T:\Data\_X\tivoli | Tivoli Storage Management client install |
| T:\Data\_X\tlog\_0x | Additional Transaction Log Directory(s), incremented by 1, e.g. 02, 03…etc. |

*Review Appendix for script to configure additional directories.*

### Database Maintenance Plans

Maintenance plans create a workflow of the tasks required to make sure that your database is optimized, regularly backed up, and free of inconsistencies. The Maintenance Plan Wizard that are included with the SQL installation are basic and have a number of limitations. The ‘SQL Server Maintenance Solution’ from Ola Hallengren is a free set of T-SQL scripts and stored procedures designed for the most mission-critical environments. *Review Appendix for script to configure the ola.hallengren solution.*

## Availability Groups Configuration

An Availability Group is only required to host Business Critical databases, a standard databases can be hosted on the individual SQL nodes without any further configuration. The following parameters have been defined for current systems.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **AAG** | **Member** | **Default Role** | **Name** | **AAG IPs** | **Port** | **Databases** |
| DB-AAG01 | DB-OC45  DB-OC46  DB-OC47  DB-DE45 | Primary  Secondary  Secondary  Secondary | DB-AAG01 | 10.129.82.191  10.34.82.191  10.34.81.191 | 5022 | SSRS |
| DB-AAG02 | DB-OC46  DB-DE45 | Primary  Secondary | DB-AAG02 | 10.129.82.192  10.34.82.192  10.34.81.192 | 5022 | NdiCdr |
| DB-AAG03 | DB-OC46  DB-OC47  DB-DE45 | Primary  Secondary  Secondary | DB-AAG03 | 10.129.82.193  10.34.82.193  10.34.81.193 | 5022 | Storm |
| DB-AAG04 | DB-OC47  DB-DE45 | Primary  Secondary | DB-AAG04 | 10.129.82.194  10.34.82.194  10.34.81.194 | 5022 |  |

***Note:*** *When configuring an application to host its Database on a SQL Availability Group, specify a Listener name for the instance name and the Listener port for the Instance port.*



### Availability Replicas Configuration

Each availability group defines a set of two or more failover partners known as availability replicas, these are assigned an initial role, either *primary* or *secondary* and a mode *synchronous*or*asynchronous*. The following table specifies the detailed availability replica configuration:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AAG** | **Server Instance** | **Initial Role** | **Automatic Failover** | **Synchronous Commit** | **Allow Readable Secondary** |
| DB-AAG01 | DB-OC45 | Primary | Yes | Yes | Yes |
| DB-OC46 | Secondary | Yes | Yes | Yes |
| DB-OC47 | Secondary | No | No | Yes |
| DB-DE45 | Secondary | No | No | Yes |
| DB-AAG02 | DB-OC46 | Primary | Yes | Yes | Yes |
| DB-DE45 | Secondary | No | No | Yes |
| DB-AAG03 | DB-OC46 | Primary | Yes | Yes | Yes |
| DB-OC47 | Secondary | Yes | Yes | Yes |
| DB-DE45 | Secondary | No | No | Yes |
| DB-AAG04 | DB-OC47 | Primary | Yes | Yes | Yes |
| DB-DE45 | Secondary | Yes | Yes | Yes |

For more information see TechNet: **Failover and Failover Modes (AlwaysOn Availability Groups) –** [http://technet.microsoft.com/en-us/library/hh213151](https://technet.microsoft.com/en-us/library/hh213151(v=sql.120))

#### Readable Secondary Option:

The AlwaysOn Availability Group (AAG) active secondary capabilities include support for read-only access to one or more secondary replicas (readable secondary replicas). A readable secondary replica allows read operations to be devolved to its secondary databases. This feature is effective with Business Intelligence (BI) systems where secondary copies of databases are necessary to offload read intensive operations. A secondary replica may be configures with the following options:

|  |  |
| --- | --- |
| **Option** | **Description** |
| No | No user connections are allowed to secondary databases of this replica. They are not available for read access. This is the default setting. |
| Read-intent only | Only read-only connections are allowed to secondary databases of this replica. The secondary database(s) are all available for read access. |
| Yes | All connections are allowed to secondary databases of this replica, but only for read access. The secondary database(s) are all available for read access. |

#### Primary Role Connections:

The primary role supports two alternatives for client connections *allow all* or *allow read/write* connections, (*explained below*). The default *Allow all* is to be applied, unless otherwise stated in application design.

|  |  |
| --- | --- |
| **Option** | **Description** |
| Allow all connections | All connections are allowed to the databases in the primary replica. This is the default setting. |
| Allow read/write connections | When the Application Intent property is set to ReadWrite or the Application Intent connection property is not set, the connection is allowed. Connections where the Application Intent connection property is set to ReadOnly are not allowed. This can help prevent customers from connecting a read-intent work load to the primary replica by mistake. |

### Endpoints Configuration

To host an availability replica for an availability group, each server instance must possess a database mirroring endpoint, there is one endpoint per SQL Server Instance. During AAG creation the endpoint URL is configured with the SQL Instance FQDN and the port number associated with the endpoint, these parameters are detailed below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Instance** | **Endpoint URL** | **Endpoint Port** | **Endpoint Name** |
| DB-OC45 | TCP://db-oc45.norfolk.police.uk:5022 | 5022 | Hadr\_endpoint |
| DB-OC46 | TCP://db-oc46.norfolk.police.uk:5022 | 5022 | Hadr\_endpoint |
| DB-OC47 | TCP://db-oc47.norfolk.police.uk:5022 | 5022 | Hadr\_endpoint |
| DB-DE45 | TCP://db-de45.norfolk.police.uk:5022 | 5022 | Hadr\_endpoint |

*Review Appendix for script to configure availability group endpoints.*

### Availability Group Service Principal Name

The domain administrator needs to manually register a Service Principal Name (SPN) with Active Directory on the SQL Server service account for the virtual network name (VNN) of the availability group listener. If the SPN is registered on an account other than the SQL Server service account, authentication will fail. *Review Appendix for script to configure AAGs SPN.*  
  
 **\*\* Important \*\*** If you change the SQL Server service account, the domain administrator will need to manually re-register the SPN.

## Server access

SQL Server access is controlled through Active Directory Role Groups and Users, the following table lists the initial required AD objects required to manage and access the SQL Server:

|  |  |  |  |
| --- | --- | --- | --- |
| **AD Object** | **Windows Access** | **SQL Access** | **Reporting Services Access** |
| Role-ICT-DBA | Local Administrator[[3]](#footnote-3) | sysadmin | Hadr\_endpoint |
| SQLSpotlightServer | Local Administrator | sysadmin | None |
| ICT Software Development Team | ReadWrite to SSIS Package folder T:\Data\_X\Packages | ictdevelopment | TBD |

*Review Appendix for script to configure necessary server role groups and access.*

## Oracle client

Many of the applications using SQL derive part of their data from remote oracle systems via linked server objects. This can only be achieved with appropriate client connection driver. Refer to the 11.2 client installation guide for setup instructions.

# Backup

## Backup and Recovery Architecture

Backup of user and system databases is managed through the SQL Agent and stored compressed on the servers file system through the implementation of Database Maintenance Plans ([see section 6.4.8](#_Database_Maintenance_Plans)). These are then integrated with Tivoli Storage Manager (TSM) through Tivoli Data Protection (TDP) for backup storage and policy management. The Database Maintenance Plans ensure that full, differential, and transaction log backups occur regularly without the dependency on 3rd party tools, the schedule and retention of these backups are detailed in the below table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Backup** | **Function** | **Schedule** | **Server Retention** |
| SYSTEM\_DATABASES - FULL | Full Backup of System Databases | Daily at 19:57. | 2 days |
| USER\_DATABASES - FULL | Full Backup of User Databases | Weekly on Wednesday, Sunday at 19:59. | 2 days |
| USER\_DATABASES - DIFF | Differential Backup of User Databases | Weekly on Monday, Tuesday, Thursday, Friday, Saturday at 19:59. | 2 days |
| USER\_DATABASES - LOG | Log Backup of User Databases | Daily every 1 hour(s) between 3:15 and 21:15:59. | 2 days |

Note, consider the backup retention period when sizing the backup device.

### Tivoli Storage Management client

SQL Server Maintenance Solution (see [6.4.8 Database Maintenance Plans](#_Database_Maintenance_Plans)) will be used for the backup of SQL databases. This will be integrated with Tivoli Storage Manager (TSM) through Tivoli Data Protection (TDP) for backup storage and policy management.

Following agents will be installed on each database server:

* TSM Client 7.1.3

The retention period Tivoli Storage Manager is 21 days.

### Recovery Mechanism

Recovery mechanism is determined by the length of time since the backup was taken, if this is within the file retention period, *2 days*, recovery can be implemented immediately through SSMS or T-SQL command; otherwise the Tivoli Storage Manager client should be used to recover the files to the server before restoring the database through SSMS or T-SQL command. For further detail review the SQL Server Operations Guide.

# Monitoring

In a virtualized shared service architecture the significance of monitoring SQL databases is to measure how well a server is performing. Constant evaluation of the database performance helps minimize response times and maximize throughput, yielding optimal performance. Some common bottlenecks that impact SQL Server performance include:

* A bad/expensive query.
* Memory pressure.
* Blocking and deadlocks.
* Storage response times.
* Growth of data, leading to a need for more memory and CPU.
* Poor index fragmentation, leading to slow searches and additional capacity.

## Monitoring Tools

For a complex monitoring requirement, it is common to allocate different services into categories of monitoring solutions, the following table outlines the existing strategic direction of each category:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Product** | **Supplier** | **Edition/Version** |
| Server Operation System | Microsoft System Center Operations Manager (SCOM) | Microsoft | 2012 R2 |
| SQL Server | Microsoft System Center Management Pack for SQL Server[[4]](#footnote-4) | Microsoft | 6.6.4.0 |
| Spotlight Enterprise for SQL Server | Dell | 11.6 |
| AlwaysOn Availability Group (AAG) | PowerShell and SQL Extended Events | Microsoft | 12.0 |

Best practice is to baseline the server before being placed into production with attention on the core resources: CPU, Memory, and IO. Diskspd is a storage testing tool that has been valuable it generating SQL IO patterns and ensuring the disk subsystem is up to standard.[[5]](#footnote-5) *Review Appendix scripts for baseline of the disk subsystem.*

Caution: establishing the monitoring goals is beyond the scope of this document, review the Organisation, or SQL estate monitoring strategy.

# Security

## Firewall

There is currently no strategy to secure the servers within the internal network, therefore windows firewall setting are disabled by design. Any external requirements to connect directly to SQL will be dealt with on an individual requirement and follow prober governance for approval.

## Anti-Virus Exclusions

The existing Anti-Virus policy is to implement Sophos Endpoint Security for Windows Servers, in addition to the on-access scanning being disabled, the following file extensions and paths are to be added to the Exclusions list:

|  |  |
| --- | --- |
| **Category** | **Product** |
| WSFC | %Systemroot%\Cluster |
| The temp folder for the Cluster Service account | \*clusterserviceaccount*\Local Settings\Temp |
| SQL Server data files | * .mdf * .ldf * .ndf |
| SQL Server backup files | * .bak * .dif * .trn |
| Full-Text catalogue files | T:\Data\_X\FTData T:\Data\_X\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\FTData |
| Trace files | These files usually have the .trc file-name extension. |
| SQL audit files | These files have the .sqlaudit file-name extension. |
| SQL query files | These files typically have the .sql file-name extension and contain Transact-SQL statements. |
| Reporting Services temporary files and Logs | T:\Data\_X\SQL2014\MSRS12.MSSQLSERVER\Reporting Services\RSTempFiles  T:\Data\_X\SQL2014\MSRS12.MSSQLSERVER\Reporting Services\LogFiles |
| SQL Service | T:\Data\_X\SQL2014\MSSQL12.MSSQLSERVER\MSSQL\Binn\ |
| SSRS | T:\Data\_X\SQL2014\MSRS12.MSSQLSERVER\Reporting Services\ReportServer\bin\ |
| sqldiag | C:\Program Files\Microsoft SQL Server\120\Tools\Binn\ |

For more information on Anti-Virus best practices:

* [How to choose antivirus software to run on computers that are running SQL Server](https://support.microsoft.com/en-gb/kb/309422)
* [Antivirus software that is not cluster-aware may cause problems with Cluster Services](https://support.microsoft.com/en-us/kb/250355)

# References

[Overview of AlwaysOn Availability Groups](https://msdn.microsoft.com/en-us/library/ff877884(v=sql.120).aspx)

[Kerberos and AvailabilityGroups – What you need to know](https://blogs.technet.microsoft.com/rhartskeerl/2012/03/04/kerberos-and-availabilitygroups-what-you-need-to-know/)

[Register a Service Principal Name for Kerberos Connections](https://msdn.microsoft.com/en-us/library/ms191153(v=sql.110).aspx)

[Create a Database Mirroring Endpoint for Always On Availability Groups](https://msdn.microsoft.com/en-gb/library/hh510204.aspx)

[Specify the Endpoint URL When Adding or Modifying an Availability Replica](https://msdn.microsoft.com/en-gb/library/ff878441.aspx#Finding_FQDN)

[Database Engine PowerShell Reference](https://msdn.microsoft.com/en-us/library/hh230864(v=sql.120).aspx)

[Before Installing Failover Clustering](https://msdn.microsoft.com/en-us/library/ms189910(v=sql.120).aspx)

[Oracle 11.2 client installation guide](https://docs.oracle.com/cd/E11882_01/install.112/e47959.pdf)

[SQL Server Maintenance Solution](https://ola.hallengren.com/)

[Overview of AlwaysOn Availability Groups](https://msdn.microsoft.com/en-us/library/ff877884(v=sql.120).aspx)

[Performance Monitoring and Tuning Tools](https://msdn.microsoft.com/en-gb/library/ms179428(v=sql.120).aspx)

[Establish a Performance Baseline](https://msdn.microsoft.com/en-us/library/ms190943(v=sql.120).aspx)

[Monitor an AlwaysOn Availability Group with PowerShell](https://blogs.technet.microsoft.com/heyscriptingguy/2013/04/30/monitor-an-alwayson-availability-group-with-powershell/)

[How to choose antivirus software to run on computers that are running SQL Server](https://support.microsoft.com/en-gb/kb/309422)

[Antivirus software that is not cluster-aware may cause problems with Cluster Services](https://support.microsoft.com/en-us/kb/250355)

[High Availability (Reporting Services)](https://msdn.microsoft.com/en-us/library/bb522745(v=sql.120).aspx)

[Reporting Services with AlwaysOn Availability Groups](https://msdn.microsoft.com/en-us/library/hh882437(v=sql.120).aspx)

[Dealing with SSRS subscription schedules in AlwaysOn environment](http://blog.dbi-services.com/dealing-with-ssrs-subscription-schedules-in-alwayson-environment/)[Troubleshooting SQL Server Reporting Service Error](http://www.mytechmantra.com/LearnSQLServer/Troubleshooting-SQL-Server-Reporting-Service-Error.html)

[Create the RSExecRole](https://msdn.microsoft.com/en-us/library/cc281308(v=sql.120).aspx)

[GenerateDatabaseRightsScript Method](https://msdn.microsoft.com/en-us/library/ms155370(v=sql.120).aspx)

# Appendix A

1. Excluding Web and Express editions. [↑](#footnote-ref-1)
2. Reporting Services has been included in this build to enable migration from DB-OCC11 [↑](#footnote-ref-2)
3. Granted via RG-CA-ServerLocalAdministrators [↑](#footnote-ref-3)
4. Provides an Enterprise view of SQL estate, at the time of writing, the rollout of SCOM 2012 R2 had not been initiated. [↑](#footnote-ref-4)
5. Take performance measurements at regular intervals over time, even when no problems occur, to establish a server performance baseline. [↑](#footnote-ref-5)