Telestream

DIVA

# Database and Backup Service Installation, Configuration, and Operations Guide

**Release: 9.0**

**Revision: 1.0**

**January 9, 2024**

2401091215

# Copyrights and Trademark Notices

# Contents

# Telestream Contact Information

To obtain product information, technical support, or provide comments on this guide, contact us using our web site, email, or phone number as listed below.

| Resource | Contact Information |
|---|---|
| DIVA Technical Support | Web Site:<br>https://www.telestream.net/telestream-support/<br>Depending on the problem severity, we will respond to your request within 24 business hours. For P1, we will respond within 1 hour. Please see the Maintenance & Support Guide for these definitions.<br>• Support hours for customers are Monday - Friday, 7am - 6pm local time.<br>• P1 issues for customers are 24/7. |
| Telestream, LLC | Web Site: www.telestream.net<br>Sales and Marketing Email: info@telestream.net<br>Telestream, LLC<br>848 Gold Flat Road, Suite 1<br>Nevada City, CA USA 95959 |
| International Distributor Support | Web Site: www.telestream.net<br>See the Telestream Web site for your regional authorized Telestream distributor. |
| Telestream Technical Writers | Email: techwriter@telestream.net<br>Share comments about this or other Telestream documents. |

# Preface

This book describes the installation, configuration, and operations of the DIVA database and Backup Service (often referred to simply as BKS). This guides is written with the assumption that the reader/operator has a working knowledge of Windows and related DIVA concepts.

## Audience

This document is intended for the Installation Team and System Administrators.

## Documentation Accessibility

For information about our commitment to accessibility, visit the Support Portal located at https://www.telestream.net/telestream-support/.

## Related Documents

For more information, see the DIVA documentation set for this release located at:

https://www.telestream.net/telestream-support/

# Document Updates

The following table identifies updates made to this document.

| Date | Update |
|---|---|
| October 2022 | Created standalone book for 9.0 release. |
| January 2023 | • Updated copyrights.<br>• Updated BKS and DBAgent configuration files. |
| February 2023 | Replaced Oracle DB instructions with Postgres DB instructions. |
| March 2023 | Updated book from DIVA Core to Content Manager. |
| May 2023 | Updated System Management App name to Web App. |
| June 2023 | Updated sample configuration files and sent for review. |
| September 2023 | Update Content Manager to DIVA.<br>Publish version 9.0 PDF. |
| January 2024 | Update DIVA to DIVA.<br>Publish version 9.0 PDF. |

# Overview

## Database Overview

DIVA is bundled with a Postgres database. The database stores all information relating to the DIVA system including its configuration. SQL queries used by DIVA are optimized to support configurations with up to 58 million components.

The JDBC Thin Driver enables replacing the Oracle SID setting with the Oracle Service Name.

When installing DIVA in a 64-bit environment, the latest 64-bit DIVA Postgres 14 release must be installed to use 64-bit support.

DIVA supports Postgres 14 or greater.

The database is not intended to be modified directly by customers; direct modification of this database by customers is not supported.

**Note:** This release is a Windows-only release and does not include a Linux release.

## BKS (DIVA Backup Service)

The Backup Service (BKS) ensures reliability and monitoring of both the DIVA database and Metadata Database backups.

The BKS component is installed as an integral part of the standard DIVA system installation. The component is typically installed on the same server as the Manager and DIVA database. BKS enables configuration of scheduled backups through its configuration file, and manages and monitors the entire backup process.

# Database Installation and Configuration

## Topics

# Overview

At the system level, settings that relate to the overall operation of each DIVA component and their interaction are configured and retained by a DIVA database. This is commonly known (and will be referred to in this document) as the DIVA database (or just simply as the database).

User modification of this database is performed through the web app. It is only intended for experienced users and caution should be exercised when altering settings. An incorrect setting can impede DIVA operations or prevent the Manager from starting successfully. Contact Technical Support for assistance if unsure about making a particular change.

When launched, the Manager obtains the DIVA system configuration from the database. However, it does not poll the database for changes made through the web app. Therefore, the Manager must be notified of any changes made. This is performed using the Notify Manager button (a check mark inside a circle on the top right) in the web app.

Most changes to the configuration can be completed while the Manager is running. There are a small number of configuration changes that require a restart of the Manager to become effective.

---

**Note:** Refer to the DIVA Installation and Configuration Guide for a full list of changes that can be made to the system configuration dynamically while the Manager is running.

---

The web app also does not dynamically poll the database for changes that are made when the Manager is running. In such cases, click the Refresh button on the page where the changes were completed to refresh the information displayed from the database.

The web app can be installed on any computer that has TCP/IP connectivity to the database and a supported Java Runtime Environment installed. DIVA release 9.0 requires the Java Runtime Environment 64-bit (build 1.8.1_45-b14), to be installed to launch the web app successfully.

In some cases, a network firewall between the two can prevent a connection. For complete operation and functionality of the web app, the Database Listener Port (typically 5432) and the Core Robot Manager Ports (typically 8500 and higher) must be opened in the firewall. Full functionality of the web app also requires that the Manager Port (typically 9000) is open.

DIVA uses a Metadata Database to support Complex Object workflows. The DIVA Backup Service ensures reliability and monitoring of both the DIVA database backups and Metadata Database backups. Refer to the DIVA Installation and Configuration Guide for details on the Metadata Database.

The information stored in the DIVA database is already stored on a RAID-1 array and is not subject to data loss if a single disk fails.

**Note:** See the DIVA Supported Environments Guide to confirm disk partitioning and recommended block sizes before proceeding.

## Prerequisites

The Postgres database has these minimum requirements:

- Windows 2016 or higher
- 16 GB of RAM

See the DIVA Supported Environments for details on server configuration requirements.

## Complex Objects

By default, Objects archived with more than 1,000 files are considered Complex Objects. Complex Objects have metadata stored in both the DIVA database and Metadata Database. Configure the threshold on the number of files before an object is considered complex in the Manager service configuration file. Complex Objects can only be stored in AXF format within the DIVA system. The DIVA BKS must be used to back up the DIVA database and Metadata Database when Complex Object workflows are used. Refer to the DIVA Installation and Configuration Guide for details on the Metadata Database.

# Installing, Upgrading, and Configuring the DIVA Database

These are the general DIVA and Database upgrade processes.

## Exporting the Database Dump Files

The initial DIVA release does not contain a process to export database dump files from the Oracle database used in previous releases.

## Importing the Database Dump Files

The initial DIVA release does not contain a process to import database dump files from the Oracle database used in previous releases into the Postgres database.

## Uninstalling the DIVA Database Server (if required)

Before installing the new Postgres Database, it is required to uninstall the existing database and database engine. If the DIVA database is already installed on the computer, then the existing database and database engine must be removed.

### Uninstalling the DIVA Database Server in Windows

Use the following procedure to uninstall the existing database in Windows environments:

---

**Caution: Use the same DIVA Database package to uninstall the database that was used to install it.**

---

1. Stop all running DIVA services.
2. Export the existing database contents using the procedures previously described.

---

**Caution: Confirm the export completed successfully before continuing.**

---

3. Extract the original database ZIP file used to perform the installation.
4. For DIVA Database package releases 2.3.4 and earlier, use the following commands in Oracle Bundle ISO mount point \Tools\uninstall subdirectory in the exact sequence shown:

   ```
   uninstall_database.cmd
   uninstall_engine.cmd
   ```

5. For DIVA Database packages release 3.0.0 and later, execute *C:\app\Oracle\product\12.1.0\db_home1\deinstall\deinstall.bat* and follow the displayed instructions.

# Installing the DIVA Database Server in Windows

Log in to the computer as an Administrator. After having backed up and uninstalled the existing database (see the previous sections), use the following procedure to install the new database:

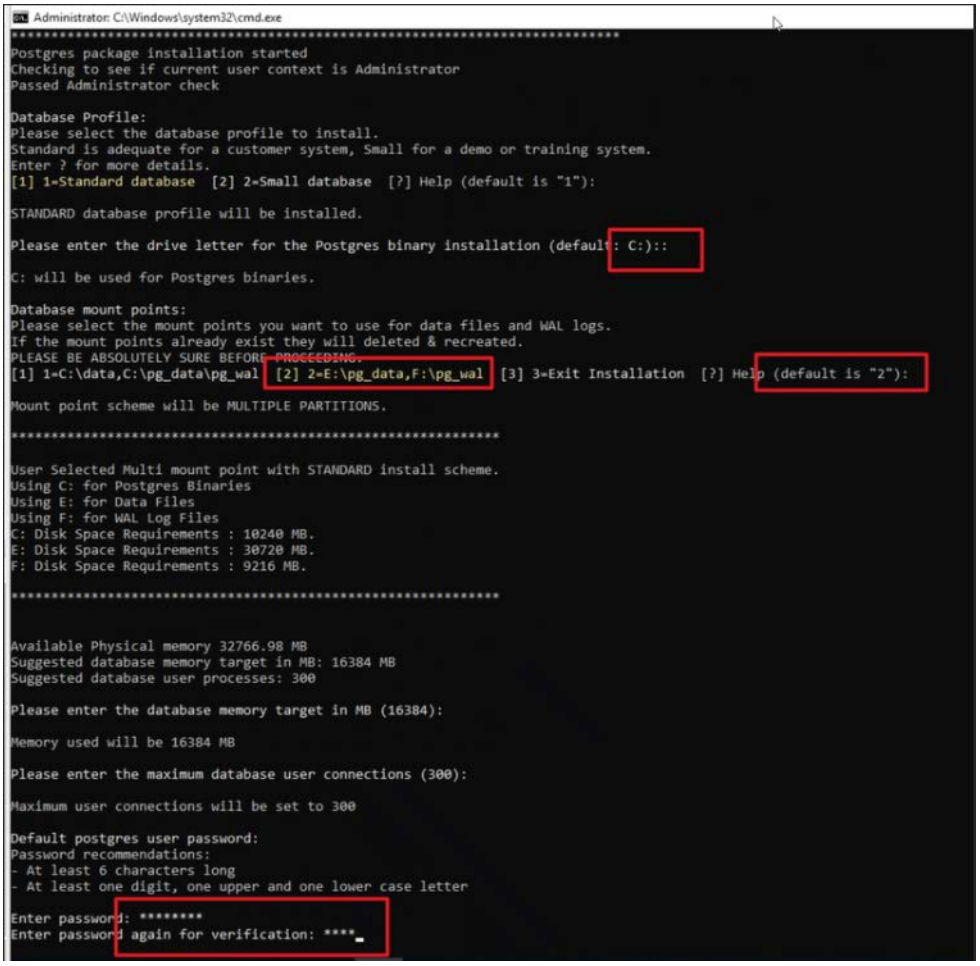
---

**Note:** The Postgres installer is not included in the initial DIVA release and must be installed separately

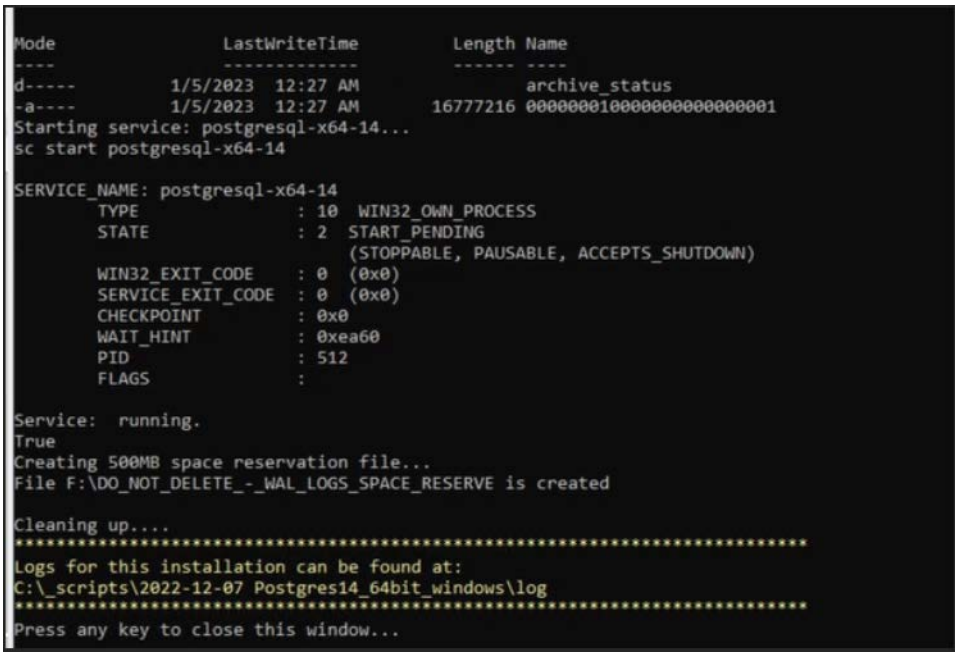
---

1. Open a Windows command line.
2. Navigate to %TSCM_HOME%\Releases\16_Postgres_Bundles.
3. Locate the Postgres zip file and unzip it.
4. Execute *install.bat*.
5. Select option 1—Standard Database, or leave this blank.
6. Enter the drive letter to install the binary files. The default and recommended drive is C:.
7. Select option 2 (`2 = E:\pg_data, F:\pg_wall`) under Database Mount Points. This is the default and recommended setting.
8. Leave the Database Memory Target at the default (16384 MB).
9. Leave Suggested Database User Processes at the default (300).
10. Set the Postgres User Password, then confirm the password that was entered. Telestream recommends the standard Postgres password of *`postgres`*.

**11.** Press ENTER to execute the installation.



**12.** When the installation has completed the results are displayed. After confirming the installation was completed successfully, the Command window can be closed.




## Postgres Administration App

**Note:** Telestream recommends that this application is only used along with assistance from Telestream Technical Support. Do not attempt to access or make any changes to the database directly.

Postgres is delivered with and administration app called `pgAdmin4.exe`. The app is located in the `C:\Program Files\PostgreSQL\pgAdmin4\bin` directory.

The first time pgAdmin4 is executed it requests creating a master password. Telestream recommends using the password *`MANAGER`*.

Next the app will request the password to connect to the database. Use the password set when installing the database (`postgres`).

## Manually Creating the Database User and Schema

The database user must be created using the DIVA operating system user account. Use the following procedure to create the database user:

1. Open a terminal console.
2. Change to the %TSCM_HOME%/Program/Database/Diva/Install directory.

3. Execute *create_diva_user.bat* (Windows), which creates the given DIVA database user and its associated tables

   Usage:

```
create_diva_user syspasswd username userpasswd
postgres_connection [-useronly|-tablesonly] [-
custom_tablespaces tables_tablespace indexes_tablespace
temp_tablespace]

create_diva_user {DIVA|SYS} current_password new_password [-
postgrespwd]
```

| Parameter | Definition |
|---|---|
| `syspasswd` | Password of the Postgres sys account. |
| `username` | Username to create |
| `userpasswd` | Associated user password |
| `postgres_connection` | Postgres service name or connection string (such as IP_ADDRESS:PORT/POSTGRES_SERVICE_NAME). |
| `DIVA\|SYS` | Use either TSCM or SYS to reset the respective password in the password file. |
| `new_password` | New password |
| `current_password` | If there is no current database password, then enter the new password for this parameter. |
| `-useronly` | Only creates the database user and no database objects. |
| `-tablesonly` | Only creates the database objects for the given user. |
| `-custom_tablespaces` | • Use of custom tablespaces<br>- `tables_tablespace`: tablespace for tables<br>- `indexes_tablespace`: tablespaces for indexes<br>- `temp_tablespace`: database temp tablespace |
| `-postgrespwd` | Option to reset/generate password file. |

# Secure Communications with DIVA Database

See the DIVA Security Guide for detailed information on secure communications with the database.

# Migrating DIVA Database Server from 11.2 to 12.1

The initial DIVA release does not contain a process to migrate from the Oracle database used in previous releases to Postgres database.

# Operations

Open the DIVA web app in a browser. The app will connect to the DIVA database upon login and the dashboard is displayed. The dashboard displays initial information about the status of the DIVA system.

On the top right of the page is a status indicator with a pull-down arrow and a colored circle. The color of the circle gives the user a quick view of the system status (green, yellow, or red). Using the pull-down arrow displays more detailed information about system components and their status.

Users can continue with normal operations after the dashboard is displayed, or work to resolve issues shown in the status pull-down box if required.

Contact Telestream Support if the app still cannot connect after attempting to resolve the error.

To disconnect the web app from the database when not in use, log out of the app and close the browser.

# BKS Installation and Configuration

This chapter provides an overview of BKS, its functionality and operation. It also describes installation and configuration, along with managerial topics.

## Topics

# BKS Overview

The DIVA Backup Service is referred to as BKS throughout this guide. It ensures reliability and monitoring of both the DIVA database and Metadata Database backups. The DIVA Backup Service enables configuration of scheduled backups through its configuration file. BKS manages and monitors the entire backup process.

The backup service as a whole is comprised of two types of services, DIVA Backup Service (BKS) and one or more DBAgents. Both services have REST APIs such that they can be integrated with a UI component. The main backup service controls command execution, DIVA archives, synchronization, and configuration. Each database implementation is in managed code and a minimal amount of scripting is utilized to future proof the solution. Backup configurations are also agnostic of the data contained within them so that the solution can be applied to any type of application database desired to be backed up assuming the routines to do so are implemented.

---

**Caution: The BKS is required when using Complex Objects. BKS is the only component backing up the Metadata Database and removing outdated Metadata files. When a Delete job for a Complex Object is sent and processed, the data is removed from the DIVA database, but the Metadata Database file is not deleted. It is removed by the backup service after the configured clean up period (defined by the Recovery Period parameter) has been reached. Users should have an elevated awareness of error messages from the backup service.**

---

Many replication locations may be configured through the BKS. These locations can be a local path or a UNC path, however the primary backup location must be local as it is used as the source of replication to all other locations. Each location can be configured with a URL to the DBAgent endpoint for that location. This is only necessary if that location is managing a remote database, in which case the database should be listed under the Managed Databases list. Any database in a Managed Database list will be part of the automated backup system and are eligible for restores or fail-overs.

A source name must be provided for any location that manages a database with DBAgent. This allows the BKS to make calls to DIVA to restore archived backups directly to the related database server for a restoration or fail-over to process.

---

**Notes:** The primary location must have the same source name that is provided in the Backup Settings section of the configuration file.
Configuration within DIVA must point to the base directory of the corresponding location.

---

One of the primary responsibilities of the BKS is to maintain a ledger of backups for each database it manages. These ledgers are located in the BKS log directory in the same folder structure the backups themselves. The default location is:

```
C:\DIVA\Program\log\backup_service\Ledgers\<Database type>\<Database profile>\Ledger.json
```

These ledgers can be queried through the API and are the primary reporting structure for the active backup or restoration state of a given database. If a ledger is lost or deleted, it will be automatically created on the restart of the BKS based off of the primary backup locations contents.

Each backup is check-summed through MD5 and logged in the database ledger for each database. After a backup occurs it is replicated across all of the backup locations. After replication, if configured to do so, an archive is made using a call to the DIVA API to persist the backups to tape storage. The source in DIVA is configured in the location itself under the Source Name parameter. The name of the Object will be `DatabaseBackups_<Unix timestamp of the archive>` and the Collection will be `Backups`. This only occurs after every full backup, after which a cleanup task will delete any archives that exceed the retention period.

If a database or system failure (or both) occurs, where restoring from a system backup is necessary, restoration of a stored backup is performed manually and should only be performed by Telestream Technical Support personnel.

DIVA database backups and Metadata Database backups are incrementally replicated to one or more remote back up systems by the DIVA Backup Service. depending on the configuration.

The backup service files are located in the %DIVA_HOME%\Program\conf\backup_service\appsettings.json folder.

See the *Appendix* for a sample BKS configuration file.

**Caution: Do not change the Metadata Location parameter when the system is running.**

# DBAgent

The DBAgent Service performs database specific tasks (that is, backups and restores), monitors their progress, and reports disk usage. Database maintenance functionality can easily be added if necessary, but only the specific backup tasks are currently implemented. Any number of DBAgents may be installed and configured, but only one per server/container. This is to support multi-server installations and automate access control. The DBAgent also exposes a REST API that the backup service will call to check the status of a backup, initiate backups/restores/fail-overs, and monitor disk space for configured mount points.

Configuration for the DBAgent is purposefully minimal with the only the space monitoring and backup location being required. The majority of the configuration resides in the BKS. By default, mount point configuration will monitor the backup location, the C, E, and F drives as expected by the default DIVA installation. These can be expanded to monitor other locations if necessary and can trigger alerts to DIVA when those locations are reaching their space thresholds.

A state file is created in the log directory of the DBAgent for a given database job. Backup job state files are stored in the BackupHistory directory, while respectively,

Restore job state files will be in the RestoreHistory directory. These files are actively updated as the backup or restore progresses to completion and are used to gather statuses about a given action. These state files include a full log of the action itself and any files that have been created as a result of the backup process.

See the *Appendix* for a sample BKS configuration file.

# Backup Initiator

A command line initiator is included in the bin installation folder. This program is a simple wrapper around the BKS API to perform backups, restores, and fail-overs. However it does not wait for their completion. It will offer four options when executed:

- Backup
- Restore
- Failover
- Quit

The user will select the related function to perform from the additional options as follows:

Backup

1. <Database 1 -x>
2. Back
3. Quit

Restore

1. <Database 1-x>
   a. <List of restore points 1-x>
   b. Back
   c. Quit
2. Back
3. Quit

Failover

1. <Eligible failover databases 1-x>
   a. X -> Y
      – <List of restore points 1-x>
      – Back
      – Quit
   b. Y -> X
   c. Back
   d. Quit
2. Back

3. Quit

# Workflows

The following subsections describe the BKS workflows.

## Archive Workflow

BKS will begin to archive backups after configuration is complete.

An archive consists of a full backup and all of the related incremental backups. Each of these files contains a Unix timestamp within their filename for the BKS to identify the correct files required to perform a restoration. The object created within DIVA will have a name that follows this format along with a fixed category/collection:

```
Object Name: <Name of the DB Profile>___<Unix timestamp>_to_<Unix timestamp>

Category/Collection: DB_BackupArchive
```

**Note:** Object Names cannot begin with a dollar sign ($).

This allows the BKS to identify a related archives range of times.

**Note:** Because an archive will need the entirety of its incremental backups to be present, an archive will not process until the next full backup is performed. This will create a lag time of one day using the default configuration; this could be longer depending on the configured full backup interval.

### Gold Archives

A gold archive is a permanent backup that is kept once per the `PermanentRetentionPeriod` in days.

These archives are saved per database and therefore could be at different intervals depending on when the database was configured and when backups commenced. It is recommended that if configuring multiple databases for a given application (for example, DIVA) that all configuration changes are made at the same time so that these Gold Archives for each database have a related timeframe.

### Archive Ledger

In order for BKS to keep track of what archives are available for restoration it keeps a ledger of every archived backup created. This ledger is copied to all backup locations and its contents are emailed if email notifications are setup in DIVA. The ledger is located in the <Location Path>\Backups\ArchiveLedger.json folder.

This ledger is automatically generated from DIVA if it does not exists, or is deleted, and will contain records for both regular archives and gold archives.

# Restore Workflow

In general, restoration is handled automatically when either a Restore or Failover job is made from the API or the Initiator.exe application. During this job the BKS performs the following steps:

1. Checks the managed backup files on a given backup location to determine if they can satisfy the job.
2. Next, BKS checks archive restoration directory to determine if there are files there that will satisfy the job.

   `<Location Path>\Restore\FromArchive\…`
3. If not, BKS checks the archive ledger to determine if any archive on the list can be restored to the above location for the job to proceed.

After the Restore or Failover job succeeds, the related files within the FromArchive directory are deleted. If the job fails for any reason, the files within this directory are preserved to attempt the action again.

## Manual Restoration

Manually placing the backup files within the FromArchive directory allows the previous restore process to be achieved manually without the job to DIVA. The files must be copied with the same relative paths that the archived object would restore them in. This is the same relative path that is contained within the Backups folder. The Backups folder contents can be copied to this directory from another system to achieve the same result.

---

**Note:** The FromArchive directory is not monitored by any process and will only be cleaned up upon the successful completion of a Restore or Failover job; this way, it can hold old backups that would normally be removed by the retention window.

---

# DIVA Database

By default, the DIVA Backup Service generates a full database backup every 24 hours, and an incremental backup every 15 minutes. The backup files are compressed with 7zip tool with the .gz extension. See *Prerequisites* for details.

# Core Metadata Database

The Metadata Database is a binary file in the file system. To support the Recovery Window for the Metadata Database, the DIVA Backup Service uses the following techniques:

- Whenever a new Complex Object is archived, the Manager creates Complex Object Metadata files in the Metadata Database Path configured in the web app.
- By default, the DIVA Backup Service backs up metadata files inside the Metadata Database every 15 minutes. The metadata file is transferred to all backup systems shortly after creation so that file alterations do not influence the backup copies.

---

**Note:** If there is a failure backing up to one of the configured backup systems, the backup service will continue to retry the failed backup until all backups to all configured backup systems are successful. Metadata files are not marked as being successfully backed up until the backup to all configured backup systems is successful.

---

- During every Metadata Database backup, the backup service searches for any Complex Object metadata files that are not backed up, and replicates them to all of the FBM_BACKUP_REMOTE_DESTINATIONS configured in the configuration file.

Technical Support recommends having the same Metadata Database Location on all main and remote backup target servers. For example, if the Metadata Database Location is set to H:\metaback\, on the main system, the backup service must copy the Metadata Database backups to the same location on all remote backup target servers. If the paths are different, the Metadata Database Location must be updated in the DIVA database after a database restore during fail-over. See *Database Service Failover* for more details.

# DIVA BKS Recommended Practices

The following are recommended practices for DIVA BKS:

- BKS must be installed on the same server as the Manager and DIVA database.
- At least two backup systems are always required to store backups. Actor computers can serve dual purposes and be used as both backup computers and Actor computers.
- Postgres incremental backups should be performed every 15 minutes.
- Metadata Database backups should be performed every 15 minutes.
- The Backup Recovery Window should be set to value greater than, or equal to, 10 days.
- The Backup Clean-up function should be performed every 24 hours.
- Postgres full backups should be performed every 24 hours.
- If required, restoration of a system backup must only be performed by Telestream Technical Support.
- DIVA database data files, database backups, and the Metadata Database must be stored on RAID disk array.
- Equal backup disk space must be allocated on the main and all remote backup systems.

# Installing and Configuring BKS

Use these procedures to install and configure BKS.

## Overview

BKS enables configuration of scheduled backups through its configuration file, and manages and monitors the entire backup process.

**Note:** It is **strictly required** to use the DIVA Backup Service when using Complex Objects.

The service uses existing DIVA backup scripts to generate full database backups, and incremental database backups of the DIVA database. Generated DIVA database backup files and Metadata Database files created by the Manager (when Complex Objects are created) are incrementally replicated by the backup service to remote backup servers.

## Installing the BKS Software

The BKS component is installed as an integral part of the standard DIVA system installation. The component must be installed on the same server as the Manager and DIVA database. Also, BKS does not support installation with the Manager and DIVA database installed on separate computers.

BKS must be configured to replicate files across multiple backup servers for redundancy. Therefore, the following systems must be identified before installation for successful use of BKS:

- Which computer is called Backup System 1 (required)
- Which computer is called Backup System 2 (required)
- Which additional computers are called Backup System additional_number. The additional_number identifies additional backup server numbering, for example Backup System 3, or Backup System 4. This is optional and only required to have more than two backup systems.
- Ensure the Database check box is selected on the Choose Components screen during DIVA installation to install BKS.

### Installing BKS and DBAgent

Use the following command-line interfaces to install BKS and DBAgent:

## Windows

- *backup_service.bat [command] [options]*

  Where command is one of the following:

  `install` (or `-i`)

  Installs the module as a system service.

  `-uninstall` (or `-u`)

  To remove the executable as a system service.

  `-start`

  Starts the module.

  `-stop`

  Stops the module if it is currently running.

  `-restart`

  Stops and subsequently starts the module.

  `-status`

  Determines whether the module is running.

  `-version` (or `-v`)

  Displays the module version information and exits.

  `-help` (or either `-h` or `-?`)

  Displays help information and exits.

  **Options:**

| Option | Description |
|---|---|
| `-log` | Path to log directory. Default: ..\..\log\backup_service |
| `-conf` | Path to configuration directory. Default: ..\..\conf\backup_service |
| `-httpport` | Port to listen for http connections. Default: 1876 |
| `-httpsport` | Port to listen for https connections. Default: 1877 |
| `-certpath` | Path to certificate located on disk. |
| `-user` | Username to install the service under. Blank entries will be installed as LocalSystem. |
| `-path` | Password for the provided user. |

- *db_agent.bat [command] [options]*

  Where command is one of the following:

  `install` (or `-i`)

  Installs the module as a system service.

`-uninstall` (or `-u`)

To remove the executable as a system service.

`-start`

Starts the module.

`-stop`

Stops the module if it is currently running.

`-restart`

Stops and subsequently starts the module.

`-status`

Determines whether the module is running.

`-version` (or `-v`)

Displays the module version information and exits.

`-help` (or either `-h` or `-?`)

Displays help information and exits.

**Options:**

| Option | Description |
|---|---|
| `-log` | Path to log directory. Default: ..\..\log\dbagent |
| `-conf` | Path to configuration directory. Default: ..\..\conf\dbagent |
| `-httpport` | Port to listen for http connections. Default: 1876 |
| `-httpsport` | Port to listen for https connections. Default: 1877 |
| `-certpath` | Path to certificate located on disk. |
| `-user` | Username to install the service under. Blank entries will be installed as LocalSystem. |
| `-path` | Password for the provided user. |

# Configuring BKS

The BKS configuration file is monitored to allow for live updating of the configuration through the API or by direct manipulation without requiring restarting the service. By default the configuration is located here:

`$DIVA_HOME\Program\conf\backup_service\appsettings.json`

This path can be modified during service installation. BKS contains all of the required information to connect to a database and passes that information on to the DBAgent when an action is required. The DBAgent itself also has a configuration, but it contains relatively few values.

The following are the relevant sections of the configuration file located as follows:

**Note:** All of the related settings can also be modified through the REST API.

## Backup Settings

The majority of the archive configuration is done within the Backup Settings configuration section. The number of days to keep a daily archive, the number of days between the creation of a gold backup (an archive that is stored in perpetuity), the name of the storage media, and the source in DIVA of the primary backup location can all be configured.

```
"DatabaseBackup": {
    "Enabled": false,
    "FullBackupInterval": {
      "ExecutionPeriod": "Daily",
      "TimeOfDay": "00:00:00",
      "InstancesInPeriod": [ 0 ]
    },
    "IncrementalPeriod": 15,
    "FullBackupFileRetention": 10,
    "FullBackupArchiveRetention": 30, <=== IN DAYS
    "ArchiveMediaGroup": "<some media, disk, or storage plan>",
<=== UPDATE
    "PermanentRetentionPeriod": 180, <=== IN DAYS
    "ArchiveSourceName": "<Source name for primary backup
location>", <=== UPDATE
    "BackupExecutionTimeout": 120,
    "RestoreExecutionTimeout": 120,
    "StatusPollingPeriod": 3,
    "StatusReportingInterval": 1440
  }
```

## DIVA API Settings

A valid API configuration must be provided for automatic archive, restoration, and events to be sent to DIVA. This can be configure in the DIVA Core API Settings section.

Typically, only the password must be added; although the URL may require updating if the Manager location is on a different system than the BKS.

```
"DIVACoreAPISettings": {
    "Url": " https://127.0.0.1:8765/",
    "User": "sysadmin",
    "Password": "changeit", <=== PASSWORD IS ENCRYPTED UPON BKS
STARTUP
    "TimeoutInMs": 20000
  }
```

See *Sample BKS Configuration File* in the appendix for a sample BKS configuration file.

The following parameters must be set in the web app's Manager Setting page. The Metadata Database file location must be set to an existing, valid location. The Manager uses this value to save the Metadata Database files. For example, F:\META_DATABASE_ROOT\.

## Complex Objects Metadata Database Location

This is the path to the Metadata Database. There is no default path specified. The path must exist, and is validated by the Manager and the backup service. A drive with ample storage must be used. See the DIVA Installation and Configuration Guide for information on calculating space requirements.

This parameter is not re-loadable and is only checked one time when the Manager and the backup service services start. If any changes to this parameter are made, the Manager and backup service must be restarted.

## Database Backup Notification

Select the desired notification level from the list as follows. The default setting is ERRORS AND WARNINGS. Connected web apps must be restarted if any changes are made to this parameter.

- ERRORS AND WARNINGS—Errors and warnings are recorded in the event log. This is the default setting.
- ERRORS—Errors and warnings are recorded in the event log.
- DISABLED—All of the errors and warnings are recorded in the event log.

## Enable Metadata Database Feature

The Manager can only archive Complex Objects and BKS can back up the Metadata Database only when this parameter is checked. When unchecked, Manager cannot archive Complex Objects and BKS cannot back up the database. This parameter must be left at the default (checked) setting.

This parameter is not reloadable and is only checked one time when the Manager and the backup service services start. The Manager and backup service services must be restarted if any changes are made to this parameter.

If the BACKUP_SERVICE_MANAGE_METADATA_BACKUPS is set to Y (indicating yes, or enabled) in the backup service configuration file, the values of Enable Metadata Database Feature and Complex Objects Metadata Database Location in the web app is validated when the backup service starts. If the Enable Metadata Database Feature parameter is set to N (indicating no, or disabled), or the Complex Objects Metadata Database Location is invalid, the backup service will fail to start.

The following values must be set on the Manager Setting page of the web app before starting the Manager and BKS services:

- DIVAMANAGER_HOST—Identifies the name of the computer where the Manager is installed. Default: localhost.
- DIVAMANAGER_PORT—Identifies the port number the Manager is listening on for connections. Default: 9000.
- SERVICE_NAME—Identifies the name of the Windows service. Default: DIVA Backup.

- SERVICE_PORT—Identifies the port number where the service is running. Default: 9300. This value must be changed if it conflicts with other services.
- DIVAMANAGER_DBHOST—Identifies the IP address of the database to connect to from the Manager.
- DIVAMANAGER_DBPORT—Identifies the port number of the database to connect to from the Manager. The DIVA database installation uses the default 5432 port number.
- DIVAMANAGER_DBUSER—Identifies the database username; typically diva.
- DIVAMANAGER_DBSID—Identifies the Database SID (typically lib5) to connect to from the Manager.
- BACKUP_SERVICE_MANAGE_DATABASE_BACKUPS—This parameter enables or disables backup of the DIVA database. Default: Y (indicating yes, or enabled).
- BACKUP_SERVICE_MANAGE_METADATA_BACKUPS—This parameter enables or disables backup of the Core Metadata Database. Default: N (indicating no, or disabled).
- CYGWIN_BIN_DIRECTORY—Identifies the location of the CYGWIN installation. The default is C:\cygwin\bin.
- DB_BACKUP_LOCATION—Identifies the location of the DIVA database backup files. The default location is H:/oraback/lib5.
- DB_BACKUP_REMOTE_DESTINATIONS—Identifies the location of the DIVA database remote backup destinations. All remote destinations must be a service module name, followed by a folder name. The backups must not be copied to the root of the module. Multiple destinations are allowed and must be delimited by commas.
- FULL_BACKUP_START_HOUR_24—Identifies the hour of day to perform a full database backup when the service is initially started. If the service is started later than the configured value, the full backup will occur at this hour on the following day. Default: midnight; 0 hours.
- FULL_BACKUP_START_MINUTE—Identifies the number of minutes after the FULL_BACKUP_START_HOUR_24 hour to start the full backup. Default: 0 minutes.
- FULL_BACKUP_FREQUENCY_HOURS—Identifies the frequency to execute a full backup of the database. Default: 24 hours.
- INCREMENTAL_FREQUENCY_MINUTES—Identifies the frequency to execute an incremental backup of the database. Default: every 15 minutes.

  The backup service will automatically determine if a full backup is required.

  If the FBM_FREQUENCY_MINUTES parameter is not set, then this value is also used to notify the Manager how often to expect a message from the DIVA BKS. If a message is not received by the Manager within the incremental minutes, all connected web apps are notified that the BKS may not be running. This event is then recorded in the event log. If the FBM_FREQUENCY_MINUTES is set, the backup service uses

the lowest parameter value to notify the Manager how often to expect a message from the BKS.

By default, the Manager expects a message from the backup service within 15 minutes after the start of the Manager service. After the backup service is started and connected to the Manager, the Manager expects a message within every INCREMENTAL_FREQUENCY_MINUTES, or FBM_FREQUENCY_MINUTES value identified in the backup service configuration file.

- FBM_FREQUENCY_MINUTES—Identifies the frequency to execute a Metadata Database backup to all remote metadata backup destinations. Default: every 15 minutes.

  If the INCREMENTAL_FREQUENCY_MINUTES parameter is set, the backup service uses the lowest parameter value to notify the Manager how often to expect a message from the backup service.

  A Metadata Database backup is executed when the services start.
- DB_FBM_RECOVERY_WINDOW_DAYS—Identifies the recovery window period for the DIVA database and Metadata Database. This value indicates how many days of backups must be retained. Obsolete backup copies are then deleted. The default is 10 days.

  The DIVA Backup Service sets this value using the RMANRecoveryWindow.bat file included in the DIVA Backup Service bin folder. If this batch file is missing the DIVA Backup Service will not start.
- CLEANUP_START_HOUR_24—Identifies the hour of the day for initial start of the backup service clean up process to delete the obsolete backup copies. Default: 2 (representing 2:00 AM).
- CLEANUP_START_MINUTE—Identifies the number of minutes after CLEANUP_START_HOUR_24 to start the clean up process. Default: 0 (representing the top of the hour).
- CLEANUP_FREQUENCY_HOURS—Identifies the frequency to run the clean up process. Default: every 24 hours.

See *Monitoring the DIVA BKS* for additional monitoring and notification options and configuration.

## Backup Interval Overrun

A Backup Interval Overrun occurs when a specific backup is taking a longer time to complete beyond the next scheduled iteration.

The following example is called a Backup Interval Overrun because the backup service must run the next incremental backup by 12:15 PM, but it cannot because the backup process started at 12:00 PM is still running.

1. The Incremental Backup is schedule to run every 15 minutes:

   ```
   INCREMENTAL_FREQUENCY_MINUTES = 15
   ```
2. The incremental backup starts at 12:00 PM and runs at the value set for the INCREMENTAL_FREQUENCY_MINUTES parameter; in this case every 15 minutes.

3. At 12:15 PM the incremental backup is incomplete and still running, causing a Backup Interval Overrun.

The DIVA Backup Service sends a Backup Timeout Warning to the Manager when a Backup Interval Overrun occurs. The Manager records the warning in the event log. If a Backup Timeout occurs three consecutive times, the timeout warning messages are elevated to an error message.

**IMPORTANT: Immediate and necessary action must be taken to modify the backup's frequency by updating the configuration file to avoid future Backup Interval Overrun occurrences**

**Note:** Updating the configuration file requires a backup service restart.

## Backup Service Running Normally

When the backup service is running, this information is displayed when you execute the `status` command:

- Running release of the service
- IP address and port the service is running on
- System statistics
- Operating system information
- Memory information
- Disk array information
- Database backup statistics including:
  - Last executed backup command and the current status
  - Number of Metadata Database files backed up
  - A list of the last 25 Metadata files backed up including the Object Name and creation date.

The information output to the console is also saved in the logs directory. This file, and the log files, must be included when submitting issues to Technical Support.

## Backup Service Not Currently Running

When the backup service is not running, the following information displays when you execute the `status` command:

- Running release of the service
- IP address and port the service runs on
- An extract from the DIVA Backup Service log files from the last error, or irrecoverable error, reported.

### Backup Service Failed to Start

If the backup service fails to start, identify the cause of the failure, correct the issue, and then try to start the service again. Contact Technical Support if assistance is required.

## Uninstalling BKS and DBAgent

The DIVA installer does not support uninstalling BKS or DBAgent, so uninstalling these has always been done manually using scripts provided in each component.

Use the following commands to uninstall BKS and DBAgent respectively:

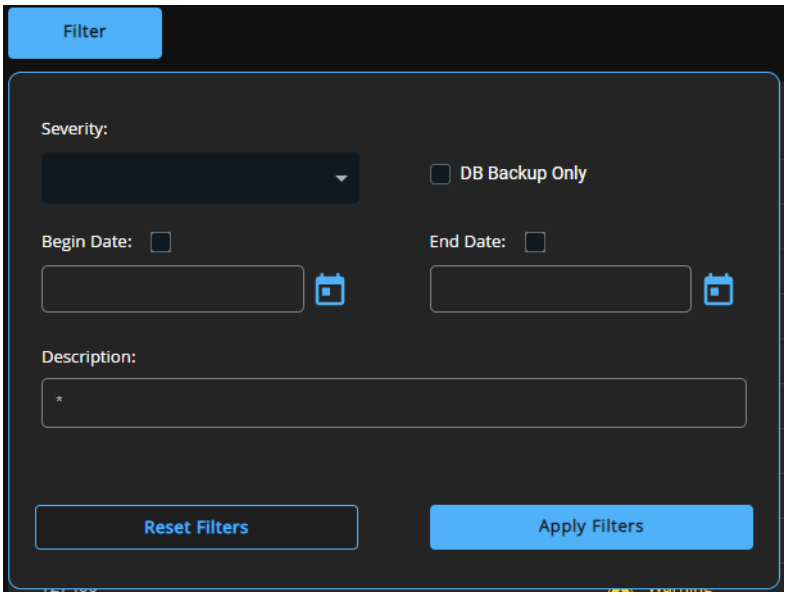
```
backup_service.bat uninstall
db_agent.bat uninstall
```

# Monitoring the DIVA BKS

The DIVA Backup Service notifies the Manager about all backup errors and warnings.

All messages generated by the backup service are also written to the Database Event Log and marked as DB Messages.

Events in the Troubleshooting > Logged Events panel may be filtered using the filter check boxes and fields to display specific types of entries being viewed. The following figure shows that the screen can been filtered to show only Warning, Error, Critical, or Information by using the pull-down menu and clicking the Filter button.




The following table describes the different warning and error notifications.

| Message Type | Code | User Message | Posted to Manager |
|---|---|---|---|
| SUCCESS | 0 | Completed successfully | Yes, informational |
| RUN | 1 | Running | No, internal only |
| ERROR | 2 | Failure: Refer to the backup service logs for more details. | Yes, error |
| TIMEOUT | 3 | Timeout: The process is taking longer to complete than the configured intervals. The backup service continues to display timeout messages as a warning. If the timeout occurs three consecutive times, the message will be elevated to an error message and displayed. | Yes, warning |

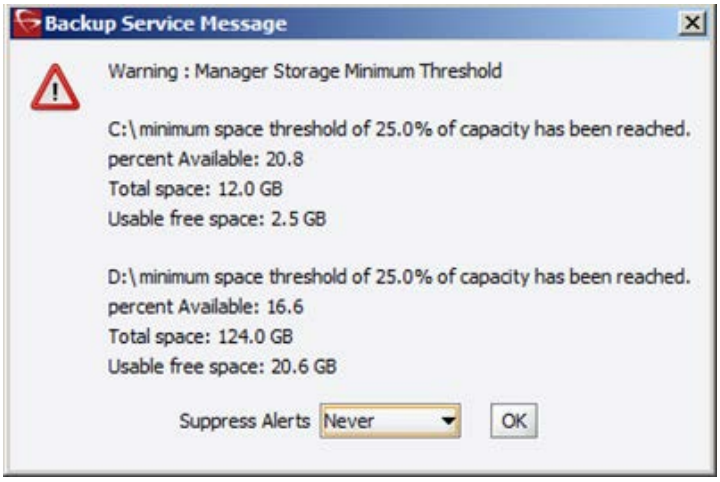
| Message Type | Code | User Message | Posted to Manager |
|---|---|---|---|
| STARTUP_FAILURE | 4 | DIVA Backup Service failed to start. Refer to the backup service logs for more details. | Yes, error |
| INITIALIZE | 5 | Scheduling Backups | No, internal only |
| TIMEOUTERROR | 6 | Timeout: The process is taking longer to complete than the configured interval. | Yes, error |
| CONFIGERROR | 1000 | Invalid Configuration Error. Refer to the backup service logs for more details. | Yes, error |
| METADATALOCATIONERROR | 6000 | The Metadata Database Location does not exist. Refer to the backup service logs for more details. | Yes, error |
| CLEANUPFBMFILEERROR | 7000 | The Metadata Database file deletion failed. Refer to the backup service logs for more details. | Yes, error |
| CLEANUPFBMFILEWARNING | 7001 | Failed deleting the Metadata Database. | Yes, error |
| DBCONNECTERROR | 9000 | Database connection error. Refer to the backup service logs for more details. | Yes, error |
| SQLERROR | 9001 | Database SQL error. Refer to the backup service logs for more details. | Yes, error |
| DBROLLBACKERROR | 9002 | Database Rollback error. Refer to the backup service logs for more details. | Yes, error |

# Monitoring Minimum Disk Space

The DISK_MIN_SPACE_THRESHOLD_PERCENT is a notification threshold percentage of the available space for each drive accessible by the Manager. Default: 5 percent. For example, DISK_MIN_SPACE_THRESHHOLD_PERCENT=25 sets the notification threshold to 25 percent. This function does not monitor removable media and drives.

When the configured threshold of available space on the media is reached, warning notifications are sent out. After the available space reaches 80 percent of the designated percentage an error message is sent out.

When the configured percentage is reached, a dialog box displays:




The Suppress Alerts list at the bottom of the dialog box functions identically to the other warning and error dialog boxes. In the previous figure a warning was issued to notify the operator that the DISK_MIN_SPACE_THRESHHOLD_PERCENT was reached.

Snoozing this alert causes no additional disk space warnings or errors to be displayed. Clicking OK without setting a suppression level enables future alerts for this particular warning to be displayed.

In the previous figure, when 80 percent of the threshold percentage is reached (2.4 GB on C drive and 24.8 GB on D drive), this dialog turns into an error rather than a warning.

# Email Notifications

BKS incorporates the ability to send out emails for issues arising from the process of backing up the DIVA database and Metadata Database files. To take advantage of this feature, DIVA must be configured to connect to an SMTP mail provider. The email notifications are configured through the web app under the Configuration > General Settings > SMTP Notifications page.

Use the following procedure to enable email notifications:

1. Open the web app.
2. Navigate to Configuration > General Settings > SMTP Notifications.
3. Set the values for the following email notification parameters as required:

**Caution: If the following parameters are misconfigured entries into the Manager Event Log will be made. However, email notification will not be sent.**

- Enable E-Mail Notification

  If you select the check box (enabled), the Manager attempts to send out email using the configured values.

- Database Backup Notification

  Use the pull-down menu to select ERRORS AND WARNINGS, ERRORS or DISABLED.

- Manager: Set The Default DIVACore Backup Service Monitor Timeout(Minutes)

  Enter the timeout value before a warning or error is identified and sent.

- (SMTP) Outgoing Mail Host

  Enter the URL of the email provider for outgoing mail in the (SMTP) Outgoing Mail Host field. This is provided by your Email Administrator.

- (SMTP) Outgoing Mail Port

  The port value is port 25 by default. However, many email providers are using a different port for security reasons. The correct port number is provided by your Email Administrator. Enter the correct port number in the (SMTP) Outgoing Mail Port field.

- (SMTP) Outgoing Mail Required Authentication

  Many email providers require you to log in to the email server to allow sending emails. The (SMTP) Outgoing Mail Required Authentication check box must be selected, and a valid account name and password (using the following two fields) provided if required to log in to the email server.

- Account Name(Full Email Address)

  Enter the full senders email address in the Account Name field if the (SMTP) Outgoing Mail Required Authentication check box is selected.

- Account Password

  The password associated with the senders email address must be entered in the Account Password field if an email address was entered in the Account Name field. Email passwords are case-sensitive.

- DIVA System Administrator's E-mail Address

  Enter the full email address for the DIVA System Administrator in the DIVA System Administrator's E-mail Address field so they receive a copy of any email notifications.

- Email Subject

  Enter the subject to display when a notification email is sent.

- Notification E-Mail Recipients

  Enter the full email addresses for anyone who should receive the email notifications in the Notification E-Mail Recipients field. This should be a comma-delimited list with no spaces.

- Number Of Hours Between E-Mail Notifications

  Enter the number of hours between when email notifications should be sent.

- Number Of Minutes Before First E-Mail Notification

  Enter the number of minutes before the first email notification should be sent.

- Determines Whether To Send An E-Mail Notification When An Actor Goes Offline

  Use the slide button to enable or disable sending an email notification when an Actor goes offline.
- Determines Whether To Send An E-Mail Notification When A Drive Goes Offline

  Use the slide button to enable or disable sending an email notification when a Drive goes offline.
- Determines Whether To Send An E-Mail Notification When A Disk Goes Offline

  Use the slide button to enable or disable sending an email notification when a Disk goes offline.
- Determines Whether To Send An E-Mail Notification When An Actor / Drive Connection Goes Offline

  Use the slide button to enable or disable sending an email notification when an Actor-Drive connection goes offline.
- Determines Whether To Send An E-Mail Notification When An Actor / Disk Connection Goes Offline

  Use the slide button to enable or disable sending an email notification when an Actor / Disk connection goes offline.
- Minimum Disk Space In MB At Or Below Which An E-Mail Notification Will Be Sent

  Enter the value in MB that when reached will trigger an email notification to be sent.
- Minimum Empty Tapes At Or Below Which An E-Mail Notification Will Be Sent

  Enter the minimum number of tapes that when reached will trigger and email notification to be sent.
- Maximum Number Of Aborted Jobs, At Or Above Which An E-Mail Notification Will Be Sent

  Enter the number of aborted jobs that when reached will trigger and email notification to be sent.

After the values have been configured, if the Manager is already running it must be notified of any changes. When the Manager starts, or when it receives notifications from the web app, it reads the configured values and attempts to send out a test email. If the test is successful, all recipients on the Notification E-Mail Recipients list will receive a Test Successful email notification. Otherwise, they will receive an email notifying them of any error that occurred.

Events are logged in the Logged Events panel of all connected web apps.

# Troubleshooting and Failovers

**Topics:**

# Failure Scenarios and Recovery Procedures

There are two types of failure scenarios; non-fail-over, and fail-over.

## Non-fail-over Scenarios

If the Main Manager computer is still fully operational, and there has been no RAID Disk failure, the DIVA system and its database can be restored and recovered from failure without moving the Manager or database to a Backup Manager computer.

The following are non-fail-over scenarios and recovery actions (in sequence) to correct them. Contact Technical Support if assistance is required or to restore from a backup.

### Manager Failure

1. Restart the Manager
2. Apply a cumulative path (if available) and restart the Manager
3. Upgrade the DIVA installation

### Instance Failure

1. Restart the Postgres instance
2. Reinstall Postgres and restore the database from a backup

### Data File Corruption

Restore the data file from a Postgres Secure Backup.

### Parameter File or Control File Corruption

Restore the parameter file, or control file, from a Postgres Secure Backup.

### DIVA Online Redo Logs Corruption

Restore the database using a Postgres Secure Backup.

### DIVA Archive Redo Logs Corruption

Shut down the database and perform a full backup.

# Failover Scenarios

If the main Manager computer fails, is not operational, or a RAID disk fails, the Manager and database must be restored and recovered on the Backup Manager computer to restore DIVA back to an operational state.

The following are fail-over scenarios. The recovery actions are the same for all of the listed scenarios.

Refer to the DIVA Installation and Configuration Guide to bring the system back online and contact Technical Support if assistance is required or to restore from a backup.

The following are possible failures that require fail-over recovery actions:

- Main Manager Computer Failure
- RAID Disk Failure where Postgres Data Files are Stored
- RAID Disk Failure where Postgres Backups are Stored
- RAID Disk Failure where Metadata Database Files are Stored

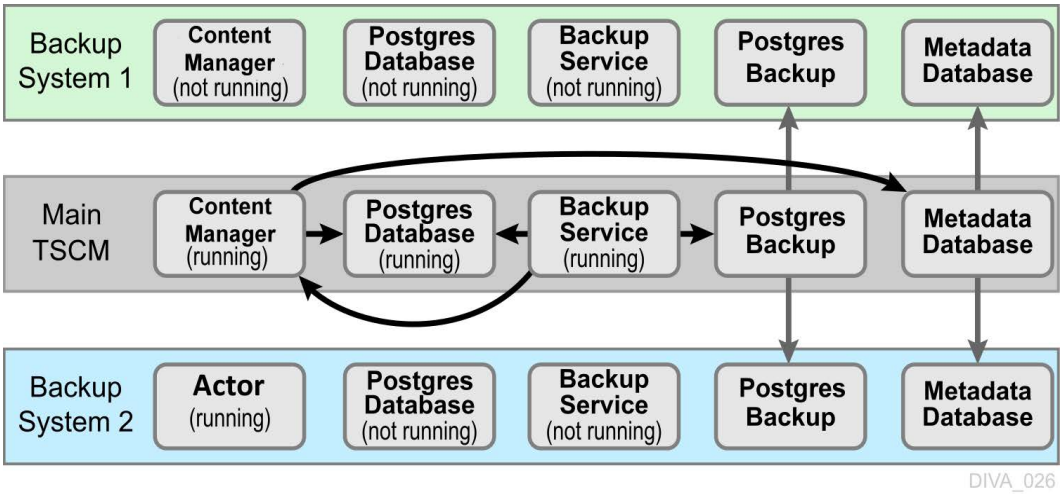
Use the following recovery sequence to complete the fail-over if any of the previous failures occur:

1. Failover to the Backup Manager computer.
2. Restore and recover the Postgres Database from a Postgres Secure Backup.
3. Discover if any Complex Objects are missing Metadata files.
4. Start the Manager.

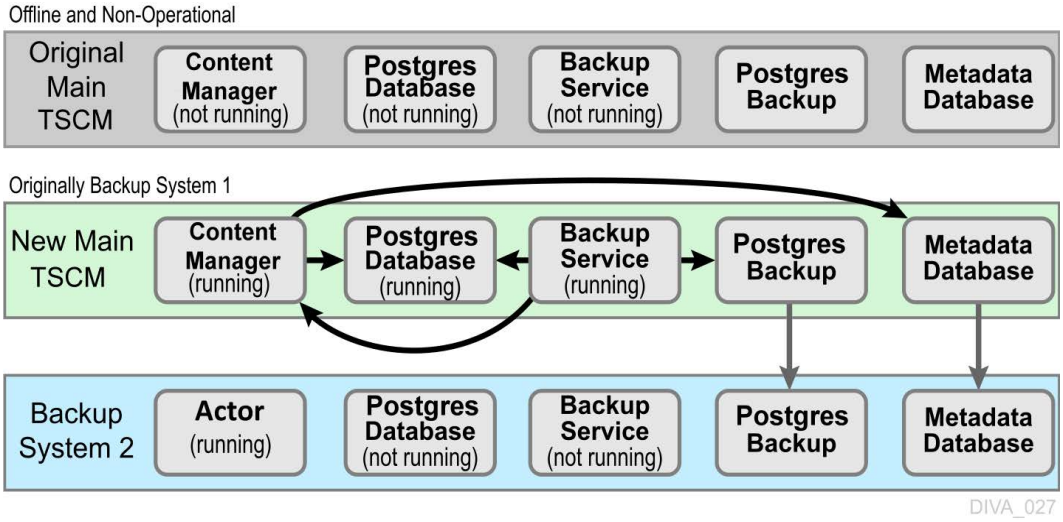
## Failover Procedures

Use the following procedure to recover the DIVA system if a failure occurs. The first figure is a typical DIVA System configuration showing the connections between the different modules, the second displays a fail-over case, and the third depicts a recovered, operational system. The Main Manager and Backup System 1 are configured identically. However, the backup service, Manager, and DIVA database are not running until they are started (see the third figure). The backup service creates the backups on the Main Manager computer and then pushes copies of them to the Backup System 1,

Backup System 2, and Backup System N. The N represents additional system numbering (if applicable), for example Backup System 3, Backup System 4, etc.




For this example, assume the Main Manager computer failed and is offline. It is effectively switching the Original Backup Manager to be the New Main Manager and the Original Main Manager will be the New Backup Manager (they are trading places), resulting in the least amount of time the system is offline.




1. Restore the DIVA database on the New Main Manager from the latest Postgres Database backup.
2. On the New Main Manager, adjust the Manager configuration file and backup service configuration file to point to the DIVA database that has just been restored (see the previous step).
3. Update the Metadata Database Location to the location where the Metadata Database files were backed up on New Main Manager system (the Original Backup

System 1). Update the parameter under the Manager Setting panel in the web app on the New Main Manager computer. **LOCATION TBD IN WEBUI**

4. Run the backup service command on the New Main Manager system. This command lists all of the Complex Objects that are missing the Metadata file in the Metadata Database.

   If a Complex Object is missing the Metadata file, it must be restored from the Original Main Manager, or Backup System 2. Complex Objects are unusable without the associated Metadata file.

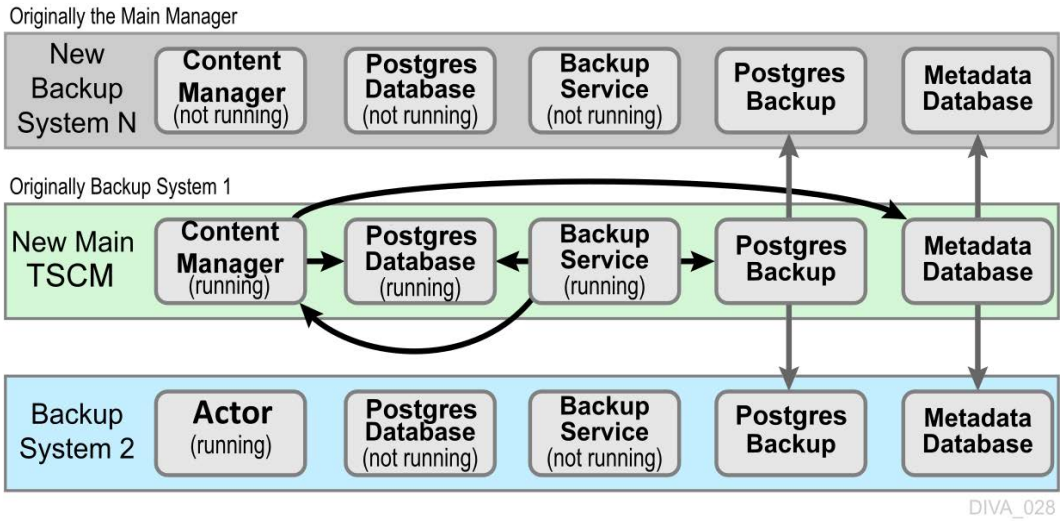
5. Start the Manager and backup service on the New Main Manager.

   After the Original Main Manager system is restored, recovered from its failure, and is operational, it is converted to the New Backup System N with no downtime.

6. Update the DB_BACKUP_REMOTE_DESTINATIONS and FBM_BACKUP_REMOTE_DESTINATIONS parameters in the backup service configuration file on the New Main Manager system by adding the New Backup System N (the Original Main Manager) as the additional remote backup location.

7. Restart the backup service on the New Main Manager for the configuration changes to take effect.

8. Copy the existing DIVA database backups and Metadata files from the Backup System 2 (or New Main Manager) to the New Backup System N in the background.




# Database Service Failover

**Caution: These procedures are critical and sensitive. They should only be performed under the control of a Telestream Support Technician.**

If a database or system failure occurs, where restoring from a system backup is necessary, restoration of a stored backup is accomplished using the following outlined procedures.

A fail-over command is very similar to the restore command though it does not guarantee the database will be up if it fails to process. During fail-over it is assumed that the existing data at the locations database is invalid and will be deleted prior to the fail-over script execution. A fail-over can be performed to the same database or a different database with the same configuration.

It is recommended that fail-over only be used on an in-place database if the database is corrupted and in an unrecoverable state. In the case of fail-over to another server, the backup files from the source database are used and the existing backups for the target are essentially invalid (although they can be used to fail-over to itself if necessary). The verification of a compatible database is done at the BKS service before the command is issued to the DBAgent.

Use the following procedure to configure a standby server for fail-over:

1. Add the configuration in a new database profile and install a DBAgent on that standby server.
2. Add a location in the configuration that points to the main backup point for that server and add the DBAgent URL to this location configuration.

---

**Note:** Do not add the database profile to the list of managed databases unless active backups are to be taken.

---

The new location will automatically be synchronized from the primary location such that all the backups are ready to be used if a fail-over is needed.

Use the following procedures to perform the fail-over:

1. Add the fail-over target to the managed list of databases for the target location.
2. Send the fail-over command with the source and target database profiles, along with a timestamp of the recovery.
3. Remove the source server from managed databases so it does not make active backups.

Also, recovery from the loss of a backup service in case the server that it was running on is down by installing the backup service on another location that it was replicating to. Any existing database profiles must also be configured because the locations are associated with any prior backup locations being replicated. This must be done in a stepwise fashion such that the new primary backup location can catalog all the backups into new ledgers before attempting any replication to remote locations. After this is complete, the fail-over procedure is the same.

# Frequently Asked Questions

**Note:** For detailed information and recovery FAQs on the Metadata Database refer to the DIVA Installation and Configuration Guide, or contact Technical Support.

- What is the recommended frequency of database backups?

  The DIVA database automatically backs up every fifteen minutes.

- Does Technical Support recommend any particular database backup application?

  A database backup service is provided in the DIVA package. Alternative backup software can be used as an additional security under the condition that it only backs up the DIVA database backup files (in H:\oraback) and not the database itself.

  Backing up the database directly is forbidden. For example, not using BKS or other non-DIVA database backup applications. Backing up the database directly with another program may interfere with the DIVA BKS. This may render database restoration impossible using the embedded DIVA restore utility, and could possibly result in data losses for which Telestream will accept no responsibility.

- Where are the backup files located?

  The database backup files are located on the Main Manager computer in the H:\oraback folder. The files are synced to the Backup Manager and an Actor in the H:\oraback\mgr1 folder.

- Are there iterated versions of the database backup, and if so, how many are retained?

  The backup files are retained for the previous ten days. The retention period is configurable for the database backup files in the DIVA Backup Service configuration file. Contact Technical Support for assistance.

- How do I fail-over to a Backup System when the Main Manager System has failed?

  Refer to *Troubleshooting and Failovers* for complete procedures.

- How do I recover when the backup disk fails, or gets corrupted, on the Main Manager System?

  Disk failures, or corruption, requires a fail-over to the Backup Manager. Refer to *Troubleshooting and Failovers* for complete procedures.

- How do I configure a full backup to start when the backup service starts?

  The DIVA Backup Service automatically determines if a full backup is required when it starts. There is no configuration required.

- Can the Manager and Database be installed on separate servers?

  No, they must be installed on the same server because the DIVA Backup Service does not support Manager and Postgres installations on separate servers in this DIVA release.

- Does the recovery window apply to both Postgres Secure Backups and Metadata Backups?

  Yes, the recovery window setting applies to both backups.

- Does the storage location of the live database affect performance or space, and is it critical?

  Yes, it is both performance and space critical. See *Installing, Upgrading, and Configuring the DIVA Database* for installation and configuration procedures.

# Appendix

## Topics

# Sample BKS Configuration File

The following is a sample BKS configuration file with field descriptions and is located in %TSCM_HOME%\Program\conf\db_agent\appsettings.json:

BKS

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information",
      "System.Net.Http.HttpClient": "None",
      "DIVACore.Common.Services.GatewayDiscoveryHostedService":
"None"
    },
    "Configuration": {
      "RetentionDays": 7
    }
  },
  "Version": "0.0.0.0",
  "AllowedHosts": "*",
  "DatabaseSettings": {
    "Databases": [
      {
        "ProfileName": "MetadataDatabase",
        "DatabaseName": "Core",
        "DatabaseType": "MongoDB",
        "DatabaseVersion": "5.0",
        "ConnectionString": "mongodb://127.0.0.1:27017/
?replicaSet=rs0",
        "RootDirectory": "",
        "User": "MongoAdmin",
        "Password": ""
      },
      {
        "ProfileName": "PostgresDatabase",
        "DatabaseName": "diva",
        "DatabaseType": "Postgres",
        "DatabaseVersion": "14.2",
        "ConnectionString": "Host=127.0.0.1;Port=5432;",
        "RootDirectory": "C:\\Program Files\\PostgreSQL",
        "DataDirectory": "E:\\pg_data",
        "User": "postgres",
        "Password": "postgres"
      },
      {
        "ProfileName": "SearchDatabase",
        "DatabaseName": "Core",
        "DatabaseType": "ElasticSearch",
        "DatabaseVersion": "7.10.2",
        "ConnectionString": "http://localhost:9200/",
        "RootDirectory": "",
        "DataDirectory": "",
        "User": "ElasticAdmin",
```

```
        "Password": ""
      }
    ]
  },
  "LocationSettings": {
    "Locations": [
      {
        "Name": "Primary",
        "Primary": true,
        "Enabled": true,
        "Location": "H:\\divaback",
        "AgentUrl": "https://localhost:1878/",
        "Type": "Local",
        "ManagedDatabases": [
          "PostgresDatabase",
          "MetadataDatabase"
        ],
        "BackupReplication": [],
        "SourceName": "",
        "User": "",
        "Password": ""
      }
    ]
  },
  "ServiceSettings": {
    "RequestExpiration": 3600,
    "RequestTimeout": 600
  },
  "HttpServer": {
    "Endpoints": {
      "Http": {
        "Host": "localhost",
        "Port": 1876,
        "Scheme": "http"
      },
      "Https": {
        "Host": "localhost",
        "Port": 1877,
        "Scheme": "https",
        "FilePath": "../../security/certificates/
BackupService.p12"
      }
    }
  },
  "BrokerSettings": {
    "Hostname": "localhost",
    "Port": 5672,
    "Username": "wsuser",
    "Password": "changeit"
  },
  "DiscoverySettings": {
    "Url": "https://127.0.0.1:8761/eureka/apps/",
    "AppName": "backup-service"
  },
  "DIVACoreAPISettings": {
    "Url": " https://127.0.0.1:8765/",
    "TimeoutInMs": 20000
```

```
  },
  "DatabaseBackup": {
    "Enabled": false,
    "FullBackupInterval": {
      "ExecutionPeriod": "Daily",
      "TimeOfDay": "00:00:00",
      "InstancesInPeriod": [ 0 ]
    },
    "IncrementalPeriod": 15,
    "FullBackupFileRetention": 10,
    "FullBackupArchiveRetention": 30,
    "ArchiveMediaGroup": "",
    "ArchivePriority": "Normal",
    "ArchiveWindowStart": "00:00:00",
    "ArchiveWindowEnd": "23:59:00",
    "PermanentRetentionPeriod": 0,
    "BackupExecutionTimeout": 120,
    "RestoreExecutionTimeout": 120,
    "StatusPollingPeriod": 3,
    "StatusReportingInterval": 1440
  }
}
```

# Sample DBAgent Configuration File

The following is a sample DBAgent configuration file with field descriptions:

```
dbagent:

{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information",
      "System.Net.Http.HttpClient": "None",
      "DIVACore.Common.Services.GatewayDiscoveryHostedService":
"None"
    },
    "Configuration": {
      "RetentionDays": 7
    }
  },
  "HttpServer": {
    "Endpoints": {
      "Https": {
        "Host": "localhost",
        "Port": 1878,
        "Scheme": "https",
        "FilePath": "../../security/certificates/DBAgent.p12"
      }
    }
  },
  "BrokerSettings": {
    "Hostname": "localhost",
    "Port": 5672,
```

```
    "Username": "wsuser",
    "Password": "changeit"
  },
  "ServiceConfiguration": {
    "BasePath": "H:\\divaback",
    "LogRetention":  30,
    "MountPointMonitors": [
      {
        "Path": "C:",
        "IsPercentBased": true,
        "ErrorThreshold": 0,
        "WarnThreshold": 0,
        "ErrorPercentage": 95,
        "WarnPercentage": 85
      },
      {
        "Path": "E:",
        "IsPercentBased": true,
        "ErrorThreshold": 0,
        "WarnThreshold": 0,
        "ErrorPercentage": 95,
        "WarnPercentage": 85
      },
      {
        "Path": "F:",
        "IsPercentBased": true,
        "ErrorThreshold": 0,
        "WarnThreshold": 0,
        "ErrorPercentage": 95,
        "WarnPercentage": 85
      },
      {
        "Path": "H:",
        "IsPercentBased": true,
        "ErrorThreshold": 0,
        "WarnThreshold": 0,
        "ErrorPercentage": 95,
        "WarnPercentage": 85
      }
    ]
  },
  "DiscoverySettings": {
    "Url": "https://127.0.0.1:8761/eureka/apps/",
    "AppName": "db-agent-service"
  }
}
```