A red and white logo

Description automatically generated with low confidence

SQL Upgrade 786

SQL Detailed Design 786

|  |  |
| --- | --- |
| Prepared by: | Adrian Sullivan, adrian@sqldba.org |
| Job Title: | Principal Consultant |
| Document Version: | 0.1 |
| Document Status: | Awesome |

In the interest of advancing the design and implementation of SQL projects globally, I am making this template available, under certain conditions. <https://github.com/SQLDBA-ORG/GroupBy/blob/main/LICENSE>

Feel free to use this template. Make sure you reference that this is **my** template. Why? If things go bad, you know who to get in touch with.

Have fun, and if you need help, just get in touch. This version of the document is the culmination of about 5 years’ worth of SQL project work. Millions of dollars of SQL projects have been executed using this document.

But a document is just a tool, it alone does not guarantee success, that would be where your experience comes into play.

Use it as a tool, and if you make it better, let me know and I’ll update the template, so we all can benefit.

* Adrian

Table of Contents

[1. Introduction 3](#_Toc86234777)

[1.1 Overview of Business Requirements 3](#_Toc86234778)

[1.2 Requirements 3](#_Toc86234779)

[1.3 Component Description 5](#_Toc86234780)

[1.4 Delivery Approach 5](#_Toc86234781)

[2. Solution Architecture 7](#_Toc86234782)

[2.1 Overview 7](#_Toc86234783)

[2.2 SQL Servers and Instances 8](#_Toc86234784)

[2.3 SQL Clusters 8](#_Toc86234785)

[2.4 Availability Groups 8](#_Toc86234786)

[2.5 Project Assumptions 8](#_Toc86234787)

[2.6 Source Servers 8](#_Toc86234788)

[2.7 CNAME redirects 9](#_Toc86234789)

[3. Technical Component Design 10](#_Toc86234790)

[3.1 Application Configuration 10](#_Toc86234791)

[3.2 Network Configuration 10](#_Toc86234792)

[3.3 Windows Virtual Server 10](#_Toc86234793)

[3.4 Failover Cluster Group Configuration 10](#_Toc86234794)

[3.5 Licensing 11](#_Toc86234795)

[3.6 SQL Service and Admin Account 11](#_Toc86234796)

[3.7 SQL Server Configuration 11](#_Toc86234797)

[3.8 SQL Database Configuration 12](#_Toc86234798)

[3.9 SQL Network Firewall Rules 12](#_Toc86234799)

[3.10 Other SQL Services 13](#_Toc86234800)

[4. Operational Considerations 14](#_Toc86234801)

[4.1 SQL Migration Considerations 14](#_Toc86234802)

[4.1.1 SQL Migration Mapping 14](#_Toc86234803)

[4.2 Backup and Consistency Checks 14](#_Toc86234804)

[4.3 SQL Maintenance and Performance Optimization 14](#_Toc86234805)

[4.4 Monitoring and Alerting 14](#_Toc86234806)

[4.5 Antivirus and malware file exclusions 15](#_Toc86234807)

[4.6 Security 15](#_Toc86234808)

[5. Schedule: List of Application databases 16](#_Toc86234809)

# Introduction

## Overview of Business Requirements

**GroupBy** have engaged SQLDBA to design and implement a new scaled-out Highly Available SQL Server environment.

This environment will consist of a local SQL cluster, providing High-Availability, along with an Azure cluster, providing BI offloading.

SQLDBA will retain the current SQL environment. The solution will leverage the current Azure implementation to create the HA SQL service.

A rolling upgrade will be carried out to uplift the SQL environment to SQL 2019

## Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Req. ID | Requirement (Use Story) | Priority | Comments |
| REQ001 | Availability of the SQL service during normal operation and limited failure events. | Must | This solution |
| REQ002 | Agile Capacity allowing for low service interruption for changes and scaling. | Must | Part of platform |
| REQ003 | **Enterprise Edition** SQL Licensing | Must | Azure |
| REQ004 | Performance optimization configurations should be preferred | Should | 3.7, 3.8, 4.3 |
| REQ005 | Ability to monitor capacity and utilization | Must | Part of platform |
| REQ006 | Operation and Systems Management Monitoring should be possible on the solution | Must | Part of platform |
| REQ007 | The solution should **allow Disaster Recovery** options to be available | Must | 2.3, 3.4, 4.2 |
| REQ008 | Must be robust. Relates in part to DR and HA | Must | 2.3, 3.4, 4.2 |
| REQ009 | Must cater for a **Production SQL environment** | Must | 2.2, 2.3, 2.4 |
| REQ010 | Could cater for a **Test SQL environment** | Could | Not included |
| REQ011 | Must handle node failures automatically | Must | 2.3, 2.4, 3.4 |
| REQ012 | Must be highly performant. At least 500 IOPS | Must | Azure |
| REQ013 | Automatic failover for all databases in Availability Groups | Must | 2.3, 2.4 |
| REQ014 | The solution should require minimal design effort to meet all requirements | Must | This solution |
| REQ015 | Definable port for SQL communication | Must | Part of platform |
| REQ016 | Must have the ability to schedule and deliver SQL daily/weekly/monthly maintenance. | Must | Part of platform  4.2, 4.3 |
| REQ017 | Can add new users, as per security guidelines. Managed through AD | Must | Managed through AD |
| REQ018 | Have SQL **encryption disabled** | Must | 3.7 |
| REQ019 | The rest is up to you 😉 |  |  |
| REQ020 |  |  |  |
| REQ021 |  |  |  |
| REQ022 |  |  |  |
| REQ023 |  |  |  |
| REQ024 |  |  |  |
| REQ025 |  |  |  |
| REQ026 |  |  |  |
| REQ027 |  |  |  |
| REQ028 |  |  |  |
| REQ029 |  |  |  |
| REQ030 |  |  |  |
| REQ031 |  |  |  |
| REQ032 |  |  |  |
| REQ033 |  |  |  |
| REQ034 |  |  |  |
| REQ035 |  |  |  |
| REQ036 |  |  |  |
| REQ037 |  |  |  |
| REQ038 |  |  |  |
| REQ039 |  |  |  |
| REQ040 |  |  |  |
| REQ041 |  |  |  |
| REQ042 |  |  |  |
| REQ043 |  |  |  |

## Component Description

This section provides descriptions of new components being implemented as part of the SQL Solution.

The scope of this solution is for the primary production environments locally and on a virtualized platform, in Azure.

The solution proposed will leverage SQL Enterprise Edition to provide a 2-node cluster for production. And the same in Azure.

Two Availability Group will be created for Karisma and non Karisma production database that requires HA protection.

Data will be committed in a synchronous manner between the 2 nodes and automatic failover will be configured to point the SQL connections to the active node.

The Availability Groups will provide virtual network endpoints that applications will use to connect to the SQL service.

## Delivery Approach

Delivery will follow a standard **waterfall** approach:

* Requirements Gathering (Business & Technical)
* Analysis
* Design
* Implementation of Platform Resources
* Installation and Configuration of MS SQL Capability
* Testing and Verification
* Transition and Handover

Delivery will occur across all environments at the same time for each of the points listed above.

SQLDBA will leverage industry-leading Microsoft experience, proven methods and a robust implementation framework.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task   | Description | Start | End | Owner |
| 1 | Solution Design and Workshops | Week 1 | Week 1 |  |
| 1.1 | Detailed Design | Day 1 | Day 5 | SQLDBA/Customer |
| 1.2 | Workshop and remediation scope confirmation | Day 2 | Day 2 | SQLDBA |
| 2 | Deployment | Week 2 | Week 2 |  |
| 2.1 | Change requests and scheduling | Day 2 | Day 3 | SQLDBA/Customer |
| 2.2 | Base deployment of SQL servers | Day 3 | Day 5 | SQLDBA |
| 2.3 | Migration planning | Day 1 | Day 2 | SQLDBA/Customer |
| 3 | SQL configuration | Week 3 | Week 3 |  |
| 3.1 | SQL instance configuration | Day 1 | Day 4 | SQLDBA |
| 3.2 | Load testing of SQL servers | Day 4 | Day 5 | SQLDBA |
| 3.3 | Requirements validation; | Day 5 | Day 5 | SQLDBA/Customer |
| 4 | Migration | Week 3 | Week 3 | SQLDBA |
| 4.1 | Data migration | Day 1 | Day 3 |  |
| 4.2 | Workload cutover | Day 4 | Day 5 | SQLDBA/Customer |
| 5 | Transition | Week 4 | Week 6 |  |
| 5.1 | Assist with any post-implementation issues | Week 4 | Week 6 | SQLDBA |
| 5.2 | Provide operational handover and training | Day 4 | Day 4 | SQLDBA/Customer |
| 6 | Services Management | Week 1 | Week 4 |  |
| 6.1 | Managing the SQLDBA resources | Week 1 | Week 4 | SQLDBA |
| 6.2 | Includes resource scheduling and related tasks Week 1 | | Week 4 | SQLDBA |

# Solution Architecture

The SQL deployment will consist of 2 servers per environment. A Distributed Availability Group will be used to implement High Availability across these servers.

Connectivity to each service will be provided by DNS provisioned CNAME’s and Availability Group listener endpoints.

## Overview

The template architecture will be used as a base design for the environment. Refer to the proper sections in this document to see the most recent server names, IP addresses, etc.

Graphical user interface, diagram

Description automatically generated

Diagram 1: Production Environment Template Architecture

## SQL Servers and Instances

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Environment | Expected Architecture \* | Intent | Location | Server Name | Instance | Reference |
| Production | AG | Live | Local | GROUPBYSQL1 | DEFAULT | S#1 |
| Production | AG | Live | Local | GROUPBYSQL2 | DEFAULT | S#2 |
| Production | AG | Live | Azure | GROUPBYSQLA1 | DEFAULT | S#3 |
| Production | AG | Live | Azure | GROUPBYSQLA2 | DEFAULT | S#4 |

\*AG – Availability Groups

## SQL Clusters

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Environment | Expected Architecture \* | Intent | Location | Server Name | Servers | Reference |
| Production | Cluster | Live | Local | SQLCLUS1 | S#1, S#2 | C#1 |
| Production | Cluster | Live | Azure | AZSQLCLUS1 | S#3, S#4 | C#2 |

## Availability Groups

The SQL deployment will consist of the following Availability Groups (AG). Each AG will manage data synchronisation and service endpoints on a per-database level.

Listeners are network endpoints where clients connect to. The listener endpoint is controlled by the cluster and enables communications to follow the active node in the cluster.

Databases listed below with no Expected Architecture will not have High Availability configured.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Environment | Expected Architecture | Database | Priority | Listener Name | IP | Reference | PRIMARY |
| Production | AG | Non-karisma datbases | High |  |  | L#1 | GROUPBYSQL1 |
| Production | AG | Karisma databases | High |  |  | L#1 | GROUPBYSQL1 |
| Production | AG/AZURE |  | High |  |  | L#2 | GROUPBYSQLA1 |
|  |  |  |  |  |  |  |  |

## Project Assumptions

* There is sufficient VM capacity (CPU, Memory and Disk) to provision the SQL VM Server
* SQL Licensing has been provisioned
* There is sufficient performance in the site firewalls to route all traffic internally and externally via the firewalls.

## Source Servers

These servers will be used as data sources during the migration process and for reference to base

configuration outside of what has been listed in this document.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Environment | Current Architecture \* | Intent | Location | Server Name | Instance | Reference |
| Production | Standalone | Live | Auckland | GROUPBYSQL1 | DEFAULT | O#1 |

## CNAME redirects

These redirects will be put in place to reduce the need for application reconfiguration and for future proofing.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | CNAME | Target | TTL | Rename old Server |
| Production | KARISMASQL | L#1 |  | No |
| Production | GROUPBYSQL | L#1 |  | N/A |
| Production | SQL1 |  |  | No |
| AD | KARISMASQL | SQL1, to change to Listener | 30min |  |

# Technical Component Design

## Application Configuration

|  |  |
| --- | --- |
| Environment | Application |
| Production | SQL Server 2017 Enterprise Edition |

## Network Configuration

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Environment | Type | Server # | IP | Subnet | Resource Group | Reference |
| Production | Server | S#1 | 10.2.6.1 | 10.2.6.0 | RG-AE-1 | N#1 |
| Production | Server | S#2 | 10.2.6.2 | 10.2.6.0 | RG-AE-1 | N#2 |
| Production | Cluster | C#1 | 10.2.6.3 | 10.2.6.0 |  | N#3 |
| Production | Listener | L#1 | <TBA> | 10.2.6.0 |  | N#4 |
| Production | Listener | L#2 | <TBA> | 10.2.6.0 |  | N#5 |

## Windows Virtual Server

|  |  |
| --- | --- |
| Item | Production |
| Servers | S#3, S#4 |
| Host OS | Windows 2016 |
| CPU | 4 CPU |
| VM CPU core count | 4 cores |
| VM CPU Socket count | 1 socket |
| Memory | 14GB |
| C: Drive. Fast. | 80GB |
| D: Drive. Data. Slow | 300GB |
| E: Drive. Logs. Fast | 125GB |
| F: Drive. TempDB. Fast – Temporary SSD | 100GB |
| Network Card(s) | X 1 |

## Failover Cluster Group Configuration

|  |  |
| --- | --- |
| Item | Details |
| Cluster Name | C#1 |
| Cluster IP | N#1 |
| Cluster Nodes | S#1, S#2 |
| Listener Name | L#1, L#2 |
| Listener IP | N#4, N#5 |
| Failover type | Automatic |
| Databases in AG\* | Operation process to add |
| Quorum failover timeout | 10 seconds |
| File Share Witness | \\AZDC1\ClusterFileShareWitness |

\*Operational consideration.

* When adding databases to an Always On Availability Group, the operational process should specify how the database/job/user is added to the other node(s).

## Licensing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | Server # | Edition | CPU count | Licensed CPUs |
| Production | S#1 | Enterprise | 4 CPU | 4 CPU |
| Production | S#2 | Enterprise | 4 CPU | 4 CPU |

## SQL Service and Admin Account

|  |  |  |
| --- | --- | --- |
| Account | Type | Scope |
| GROUPBYG\svc\_SQL2016Prod | Service Account | Prod |
| GROUPBYG\SEC\_GROUPBYSQL2016\_Admins | AD Group | Prod |

## SQL Server Configuration

|  |  |  |
| --- | --- | --- |
| Item | S#1/2 | S#3/4 |
| Version | SQL 2017 Enterprise | SQL 2017 Enterprise |
| Instance | Default | Default |
| Port | 1433 | 1433 |
| Transport/Communication  Encryption\* | Disabled | Disabled |
| Login Type | AD & SQL | AD & SQL |
| Collation\*\* | Latin1\_General\_CI\_AS | Latin1\_General\_CI\_AS |
| Database Containment  Enabled\*\*\* | True | True |
| Backup Compression | Yes | Yes |
| Cost Threshold for Parallelism | 50 | 50 |
| MAXDOP | 0 | 0 |
| Ad hoc Workloads | Yes | Yes |
| SA Disabled | No | No |
| Analysis Services | Tabular | Tabular |
| Location | Data Center | AZURE |
| Reporting Services | Yes | Yes |

\*Transport/Communication Encryption.

* <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017>
* This relates to the network protocol and will allow all communication between the application driver and the SQL instance to be encrypted.

\*\* Collation.

* This defines the code page format in which data is stored and impacts how data is sorted.
  + Collation can be defined at the following levels: SQL Instance, Database, Table, Column.
* Multiple database collations can exist in the same SQL instance, even with different collations to each other and the SQL server

\*\*\* Database Containment.

* This feature allows each database to have persisted code page settings in the Temporary database. Enabling this feature allows different database collations on the same server using the same TempDB database and SSRS services.

## SQL Database Configuration

This base configuration will be configured for all databases in all environments.

|  |  |
| --- | --- |
| Item | Setting |
| Auto growth | Enabled |
| Auto Create Statistics | Enabled |
| Database Containment | Partial |
| Page verification | Checksum |
| File Growth | 256MB |
| Parameterization | Enabled |
| Database recovery time | 60 seconds |

## SQL Network Firewall Rules

The base firewall rules are the known basic requirements for the rule to be added to the firewalls at all sites. These rules should allow SQL to function correctly.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type | Port/s | Protocol | Expected Source | Destination | Comment |
| SQL | 1433 | TCP | Any | SQL Servers\* | SQL Server default instance running over TCP |
| SQL | 1434 | TCP, UDP | Any | SQL Servers\* | Dedicated Admin Connection, SQL Server Browser service |
| SQL | 4022 | TCP | Any | SQL Servers\* | Service Broker |
| SQL | 5022-5030 | TCP | SQL Servers\* | SQL Servers\* | Availability Group Listeners |
| SQL | 2383 | TCP | Any | SQL Servers\* | Analysis Services |
| SQL | 2382 | TCP | Any | SQL Servers\* | SQL Server Browser service for AS |
| SQL | 80 | TCP | Any | SQL Servers\* | Reporting Services Web Services |
| SQL | 135 | TCP | SQL Servers\* | SQL Servers\* | Microsoft Distributed Transaction Coordinator (MS DTC) |
| SQL | 7022 | TCP | SQL Servers\* | SQL Servers\* | SQL Mirroring |
| Windows | 135 | TCP | SQL Servers\* | SQL Servers\* | SQL Server Configuration Manager uses WMI to list and manage services. |
| Cluster | 3343 | TCP | SQL Servers\* | SQL Servers\* | Cluster communication port |
| Cluster | 3343 | UDP | SQL Servers\* | SQL Servers\* | Cluster Service |
| Cluster | 3343 | TCP | SQL Servers\* | SQL Servers\* | Cluster Service. (This port is required during a node join operation.) |
| Cluster | 135 | TCP | DC, CA | SQL Servers\* | RPC |
| Cluster | 137 | UDP | SQL Servers\* | SQL Servers\* | Cluster Administrator |
| SMB | 445 | TCP | SQL Servers\* | SQL Servers\* | SMB share port for file share witness |
| AD | 9389 | TCP | DC | SQL Servers\* | Active Directory Web Services (ADWS) |
| AD | 9389 | TCP | DC | SQL Servers\* | Active Directory Management Gateway Service |
| AD | 3269 | TCP | DC | SQL Servers\* | Global Catalog |
| AD | 3268 | TCP | DC | SQL Servers\* | Global Catalog |
| AD | 389 | TCP, UDP | DC | SQL Servers\* | LDAP Server |
| AD | 636 | TCP | DC | SQL Servers\* | LDAP SSL |

\* SQL Servers are defined as any SQL servers in the environment that might interact with the SQL cluster or Availability Groups. This might also include central SQL management servers or other SQL servers in different networks.

* **Reference:**

<https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-2017>

<https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows>

## Other SQL Services

Where other SQL services are being consumed on source servers, they will be migrated to the appropriate equivalent on the new servers.

Each SQL server in a cluster will have the same services installed, the availability of any SQL service will be determined by the ability of the service to interact with the underlying database.

Where possible each critical service database will be configured to run under an Availability Group and the services will be configured to connect to the appropriate listener name.

# Operational Considerations

## SQL Migration Considerations

* During migration special tooling will be deployed to ensure all SQL artefacts are copied across.
* It would be advisable to run full regression testing on the initial build of the new SQL environment before implementing the final cutover.
* During the cutover window a final data synchronisation will be carried out.
* Existing SQL servers will be renamed during cutover and new DNS entries added to route traffic to the new servers, these CNAME’s will only be implemented during cutover.

### SQL Migration Mapping

|  |  |  |
| --- | --- | --- |
| Source Server | Target Server | Objects |
| OldSQL | NewSQL | Logins, jobs, all DBs |

## Backup and Consistency Checks

The SQL backup location will be an external file share, which will be exposed as a UNC path to the SQL servers.

|  |  |  |
| --- | --- | --- |
| UNC Path | Backup Type | Geo-Location backup strategy |
| <TBA>\\AzureUNC\SQLBackup | All | To Be Determined |

Backup allocation for SQL database backups should be roughly double the size of the databases.

|  |  |  |
| --- | --- | --- |
| Schedule | Task Type | Retention |
| Daily | Differential | 7 days |
| Weekly | Full | 14 days |
| 10 minutes | Transaction Log | 7 days |
| VM | Daily |  |
| Daily | DBCC Checks on all databases | No sign |

## SQL Maintenance and Performance Optimization

|  |  |
| --- | --- |
| Schedule | Type |
| Daily | Ola Hallengren Index Rebuild |
| Daily | Statistics Update |

## Monitoring and Alerting

The preferred minimum monitoring tool for this solution would be a paid SQL Server specific monitoring tool. Generic tools which also monitor SQL as a subset of monitoring should be disregarded. We would recommend the toolsets available from SQLDBA.ORG for this.

Monitoring will allow for the validation of performance and growth expectations. Built-in Dynamic Management View information can be queried and contains SQL internal monitoring information since the last service restart.

SQL level alerts will be configured on each SQL instance as part of the implementation.

SQL alerts will be sent to:

sqlsupport@GroupBy.co.nz

|  |  |
| --- | --- |
| Alert Name | Severity/Error |
| Alert - Sev 19 Error: Fatal Error in Resource | 19 |
| Alert - Sev 20 Error: Fatal Error in Current Process | 20 |
| Alert - Sev 21 Error: Fatal Error in Database Process | 21 |
| Alert - Sev 22 Error: Fatal Error: Table Integrity Suspect | 22 |
| Alert - Sev 23 Error: Fatal Error Database Integrity Suspect | 23 |
| Alert - Sev 24 Error: Fatal Hardware Error | 24 |
| Alert - Sev 25 Error: Fatal Error | 25 |
| Alert - Error 823: The operating system returned an error | 823 |
| Alert - Error 824: Logical consistency-based I/O error | 824 |
| Alert - Error 825: Read-Retry Required | 825 |
| Alert - Error 832: Constant page has changed | 832 |
| Alert - Error 855: Uncorrectable hardware memory corruption detected | 855 |
| Alert - Error 856: SQL Server has detected hardware memory corruption, but has recovered the page | 856 |
| Alert - Error 1205: Deadlock | 1205 |
| Alert - Error 3928: Deadlock | 3928 |
| Alert - AG 35265: AG Data Movement - Resumed | 35265 |
| Alert - AG 35264: AG Data Movement - Suspended | 35264 |
| Alert - AG 1480: AG Role Change | 1480 |

## Antivirus and malware file exclusions

Antivirus scanning should at least exclude the following file extensions:

• .mdf

• .ndf

• .ldf

• .bak

• .trn

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

Please ensure that the current Antivirus exclusions include the recommended SQL exclusions.

## Security

Only Active Directory authentication will be used by this solution. This will allow for management of passwords and user permission at an organisational level.

Managing user accounts and related permission fall outside of the scope of this document.

The solution will allow for management of AD accounts and groups as security objects within SQL server.

Any requirements outside of AD accounts or AD groups will be dealt with on a case by case basis and will be handled by the security team.

Security granularity for any AD user or AD group can be set at the following levels:

* SQL Instance
  + Define access to connect to the SQL Instance
* Database
  + Define access to connect to and access the database, inside of a SQL Instance
* Table
  + Define access to a specific table inside a database, inside of a SQL Instance
* Column
  + Define access to a specific column, inside of a database, inside of a SQL Instance

Permissions can also be defined on an exception basis. This would be where a certain security context, such as an AD user, can do a specific broad action like reading a database. The same AD user can have permissions revoked on a child item of the database, like and accounts table.

In this manner nested security exceptions can be applied to child items.

# Schedule: List of Application databases

The List of Application databases will be used as the source of databases for the establishment of availability groups. All recovery models will be changed to full if not already.

|  |  |
| --- | --- |
| Server | DBName |
| GROUPBYSQL1 | TESTDATA |
| GROUPBYSQL1 | CTX\_IMA |
| GROUPBYSQL1 | CTX-XA6 |

The following system databases on SQL1 will not be migrated, but any specific sql objects such as logins, configuration info and scheduled jobs will be where applicable.

|  |  |
| --- | --- |
| Server | Database |
| GROUPBYSQL1 | distribution |
| GROUPBYSQL1 | master |
| GROUPBYSQL1 | msdb |
| GROUPBYSQL1 | tempdb |
| GROUPBYSQL1 | model |