|  |
| --- |
| MMC - Database SERVICES  Automated Database Deployment    February 2021  V 5.0 |

**Document Control**

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Number** | **Author** | **Revision Date**  **(mm/dd/yyyy)** | **Revision Description** |
| 1 | Hema Mutreja | 02/02/2021 | Initial Draft |
| 2 | Hema Mutreja | 04/02/2021 | Scope discussions |
| 3 | Hema Mutreja | 09/02/2021 | Updates to SQL Server and MongoDB approved and restricted actions. |
| 4 | Hema Mutreja | 08/03/2021 | Final version updates |
| 5 | Hema Mutreja | 17/03/2021 | Updates for Postgres and MS SQL |
| 6 | Hema Mutreja | 23/02/2021 | Added Approval details |
| 7 | Hema Mutreja | 15/09/2021 | Updates to permissions to incorporate automated backups |

Contents

1. Overview - 1 -

* Scope - 1 -
* Audience - 1 -
* DevOps and Automated Database Deployment - 1 -

1. Assumptions - 2 -
2. Scope - 3 -

* Approved Activities - 3 -
* Restricted Actions - 3 -

1. Stakeholders - 4 -
2. Reporting and Auditing - 5 -
3. Appendix - 6 -

* ORACLE - 6 -
* MS SQL Server - 8 -
* PostgreSQL - 11 -
* MySQL - 14 -
* DB2 - 15 -
* MongoDB - 15 -

1. Glossary - 17 -
2. Approvals - 18 -

# Overview

## Scope

The scope is to define the process and data elements for the automated database deployment for user applications, irrespective of the technology. Out of scope of this document is technology specific solutions to implement release pipeline and DBA actions that can be automated using a release pipeline.

## Audience

This document is intended for the Database Services team, the release management team, application development team for inclusion in Continuous Deployment and want to understand allowed & restricted actions under automated deployment.

## DevOps and Automated Database Deployment

DevOps – A combination of Development (Dev) and Operations (Ops) aims to bring the teams out of their respective role silos and collaborate as one unit for better, efficient and reliable software delivery in shorter cycles. The companies are able to adapt to new emerging scenarios, respond to changing customer needs with increased reliability and achieve business goals.

Database Release pipeline is focused on improving the efficiency of database management. It helps with streamlining the process of deploying and improving databases by giving the ability to automate many aspects of the database lifecycle, thus speeding them up and simplifying them.

Automation is suitable where there is a standard repeatable number of changes.

2

# Assumptions

This document is based on certain assumptions:

1. The application team ensures that the same code must progress from the lowest available environment to production. When there are any changes required mid cycle, it must go back to the lowest environment and follow the same cycle before moving to the next available higher environment.
2. The database code should comply with the respective technology coding standards.
3. It is responsibility of the application team to get the application approved for release management via CD.
4. The responsibility of reviewing and approving the database code to be deployed lies with the application team as per the approval matrix defined for the application in question.
5. All deployments must have a verified rollback plan in place that can automatically run or manually triggered by the application team in case of any issues.
6. If a deployment requires a manual DBA intervention, that DBA intervention should be catered via a separate Change Order outside of the release pipeline with the correct category and lead time.
7. The validations on the deployment packet needs to ensure that actions listed below are not a part of any deployment packet and do not hit the release pipeline:
   1. Extracting data via SELECT\find statement without a supporting statement which is using that data.
   2. Any cross database\schema reference which could lead to situations where the code change in one database unintentionally causes changes to another database. This could lead to:
      1. Potential security breach if the application contains PII data.
      2. Potential outage or negative performance impact for the affected application.

3

# Scope

## Approved Activities

Below is the high-level categorization of the approved actions for automated deployment via release pipeline:

|  |  |
| --- | --- |
| **Category** | **Comments** |
| DDL Commands on User DB Objects | These actions are database objects only in a User database. For example: working with tables, views, functions, triggers etc. |
| DML statements | These actions are any Data Manipulation statements which affect the state of data. For example: Insert, update & Delete.  This also includes Migration scripts. |
| DCL statements | These actions include commands such as GRANT and REVOKE on a DB object to an existing role or user. |
| Instance Level access | This is to enable the Pipeline to trigger the application specific database backup process. |

For a detailed list refer to [Appendix](#_Appendix) section of the document.

## Restricted Actions

Below is the high-level categorization of the restricted actions for automated deployment via release pipeline:

|  |  |
| --- | --- |
| **Category** | **Activity** |
| Infrastructure Changes | Any action that affects the Infrastructure |
|  | Any action at the Server Instance level |
| Database Changes | Any action that affects the database level settings. For Example: Creating new databases, adding a data or a log file to the database etc. |
| Changes to HA features | Any action that affects the HA solution implemented for the database in question. |
| Database Backup and recovery | Any Database Backup and restore commands. |
| Changes to System databases | Any action that affectes the funcationality of system databases, moving their files. |
| Security | Any actions on logins or users |
| SSIS | Deploy\delete SSIS packages. |
| Scheduled jobs | Any action that updates the scheduled jobs |

For a detailed list refer to [Appendix](#_Appendix) section of the document.

4

# Stakeholders

The stakeholders for automated database deployment include:

* Database Services Team
* Application Development Team
* Release Management Team
* Change Management Team
* MMC Common Tech Stack Ops Team

5

# Reporting and Auditing

As of writing of this document, there are no changes to the data being captured in the AuditDB framework.

All the actions done by the automated framework need to be captured in a format that is available for on Demand reporting.

The information to be captured should include, but not restricted to:

* Workflow details
* Submitter
* Approver
* Date\Time of deployment
* Execution logs
* Change order/Ticket Number

6

# Appendix

This section is an extension of the scope and lists the complete list of approved and restricted actions via automated database deployment by Database technology.

By default, any action not specified in the below section should be considered as Restricted unless and otherwise specified as approved.

## ORACLE

In Oracle every user who can connect to the database have their own schema. For Automated deployments on Oracle DB, we need to ensure:

1. There should be a separate account for each application for their respective app code deployment. This will help mitigate the risk associated with a common account in case of shared databases.
2. This account should have to access to make code changes only on application related schemas and should not have any access to user or DBA related schemas.
3. Under Oracle 19c new database feature PDB\CDB are being introduced, under which the privileges will need to be controlled at PDB level.

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **DDL - User DB Objects** | Create\alter\drop table | This is allowed only within the application schema. No changes allowed to user\DBA specific schemas. |
|  | Create\alter\drop constraint |  |
|  | Create(replace)\alter\drop user defined procedure |  |
|  | Create(replace)\alter\drop user defined function |  |
|  | Create(replace)\alter\drop view |  |
|  | Create(replace)\alter\drop synonyms | Applicable only to Private synonyms. |
|  | Create(replace)\alter\drop user defined type |  |
|  | Create\alter\drop index |  |
|  | Create(replace)\alter\drop package |  |
|  | Create(replace)\alter\drop DDL and DML triggers |  |
|  | Create(replace)\alter\drop Sequence |  |
|  | Create(replace)\alter\drop Materialized Log |  |
|  | Create(replace)\alter\drop\Refresh Materialized view |  |
|  | Create\alter\drop Table Partitions |  |
|  | Create Java |  |
|  | Compile user defined Stored Procedures and Functions |  |
|  | Truncate Table |  |
| **DML** | Insert \ Update \ Delete \ Merge |  |
| **DCL** | Grant\Revoke permissions on a DB object to an existing role\user. \* | The account using which the deployment will happen should have privilege to grant permissions |
|  | Grant\Revoke application role to a user. \* | The account using which the deployment will happen should have privilege to grant permissions |
|  | Alter Roles | These are application-based database level roles. |

### Restricted Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **Infrastructure\Database** | Any Database Configuration settings | For example: Alter System |
|  | Changes to DB Link | Create\Drop DB link |
|  | Logon Triggers | Requires higher level of access. |
|  | Create\Drop Database |  |
|  | Add files to a database |  |
|  | Backup Database\Log |  |
|  | Restore Database\Log |  |
| **DDL** | Drop Java |  |
| **DML** | Select Statement | Extracting data via SELECT statement without a supporting statement which is using that data.  \*Refer to Section 2 Assumption |
| **DCL** | Create\Alter\Drop Users |  |
|  | Create\Drop Roles |  |
|  | Create Any\* | Example: Create Any Index, Create Any Procedure etc. |

## MS SQL Server

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **DDL - User DB Objects** | Create\alter\drop\Rename table | The user will need to be added to db\_ddladmin fixed database role. |
|  | Create\alter\drop\Rename constraint\* | Make sure the changes do not impact HA features. |
|  | Create\alter\drop\Rename user defined procedure | The user will need to be added to db\_ddladmin fixed database role. |
|  | Create\alter\drop\Rename user defined function | The user will need to be added to db\_ddladmin fixed database role. |
|  | Create\alter\drop\Rename view | The user will need to be added to db\_ddladmin fixed database role. |
|  | Create\alter\drop\Rename synonyms | The user will need to be added to db\_ddladmin fixed database role. |
|  | Create\alter\drop\Rename ud data type | Control, execute and View Definition on schema\_name |
|  | Create\alter\drop\Rename index\* | Make sure the changes do not impact HA features.  The user will need to be added to db\_ddladmin fixed database role. |
|  | Create/drop/alter DML triggers |  |
|  | Create\alter\drop Partition function and Partition Scheme | The user will need to be added to db\_ddladmin fixed database role. |
|  | Truncate Table |  |
| **DML** | Insert\Update\Delete | db\_datareader\db\_datawriter, execute |
| **DCL** | Grant\deny permissions on a DB object to an existing role\user.\* | SecurityAdmin will NOT be granted. The account using which the deployment will happen should have privilege to grant permissions |
|  | Grant\deny application role to a user.\* | SecurityAdmin will NOT be granted. The account using which the deployment will happen should have privilege to grant permissions |
|  | Create\Alter\Drop user Application roles | These are application based database level roles. |
| Instance Level Access | Run a SQL Agent job owned by CD Service account | To enable automated backups for the application in question. The owner of the job would be the CD Service account for internal servers & SSP Service account for DMZ servers.  Access on msdb will be required to trigger the specific job and check the status.  db\_backupoperator, db\_datareader, SQLAgentReaderRole, SQLAgentUserRole |

### Restricted Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **Infrastructure** | Instance Configuration changes | Sp\_configure, like memory changes, xp\_cmdshell, Database mail. |
|  | Linked Servers | Creating or updates to linked Servers |
|  | Changes to Service state |  |
|  | Changes to DDL & Logon Triggers | DDL triggers requires CONTROL SERVER Permission |
|  | Changes to Instance level Encryption Keys |  |
|  | Changes to AVAILABILITY GROUP |  |
|  | Create\Alter Endpoints |  |
|  | Create\Alter Events |  |
|  | Create\Alter Audits |  |
|  | Changes to DAC settings |  |
|  | Changes to Resource Governor |  |
|  | ALTER TRACE |  |
|  | ALTER Settings | Example: Filestream, AlwaysOn |
| **Database** | Create\Alter\Drop\Rename Database | Sp\_renamedb |
|  | Changes to File group to a database | Add, remove file groups |
|  | Changes to files to a database | Add, remove, and shrink files.  Changes to auto growth settings |
|  | Change of database state | Read-only, offline, online |
|  | Backup Database\Log | Any kinds of backups |
|  | Restore Database\Log |  |
|  | Changes to system databases | Master, msdb, model, tempdb, distribution, SSISDB |
|  | Changes to HA configurations | Replication settings, log shipping etc |
|  | Changes to system DB objects with in a user DB |  |
|  | Changes to Database Settings | Examples: Service Broker, Filestream, trustworthy etc. |
|  | DB\_Owner privileges | Database Owner privileges to the Automation Login |
| DCL\Security | Create\Alter\Drop Logins |  |
|  | Create\Alter\Drop Users |  |
|  | Create\Drop Server Roles |  |
|  | Grant\Deny system permissions |  |
|  | Grant\deny a system role to a user | Grant sysadmin, SecurityAdmin or any other system roles to a user. |
|  | Grant\deny a non-application database role to a user | Grant dbowner, db\_datareader or any other database roles to a user. |
|  | IMPERSONATE ANY LOGIN \ EXECUTE AS | Assess the permissions and the practicality of restricting this. |
|  | Changes to Database Keys |  |
|  | Alter Credentials |  |
|  | Create\Alter Proxy |  |
|  | Changes to Certificates |  |
|  | Take Ownership |  |
| **DML** | Select Statement | Extracting data via SELECT statement without a supporting statement which is using that data.  \*Refer to Section 2 Assumption |
| SSIS Packages | Deploy SSIS packages |  |
| Scheduled jobs | Create\alter\drop SQL Server Agent Jobs |  |

## PostgreSQL

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **DDL - User DB Objects** | Create\alter\drop table | This is allowed only within the application schema. No changes allowed to user\DBA specific schemas. |
|  | Create\alter\drop constraint |  |
|  | Create(replace)\alter\drop user defined procedure |  |
|  | Create(replace)\alter\drop user defined function |  |
|  | Create(replace)\alter\drop view |  |
|  | Create(replace)\alter\drop synonyms | Applicable only to Private synonyms. |
|  | Create(replace)\alter\drop user defined type |  |
|  | Create\alter\drop index |  |
|  | Create(replace)\alter\drop package |  |
|  | Create(replace)\alter\drop DDL and DML triggers |  |
|  | Create(replace)\alter\drop Sequence |  |
|  | Create(replace)\alter\drop Materialized Log |  |
|  | Create(replace)\alter\drop\Refresh Materialized view |  |
|  | Create\alter\drop Table Partitions |  |
|  | Create Java |  |
|  | Compile user defined Stored Procedures and Functions |  |
|  | Truncate Table |  |
| **DML** | Insert \ Update \ Delete \ Merge |  |
| **DCL** | Grant\Revoke permissions on a DB object to an existing role\user. \* | The account using which the deployment will happen should have privilege to grant permissions |
|  | Grant\Revoke application role to a user. \* | The account using which the deployment will happen should have privilege to grant permissions |
|  | Alter Roles | These are application-based database level roles. |

***Restricted Actions***

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **Infrastructure\Database** | Any Database Configuration settings | For example: Alter System |
|  | Changes to DB Link | Create\Drop DB link |
|  | Logon Triggers | Requires higher level of access. |
|  | Create\Drop Database |  |
|  | Add files to a database |  |
|  | Backup Database\Log |  |
|  | Restore Database\Log |  |
| **DDL** | Drop Java |  |
| **DML** | Select Statement | Extracting data via SELECT statement without a supporting statement which is using that data.  \*Refer to Section 2 Assumption |
| **DCL** | Create\Alter\Drop Users |  |
|  | Create\Drop Roles |  |
|  | Create Any\* | Example: Create Any Index, Create Any Procedure etc. |

## MySQL

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| DDL - User DB Objects | Create\alter\drop table |  |
|  | Create\alter\drop constraint |  |
|  | Create\replace\alter\drop user defined procedure |  |
|  | Create\replace\alter\drop user defined function |  |
|  | Create\replace\alter\drop view |  |
|  | Create\alter\drop table partitions |  |
| DML statements | Insert\Update\Delete |  |
|  | Migration Scripts |  |
| DCL | Grant\deny permissions on a DB object to an existing role\user. |  |

### Restricted Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **DML** | Select Statement | Extracting data via SELECT statement without a supporting statement which is using that data.  \*Refer to Section 2 Assumption |
|  |  |  |

## DB2

Under current implementation, there isn’t a concept of LDAP when working with DB2. The user needs to have a local login on the server to be able to connect and work with database.

***Note:*** *the current volumn of deployment changes for DB2 is very low.*

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| DDL - User DB Objects |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Restricted Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| **DML** | Select Statement | Extracting data via SELECT statement without a supporting statement which is using that data.  \*Refer to Section 2 Assumption |
|  |  |  |

## MongoDB

This is a NoSQL Database, where an instance is created by the DB Services team, a mapping of the database name and the respective role is done by the DBA. The database is created when a connection is made by the application or a user to create collections under the respective database.

### Approved Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| DDL - User DB Objects | collStats |  |
|  | convertToCapped |  |
|  | createCollection |  |
|  | dbHash |  |
|  | dbStats |  |
|  | dropCollection |  |
|  | createIndex |  |
|  | dropIndex |  |
|  | listIndexes |  |
|  | listCollections |  |
|  | renameCollectionSameDB |  |
| DML statements | Insert\Update\Delete |  |

### Restricted Actions

|  |  |  |
| --- | --- | --- |
| **Category** | **Action** | **Comments** |
| Infrastructure | Role & DB mapping |  |
|  | Changes to Sharding |  |
|  | Cluster Management |  |
|  | Changes to Replication |  |
| Database | Backup Database |  |
|  | Restore Database |  |
| Management | User Management |  |
| DDL | killCursors |  |

7

# Glossary

CI – Continuous Integration

CD – Continuous Delivery

DDL – Data Definition Language

DML – Data Manipulation Language

DCL – Data Control Language

8

# Approvals

Below is a record of sign off received for the DB release Scope.

|  |  |  |
| --- | --- | --- |
| **Technology** | **Approval Date (mm/dd/yyyy)** | **Approval by** |
| Oracle | 03/09/2021 | Aejaz Khan |
| PostgreSQL | 03/17/2021 | Sanjeeb Parida |
| MongoDB | 03/17/2021 | Tony Thomas, Anil Singh |
| Audit | 03/17/2021 | Leeland Krueger |
| MS SQL | 03/18/2021 | Jennifer Champagne |