

telestream



**DIVA**

# **Installation and Administration Guide**

**Release: 9.2**

**Revision: 1**

## Copyrights and Trademark Notices

Copyright © 2024 Telestream, LLC and its Affiliates. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, altered, or translated into any languages without written permission of Telestream, LLC. Information and specifications in this document are subject to change without notice and do not represent a commitment on the part of Telestream. Specifications subject to change without notice.

Telestream, Aurora, CaptionMaker, CaptureVU, Cerify, Content Manager, ContentCentral, Cricket, DIVA, DIVAdirector, DIVADocs, DIVAGrid, DIVANet, DIVAProtect, DIVASolutions, Episode, Encoding Intelligence, Episode, FLEXVU, Flip4Mac, FlipFactory, Flip Player, Geminus, Glim, GraphicsFactory, Inspector, IQ & Design, Kumulate, Lightspeed, MassStore, MassTech, MetaFlip, Post Producer, Prism, ScreenFlow, Sentry, Singulus, Split-and-Stitch, Stay Genlock, Surveyor, Tempo, TrafficManager, Vantage, Vantage Cloud Port, VOD Producer, and Wirecast are registered trademarks of Telestream, LLC and its Affiliates and its Affiliates.

Argus, ContentAgent, Cricket, e-Captioning, Inspector, iQ, iVMS, iVMS ASM, MacCaption, Pipeline, Switch, and Vidchecker are trademarks of Telestream, LLC and its Affiliates. All other trademarks are the property of their respective owners.

**Adobe.** Adobe® HTTP Dynamic Streaming Copyright © 2014 Adobe Systems. All rights reserved.

**Apple.** QuickTime, MacOS X, and Safari are trademarks of Apple, Inc. Bonjour, the Bonjour logo, and the Bonjour symbol are trademarks of Apple, Inc.

**Avid.** Portions of this product Copyright 2012 Avid Technology, Inc.

**CoreOS.** Developers of ETCD.

**Dolby.** Dolby and the double-D symbol are registered trademarks of Dolby Laboratories Licensing Corporation.

**Fraunhofer IIS and Thomson Multimedia.** MPEG Layer-3 audio coding technology licensed from Fraunhofer IIS and Thomson Multimedia.

**Google.** VP6 and VP8 Copyright Google Inc. 2014 All rights reserved.

**MainConcept.** MainConcept is a registered trademark of MainConcept LLC and MainConcept AG. Copyright 2004 MainConcept Multimedia Technologies.

**Manzanita.** Manzanita is a registered trademark of Manzanita Systems, Inc.

**MCW.** HEVC Decoding software licensed from MCW.

**MedialInfo.** Copyright © 2002-2013 MediaArea.net SARL. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**Microsoft.** Microsoft, Windows NT|2000|XP|XP Professional|Server 2003|Server 2008 |Server 2012|Server 2016|Server 2019|Server 2022, Windows 7, Windows 8, Windows 10, Windows 11, Media Player, Media Encoder, .Net, Internet Explorer, SQL Server 2005|2008|2012|2016|2019, and Windows Media Technologies are trademarks of Microsoft Corporation.

**NLOG, MIT, Apache, Google.** NLog open source code used in this product under MIT License and Apache License is copyright © 2014-2016 by Google, Inc., © 2016 by Stabzs, © 2015 by Hiro, Sjoerd Tieleman, © 2016 by Denis Pushkarev, © 2015 by Dash Industry Forum. All rights reserved.

**SharpSSH2.** SharpSSH2 Copyright (c) 2008, Ryan Faircloth. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer:

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Diversified Sales and Service, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**Swagger.** Licensed from SmartBear.

**Telerik.** RadControls for ASP.NET AJAX copyright Telerik All rights reserved.

**VoiceAge.** This product is manufactured by Telestream under license from VoiceAge Corporation.

**x264 LLC.** The product is manufactured by Telestream under license from x264 LLC.

**Xceed.** The Software is Copyright ©1994-2012 Xceed Software Inc., all rights reserved.

**ZLIB.** Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler.



Other brands, product names, and company names are trademarks of their respective holders, and are used for identification purpose only.

## MPEG Disclaimers

### MPEGLA MPEG2 Patent

ANY USE OF THIS PRODUCT IN ANY MANNER OTHER THAN PERSONAL USE THAT COMPLIES WITH THE MPEG-2 STANDARD FOR ENCODING VIDEO INFORMATION FOR PACKAGED MEDIA IS EXPRESSLY PROHIBITED WITHOUT A LICENSE UNDER APPLICABLE PATENTS IN THE MPEG-2 PATENT PORTFOLIO, WHICH LICENSE IS AVAILABLE FROM MPEG LA, LLC, 4600 S. Ulster Street, Suite 400, Denver, Colorado 80237 U.S.A.

### MPEGLA MPEG4 VISUAL

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

### MPEGLA AVC

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR

ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

## MPEG4 SYSTEMS

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 SYSTEMS PATENT PORTFOLIO LICENSE FOR ENCODING IN COMPLIANCE WITH THE MPEG-4 SYSTEMS STANDARD, EXCEPT THAT AN ADDITIONAL LICENSE AND PAYMENT OF ROYALTIES ARE NECESSARY FOR ENCODING IN CONNECTION WITH (i) DATA STORED OR REPLICATED IN PHYSICAL MEDIA WHICH IS PAID FOR ON A TITLE BY TITLE BASIS AND/OR (ii) DATA WHICH IS PAID FOR ON A TITLE BY TITLE BASIS AND IS TRANSMITTED TO AN END USER FOR PERMANENT STORAGE AND/OR USE. SUCH ADDITIONAL LICENSE MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com) FOR ADDITIONAL DETAILS.

## Limited Warranty and Disclaimers

Telestream, LLC (the Company) warrants to the original registered end user that the product will perform as stated below for a period of one (1) year from the date of shipment from factory:

*Hardware and Media*—The Product hardware components, if any, including equipment supplied but not manufactured by the Company but NOT including any third party equipment that has been substituted by the Distributor for such equipment (the “Hardware”), will be free from defects in materials and workmanship under normal operating conditions and use.

## Warranty Remedies

Your sole remedies under this limited warranty are as follows:

*Hardware and Media*—The Company will either repair or replace (at its option) any defective Hardware component or part, or Software Media, with new or like new Hardware components or Software Media. Components may not be necessarily the same, but will be of equivalent operation and quality.

## Software Updates

Except as may be provided in a separate agreement between Telestream and You, if any, Telestream is under no obligation to maintain or support the Software and Telestream has no obligation to furnish you with any further assistance, technical support, documentation, software, update, upgrades, or information of any nature or kind.

## Restrictions and Conditions of Limited Warranty

This Limited Warranty will be void and of no force and effect if (i) Product Hardware or Software Media, or any part thereof, is damaged due to abuse, misuse, alteration,

neglect, or shipping, or as a result of service or modification by a party other than the Company, or (ii) Software is modified without the written consent of the Company.

## Limitations of Warranties

THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No oral or written information or advice given by the Company, its distributors, dealers or agents, shall increase the scope of this Limited Warranty or create any new warranties.

**Geographical Limitation of Warranty**—This limited warranty is valid only within the country in which the Product is purchased/licensed.

**Limitations on Remedies**—YOUR EXCLUSIVE REMEDIES, AND THE ENTIRE LIABILITY OF TELESTREAM, LLC WITH RESPECT TO THE PRODUCT, SHALL BE AS STATED IN THIS LIMITED WARRANTY. Your sole and exclusive remedy for any and all breaches of any Limited Warranty by the Company shall be the recovery of reasonable damages which, in the aggregate, shall not exceed the total amount of the combined license fee and purchase price paid by you for the Product.

## Damages

TELESTREAM, LLC SHALL NOT BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE PRODUCT, OR THE BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, EVEN IF THE COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES, OR ANY REMEDY PROVIDED FAILS OF ITS ESSENTIAL PURPOSE.

Further information regarding this limited warranty may be obtained by writing:  
 Telestream, LLC  
 848 Gold Flat Road  
 Nevada City, CA 95959 USA

You can call Telestream during U. S. business hours via telephone at (530) 470-1300.

## Regulatory Compliance

**Electromagnetic Emissions:** FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A

**Electromagnetic Immunity:** EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)

**Safety:** CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)

California Best Management Practices Regulations for Perchlorate Materials:  
This Perchlorate warning applies only to products containing CR (Manganese Dioxide)  
Lithium coin cells. Perchlorate Material-special handling may apply. See  
[www.dtsc.ca.gov/hazardouswaste/perchlorate](http://www.dtsc.ca.gov/hazardouswaste/perchlorate).

# Contents

## Getting Started 14

- System Administrators 14
- Media Managers 14
- Users 15
- Typical Questions to Consider 16

## Supported Environments 17

- Overview 17
- Product Compatibility 18
  - Postgres Database and DIVA Backup Service 18
  - DIVA Connect 18
  - FlashNet to DIVA Migration 19
  - Supported API Releases 19
    - DIVA REST API 19
    - Web Services APIs 19
    - Supported and Tested Legacy API Configurations 20
    - Untested Configurations 20
- Hardware and Software 20
  - DIVA Core Architecture 20
    - Manager 21
    - Manager Cluster 21
    - Actor 21
    - Actor and Manager (Single Computer) 21
    - DIVA Connect 2.1 and later 21
    - DIVA Web App 21
  - System Component Interconnectivity 22
    - Storage Connection 22
  - Intel and Microsoft Windows 22
    - DIVA Appliance 23
    - Operating System Compatibility 23
      - Manager 23
      - Manager Cluster 24
      - Actor 25



Actor and Manager (Single Computer)	26
DIVA Connect 4.x	26
General Storage Requirements	27
Minimum Partition Sizing for a Server Hosting Databases	27
Supported Libraries and Control Software	28
Supported Drives	31
Supported Disks	32
Supported Object Storage	33
Configuring HCP (Hitachi Content Platform) for Multi-part Upload	35
Supported Partial File Restore Formats	35
GXF (General Exchange Format)	36
AVI (Audio Video Interleaved)	37
Adobe Premiere	37
Harris Corporation Nexio 3600	37
AVI with Separate WAV Files	37
AVI with FFV1 or FFVH	38
QuickTime/MP4	38
QuickTime Self-Contained Clips	38
MP4 Clips	39
LXF (Leitch Exchange Format)	39
DIF with Separate WAV Files, and DV with Separate Audio, or Self-contained DV Types	40
BWA (Broadcast WAV)	40
Supported Unmanaged Storage Repositories	40
Unmanaged Storage Repositories	40
Supported Transcoders	42
Supported Avid Environments	42
Avid Interplay Compatibility	42
MediaCentral Compatibility	43

## Security Guidelines 44

Security Overview	44
Keep Software up to Date	44
Restrict Network Access to Critical Services	44
Run as DIVA User and use Principle of Least Privilege Where Possible	45
DIVA User Profiles in the DIVA Web App	45
Postgres Database Security	45
Monitor System Activity	45
Keep up to Date on Latest Security Information	46
Using Anti-virus Software	46
Installation planning	46
The Installation Environment	46
Which Resources Need to be Protected?	46
From whom are the resources being protected?	47
What will happen if the protections on strategic resources fails?	47
Recommended Deployment Topologies	47
Separate Metadata Network	47

Fiber Channel Zoning	47
Safeguard SAN Disks Configuration Access	48
Install the DIVA Package	48
Tape Security	48
Backup Production Databases	48
The Security Model	49
Authentication	49
Authorization	49
Tape Group Encryption	49
SSL Authentication and Secure Communications	49
DIVA Web App Access Control	49
System Administrator (sysadmin)	49
Administrator (admin)	49
Advanced Operator ( <i>advoperator</i> )	50
Operator (operator)	50
User (user)	50
Internal Communication Security	50
Secure Sockets Layer and Authentication	50
External Certificate Authorities	51
Security Tools	51
DIVA REST API Security Changes	51
Secure Deployment Checklist	53

## **DIVA Installation and Setup 54**

Software Component Distribution	54
Database Setup	55
Installation and Configuration Overview	55
Complex Objects	57
Database Installation, Upgrade, and Configuration	57
Prerequisites	57
Database Dump Files	57
DIVA Database Server Removal	57
Uninstalling the DIVA Database Server in Windows	57
Installing the DIVA Database Server in Windows	58
Manually Creating the Database User and Schema	59
Migrating DIVA Database Server from 8.3 to 9.1	60
DIVA Installation	60
Steps for Installation and Setup of DIVA	60
Installed Features and Services	61
Downloading the Software	62
Installing or Upgrading DIVA	62
Options for Select Components to Install	62
Installing Metadata Database Installation (Optional)	62
Notification Service Installation (Optional)	63
Database Schema (Optional)	65
DIVA Appliance (Optional)	65
DIVA Demo (Optional)	66

## Post-Installation Configuration 67

Configuration Overview	67
Module Configuration Files	69
Environment Variables	69
Configuring the DIVA JAVA Home Environment	70
Manager Configuration	70
Local Manager Configuration	71
Basic Settings	73
Database Settings	75
Advanced Settings	76
Settings for Logging	87
Configuring Job Priorities	87
Rerouting Destinations (restore_translations.conf)	88
Manager Control	89
Installing and Removing the Manager Service in Windows	89
Manager Service Management	90
Manager Activity Logging	91
Confirming System Connectivity	91
Confirming Remote Client to Manager Connectivity	91
Manager to Actors Connectivity Confirmation	92
Confirming Manager to Robot Manager Connectivity	92
Initiating Manager Failover	92
Configuring the DIVA REST API Gateway	93
Accessing the DIVA Web App	94
Navigation Menu	94
Back-end Support	95
Importing the License	95
Database Backup Configuration	95
Backup Service (BKS) Overview	95
Configuring BKS	97
DBAgent	97
Backup Initiator	97
Backup Timing	98
ArchivePriority Settings	99
ArchiveWindowStart Settings	99
ArchiveWindowEnd Settings	99
Workflows	99
Archive Workflow	99
Restore Workflow	100
BKS Recommended Practices	100
BKS Installation and Configuration	101
BKS Software Installation	101
BKS Configuration	103
BKS and DBAgent Removal	104
The DIVA Backup Service (BKS)	105
The Actor	105
Actor Configuration Overview	106

Actor Executables	107
Local Actor Configuration File (actor.conf)	108
Actor Service Installation and Removal	108
Actor Service Management Functions	109
Actor Launch	110
Actor Definition and Declaration	110
Actor Settings	110
Actor Advanced Settings	112
Partial File Restore Settings	113
Actor to Drive Connections	123
Core Proxy Actor Definitions	123
Resource Selection and Manager-Actor Communication	124
Actor and Tape Clones	124
Actor Activity Logs	125
Configuring SMTP Messages	125
The Metadata Database	127
Metadata Database Configuration	127
Metadata Database Sizing	128
MDDDB (Flat File Metadata Database) to MDS (Metadata Service) Migration	129
Troubleshooting	130
Metadata Database Failure Scenarios	130
Scenario 1: Metadata Database Storage Disk Failure	130
Scenario 2: Metadata Database File Corruption	131
Scenario 3: Lost or Manually Deleted Metadata Database File	132
Scenario 4: Failure to Backup Metadata Database to All Backup Systems	133
Scenario 5: Failure of the Metadata Database Backup to One Backup System	133
Manager Will Not Start	134
Backup Service Will Not Start	134
Troubleshooting and Failovers	134
Failure Scenarios and Recovery Procedures	134
Failover Scenarios	135
Database Service Failover	138

## **System Maintenance and Monitoring 140**

The DIVA Launch Process	140
Starting DIVA Hardware	140
Starting DIVA Software	141
Stopping DIVA	142
Shutting Down the Software	143
Shutting Down the Hardware	143
Backup Service Warnings and Notifications	143
Failover Procedures	143
Scenario 1—Failover with Multiple BKS Installations (Recommended)	144
Scenario 2—Failover from a Single BKS Instance	145
Job Monitoring	147
Job Warnings	147

Initiating a Cluster Failover	147
System Information and Log Collection Tool	148

## **Frequently Asked Questions 151**

### **DIVA Installation Questions and Answers 151**

When a Metadata file is manually deleted from Main Manager System, is it also deleted from all backup systems? **153**

How do I recover when a Complex Object's Metadata File is lost on the Main Manager System and all backup systems? **153**

How do I locate a Complex Object's Metadata inside the Metadata Database?  
**153**

### **Database Backup Questions and Answers 155**

# Getting Started

This guide describes initial and general installation, configuration, utilization and monitoring of the DIVA system. The manual assumes a working knowledge of the Windows operating system, and additional concepts such as networking, RAID, tape drives, and fiber channel technologies.

## Topics

- [System Administrators](#)
- [Media Managers](#)
- [Users](#)
- [Typical Questions to Consider](#)

## System Administrators

To get started on the right track with DIVA, system administrators should review [Supported Environments](#). This provides information about the hardware and software DIVA supports.

Before the DIVA installer arrives, confirm everything required to run DIVA is installed and setup so the Telestream Installer can put the necessary DIVA software on the server(s). This basic information can be found in the Architecture, Concepts and Glossary book, while the specific server and network configurations are in the Supported Environments and the DIVA Installation and Configuration Guide books.

## Media Managers

Media Managers should work along with users to determine what type of media will be necessary to use with DIVA and which other DIVA products may be necessary to complete the environment. Media Managers should also work along side of the System Administrators and Telestream Sales and/or Technical Support to identify what type of

hardware (servers, tape drives, disk arrays, and so on) are necessary to meet the needs of the company and their mission.

## Users

Users should be an integral part of the system planning and should work along with both the System Administrators and Media Managers in identifying what DIVA components are best suited for their daily use. The technical aspects can be left to the System Administrators, but users typically know best what they need to fulfill their daily operations. User input on media formats, archival operations, restore operations, and other specific tasks are valuable input for creating a successful and functional environment.

## Typical Questions to Consider

These questions will help administrators decide which components, both hardware and software, should be considered for a DIVA system.

---

**Note:** You can always upgrade or expand your initial DIVA system. Contact your Telestream Sales representative or Telestream Technical Support with any questions.

---

- How many Actor Servers are necessary?
- How many Manager Servers are necessary?
- Which operating system will be used (Windows)?
- Will a Microsoft Cluster Server configuration be used?
- Which network speed is best for the environment?
- Will fiber optic networking be used?
- Will complex objects (1000 or more files/object, configurable) be used, or only non-complex objects (less than 1000 files/object, configurable)?
- How large should the database be?
- How large should the disks be for the arrays?
- Will tapes be used, and if so, which type and which format?
- Will Cloud Object Storage be used, and if so, with which vendor?
- Will the Storage Policy Manager be used?
- Will one or more APIs be used, and which ones (DIVA REST API, DIVA C++ API, DIVA-Java API, or DIVA Web Services API)?
- Which media formats are required?
- Which typical daily operations and functionality are required?
- Will watch folders be used to automate some tasks?
- Will Avid AMC, TMC and/or Interplay be used?
- Which specific “must have” items need to be addressed?



# Supported Environments

This chapter provides setup details for environments that DIVA supports.

## Topics

- [Overview](#)
- [Product Compatibility](#)
- [Hardware and Software](#)
- [Supported Libraries and Control Software](#)
- [Supported Drives](#)
- [Supported Disks](#)
- [Supported Object Storage](#)
- [Supported Partial File Restore Formats](#)
- [Supported Unmanaged Storage Repositories](#)
- [Supported Transcoders](#)
- [Supported Avid Environments](#)

## Overview

The DIVA architecture allows the integration of many different types of servers and technologies, such as Broadcast Video Servers, Storage Area Networks, and Enterprise Tape Group Managed Storage. DIVA can support interoperability among systems, helping to ensure long term accessibility to valued content, and keeping up with evolving storage technologies.

DIVA supports system installations in Windows 2016, 2019, and 2022. All Windows installations must be in English only.

The installation of DIVA varies from site to site. The exact configuration of your specific DIVA platform is not covered in this guide. For details on your specific DIVA System installation and configuration, consult with the Telestream Installation and Delivery Team.

---

**Note:** Telestream recommends keeping the operating system up to date with the latest security patches.

---

The following table identifies Core options and licensing metrics.

Description	Licensing Metric
DIVA System	Per Server
DIVA Single	Per Server
DIVA Actor	Per Server
DIVA Avid Connector	Per Avid Archive Provider
DIVA Partial File Restore	Per System
DIVA Analytics	Per Server
Managed Storage Capacity	Per 500 TB Block
Unlimited Storage Capacity	Per System

## Product Compatibility

DIVA is compatible with other DIVA Core product lines including the following:

- [Postgres Database and DIVA Backup Service](#)
- [DIVA Connect](#)
- [FlashNet to DIVA Migration](#)
- [Supported API Releases](#)

### Postgres Database and DIVA Backup Service

The Database and Backup Service components are installed as an integral part of the standard DIVA system installation. The components are typically installed on the same server as DIVA.

Scheduled backups using the DIVA Backup Service are configured in its configuration file. The DIVA Backup Service manages and monitors the entire backup process. DIVA supports Postgres Database version 14.

The DIVA Backup Service is also used to backup the MongoDB database and Elasticsearch, which are both required for metadata storage and searching.

### DIVA Connect

DIVA Connect 4.0 supports DIVA 8.0, 8.1, 8.3, 9.0 and above. DIVA Connect 4.0 works with DIVA API versions 9.0 and below. The DIVA Connect 4.0 ClientAdapter doesn't inter-operate with the DIVA Connect Core Adapter 3.2 and below. Either DIVA Connect

2.0 or Legacy DIVA Connect must be used when running DIVA Core releases earlier than DIVA Core 7.3.1.

If operating a DIVA Core release earlier than 7.3.1, refer to the *DIVA Connect Installation, Configuration, and Operations Guide*.

## FlashNet to DIVA Migration

---

**Note:** Refer to the FlashNet Product Retirement Announcement located at:  
<https://www.telestream.net/pdfs/support/FlashNet-EOL-Notice.pdf>

---

FlashNet customers can upgrade to DIVA or Kumulate while keeping their yearly payments at the same price as their existing support fees. While the FlashNet licenses will be transferred over at no cost, a modest one-time surcharge will be applied for the professional services needed for the upgrade.

Customers can trade-in their existing FlashNet licenses for either subscription or perpetual licenses. For customers who choose subscription licensing, any content written to storage will continue to be accessible even if that subscription were to lapse.

This upgrade is designed to use the FlashNet-written archives on their existing media, so that customers can avoid a time-consuming media migration.

See the FlashNet Trade-In Program Product Sheet located at:

<https://www.telestream.net/diva/resources/dat-Flashnet-to-DIVA-upgrades.pdf>.

## Supported API Releases

The following legacy API releases and configurations are supported for each major DIVA Core and DIVA release. That is, the last two version-number changes.

---

**Note:** Telestream has deprecated the DIVA C++ API and the DIVA Java API.

---

**Note:** Telestream strongly recommends that you use the DIVA REST API rather than previous APIs such as the DIVA C++ API. The DIVA C++ API is deprecated, but supported for backward compatibility. The DIVA REST API offers new and enhanced features and security.

---

### DIVA REST API

DIVA exposes its functionality through a REST interface. It is self-contained in DIVA and all future DIVA releases. The API is used by the DIVA web app and other internal components (for example, SPM, Migration Service, and so on).

For detailed information, see the *DIVA Application Programming Guide*.

### Web Services APIs

- DIVA REST API: the DIVA REST API is embedded in DIVA.

- WS 2.1: REST and SOAP require the DIVAS component. (Deprecated)
- WS 2.2: REST and SOAP require the DIVA Enterprise Connect component. (Deprecated)

## Supported and Tested Legacy API Configurations

The following API configurations are supported in DIVA and later:

- DIVA C++ API 7.5 to 5.5 on Windows
- DIVA Java API 7.5 to 6.5 on Windows
- Enterprise Connect (latest release) on Windows with the following configurations:
  - http, rest, xml, connect directly to DIVA
  - http, rest, form\_url\_encoded, connect directly to DIVA
  - http, soap, xml, connect directly to DIVA
  - https, rest, xml, connect directly to DIVA
  - https, rest, form\_url\_encoded, connect directly to DIVA
  - https, soap, xml, connect directly to DIVA

## Untested Configurations

The following API configurations are untested. Use them at your own risk:

- C++ and Java Legacy API 7.6 and newer.
- DIVA Core Symphony; that is, DIVAS that uses WSO2 application server.
- Older Enterprise Connect (older than latest release). That is, if another EC is released, only the latest release will be tested.
- Enterprise Connect connected using the DIVA Core Adapter mode.

## Hardware and Software

These are the minimum hardware and software requirements to install and operate the DIVA software. Refer to [General Storage Requirements](#) for detailed disk configuration information.

---

**Note:** MongoDB, in its default configuration, can use up to half the available RAM minus 1GB on the server on which it is installed. You have to plan the location of MDS MongoDB installation accordingly.

---

## DIVA Core Architecture

A DIVA system uses a combination of software modules which can run on a single computer, or can be distributed across different systems.

The main DIVA components are as follows:

## Manager

The DIVA component of the archive also hosting the archive system database.

## Manager Cluster

Based on the Microsoft Cluster configuration. Manager Cluster is only valid in a Windows based environment.

## Actor

Responsible for all data transfers to storage media (Archive, Restore, Copy, Repack, and so on).

## Actor and Manager (Single Computer)

Systems running both Actor and Manager functions on a single computer. Try to avoid this configuration for performance reasons. This is only usable for entry level configurations.

## DIVA Connect 2.1 and later

Used in DIVA Connect configurations for unified access. DIVA Connect 2.1 (and later) is not a drop in replacement for the legacy DIVA Connect. DIVA Connect 2.1 (and later) is specifically for compatibility with DIVA Core 7.5 and later Linux and Windows installations, and not backward compatible with earlier DIVA Core releases before 7.3.1.

---

**Note:** DIVA Connect 4.0 has been released with DIVA.

---

See the DIVA Connect documentation on the Telestream DIVA Support Portal for detailed DIVA Connect information.

## DIVA Web App

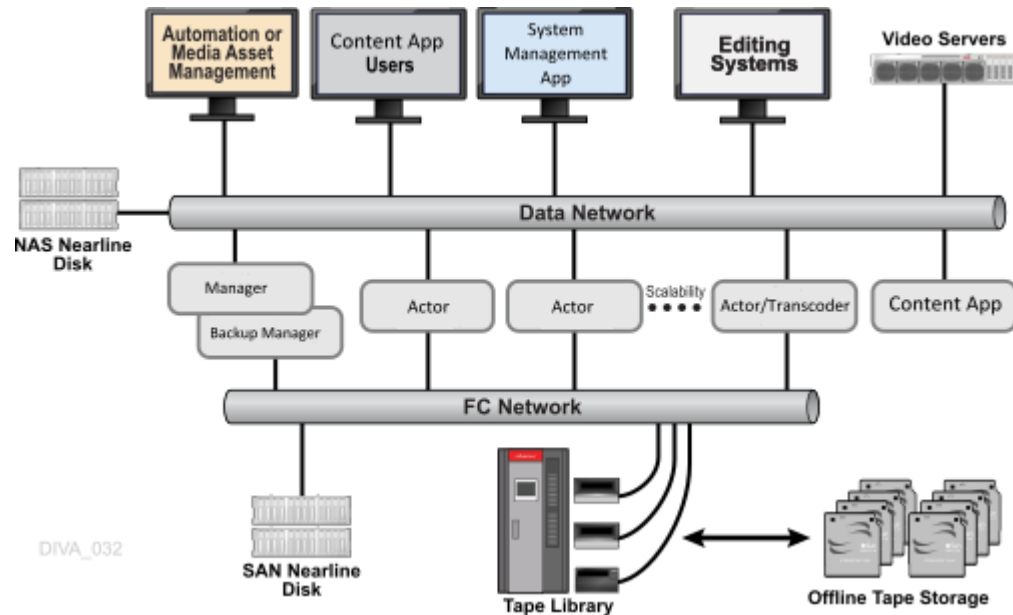
Used for configuring, monitoring and managing the DIVA system.

---

**Note:** Telestream recommends using the Chrome browser to use the DIVA web app.

---

The following figure represents a DIVA configuration with the main DIVA software components installed on different servers. DIVA Connect (used to access multiple DIVA systems) is not represented and is generally installed on a dedicated server.



## System Component Interconnectivity

On the data path, a DIVA solution is connected on the storage side to the Tape Group library, or shared disks, or both. On the source and target side, it is connected to the video servers, NLE, or file servers.

### Storage Connection

SAN (Storage Area Networks), NAS (Network Attached Storage), or Direct Attached technologies can be used. Different types of interfaces are required on the servers to support the different types of storage devices as follows:

- Fiber Channel HBA (Host Based Adapter) for SAN
- SCSI Bus or HBA for Direct Attach
- 10 Gigabit Ethernet for NAS
- Cloud Storage
- Tape Libraries

## Intel and Microsoft Windows

Telestream can deliver x86 architecture servers matching or exceeding the recommendations provided in the following sections (except the Windows license to be purchased). Partners can also purchase servers from other vendors if the minimum requirements are met. Telestream does not qualify or recommend specific models from other vendors.

---

**Note:** The operating system installed on all computers must be installed in the English language. Telestream does not support DIVA computers that have the operating system installed in other languages.

---

## DIVA Appliance

The release of DIVA introduces the DIVA Appliance. The appliance is a pre-built system available to customers that includes hardware and software ready to rack and turn on.

The appliance is supported by the DIVA installer and creates a site/production system that includes some arrays to match the expected hardware. There is currently no special implementation in the DIVA web app for the appliance at this time.

Telestream has generated a wizard on startup to guide customers through importing a license, along with any other configuration required; this has not been implemented at this time.

## Operating System Compatibility

Use the following table to confirm that you have the proper operating system installed for each computer in the system when upgrading your DIVA installation.

---

**Note:** The minimum server operating system for using complex objects is Windows Server 2016.

---

Component	DIVA Release	Operating System Compatibility (for upgrades only)
DIVA and Actor	9.0 and later	Windows Server 2016 Windows Server 2019 Windows Server 2022
DIVA Connect	2.3.1 and later	Windows Server 2016 Windows Server 2019 Windows Server 2022 Oracle Linux 7 x86_64 and later (64-bit)

## Manager

HDD sizing for the Manager is now more complex. With the addition of MongoDB, Elasticsearch, and Postgres, more space is required for successful operations. The following server platform is the minimum requirement recommended for the installation of the Manager software:

- Rack mount chassis
- Intel® Xeon® Silver 4214R 2.4Ghz 12C/24T or equivalent (optional second processor possible)
- 64GB RAM

- Two 2 TB HDD 15,000 RPM or SSD (configured in RAID 1) system disks (and an optional third disk used as a hot spare)

---

**Note:** If DIVA is used to archive complex objects like DPX or Avid sequences, it is advisable to ask for a specific recommendation based on the estimated traffic (in terms of size and number of objects to be archived per day). In general, if complex objects need to be archived, Telestream recommends using a minimum of two 2 TB HDD with 15,000 RPM. This recommendation is also valid for the Backup Manager or an Actor if an Actor server is used for the Backup Manager.

---

- Redundant power supply and fans
- Dual on-board GbE or 10GbE interfaces (copper RJ45 interfaces)
- Dual port 16Gb Fiber Channel HBA (Host Bus Adapter) for Tape library control (only if a tape library is used and requires the use of a dedicated FC connection)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

See the [Minimum Partition Sizing for a Server Hosting Databases](#) table for detailed partition information.

## Manager Cluster

---

**Note:** DIVA has not been tested with clusters at this time.

---

The following server platform (two identical servers) is the minimum requirement recommended for the installation of the Manager software in a cluster environment. A Manager Cluster is only valid in a Windows-based environment.

- Rack mount chassis
- One Intel® Xeon® Silver 4214R 2.4Ghz 12C/24T or equivalent (optional second processor possible)
- 64GB RAM
- Two 2TB HDD 15,000 RPM or SSD (configured in RAID 1) system disks (and an optional third disk used as a hot spare)

---

**Note:** If DIVA is used to archive complex objects like DPX or Avid sequences, it is advisable to ask for a specific recommendation based on the estimated traffic (in terms of size and number of objects to be archived per day). In general, if complex objects need to be archived, Telestream recommends using a minimum of two 2TB HDD with 15,000 RPM. This recommendation is also valid for the Backup Manager or an Actor if an Actor server is used for the Backup Manager.

---



- Redundant power supply and fans
- Two on-board GbE or 10GbE interfaces (copper RJ45 interfaces)
- Dual port SAS or FC HBA (for the shared disk bay connection)

---

**Note:** A shared disk bay with dual RAID controller (SAS or FC Interface) and seven 300 GB SAS disks connected to both servers to accommodate the database.

---

- Dual port 16Gb Fiber Channel HBA for Tape library control (only if a tape library is used and requires the use of a dedicated FC connection)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

See the [Minimum Partition Sizing for a Server Hosting Databases](#) table for detailed partition information.

## Actor

The following is the minimum server configuration recommended for the installation of the Actor software:

- Rack mount chassis
- One Intel® Xeon® Silver 4214R 2.4Ghz 12C/24T or equivalent
- 32GB RAM
- Two 300 GB HDD 15,000 RPM or SSD (configured in RAID1) system disks (optional third disk can be used as a hot spare)
- RAID5 disk space for cache, at least five 1.8TB disks
- Optional RAID5 disk space for Nearline storage (DIVAgrid Architecture)

---

**Note:** The DIVAgrid Architecture consists of aggregating direct attached disks from multiple Actors into one single DIVA array. The Manager distributes content it needs to store on this array across the different Actors composing the array. This provides a cost-effective, high performance solution for Nearline disk storage and is ideal in workflows requiring temporary disk storage to enable the creation of multiple object instances and transcoding.

---

- Redundant power supply and fans
- Two on-board GbE interfaces (copper RJ45 interfaces)
- Dual 10 GbE ports interface
- Dual port Fiber Channel HBA for the connection to an external shared SAN disk (optional)
- Dual port Fiber Channel HBA for the connection to the Tape drives (Qlogic recommended)
- Windows Server 2016

- Windows Server 2019
- Windows Server 2022

See the [Minimum Partition Sizing for a Server Hosting Databases](#) table for detailed partition information.

### Actor and Manager (Single Computer)

The following is the minimum server configuration recommended for the installation of the Actor and Manager software on a single computer. This configuration should be limited to entry level systems for performances reasons:

- Rack mount chassis
- One Intel® Xeon® Silver 4214R 2.4Ghz 12C/24T or equivalent (optional second processor possible)
- 64GB RAM
- Two 2TB HDD 15,000 RPM (configured in RAID1) system disks (optional third disk can be used as a hot spare)

---

**Note:** If DIVA is used to archive complex objects like DPX or Avid sequences, it is advisable to ask for a specific recommendation based on the estimated traffic (in terms of size and number of objects to be archived per day). In general, if complex objects need to be archived, Telestream recommends using a minimum of two 900 GB HDD with 15,000 RPM. This recommendation is also valid for the Backup Manager or an Actor if an Actor server is used for the Backup Manager.

---

- RAID5 disk space—at least five 2TB disks, Redundant power supply, and fans
- Two on-board GbE interfaces
- Two 10 GbE interface (optional)
- Dual port Fiber Channel HBA for the connection to an external shared SAN disk (optional)
- Dual port 16Gb Fiber Channel HBA for the connection to Tape drives (Qlogic recommended)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

See the [Minimum Partition Sizing for a Server Hosting Databases](#) table for detailed partition information.

### DIVA Connect 4.x

The DIVA Connect configuration provides a consolidated view of a distributed DIVA system. The following is the minimum server configuration recommended for the installation of DIVA Connect 4.x:

- Rack mount chassis

- One Intel® Xeon® Silver 4214R 2.4Ghz 12C/24T or equivalent
- 64GB RAM
- Two 480GB HDD 15,000 (configured in RAID1) system disks (optional third disk can be used as a hot spare)
- One 10 GbE interfaces (optional)
- Oracle Linux 7 x86\_64 and later
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

See the DIVA Connect documentation on the Telestream DIVA Support Portal for detailed DIVA Connect information.

## General Storage Requirements

The following table describes the main storage characteristics of the various components:

Server	CPU	System Disks	Cache and Disk	Data Disks
Manager Cluster <sup>1</sup>	1	RAID1	No	No
Manager	1	RAID1	No	No
Actor	1	RAID1	RAID5	Nearline (optional)
Actor and Manager	1	RAID1	RAID5	Nearline (optional)
Actor and Transcoder	2	RAID1	RAID5	Transcoding area plus optional Nearline disk.
DIVA Connect	1	RAID1	No <sup>3</sup>	No

1. Manager Cluster is only valid in a Windows based environment.

### Minimum Partition Sizing for a Server Hosting Databases

The following are the minimum partition sizes for the Manager computer. These minimum sizes are also valid for a Manager Backup configuration or an Actor used as a Backup Manager.

The Postgres database has these minimum requirements:

- Windows 2016 or higher
- 16 GB of RAM

**Caution: All partitions must be protected by RAID.**

Windows Partition	Minimum Size	Recommended Block Size	Comments
C:\	80 GB	Operating System Default	DIVA Software, Operating System, and DB engines
E:\	100 GB	8 kb	Database Data Files
F:\	Windows: 50 GB (exactly)	4 kb	Database Archive Logs
H:\	300 GB	64 kb	Database Backup Folder
G:\	100 GB	Operating System Default	Complex object Metadata Database (optional).
S:\	200 GB	Operating System Default	ElasticSearch Database

## Supported Libraries and Control Software

The following table identifies Managed Storage and associated control software supported by DIVA LibAttach is only valid in a Windows based environment.

**Note:** The latest qualified release of ACSLS is 8.5.1.

Manufacturer	Library	Control Software	Robot Manager Module
Alto	Disk Library	Alto Protocol	ALTO_Robot.dll
Dell	TL4000/TL2000 <sup>1</sup> ML6010 <sup>2</sup>	Direct SCSI/FC	Robot_SCSI
HP	StoreEver, ESL-G3-700, ESL-G3-1500, ESL-G3-3000, ESL-G3-5000, MSL-2024, MSL-2048, MSL-6480	Direct SCSI/FC	Robot_SCSI

<b>Manufacturer</b>	<b>Library</b>	<b>Control Software</b>	<b>Robot Manager Module</b>
IBM	TS3100, TS3200, TS3310, TS3500, TS4500	Direct SCSI/FC	Robot_SCSI
Oracle StorageTek	SL8500 <sup>3</sup> SL500 <sup>4</sup> SL150 9310 5500 L180  L7000 SL24 L80 L40 L20 L1400M	LibAttach 1.4.2 <sup>5</sup> Direct SCSI/FC Direct SCSI/FC ACSL ACSL ACSL or Direct SCSI/FC  ACSL LibAttach 1.4.2 <sup>5</sup> Direct SCSI/FC Direct SCSI/FC Direct SCSI/FC Direct SCSI/FC	Robot_ACSL Robot_SCSI Robot_SCSI Robot_ACSL Robot_ACSL Robot_ACSL or Robot_SCSI  Robot_ACSL Robot_ACSL Robot_ACSL Robot_ACSL Robot_ACSL Robot_ACSL
Oracle StorageTek	SL4000	LibAttach 1.4.25 Direct SCSI/FC	Robot_ACSL Robot_SCSI
Oracle StorageTek	SL3000	LibAttach 1.4.25 Direct SCSI/FC	Robot_ACSL Robot_SCSI
Overland Tandberg	NEO XL Series	Direct SCSI/SAS	Robot_SCSI
Qualstar	TLS-5000 RLS-85210 Q series	Direct SCSI/FC Direct SCSI/FC Direct SCSI/FC	Robot_SCSI Robot_SCSI Robot_SCSI

<b>Manufacturer</b>	<b>Library</b>	<b>Control Software</b>	<b>Robot Manager Module</b>
Quantum (ADIC)	Scalar i6000	Direct SCSI/FC	Robot_SCSI
	Scalar i500	Direct SCSI/FC	Robot_SCSI
	Scalar i40/i80	Direct SCSI/FC	Robot_SCSI
	Scalar i3/i6	Direct SCSI/FC	Robot_SCSI
	Scalar 100	Scalar DLC or Direct SCSI/FC	Robot_ADIC or Robot_SCSI
	Scalar 1000	Scalar DLC or Direct SCSI/FC	Robot_ADIC or Robot_SCSI
	Scalar 10000	Scalar DLC or Direct SCSI/FC	Robot_ADIC or Robot_SCSI
	Scalar 12000	Scalar DLC or Direct SCSI/FC	Robot_ADIC or Robot_SCSI
	Scalar i2000 <sup>6</sup>	Scalar DLC or Direct SCSI/FC	Robot_ADIC or Robot_SCSI
Sony Petasite	S60	PSC 5.00	Robot_Sony
Sony ODA	ODS-L10	Core Robot Manager	Robot_SCSI
	ODS-L30M	Core Robot Manager	Robot_SCSI
	ODS-L60E	Core Robot Manager	Robot_SCSI
	ODS-L100E	Core Robot Manager	Robot_SCSI
Spectralogic	T-Finity	Direct SCSI/FC	Robot_SCSI
	T950	Direct SCSI/FC	Robot_SCSI
	T680, T380, T200	Direct SCSI/FC	Robot_SCSI
	T120	Direct SCSI/FC	Robot_SCSI
	T50e	Direct SCSI/FC	Robot_SCSI
ALTO	ALTO-III	ALTO Manager	Robot_ALTO
	ALTO-ARX		

1. The Dell TL2000 is an IBM TS3100 library.
2. The Dell ML6010 is an AIDC i500 library.
3. Operational upon robot failure when configured with multiple LSMs and one robot per LSM.
4. The SL500 library will be transitioned to End of Life (EOL) soon.
5. DIVA only supports 32-bit LibAttach and not 64-bit.

6. Autoclean is not supported, but the Scalar i2000 with partitioning is supported.

### Disk Archive Corporation ALTO

ALTO is an offline, cold storage archive; a secure and convenient alternative to data tape, optical disk, and cloud for Petabyte sized volumes of valuable media assets. ALTO uses data file replication to create multiple non-segmented replicas of files on removable media. ALTO systems can be distributed between on-premises and other geographically separated locations. Disks can be bar-coded and externalized to vault storage for air-gap security providing a copy of last resort for disaster recovery.

DIVA supports ALTO storage in two different ways:

- With Virtual File System (VFS), in which case multiple Alto disks are combined and presented by VFS as a Virtual Disk. From the DIVA web app the storage appears as a DIVA Array.
- Direct API integration, in which case Alto is considered as a removable storage system like tape libraries or Sony ODA. DIVA tracks and exposes the content stored on each disk and groups can be created as with tapes or ODA.

## Supported Drives

The following drives are supported by DIVA.

Manufacturer	Drive Model
HP	LTO-3, LTO-4, LTO-5, LTO-6, LTO-7, LTO-8, LTO-9
IBM	LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, LTO-6, LTO-7 <sup>1</sup> , LTO-8, LTO-9  <b>Note:</b> When a virgin LTO-9 tape is mounted into a drive for the first time, it will require an initialization that may take between 30 minutes and 2 hours. In DIVA, the consequence is the positioning step will take between 30 minutes and 2 hours.  3592 Jaguar TS1120, TS1140, TS1150, TS1155, TS1160
Oracle StorageTek	Titanium 10000-A, 10000-B, 10000-C, 10000-D 9840A, 9840B, 9840C, 9840D, 9940A, 9940B
Sony (Optical)	ODS-D55U, ODS-D77F, ODS-280F, ODS-280U <sup>2</sup> , ODS-D380F

1. Drivers for the IBM LTO-7 and LTO-8 drives only exist for Windows Server 2012.

2. The ODS-280U has not been qualified for use with DIVA.

### Sony ODA Optical Drives

Sony ODA Blu-ray Optical Drives are supported in DIVA on Windows only. The drives are viewable as a Tape Group Drive and Cartridge (having UDF format) in the DIVA web app on the Resource Management > Drives page.

The drives must be configured using the Optical Disk Archive Utility before configuring DIVA on the system.

The Windows Device Manager will display the drives as an Unknown Device because there are no drivers available for them. Several configuration files must be modified to include these drives in the DIVA System. See the DIVA Installation and Configuration Guide for detailed information.

The details of these drives are as follows:

- DIVA has only been tested with the ODS-280F Fiber Channel type. These drives are twice as fast as the Gen1 drives. The ODS-280U has not been qualified for use with DIVA.
- The cartridge available for the ODC3300R WORM drive has a 3.3 TB capacity.
- Gen2 drives can read content written on Gen1 media with Gen1 drives. DIVA does not support the READ-ONLY media drive compatibility. Telestream recommends isolating Gen1 media from Gen2 media in the configuration (no cross-generation compatibility), and there must be at least one Gen1 drive in a library containing Gen1 cartridges.
- Sony ODA Gen 3 is supported. The drive type is ODS-D380F and uses the following new cartridge:

**–Cartridge Type:**

ODC5500R

**–Capacity**

5.5 TB

**–Drive Type**

WORM

---

**Note:** The drive is still R/W compatible with ODC3300R and read-only compatible with older cartridge types.

---

## Supported Disks

DIVA supports the following disks:

- Direct Connection using a local path  
For example drive letters in Windows such as M:\managed\_disk.
- CIFS Connection
- FTP Connection
- Harmonic MediaGrid
- Tiger MetaSan
- Quantum StoreNext Filesystem
- IBM GPFS (General Purpose Filesystem)
- Huawei OceanStore 9000



- Dell PowerScale (Isilon)

### Cache Disk

This disk is only used for caching, Tape Group to Tape Group copying, Tape Group spanning, and Tape Group repacking operations. The cache does not have to be on a RAID protected disk, but it is recommended.

The size of this disk must be at least the size of the largest object. The cache disk can be a local disk, SAN, NFS, or SMB connected. Telestream recommends setting the cache disk block size to at least 64KB.

### Storage or Storage and Nearline

The disk will be used for storing objects and Nearline operations. The storage size depends on the amount of space desired to store objects. This disk must be RAID protected.

A storage disk can also be used for cache. The storage disk can be a local disk, SAN, NFS, or SMB connected. Telestream recommends setting the storage disk block size to at least 64KB.

## Supported Object Storage

The following table identifies object storage accounts supported by DIVA Core 9.0.

Object Storage Type	Protocol	Supported Storage Classes	AXF Reference-File	Auto-Indexing	AXF Discovery
Alibaba OSS	S3	Standard, IA (Infrequent Access), Archive, ColdArchive	Yes	Yes	Yes
AWS S3	S3	Standard, Intelligent-Tiering, Standard-IA, One Zone-IA, Glacier, Glacier-Deep-Archive, Glacier-Instant-Retrieval	Yes	Yes	Yes
Azure Blob Storage	Blob REST API	Standard, Hot, Cool, Cold, Archive	Yes	Yes	Yes
Ceph	S3	Standard	Currently Not Tested	Yes	Yes
Cloudian	S3	Standard, Archive	Yes	Yes	Yes

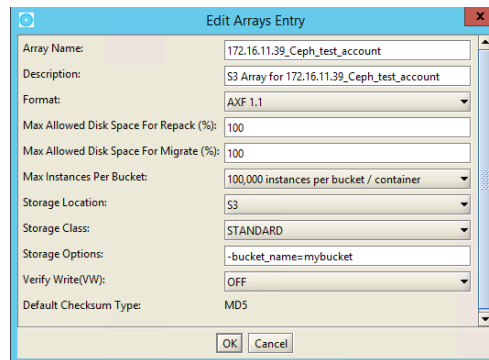
Object Storage Type	Protocol	Supported Storage Classes	AXF Reference-File	Auto-Indexing	AXF Discovery
EMC ECS	Swift / S3	Standard	Yes	Yes	Yes
Google Cloud Storage	JSON API	Standard, Nearline, Coldline, Archive	Yes	Yes	Yes
HCP (Hitachi Content Platform)	S3	Standard	Yes	Yes	Yes
Isilon OneFS (8.2 and later)	S3	Standard	Yes	Yes	Yes
NetApp StorageGRID	S3	Standard	Currently Not Tested	Yes	Yes
ObjectMatrix MaxiStore	S3	Standard	Yes	Not currently tested.	Not currently tested.
Oracle Cloud Storage	OCI	Standard, Archive	Yes	No	No
Scality	S3	Standard	Not Supported Yet	Yes	Yes
Tata Cloud Storage	S3	Standard	Yes	Yes	Yes
Backblaze	S3	Standard	Yes	No	Yes
Wasabi	S3	Standard	Yes	Yes	Yes

### Ceph Implementation Notes

The current Ceph implementation cannot create a bucket in Ceph storage yet due to the Ceph current implementation of the S3 protocol, so the bucket must exist before it can be written to. For use as disk (versus use as a server) the user must provide the bucket to use through the `-bucket_name` option in the Storage Option of the corresponding array definition.

There must be two buckets created prior using Ceph as a Storage Array, one for storing data and one for metadata. For example, `mybucket` and `mybucket-metadata`. Those

two buckets must be created and specify `-bucket_name=mybucket` in the array configuration in Storage Options as shown in the following figure:



## Configuring HCP (Hitachi Content Platform) for Multi-part Upload

To configure HCP for multi-part upload, do the following:

1. Disable the etag verification. To disable etag verification, browse to *Configuration > Resources > CLOUD STORAGE CLOUD BUCKETS*. Set the parameter *Additional Checksum Verification* to *None*.
2. In the HCP Management Console, browse to *Namespace > Settings > Optimization*. Set only the option *Optimized for Cloud Protocols*.

## Supported Partial File Restore Formats

Numerous object formats have been tested successfully with the DIVA Partial File Restore operation. Testing with samples provided by the customer is recommended to confirm interoperability. Telestream makes no commitment if variations in the encoding profiles cause issues with the DIVA Partial File Restore feature. All formats support AUTO\_DETECT.

Access the Partial File Restore settings in the DIVA web app under *Configuration > System Settings > Actors > Edit Actor > Partial Restore Settings*, and in the DIVA configuration file.

Contact Telestream Support for more details about each implementation.

---

**Notes:** All formats are supported on Windows. However, Linux currently supports only GXF, QuickTime, MPEG2 Transport Stream, BWA, and MXF. The initial DIVA release does not support Linux.

---

## GXF (General Exchange Format)

GXF Partial File Restore is supported in the following formats:

Type	Formats
Aurora Edit	MPEG2 D10 MPEG2 I-frame MPEG2 D10 MPEG2 LGOP
BitScream	DV25
K2 Media System	MPEG2 D10 MPEG2 I-frame MPEG2 D10 MPEG2 LGOP
K2 Media System / Summit	AVC-I DVCPRO XDCAM HD
Mseries	MPEG2 D10 MPEG2 I-frame MPEG2 LGOP
NewsEdit	DV25 DV50 MPEG2 D10 MPEG2 I-frame
PDR	MJPEG
Profile XP	DV25 DV50 MPEG2 D10 MPEG2 I-frame

### ■ MXF (Material Exchange Format)

MXF standard specification (SMPT377M) defines multiple operational patterns. Only OP1a is supported. MXF Partial File Restore is supported on Windows and Linux in the following video essence formats:

- DV25, DV50, DV100
- DVCPRO (SD and HD)
- DNxHD
- MPEG2 D10<sup>1</sup>
- MPEG2 LGOP (SD and HD)
- SONY XDCAM HD
- H.264/MPEG-4 AVC
- AVC-Intra (subset of H.264)

---

1. MXF generated by Seachange are supported as standalone MXF files (no .pd or .vix file).

- SONY XACV (subset of H264, HD and 4K)
- DNxHR (new codec from AVID for high definition)

---

**Note:** Although these video formats are supported, qualifications are still required because there might be many variations of MXF wrapper for a given video essence format.

---

For Windows, BMX is the default library. MOG SDK can only be used for temporary compatibility by going to the DIVA web app under Configuration > System Settings > Actors > Edit Actors > Partial Restore Settings and click the down arrow for MXF. Under the settings, changing the Use BMX Library parameter to off using the slide switch.

## AVI (Audio Video Interleaved)

The applicable wrapper format is a single AVI file per object, and may contain audio tracks. This Partial File Restore is supported by AUTO\_DETECT only.

### Adobe Premiere

Supports DVSD and PCM video and audio essences.

### Harris Corporation Nexio 3600

Supports DVSD and PCM video and audio essences.

## AVI with Separate WAV Files

The applicable file format is a single AVI file with separate WAV files. The AVI file contains a single video track, and the WAV files contain a PCM sample format. This Partial File Restore is supported by VIDEO\_FORMAT\_AVI and AUTO\_DETECT in Windows only.

Manufacturer	Product	Release	Supported Video and Audio Essence
Insipiens	AVI Writer	1.0.0.0	MPEG2 LGOP
Matrox	MQSink Filter Format 4	2.0.0.271	DV25, DV50
	MQSink Filter Format 6	2.0.0.271	Dv25, DV50, DVSD
	MQSink Filter for MPEG Format 4	2.0.0.270, 2.0.0.271	MPEG2 LGOP, MPEG2 I-Frame <sup>1</sup>
	DSX AVI File Format 6	1.0.0.362, 1.0.0.401	MPEG2 LGOP <sup>2</sup> , M701 HD

1. MPEG2 I-Frame supported on 2.0.0.271 only.

2. MPEG2 LGOP supported on 1.0.0.362 only.

## AVI with FFV1 or FFVH

AVI clips containing FFV1 or FFVH video essence are supported. Use these formats for video preservation purposes. These codecs are lossless and generate intra-coded frame only (no GOP).

## QuickTime/MP4

QuickTime is a file wrapper and may contain multiple tracks of various types (audio, video, and so on). QuickTime self-contained clips are supported using OMNEON and AUTO\_DETECT.

QuickTime Partial File Restore is supported by Windows Actors only.

Partial File Restore support for QuickTime with MPEG2 LGOP (XDCAM HD 422 with sixteen tracks of audio) is supported as follows, regardless of the type of video or audio content:

- The number of tracks per clip is currently limited to thirty.
- Tracks must have the same duration and start time.
- QuickTime standards support advanced edit list features that are not supported by Partial File Restore.
- Each track must be composed of a single valid edit list entry that may or may not start from zero.

Some content types are not supported, including some video and audio combinations. The following table identifies supported types:

Supported Track Types	Cardinality
Video	One video track per clip
Video	Two video tracks per clip <sup>1</sup>
Audio	Zero or multiple tracks per clip
Closed Caption <sup>2</sup>	One track per clip
Timecode with a single entry	One track per clip
Timecode with multiple entries	One track per clip

1. When a QuickTime clip contains two video tracks, the tracks must be synchronized and have the same duration and start from 00:00:00:00.
2. Empty Closed Caption tracks are supported.

## QuickTime Self-Contained Clips

The format of the video essence is not a criterion in QuickTime Self-Contained clips. In theory, the Partial File Restore for QuickTime should be able to support any type of video essence. Partial File Restore is not recommended for the following variations in the video essence format:

- Where the video quality supports 420 or 422
- Where the number of pixels is not a factor
- Where the clip is bit rate independent

The following table describes what has already been tested and does not guarantee that Partial File Restore will support it. The only supported audio formats are AIFF and WAV (LPCM).

Manufacturer	Product	Release	Supported Video Essence
Dalet			DVCPRO100
Omneon	Spectrum	5.x	DV25, DVCPRO, DVCPRO50, DVCPRO HD, MPEG2 D10, MPEG2 I-Frame, MPEG2 LGOP, MPEG2 LGOP HD
Oracle	SAMMA solo	Unknown	DV25

### MP4 Clips

MP4 wrapper is also known as MPEG-4 Part 14. This format has been developed based on QuickTime specifications. All the formats currently supported by the QuickTime partial restore are also supported with MP4.

## LXF (Leitch Exchange Format)

LXF (Leitch Exchange Format) is well defined, and Partial File Restore supports specific releases of the file format regardless of the source of the clip (Nexio, Flip Factory, and so on). The supported job format is either AUTO\_DETECT or VIDEO\_FORMAT\_LEITCH.

The LXF Release 0 supported video and audio essences are:

- MPEG2 I-frame Standard Definition (SD)
- MPEG2 LGOP SD
- DV
- DVCPRO
- DVCPRO50

The LXF Release 1 supported video and audio essences are:

- MPEG2 4:2:2 (1080i and SD only)
- DV SD
- DVCPRO SD
- DVCPRO50 SD
- DVCPRO HD

## DIF with Separate WAV Files, and DV with Separate Audio, or Self-contained DV Types

The applicable file format is a single DIF or DV file with separate WAV files, and DV with separate audio or self-contained DV types. WAV files contain the PCM sample format. This Partial File Restore supports Avid Liquid and Omneon Spectrum with DV25 and WAV PCM using either AUTO\_DETECT or VIDEO\_FORMAT\_OMNEON.

## BWAV (Broadcast WAV)

BWAV (Broadcast WAV) is a regular WAV file that includes additional information—Bext and iXML (optional). Bext is a broadcast extension containing metadata, including TimeReference (timecode reference in milliseconds). DIVA Core uses Bext as a timecode reference for Partial File Restore.

BWAV may also contain an optional metadata called iXML. The metadata iXML contains an additional TimeReference and a frame rate. When iXML and Bext are both present, DIVA uses iXML because it contains an accurate frame rate (useful to convert milliseconds to and from a timecode). Without iXML, the millisecond to timecode conversion is only an approximation.

## Supported Unmanaged Storage Repositories

DIVA transfers content to and from external equipment such as broadcast video servers, video editing systems, and generic computer systems. The following are the certified interfaces and protocols supported by DIVA.

### Unmanaged Storage Repositories

The following table identifies the source and target servers supported by DIVA.

Manufacturer	Server Model	Protocol	Unicode Support
Avid Airspace	See FTP_STANDARD table.	FTP	See the Avid Connectivity and Tools Guide.
Avid Interplay	ISIS or NEXIS	AVID_DHM AVID_DET AVID_AMC AVID_DIRECT	Yes, currently for AMC only.
DataExpedition	Expedat 1.15, Expedat 1.16	MTP	Yes
Dell PowerScale	Isilon	SMB	Yes
Disk (Local)	Internal disk	Direct	Yes
Disk (Network)	Shared File System, SAN, NAS	CIFS	Yes



Manufacturer	Server Model	Protocol	Unicode Support
EVS	Little Big Server, XT3	FTP	No
Grass Valley	NewsEdit, NewsFTP (Aurora Edit HD), UIM Gateway with MXF <sup>1</sup> , K2 <sup>2</sup>	FTP	Only K2 is supported.
Leitch	VR Series <sup>3</sup> , Nexio 3600	FTP	Only Nexio 3600 is supported.
Omneon	Spectrum 4.6 SR2 Spectrum 4.7 SR2 Spectrum 5.0 SR1	FTP and AVI player FTP and AVI Player FTP and AVI Player	Only Spectrum 5.0 SR1 is supported.
Omneon	Spectrum 6.1 with System Manager 5.14	FTP Only	Yes
Omneon	MediaGrid <sup>4</sup> 1.1	Mapped drive using MediaGrid file system drivers	Yes
Quantel	SQserver regional server with ISA gateway <sup>5</sup>	FTP	No
Sony	News Base Hyper Agent	FTP	No
Various (UNIX, Windows, Mac)	Any standard FTP server (RFC-959)	FTP	No
	Secure FTP server V3 (limited support)	SFTP	No

1. UIM Gateway with MXF is supported for release 2.0.6.3.
2. GXF and MXF formats are supported.
3. Supported only using WanStreamer or ArchiveStreamer.
4. Linux does not support MediaGrid because the API it depends on is not Linux compatible.
5. MXF supports release 2.1-22.09. Release 2.1-22.10 supports intelligent archive in TAR format.

The following table identifies FTP servers supporting FTP\_STANDARD.

Manufacturer	Product Name	Core Actor Qualified	Unicode Support	WFM Qualified	OTU Qualified
Microsoft	IIS	Yes <sup>1</sup>	No	Yes <sup>2</sup>	Yes
FileZilla	FileZilla FTP Server	Yes	Yes	No	Yes
Gene6	Gene6 FTP Servers	Yes	Yes	No	No

1. Actor supports IIS with UNIX-like listing type configured.
2. WFM supports IIS with DOS-like listing type configured.

## Supported Transcoders

DIVA supports the use of Vantage for performing transcoding operations. The following table lists the DIVA | DIVA Core and DIVA version and the qualified versions of Vantage:

DIVA   Content Director Version	Vantage Version
DIVA 7.1	4.1
DIVA 7.2	6.2
DIVA 7.3	6.3
DIVA 7.4	6.3
DIVA 7.5	7.1
DIVA 7.6	7.1
DIVA 7.7	8.1
DIVA 8.0	8.1
DIVA 8.1	8.1
DIVA 8.2	8.1
DIVA 8.3	8.1
DIVA 9.0	8.1

## Supported Avid Environments

DIVA supports Avid Connectivity and MediaCentral | Asset Management DIVA Connector version 4.6.0. For more detailed information see the Avid Connectivity and Tools User Guide.

## Avid Interplay Compatibility

The following identifies current Avid Interplay release compatibility for DIVA:

The following are supported for Avid connectivity and Interplay:

- AMC [2.1]: Interplay 2.2 or later: DIVA Core 8.0 or later
- AWD [1.0]: Interplay 3.6 or later: DIVA Core 8.3 or later

## MediaCentral Compatibility

The MediaCentral | Asset Management DIVA Connector version 4.6.0 is now tested and qualified with DIVA. This means DIVA and this DIVA Connector release can be updated if it is not release 4.6.0, and then all the releases of MediaCentral listed can be supported. This new connector release can be used in the following MediaCentral | Asset Management systems:

MC   AM Release Date	AM Build Number
2019.6	7.2
2019.9	7.3
2020.4	7.4
2020.9	7.5
2021.3	7.6
2021.7	7.7
2021.11	8.0
2022.3	8.0.1
2022.12	8.1
2023.7	8.1

# Security Guidelines

This chapter provides security guidelines for DIVA.

## Topics

- [Security Overview](#)
- [Installation planning](#)
- [The Security Model](#)
- [DIVA Web App Access Control](#)
- [Internal Communication Security](#)
- [Secure Deployment Checklist](#)

## Security Overview

### Keep Software up to Date

Stay current with the version of DIVA that is being run. Current versions of the software are available for download at the Software Delivery Cloud located at:

<https://www.telestream.net/telestream-support/content-manager/support.htm>

### Restrict Network Access to Critical Services

DIVA uses an identified list of TCP and UDP ports, as well as HTTPS access for REST APIs. For DIVA to operate correctly, these ports may have to have access restricted, or permission granted, on a per server basis.

## Run as DIVA User and use Principle of Least Privilege Where Possible

Don't run DIVA services using an Administrator (or root) operating system user account. Always run all DIVA services using a dedicated operating-system user named diva.

## DIVA User Profiles in the DIVA Web App

Configure DIVA user profiles by navigating to the Configuration > User Management page on the left menu of the DIVA web app.

The DIVA system provides five fixed user profiles as follows:

- System Administrator
- Administrator
- Advanced Operator
- User
- Service

All accounts require a password to obtain access. Passwords must be assigned in the DIVA web app before using these profiles.

Passwords are created during installation and configuration for both the Administrator and Operator accounts. Telestream recommends that the passwords be changed every 180 days (minimum) thereafter. Passwords must be made available for Technical Support if needed.

---

**Note:** Each DIVA component uses its own dedicated user name and password to connect to the main application.

---

## Postgres Database Security

Access rules are defined in Postgres configuration to control and restrict access to the DIVA database. Make changes to those settings carefully, so that you don't jeopardize database access restrictions.

The databases (PostgreSQL and MongoDB) are secured via https connections and credentials stored within encrypted files.

## Monitor System Activity

Monitor system activity to determine how well DIVA is operating and whether it is logging any unusual activity. Check the log files located in the installation directory under /Program/log/. Refer to the DIVA Operations Guide for details on system monitoring and logs.

## Keep up to Date on Latest Security Information

For security information and alerts for a large variety of software products, see <http://www.us-cert.gov>.

The primary way to keep up to date on security matters is to run the most current release of the DIVA software.

## Using Anti-virus Software

Install Anti-virus and exclude the DIVA processes and storage (for performance reasons).

## Installation planning

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

## The Installation Environment

To better understand security needs, ask the following questions:

### Which Resources Need to be Protected?

Many of the resources in the production environment can be protected. Consider the type of resources that to protect when determining the level of security to provide.

Protect the following resources when using DIVA:

#### Primary Data Disks and Disk Arrays

There are Data Disk and Cache Disk resources used to build DIVA systems. They are typically local or remote disks connected to the DIVA systems. Independent access to these disks (other than by DIVA) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

#### Database Disk, Metadata Disk, and Backup Disks

There are Database Disk, Metadata Disk and Backup Disk resources used to build DIVA systems with complex objects. They are typically local or remote disks connected to the DIVA systems. Independent access to these disks (other than by DIVA) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

#### Tapes and Tape Groups

It is a security risk to allow independent access to tapes where data is written; typically in a tape library controlled by DIVA systems.

### **Export Tape Metadata**

Tape Metadata dumps that are created from export operations contain data and metadata. This data and metadata permissions must be restricted to only the Administrator (or root) operating system account, or the DIVA operating system user (or Tape Group) during a routine export or import activity.

### **Configuration Files and Settings**

DIVA system configuration settings must be protected from operating system level non-administrator users. Making the configuration files writable to non-administrative operating system users presents a security risk, therefore, these file permissions must be restricted to only the Administrator (or root) operating system account, or the DIVA operating system user.

### **From whom are the resources being protected?**

In general, the resources described in the previous sections must be protected from all non-administrator access on a configured system, or from a rogue external system that can access these resources through the WAN or FC Fabric.

### **What will happen if the protections on strategic resources fails?**

Protection failures against strategic resources can range from inappropriate access (that is, access to data outside of normal operations) to data corruption (writing to disk or tape outside of normal permissions).

## **Recommended Deployment Topologies**

This section focuses on security concerns. Consider the following points when installing and configuring DIVA, and refer to the DIVA Installation and Configuration Guide for details.

### **Separate Metadata Network**

For connections between DIVA services components, connection to the Metadata Database, and the connection from its clients, provide a separate TCP/IP network and switch hardware that is not connected to any WAN. Because the metadata traffic is implemented using TCP/IP, an external attack on this traffic is theoretically possible. Configuring a separate metadata network mitigates this risk and also provides enhanced performance. If a separate network is infeasible, at least deny traffic to the DIVA ports from the external WAN and any untrusted hosts on the network. Refer to the DIVA User Guide for complete procedures.

### **Fiber Channel Zoning**

Use Fiber Channel Zoning to deny access to the DIVA disks connected through the Fiber Channel from any server that does not require access to the disks. Preferably, use a separate FC switch to physically connect only to the servers that require access.

## Safeguard SAN Disks Configuration Access

SAN RAID disks can usually be accessed for administrative purposes through TCP/IP or more typically HTTP. Protect the disks from external access by limiting the administrative access to SAN RAID disks to systems only within a trusted domain. Also, change the default password on the disk arrays.

## Install the DIVA Package

First, install only required DIVA services for the environment. For example, if not planning to run the DIVA web app from a system, then deselect them in the list of components to be installed during installation. The default DIVA installation directory permissions and owners must be restricted to only the Administrator (or root) account, or the DIVA operating system user. Refer to the DIVA Installation and Configuration Guide for full installation details.

## Tape Security

Prevent external access to tapes inside a tape library controlled by the DIVA system. Unauthorized access to tapes can compromise or destroy user data.

## Backup Production Databases

Set up and perform database backups using the DIVA Backup Service. Permissions for the backup dump must be restricted to only the Administrator (or root) operating system account, or the DIVA operating system user. Telestream recommends configuring a minimum of one (ideally two) remote database backup location other than the primary one located on the Manager primary location.

Refer to the DIVA Database and BKS Installation, Configuration and Operations Guide for details.



# The Security Model

The critical security features that provide protections against security threats are:

## Authentication

Ensures that only authorized individuals are granted access to the system and data.

## Authorization

Access control to system privileges and data. This feature builds on authentication to ensure that individuals get only appropriate access.

## Tape Group Encryption

Tape drive encryption securely supports bulk tape migration between DIVA systems.

## SSL Authentication and Secure Communications

DIVA includes SSL Authentication for services, and to secure DIVA internal and API communications. Certificate authentication provides unique identification and secure communication for each DIVA Service in a network.

## DIVA Web App Access Control

Access control in DIVA is divided into profiles as described below. Accounts require a password to obtain access. Account passwords must be assigned in the DIVA web app before using these profiles.

### System Administrator (sysadmin)

The System Administrator uses the sysadmin profile to log into the DIVA web app. This profile allows access to all functions of the DIVA web app and should only be used by System Administrator when making additions, deletion, or changes to the DIVA system.

### Administrator (admin)

To issue jobs to DIVA, such as archive or restore jobs, or to eject a tape from a library, the Administrator profile must be used. The password for this profile must be assigned in the DIVA web app before using the profile. For more information, refer to the DIVA Installation and Configuration Guide on the DIVA Technical Support site.

## Advanced Operator (*advoperator*)

In addition to User profile permissions, the Advanced Operator profile in the DIVA web app can now optionally enable privileges for canceling and changing the priority of jobs. The options are defined in the DIVA web app. By default, this option is disabled.

## Operator (*operator*)

In addition to User profile permissions, the Operator profile in the DIVA web app can now optionally enable privileges for canceling and changing the priority of jobs. The options are defined in the DIVA web app. By default, this option is disabled.

## User (*user*)

This is a very restrictive profile. After the connection to the Manager is established, the DIVA web app will only allow the user to monitor DIVA operations. This is known as the User profile. Not all functions that issue commands to DIVA are accessible while in the User profile mode, enabling situations where monitoring is required but no commands are permitted to be sent to DIVA.

# Internal Communication Security

## Secure Sockets Layer and Authentication

DIVA includes SSL Certificate Authentication for authentication of services, and securing the internal and API communications in DIVA. Certificate authentication provides unique identification and secure communications for each DIVA service in a network.

DIVA includes a Default Root CA (Certificate Authority) called DIVA\_CA. The DIVA\_CA Certificate Authority is a self-signed authority that signs all SSL certificates for the DIVA Core services. Every DIVA service now has its own password protected private key and a SSL certificate signed by the DIVA\_CA authority.

Certificate authentication functions similar to identification cards like passports and drivers licenses. For example, passports and drivers licenses are issued by recognized government authorities. SSL certificates are signed by a recognized CA. An SSL certificate verifies the identity of its owner. When the SSL certificate is presented to others, it helps verify the identity of its owner based on the quality of the contents of the certificate.

An external third party CA (for example, VeriSign and Comodo) can be used to generate and sign the certificates.

## External Certificate Authorities

External third party CAs (for example, VeriSign, Comodo, and so on) are usable with DIVA. The external CA must create a CSR (Certificate Signing Request) for DIVA\_CA, signed by the third party CA, and the third party certificate must be added to the Trust Store to satisfy the SSL Certificate Chain.

When connecting to the DIVA web app for the first time, there is usually a security error page displayed by the web browser. This error means that the HTTPS server certificate is not trusted by the browser. This is the certificate for the DIVA REST API Gateway (*DIVA\Program\security\certificates\RestAPIService.p12*). This issue is caused by the fact that the certificates generated by DIVA were self-signed. This is verifiable by showing the certificate because it has been issued “by” and “to” the same organization. You may accept the risk and continue to connect, but you will always get the same error for every new connection.

The DIVA security tool (*DIVA\Program\security\bin\DIVASecurityTool.bat*) has been fixed to generate certificates signed DIVA certificate authority (DIVA\_CA). With the new security tool, the new certificates are no longer self-signed.

Before applying the security tool (before DIVA 9.0), make sure to make a backup copy of *DIVA\Program\DIVA\_CA\DIVA\_CA.cnf* because it contains the list of domains or IP addresses to connect to the DIVA web app. If the DIVA web app is being accessed using `https://IP_Address/DIVASecurityTool/login`, the IP address must be listed in the `alt_names` section. This also applies to domain names or host names. The second security tool option will automatically add the IP address and the host name of the server to the `alt_names` section is at the end of the file.

With the fixed security tool, you must generate new certificates (option 2) and restart all the DIVA services. Contact Telestream Technical Support for assistance as necessary.

## Security Tools

DIVA release includes *DivaSecurityTool.bat*, a Windows security tool.

The tool is located in the `%TSCM_HOME%/security/bin` directory. You can use it to generate SSL certificates used for secure communication in DIVA.

## DIVA REST API Security Changes

The DIVA REST API includes the ability to establish secure communications with the Manager.

---

**Note:** Telestream strongly recommends that you use the DIVA REST API rather than previous APIs such as the DIVA C++ API. The DIVA C++ API is deprecated, but supported for backward compatibility. The DIVA REST API offers new and enhanced features and security.

---

## Dual Ports

All internal DIVA services can only connect to secure ports. The DIVA web app will report an SSL Handshake Timeout if attempting to connect to the non-secure port.

## SSL and Authentication

DIVA consist of services in Java and C++. The format in how certificates and keys are represented are different in each. DIVA has the keys and certificates for JAVA services in a Java Keystore file, and in PEM (Privacy Enhanced Mail) format files for the C++ services.

The Manager can simultaneously support two communications ports—one secure, and one unsecure. The default secure port number is 8000 and the unsecure default port number is 9000.

All internal DIVA Core 8.x services (DIVA web app, Migration Utility, Actor, SPM, WFM, SNMP, Robot Manager, RDTU, and Migration Services) can connect only to secure ports. The DIVA web app will report an SSL Handshake Timeout if attempting to connect to the non-secure port. Clients using the DIVA Java API or DIVA C++ API are allowed to connect to either port.

The following is a relative snippet from the Manager configuration file:

```
# Port number on which the DIVA Manager is waiting for incoming
connections.
# Note: If you are using a Sony library and plan to execute the
DIVA Manager
# on the same machine as the PetaSite Controller (PSC) software, be
aware
# that the PSC server uses the 9000 port and that this cannot be
modified.
# In that situation, you have to use a different port for the DIVA
Manager.
# This same warning applies to FlipFactory which uses ports 9000
and 9001.
# The default value is 9000.
DIVAMANAGER_PORT=9000

# Secure port number on which the DIVA Manager is waiting for
incoming connections.
# The default value is 8000.
DIVAMANAGER_SECURE_PORT=8000
```

A new folder called %TSCM\_API\_HOME%/security is added to the DIVA API installation structure as follows:

```
%TSCM_API_HOME%
  security
    conf
```

The conf folder contains the SSLSettings.conf file that is used to configure the SSL handshake timeout.

# Secure Deployment Checklist

After the post-install configuration of DIVA, go through this security checklist:

1. Set strong passwords for Administrator (or root) and any other operating system accounts that have any DIVA administrator or service roles assigned to them, including:
  - Postgres User IDs (if being used)
  - Any disk array administrative accounts.
2. Do not use a Local Administrator operating system account. Assign roles as needed to other user accounts.
3. Change the default password for the sysadmin user. Upon installation the default is `changeit`.
4. Set a strong password for Administrator and Operator for the DIVA web app. A password must be assigned for these profiles in the DIVA web app before use.
5. Set a strong password for the database login.
6. Install a firewall on every system and apply the default DIVA port rules. Restrict access to the DIVA API (TCP/9000) to IP addresses that require access using firewall rules.
7. Install operating system and DIVA updates on a periodic basis since they include security updates.
8. Install Anti-virus and exclude the DIVA processes and storage (for performance reasons).
9. It is best practice to segregate FC disks and FC tape drives either physically or through FC Zoning so that disks and tape devices do not share the same HBA port. For managed disks, only Actors should have access to disk and the tape drives. This security practice helps prevent loss-of-data accidents resulting from accidental overwriting of tape or disk.
10. Set up an appropriate set of backups of the DIVA configuration and database. Backups are part of security and provide a way of restoring data lost either accidentally, or through some type of breach. Backups should include some policy while being transported to an off-site location. Backups need to be protected to the same degree as tape groups and disk.
11. Technical Support strongly recommends using an external Certificate Authority for additional security.

# DIVA Installation and Setup

This chapter describes DIVA software components and system installation.

## Topics

- [Software Component Distribution](#)
- [Database Setup](#)
- [DIVA Installation](#)

## Software Component Distribution

The DIVA platform is flexible and scalable, so the installation of some software components can vary depending on the degree of storage and servers that are managed. Small installations can have all DIVA software components installed on a single computer. A very large installation will have these components distributed among several servers. All of these components run as system services.

The following table identifies where the components typically are installed:

Component	Location
Managers	Main and Backup Manager servers
Postgres Database	Main and Backup Manager servers
Metadata Database	Main and Backup Manager servers
Backup Service	Main and Backup Manager and Actor servers

Component	Location
Robot Managers	Main and Backup Manager servers. Robot Managers can also be installed on a separate server when the tape library is installed a substantial distance from the Manager servers.
Storage Policy Manager	Main and Backup Manager servers
VACP Services	Main and Backup Manager servers
SNMP Agent	Main and Backup Manager servers
Connect	Main and Backup Manager servers
Actors	Actor servers
Transfer Manager Communicator (TMC)	Actor servers
Archive Manager Communicator (AMC)	Actor servers
Watch Folder Monitor	Actor servers
Proxy Service	Main and Backup Manager servers
Metadata Service	Main and Backup Manager servers
Rosetta	Main and Backup server

## Database Setup

### Installation and Configuration 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.

---

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 DIVA 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 DIVA 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 DIVA 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 DIVA 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 DIVA 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 DIVA web app successfully.

In some cases, a network firewall between the two can prevent a connection. For complete operation and functionality of the DIVA 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 DIVA 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.

---

## 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 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.

## Database Installation, Upgrade, and Configuration

These are the general Database installation and upgrade processes.

### Prerequisites

Before starting a new installation, review the [Supported Environments](#) that provides the supported operating systems, databases, and especially the [Minimum Partition Sizing for a Server Hosting Databases](#).

### Database Dump Files

The initial DIVA release doesn't contain a process for exporting database dump files from the Oracle database; nor a process for importing database dump files into Postgres database.

### DIVA Database Server Removal

Before installing the new Postgres Database, uninstall the existing database and database engine. If the DIVA database is already installed on the computer, then you must remove the existing database and database engine.

### 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. To install the new database, do the following:

---

**Note:** The Postgres installer isn't included in the initial DIVA release. Install Postgres separately.

---

1. Back up and uninstall the existing database.  
See [Uninstalling the DIVA Database Server in Windows](#).
2. Open a Windows command line.
3. Navigate to %TSCM\_HOME%\Releases\16\_Postgres\_Bundles.
4. Locate the Postgres zip file and unzip it.
5. Execute *install.bat*.
6. *Standard Database*: select option 1 or leave this blank.
7. *Please enter the drive letter for the Postgres binary installation*: The default and recommended drive is C:.
8. *Database Mount Points*: The default and recommended option is 2 (2 = E:\pg\_data, F:\pg\_wall).
9. *Database Memory Target*: The default and recommended option is 16384 MB.
10. *Suggested Database User Processes*: The default and recommended option is 300.
11. *Postgres User Password*: set and confirm the password.  
Telestream recommends the standard Postgres password of *postgres*.

**12.** To execute the installation press ENTER.

When the installation has completed Command displays the results.

**13.** After confirming the installation was completed successfully, press any key to close the Command window.

### Postgres Administration App

**Note:** Telestream recommends you use this application only with assistance from Telestream Technical Support. Don't attempt to access or make any changes to the database directly.

Postgres is delivered with an 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|-tableonly] [-
custom_tablespaces tables_tablespace indexes_tablespace
temp_tablespace]

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

Parameter	Definition
<code>syspasswd</code>	Password of the Postgres sys account.
<code>username</code>	Username to create
<code>userpasswd</code>	Associated user password
<code>postgres_connection</code>	Postgres service name or connection string (such as <code>IP_ADDRESS:PORT/POSTGRES_SERVICE_NAME</code> ).

Parameter	Definition
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	<ul style="list-style-type: none"> <li>• Use of custom tablespaces               <ul style="list-style-type: none"> <li>-tables_tablespace: tablespace for tables</li> <li>-indexes_tablespace: tablespaces for indexes</li> <li>-temp_tablespace: database temp tablespace</li> </ul> </li> </ul>
-postgrespwd	Option to reset/generate password file.

## Migrating DIVA Database Server from 8.3 to 9.1

Contact Telestream Support for help migrating DIVA Database Server from 8.3 to 9.1.

## DIVA Installation

The following sections describe installation of the DIVA system. Contact Technical Support if you need assistance.

---

**Notes:** The Postgres Database must be available for DIVA before installation. See [Database Setup](#), and [Backup Service \(BKS\) Overview](#).

Before upgrading from DIVA 8.3 to DIVA 9.x on a system with cloud storage, you must confirm that the Array Name, Disk Name, and Cloud Account Name are all the same. If you configured multiple arrays per cloud account it will not work because of database constraints. In this case, you will need to convert this manually after the upgrade is complete by using the Configuration Utility. Otherwise, the DIVA web app will not be able to display the cloud array settings correctly.

---

## Steps for Installation and Setup of DIVA

DIVA 9.0 installer includes an option to install the MDDB (Metadata Database). It is run in silent mode during installation.

The following procedure is a basic overview of the installation process on Windows. See the following operating system-specific sections for detailed instructions.

1. Install the DIVA Database user when running the DIVA installer. In Windows this is a check box.
2. While installing the database user, make sure to import the license (otherwise the Manager Service will not start until the license is imported using the DIVA web app after installation).
3. Configure the basic, essential, Manager settings to get the Manager Service operational.
4. Configure the DIVA REST API.
5. Start the DIVA web app and log in under the sysadmin account; then create a DIVA web app user. This is done so the sysadmin account is not being used to configure or view the DIVA system in the DIVA web app.
  - a. Click the *Add User* button.
  - b. In the displayed dialog box enter the Username, Password, and select the user's role. In this case, the new user should be assigned an admin role. Sysadmin and admin have the same authority in the system with the exception that an admin cannot manage users.
  - c. Click Save to save the new user. The user will now appear in the Users list.
6. Log out of the DIVA web app and then log back in with the user account just created (not the sysadmin account).
7. Configure the Network Servers, and so on until DIVA is fully installed and configured.

## Installed Features and Services

The following Windows Services are installed by the DIVA installer, based on your selections:

- DIVA Connect REST API Adapter
- DIVA Backup Service
- DIVA DB Agent
- DIVA Metadata Service
- DIVA REST API Data Service
- DIVA REST API Discovery
- DIVA REST API Gateway
- DIVArchive Actor
- DIVArchive WFM
- DIVArchive Manager
- DIVArchive Robot Manager
- DIVArchive VACP
- MongoDB Set 0
- RabbitMQ

## Downloading the Software

You must stay current with the release of DIVA that you install and operate. Current releases of the software are found on the Software Delivery Cloud.

Use the following procedure to obtain the DIVA software:

1. Log in to the Software Delivery Cloud and search for DIVA.
2. Select the licenses you require (for example, Actor, Manager, and so on). You must search each time after adding a new license to the list.
3. Select the operating system you run for each selected license using the Select Platform button.
4. Continue through the download wizard, accepting the terms, until the final download screen appears.
5. Confirm that all the licenses you require are listed.
6. Click Download All on the bottom right of the screen, or click the file name link, to download the software.
7. Save the download where it is easily accessible.

## Installing or Upgrading DIVA

1. Open the *DIVACore Setup* dialog.
2. In the *Destination Folder* field, browse to or enter the path to the destination folder. Click *Next*.
3. Choose either *Install* or *Upgrade*, as desired. Click *Next*.
4. From the list in the *Select components to install* field, choose the options to install, as desired.
5. Click *Next*.  
DIVA displays dialogs for the options selected.
6. Complete the dialogs for the options selected.  
For details about these options, see [Options for Select Components to Install](#).

## Options for Select Components to Install

### Installing Metadata Database Installation (Optional)

To install the service, do the following:

1. Run cmd.exe as administrator.
2. Change directory to the DIVA\Program\Metadataservice\bin folder.
3. Type metadata\_service.bat install.

For more details about other options this script supports, see metadata\_service.bat help.

This option installs MongoDB and supports the following configuration options:

- **MDDB Data Folder:** this is where MongoDB stores its data. The default is H:\MDDBData. If H: drive does not exist, the default is C:\MDDBData.
- **MDDB Port:** the default is 27017.

---

**Note:** If this port is changed, DIVA services that use this port will still default to 27017, so you will need to change those service configurations too).

---

After the MDDB (Metadata Database) is installed, it can be used by the DIVA MDDB Service. The MDDB service is the DIVA REST API micro-service that allows Manager and other services to access the database. The MDDB Service is installed in the DIVA\Program\Metadataservice folder. The configuration file is located in the DIVA\Program\conf\metadata\_service folder, and log file is located in the DIVA\Program\log\metadata\_service folder.

---

**Note:** This command accepts parameter such as -dburl, -certpath, and so on, which will reset values configured in appsettings.json file. If you decide to modify the appsettings.json file directly, their values will be overwritten if the service is re-installed again.

---

The MDDB service requires MDDB to work correctly; which must be configured in the ~\DIVA\Program\conf\metadata\_service\appsettings.json file as a ConnectionString. The metadata-service.bat assumes ConnectionString = "mongodb://127.0.0.1:27017/Core" by default. However, this only works if MDDB is installed on the same server. If the MDDB Service is running on an operating system that MDDB does not support, you must manually update the connection string to point to correct server where MDDB is installed.

You can verify whether the MDDB Service is running correctly by navigating to <https://127.0.0.1:1777/index.html> which shows the Swagger documentation page for this service.

## Notification Service Installation (Optional)

The DIVA installer refers to RabbitMQ as the Notification Service instead of RabbitMQ, because RabbitMQ is simply an implementation.

### New windows installation

This option installs RabbitMQ and requires the following configuration setting:

- **Notification Data:** This is the folder where rabbitmq stores persistent notification queues. Logs and some configuration files are also stored in this folder.

---

**Note:** The path to this folder is specified in a text file: ~\DIVA\rabbitmq\_server\etc\NOTIFICATIONDataDir.txt. This file is used by the installer when DIVA is upgraded into identify the path. However, the actual setting for the

RabbitMQ service is in the Windows registry. Do not change the value in this file to cause RabbitMQ to use a new data directory. You must modify the registry if a different directory is desired.

---

The RabbitMQ application (the binary) folder is the DIVA\rabbitmq\_server folder. After the installation, RabbitMQ runs as a Windows service.

The install\_rabbitmq.bat and uninstall\_rabbitmq.bat are not meant to be used by regular users. Support and admin users may edit these files to understand how RabbitMQ was installed or uninstalled.

Name	Date modified	Type	Size
CollectSysInfo.bat	2021-03-01 9:28 AM	Windows Batch File	23 KB
CollectSysInfo.ksh	2019-08-03 9:11 AM	KSH File	8 KB
DivaApi.dll	2015-12-18 2:27 AM	Application exten...	873 KB
DIVAConfigurationPrinter.bat	2021-09-16 10:19 AM	Windows Batch File	5 KB
DivaScript CLI reference.docx	2016-10-15 11:56 AM	Microsoft Word D...	62 KB
DivaScript CLI reference.pdf	2016-10-15 11:56 AM	Adobe Acrobat D...	264 KB
DivaScript.exe	2016-10-17 11:14 AM	Application	181 KB
DivaService.exe	2017-10-27 7:18 AM	Application	38 KB
FindMetadataFile.bat	2021-09-16 10:19 AM	Windows Batch File	4 KB
FlashnetMigration.bat	2021-09-16 10:19 AM	Windows Batch File	3 KB
Gather_Activity_Statistics.bat	2021-09-16 10:19 AM	Windows Batch File	51 KB
GetVersion.exe	2019-08-03 5:21 AM	Application	49 KB
install_rabbitmq.bat	2021-09-16 10:19 AM	Windows Batch File	2 KB
lynxLocalDelete.bat	2021-09-16 10:19 AM	Windows Batch File	6 KB
rdtu.bat	2021-09-16 10:19 AM	Windows Batch File	1 KB
servicetag.vbs	2019-08-03 9:11 AM	VBScript Script File	1 KB
uninstall_rabbitmq.bat	2021-09-16 10:19 AM	Windows Batch File	1 KB
wrapper.dll	2021-09-16 10:19 AM	Application exten...	366 KB
wrapper.exe	2021-09-16 10:19 AM	Application	677 KB
wrapper.jar	2021-09-16 10:19 AM	Executable Jar File	122 KB

The install\_rabbitmq.bat batch file requires erlang installer to be placed inside the C:\DIVA folder; this script does not work as delivered. The DIVA installer also does not use it directly; it is just there to document the install procedure.

However, the uninstall\_rabbitmq.bat batch file can be used as delivered to uninstall RabbitMQ service. To execute the file (also not intended to be used by regular DIVA users), run *uninstall\_rabbitmq.bat C:\DIVA*.

---

**Note:** The uninstall\_rabbitmq.bat will also uninstall Erlang runtime. After it is uninstalled, you cannot reinstall it by running install\_rabbitmq.bat unless you have a copy of Erlang installer in the C:\DIVA folder.

---

The DIVA installer also creates the RabbitMQ advanced.config file, which is stored in the DIVA\Program\rabbitmq\advanced.config folder. This file enables a secure web socket connection that is required for the DIVA web app Running Requests page to display new requests in real-time.

After a successful installation use the following URL to access the RabbitMQ admin console and DIVA installer will always create a default admin user (username wsuser and password changeit): <http://127.0.0.1:15672>.



## Windows Installation Upgrade

When you upgrade DIVA, the installer overwrites files that already exist.

During upgrade, you can change the location of data folder but by default, installer will take the value from the DIVA\rabbitmq\_server\etc\NOTIFICATIONDataDir.txt file. If the user does not want to change it, it will be use the same folder as the previous RabbitMQ installation.

---

**Note:** Other than the data folder setting, no other settings are preserved after performing the upgrade; every setting will be reset back to defaults. There are no settings that the user should change in RabbitMQ.

---

## Database Schema (Optional)

This option requires Postgres Database to be installed and setup properly and it will install the DIVA database schema and user to that database. It supports the following options:

- **DB User:** Schema User
  - **DB Password:** Schema User's password
  - **DB Master Password:** The master user (the postgres password when you install setup Postgres DB).
  - **DB Name:** Schema's Name. Unlike Oracle, we recommend use same value as Schema's User because if you want to install more than one schema on the same Postgres DB, each schema must have unique DB Name and user
  - **License File Path:** path to the DIVA license file
  - **DB Agent Base Path:** This is the folder where DIVA will store DB Backups
  - **DBA Service User:** The user name to run DBAgent service (this needs to be an administrator user because DBA needs to access network shares to copy backup files to and from)
  - **DBA Service Pass:** The password for the user to run DBAgent service
- If the DB Agent File Path does not exist the following error message is displayed. Create the desired path to proceed.

## DIVA Appliance (Optional)

This option requires all other options to be also selected except the DEMO option. It sets up a DIVA system with one Actor and an empty configuration. It is designed to install DIVA on a customer's production server, but due to the specific details of the production environment being unknown, it only starts DIVA with an empty configuration. The DIVA web app must be used to complete the rest of the DIVA setup. It supports the following options:

- **Localhost Ip:** It is recommended to use the actual IP of the production server instead of the loopback IP (127.0.0.1).
- **Manager Port:** Manager's legacy API port.

## DIVA Demo (Optional)

This option requires all other options to be also selected except the Appliance option. It sets up a DIVA system with two Actors, local disk servers, a simulated tape library (and so on) to allow demonstrating DIVA features. This option should work on most DIVA servers, but is not designed to be flexible enough to work on any DIVA server. For example, if your DIVA server does not have a C: drive or H: drive, it may not work correctly. When the DEMO installation is complete, a fully working DIVA system should be installed and setup.

DEMO supports the same options as Appliance, but also asks you to enter:

- **DIVA Data Folder:** this is the folder where DIVA managed and unmanaged storages will be stored under (for example, source/destinations, disk arrays, simulated tape libraries, and so on).

The installation logs are available in:

```
C:\DIVA\Program\log\diva_upgrade\diva_upgrade.trace.log
```

# Post-Installation Configuration

This chapter describes DIVA configuration after a fresh installation.

## Topics

- [Configuration Overview](#)
- [Module Configuration Files](#)
- [Environment Variables](#)
- [Manager Configuration](#)
- [Configuring the DIVA REST API Gateway](#)
- [Accessing the DIVA Web App](#)
- [Importing the License](#)
- [Database Backup Configuration](#)
- [The Actor](#)
- [Configuring SMTP Messages](#)
- [The Metadata Database](#)

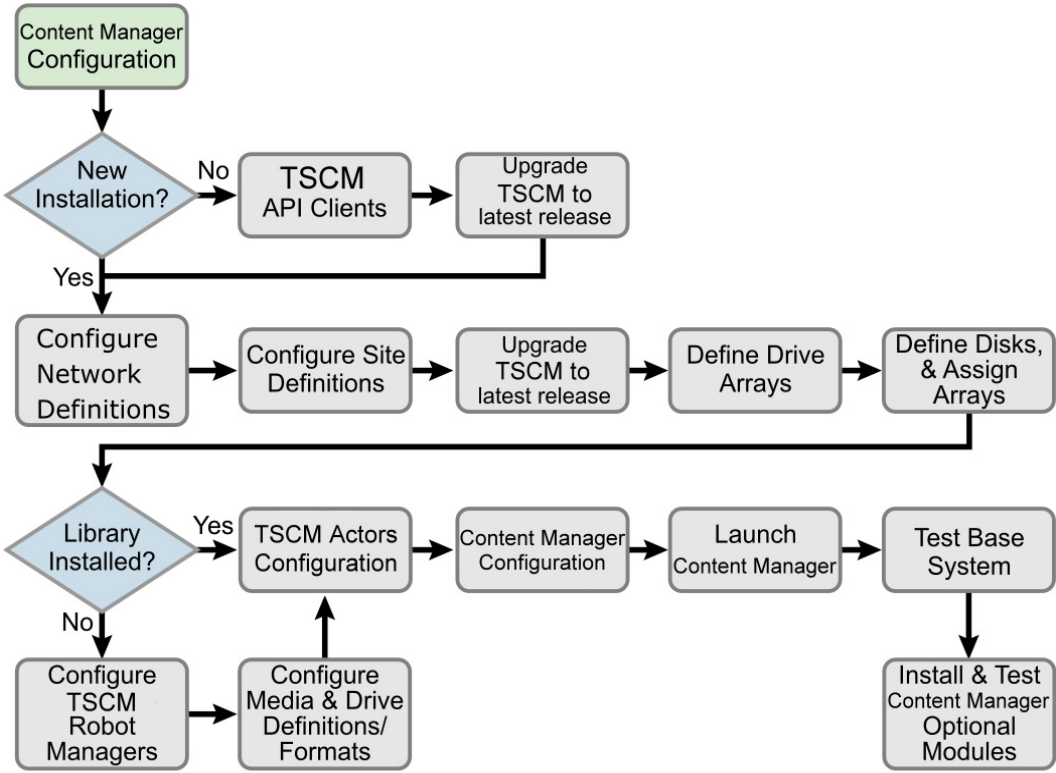
## Configuration Overview

There are many interrelated components in a DIVA System. The following figure shows the basic configuration workflow.

The configuration of DIVA is hierarchical and top-level parameters such as Networks, Sites, Arrays, and Disks need to be configured before configuring other components such as Actors.

If you intend to modify an existing DIVA system, you must always start by backing up the existing DIVA installation, configuration files, and especially the DIVA and Metadata Databases.

Contact Technical Support before making any modifications to your DIVA platform if you are unsure about any steps in the procedures, or require clarification.



DIVA 031

## Module Configuration Files

Each DIVA software module has its own static configuration text file with parameters needed to launch that particular application. The files are typically denoted with the “.conf” file name extension. There are some DIVA modules that use an XML based file rather than a text file for their configuration and those will be noted where applicable.

Unlike older releases of DIVA Core that stored these configuration files in the same folder as the application itself, DIVA centralizes them to a dedicated conf subfolder under the DIVA Program Group.

The configuration files are typically updated with additional or changed settings in newer releases of the software. A new or patch release of DIVA will have the new releases of the .conf files appended with an .ini extension. For example, the new release of the Manager Configuration file will be named manager.conf.ini. You must remove the .ini extension after the installation is complete and the new configuration file updated.

Each configuration file can be opened and edited with any plain text editor (for example, Windows Notepad or Notepad++).

Any changes made to the configuration file of a DIVA software component requires that the component be shut down and then restarted for the changes to take effect. The exceptions to this are the Manager and DIVA Connect options, both of which allow configuration changes to be reloaded while they are still running. There are code dependencies between some applications in the DIVA platform, so other components may also need to be restarted for changes to take effect.

## Environment Variables

Some DIVA software components may require defining one or more Windows operating system environment variables for those components to launch successfully.

An environmental variable allows the configured variable to be available to all programs rather than requiring it to be configured from the application each time it is executed. This makes the variable independent of the application and therefore you do not need to manually insert or update the value when the application software is updated or modified.

A User Environmental Variable only applies to an individual Windows User Profile. A System Environmental Variable is applicable to all Windows User Profiles.

This variable defines the path of the Java Runtime Environment for DIVA applications on the Windows host. This particular parameter is required on any Windows computer that will run the DIVA web app.

## Configuring the DIVA JAVA Home Environment

---

**Note:** This is simply an example and not required for DIVA\_JAVA\_HOME. DIVA\_JAVA\_HOME already points to a valid JRE after installation.

---

To configure the DIVA\_JAVA\_HOME environment variable on a Windows system, do the following:

Use the following procedure to configure an environment variable:

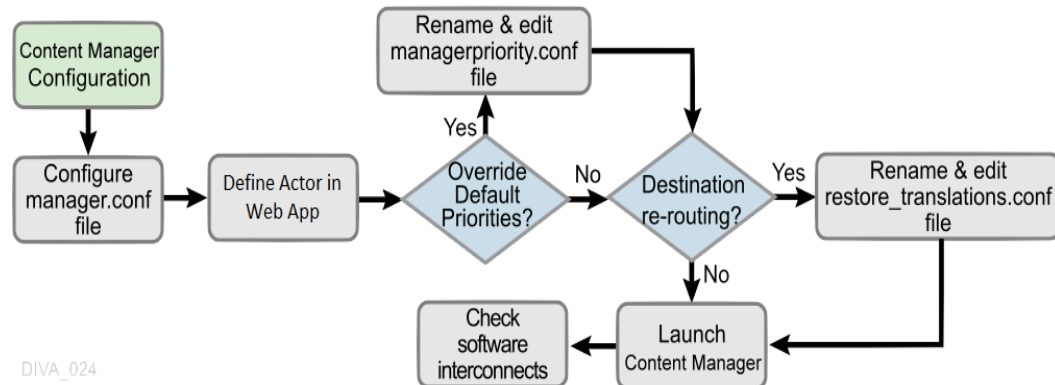
1. Open the Windows Control Panel.
2. Double-click the System icon.
3. Click the Advanced tab.
4. Click the Environment Variables button.
5. Click the New button.
6. Enter the variable name in the Variable name field. In this example the name is DIVA\_JAVA\_HOME.
7. Enter the variable value in the Variable value field. This is the path (or other value) to use for the named variable. In this example the value is C:\DIVA\java.
8. Click OK to complete the process.

You have now defined the variable and it is displayed in the System variables list. The DIVA\_JAVA\_HOME environment variable is now accessible to all users (and applications) on the system and does not need to be defined each time an applications is executed.

## Manager Configuration

The Manager module is located in %DIVA\_HOME%\Programs\Manager\bin and runs as a Windows service. The static configuration file for the Manager is manager.conf. You can typically leave most settings in this file left at the default values. The settings that would normally require updating are highlighted in bold type.

The following figure is the workflow for installing a Manager:



## Local Manager Configuration

The Manager is the main component in a DIVA system. All archive operations are controlled and handled by the Manager. Operation jobs are sent by initiator applications through the Client API. As a purchasable option, Manager also supports Main and Backup systems.

The Manager runs as a Windows Service. The service can be managed through the Windows Services screen. The static configuration file for the DIVA is `diva.conf`. Most settings in this file can typically be left set to the default values. Operations of DIVA can be monitored by launching the DIVA web app.

The batch files in the DIVA bin folder can be used to perform the following major operations:

- Start, stop, and restart the DIVA Service. All of these operations can be executed using the DIVA batch file by specifying `start`, `stop`, or `restart` after the `diva.bat` command respectively (for example, `diva.bat start`).
- You can also terminate all jobs with a `graceful_shutdown` command. The `graceful_shutdown` command waits until all jobs have terminated before stopping the Manager instead of the abrupt shutdown that occurs with the `stop` command.
- Notify the Manager of any changes to the DIVA configuration using the `NotifyManager` batch file.
- Import tapes into a Tape Group using the `importtapes` batch file.
- List all active connections and end some connections (by connection identifier) with the `ConnMgr` batch file.

The `diva.bat` file enables running DIVA as a service or using a console window. Execute the batch file using the following command and parameters:

```
%DIVA_HOME%\Program\diva\bin\diva.bat [command] [options]
```

For example:

```
%DIVA_HOME%\Program\diva\bin\diva.bat start -conf config_file_name.conf
```

Appending the `-conf` (or `-f`) option after one of the following commands specifies a specific configuration file to load settings from. The `diva.bat` command parameters are as follows:

- `install (-i)`  
Installs DIVA as a system service.
- `uninstall (-u)`  
Removes DIVA service.
- `start`  
Starts DIVA.
- `stop`  
Stops DIVA immediately if it is running.
- `graceful_shutdown`  
Stops DIVA after all jobs running at the time of the shutdown have terminated and ignores any new jobs.
- `restart`  
Stops and subsequently starts DIVA.
- `reload`  
Requests that the current service reloads its settings.
- `status`  
Determines whether the service is running and displays the status.
- `dump`  
Requests that DIVA Service create a system dump.
- `version (-v)`  
Displays DIVA version information and then exits.
- `help (-h)`  
Displays help information and then exits.

The static configuration file in new installations is initially named `manager.conf.ini`. You must remove the `.ini` extension for it to be recognized by the Manager.

The configuration file is divided into five distinct groups; Basic, Database, Advanced, Logging, and Service settings. You must not modify the Service settings section, and therefore, not covered in this manual. Values defined in this section must only be altered with instruction from Technical Support.

Each parameter section in the configuration file contains information on defining that parameter. The information lines are commented out (start with `#`) and ignored by the Manager. Any parameter definition that is missing the equal sign is also ignored.

Spaces in the parameter settings are significant. Do not put extra spaces before or after the parameter names or their values. If you have trouble running the Manager after



configuring the manager.conf file, confirm that spaces are not present in any of the parameter values you have defined.

Restarting the Manager can disrupt a live Network. You can make most of the customizations in the configuration file effective immediately using the restart command line switch.

If you intend to update your existing DIVA system with a newer software release, you must use the manager.conf.ini from the new release. You must update the Basic and Database settings with the values from the old configuration file. The new release configuration file may have additional settings or updates included; this applies to all DIVA software modules when installing a release updated.

## Basic Settings

Except for the SERVICE\_NAME, these parameters are always required and must be defined for the Manager to start successfully. These settings define how other DIVA software components and DIVA API clients connect to the Manager.

---

**Note:** These settings are not re-loadable while the Manager is running. You must restart the Manager for them to take effect.

---

The following table describes the Basic settings in the manager.conf file:

Parameter	Parameter Type	Description	Default
SERVICE_NAME	Name	You can use this parameter to specify the name of the service. If not defined, the Service Name defaults to Manager.	
DIVAMANAGER_NAME	Name	The name this Manager instance uses to identify itself to other Managers sharing its resources. Otherwise, this is arbitrary. It must be unique in a system running multiple Managers except for Main and Backup Managers (configured as a cold standby). In this instance, the names should be identical.	DIVA
DIVAMANAGER_PORT	TCP Port Number: unsecure connections	This is the name this Manager instance uses to identify itself to other Managers sharing its resources. Otherwise, this is arbitrary. It must be unique in a system running multiple Managers except for Main and Backup Managers (configured as a cold standby). In this instance, the names should be identical.	DIVA
DIVAMANAGER_SECURE_PORT	TCP Port Number: secure connections	The secure TCP port used by DIVA Services and the DIVA API.	8000

## Database Settings

These parameters define the location and instance of the DIVA Database. Except for the DIVAMANAGER\_TNSNAME parameter, you must define all settings in this section for the Manager to launch successfully.

The following table describes the Database settings in the manager.conf file:

Parameter	Parameter Type	Description	Default
DIVAMANAGER_TNSNAME	Name	<p>The TNS Name of the DIVA Schema within the Postgres database. DIVA ignores this setting if the DIVAMANAGER_DBHOST and DIVAMANAGER_DBPORT settings are defined.</p> <p>This feature requires Postgres installed on the host running the Manager. If this setting is defined, the location of the Postgres driver must be added to the wrapper.java.library.path setting (located in Service settings section of the file); otherwise, the Manager will not start as a service.</p> <p>Example:            wrapper.java.library.path=.;C:\app\postgres\product\11.1.0\BIN</p>	
DIVAMANAGER_DBHOST	IP Address or Host Name	This specifies the Host Name or IP Address of the computer containing the DIVA Database. If using a host name, this must be present in the hosts file on the computer where the Manager is installed.	
DIVAMANAGER_DBPORT	TCP Port Number	The Postgres Listener port configured during the DIVA Database installation.	5432
DIVAMANAGER_DBSID	Name	The DIVA Database SID (Instance System Identifier) in Postgres where Manager connects.	

Parameter	Parameter Type	Description	Default
DIVAMANAGER_DBUSER	Name	The user name the Manager uses to connect to the DIVA Database. This is typically diva (case sensitive).	diva
DIVAMANAGER_DBSERVICENAME	Name	Postgres ServiceName setting. Either this value or DIVAMANAGER_DBSID must be set. If both are set, this takes precedence over the SID.	No default value, but lib5.world is recommended.
DIVAMANAGER_DBSID	Name	Postgres ServiceName setting. Either this value or DIVAMANAGER_DBSERVICENAME must be set. If both are set, DIVAMANAGER_DBSERVICENAME takes precedence over SID.	No default value, but lib5.world is recommended.

## Advanced Settings

You typically leave the parameters in this section are typically left at their defaults. They customize the DIVA default behavior for task execution, resource allocation, and the number of connections it will accept from DIVA applications and DIVA API clients. These parameters are normally adjusted or fine-tuned after completing the initial installation of DIVA.

Most (but not all) of these settings can be altered while the Manager is running by using the reload option.

The following table describes the Advanced settings in the manager.conf file:

Parameter	Parameter Type	Description	Default
DIVAMANAGER_TO_LOWER	true or false	Sets case sensitivity for DIVA. If set to true, then all Object names, categories and tape groups will be set to lowercase.	false
DIVAMANAGER_REQUEST_SCHEDULING_QUEUE_SIZE	Number of jobs	The maximum number of jobs that can be queued for processing by DIVAMANAGER_MAX_CONCURRENT_REQUESTS processors of the Job Scheduler.	500
DIVAMANAGER_MAX_CONNECTIONS	Number of Connections	Specifies the maximum number of simultaneous client connections the Manager will accept. This includes Actors, web apps, API connections, and support tools.	200
DIVAMANAGER_MAX_SIMULTANEOUS_REQUESTS	Number of Jobs	The maximum number of jobs processed by the Manager. When this limit is reached, any further jobs will be rejected. The maximum tested value for this setting is 2000.	500
DIVAMANAGER_API_TASK_QUEUE_SIZE	Number of tasks	The number of tasks that will be accepted to the API command processing queue. If this queue is full, subsequent commands will be rejected. The maximum tested value is 2000.	
DIVAMANAGER_MAX_INACTIVE_REQUESTS	Number of Jobs	Maximum number of inactive jobs that cannot find resources examined by the Job Scheduler each time it is activated.	0
DIVAMANAGER_TYPICAL_VIRTUALOBJECT_SIZE	Percentage	<p>During operation an Actor retrieves the file size of an Object before an archive transfer. This value determines the best location on the tape for the file.</p> <p>Some servers do not indicate the file size of an Object before a Direct Archive. Therefore, DIVA will use this value as an estimate for tape selection.</p> <p>You must define this setting so that most Objects to be archived in the DIVA system are below this size.</p>	10 (percent)
DIVAMANAGER_MAX_CONCURRENT_REQUESTS	Number of Jobs	The maximum number of concurrent jobs executed by the Manager. The maximum tested value for this setting is 16.	8

Parameter	Parameter Type	Description	Default
DIVAMANAGER_MAX_SPAN_SEGMENTS	Number	DIVA will attempt to span the file across two or more tapes if no more writable tapes with enough free space are available to archive a file. This setting defines the maximum number of tapes across which the Object will be spanned.	2 (segments)
DIVAMANAGER_INITIAL_DB_CONNECTION_LIMIT	Number of Connections	The initial number of database connections available to the Manager.	1
DIVAMANAGER_MIN_DB_CONNECTION_LIMIT	Number of Connections	The minimum number of database connections available to the Manager.	1
DIVAMANAGER_MAX_DB_CONNECTION_LIMIT	Number of Connections	The maximum number of database connections available to the Manager.	10
DIVAMANAGER_CAPACITY_LOW_WATER_MARK	Percentage	When the percentage of the total used capacity reaches this amount, periodic warning messages are issued in the DIVA web app.	90 (percent)
DIVAMANAGER_ENABLE_SPANNING_LARGE_VIRTUALOBJECTS	true or false	Enables spanning of large Objects. This parameter overrides SPAN_SEGMENTS if any Object in the system is known to be too large.	true
DIVAMANAGER_INACTIVITY_TIMEOUT	Time in Seconds	The maximum time a physical connection can remain idle in a connection cache before it is terminated (in seconds).	3600
DIVAMANAGER_MAX_VIRTUALOBJECTS_FOR_REPACK	Number	Repacking a tape with many Objects can consume resources for a lengthy period without reclaiming a great deal of unused space in the process. This setting prevents this by limiting the selection of tapes in manual and automatic repacks based on the number of Objects.	500
DIVAMANAGER_SIZE_OF_STATEMENT_CACHE	MB	The size of the database statement cache.	10
DIVAMANAGER_STOP_IMMEDIATELY_FOR_REPACK	true or false	This setting specifies whether to complete any repack jobs still running or to terminate them after the Automatic Tape Repack period. If this is set to true then repack jobs still in progress after the Automatic Repack period will be stopped.	true

Parameter	Parameter Type	Description	Default
DIVAMANAGER_DEFAULT_ROW_PREFETCH	Number of Rows	The default number of rows to prefetch from the database per query.	1000
DIVAMANAGER_DISMOUNT_AFTER	Time in Milliseconds	This specifies the time in milliseconds to automatically dismount a mounted tape no longer needed by any other job.	120000 (two minutes)
DIVAMANAGER_FAILOVER_ENABLED	Boolean	Whether to enable Fast Connection Failover. This feature introduces a slight performance penalty.	false
DIVAMANAGER_UPDATE_PRIORITIES_PERIOD	Time in Milliseconds	DIVA periodically examines all jobs in its job queue and increments the job priority. This prevents a condition where low priority jobs might be continually superseded by higher priority jobs. This setting specifies the period between updates of the queue by the Manager. You set this value to 0 to disable priority updates.	60000 (one minute)
DIVAMANAGER_NUM_RESOURCES_SOLUTIONS_TO_EVALUATE	Boolean	The number of immediate solutions to evaluate per invocation of the Best Solution Finder during resource selection. Values are 0 (disabled) or 1 (enabled).	0 (disabled)
DIVAMANAGER_MAX_DELAY_BETWEEN_SCHEDULER	Time in Milliseconds	The maximum number of milliseconds between two Job Scheduler activations when the Manager is constantly busy.	5000 (five seconds)
DIVAMANAGER_SCHEDULER_AFTER_INACTIVITY	Time in Milliseconds	The number of milliseconds after which a requested Job Scheduler activation can be launched if the Manager is idle. This duration should be significantly lower than DIVAMANAGER_MAX_DELAY_BETWEEN_SCHEDULER. You should not need to modify this value.	500
DIVAMANAGER_PING_INTERVAL	Time in Milliseconds	The interval in milliseconds between Manager checks to see if the connections to its clients and services are still active (Actors, SPMs, web apps, etc.).	600000 (ten minutes)

Parameter	Parameter Type	Description	Default
DIVAMANAGER_EXPORT_ROOT_DIR	Directory Path	The Export Tapes command enables the sharing of tapes between two or more separate DIVA platforms. This setting defines the root folder for the exported tape's Metadata files. The folder must exist and have write permissions enabled on the host computer where the Manager is running.	Exported
DIVAMANAGER_MAX_RESTORE_SERVERS	Number between 2 and 200	The maximum number of servers allowed in an N-Restore job by an Actor.	5
TAPE_FULL_ON_SPAN_REJECTED	true or false	If true, and spanning is disabled, the Manager marks a tape full when spanning occurs.	false
DIVAMANAGER_MAX_EXPORT_TAPES	Number between 1 and 100	The maximum number of tapes allowed in an Export Tapes job.	10
DIVAMANAGER_MAX_EXPORT_ELEMENTS	Number between 1 and 10,000,000	The maximum number of elements that can be exported using the Export command.	1000000
DIVAMANAGER_MAX_FILES_IN_ARCHIVE	Number between 1 and 1,000,000	The maximum number of files allowed in an Archive job.	1000000
DIVAMANAGER_MAX_FILES_IN_PARTIAL_RESTORE	Number between 1 and 1,000,000	The maximum number of files allowed in a Partial File Restore job.	1000000
USE_IMPROVED_BEST_WORST_FIT_ALGORITHM	true or false	When a file was archived to tape in earlier DIVA releases, the Best/Worst Fit algorithm selected the tape with the largest remaining free size. This could result (over time) in a low number of blank tapes for tape repacking, and so on.  The current algorithm selects the tape based on the smallest free space and then fills all tapes before using more free tapes.	true



Parameter	Parameter Type	Description	Default
DIVAMANAGER_SITE_SUPPORT_ENABLED	true or false	Resources within DIVA can be defined by their location. If you set this parameter to true, the Manager first tries to perform the job from the sites identified as MAIN. If unsuccessful, it retries the job with resources from all other sites. If you set this parameter to false, DIVA ignores site identification and all site resources are considered equally.	false
DIVAMANAGER_CACHE_QOS_USE_DISK	true or false	In earlier DIVA releases, a Restore job with a Quality of Service of CACHE or CACHE and DIRECT resulted in the tape instance being used as first priority, even if a disk instance existed. This setting instructs DIVA to use the disk instance regardless of the QOS method specified.	true
DIVAMANAGER_PRIORITY_TIER	Number between 0 and 100	<p>DIVA bases the execution of jobs in its job queue by the job priority number. However, there are instances where a job in the queue with lower priority uses a tape that is already mounted. Giving this job priority over others lower in the queue can save a substantial amount of time in tape mount and dismount operations, and help reduce wear and tear on the tape drives.</p> <p>If this setting is enabled, DIVA examines the job queue for lower priority jobs involving a tape that is already mounted in a drive and adds the number specified here to the job priority.</p> <p>For example, if the job priority is 25, and the Priority Tier value is 50, the total job priority is 75.</p> <hr/> <p><b>Note:</b> This feature applies only to Restore and Copy Jobs that read from tape. Archive and Copy jobs that write to tape are not supported by this feature.</p> <hr/>	0 (disabled)

Parameter	Parameter Type	Description	Default
DIVAMANAGER_ETC_FEATURE	true or false	This parameter enables the Estimated Time to Complete feature. This function gathers statistics (over time) on the time for completion of all execution states of each DIVA job. Setting this value to true enables this feature.	false
DIVAMANAGER_ETC_CONFIDENCE_LEVEL	Number	The percentage of Slope Confidence Interval for the simple regression statistical function used in the Estimated Time to Complete feature. DIVA ignores this setting if the DIVAMANAGER_ETC_FEATURE is disabled.	50
DIVAMANAGER_OVERWRITE_POLICY	Number between 0 and 2	This value determines how DIVA handles files that already exist on a Destination Server when executing a Restore, Partial File Restore, or N-Restore job as follows:  0—If the file to be restored to the Destination Server already exists no overwrite will occur.  1—The Actor does not verify if the files with the same names exist before attempting to overwrite these files. If files with the same names do exist, a backup of the existing files is made before overwriting them.  2—The Actor attempts to delete and then write to files with the same names.	1
DIVAMANAGER_OVERWRITE_OVERRIDE	true or false	Overrides the policy sent by the external application through a job with the policy set in DIVAMANAGER_OVERWRITE_POLICY.	false
LICENSE_EXPIRATION_NOTIFICATION_PERIOD	Number of Days	Number of days before a temporary license is to expire that a notification message will be displayed on the GUI. The range of possible values is 1 to 99.	15
LICENSE_EXPIRATION_TIME_OF_DAY	Time of Day	The time of day the Manager will shut down if the license has expired. The Manager will stop at the designated time on the day after the license validity date. (00-23:00-59)	8:00

Parameter	Parameter Type	Description	Default
ATTEMPT_ACCESS_TO_OFFLINE_DISK	true or false	If a disk is offline or not visible to all available Actors, the Manager will automatically terminate a transfer job for Objects residing on that disk. If this is set to true, the Manager attempts the transfer irrespective of disk status.	false
CHANGE_DISK_STATE_ON_ERROR	true or false	Defines whether the Manager will automatically vary a disk's status to Offline if a transfer error occurs.	true
MANAGER_ACTOR_DISK_RETRY_NUMBER	Number	If a disk I/O error occurs during a transfer, this sets the maximum number of transfer retry attempts with alternate Actors that also have access to the disk. Values are 0 to 7.	3
DISK_STATUS_POLLING_RATE	Number	This defines the rate in milliseconds in which each disk in the system is polled to obtain its total and remaining free space.	60000 (one minute)
DISK_BUFFER_SPACE	Number	This defines the percentage of the overall space of a disk to keep free.	0.05 (percent)
DISK_CONNECTION_STATE_RESET_DELAY	Time in Minutes	A disk connection will be reset from the Out of Order state when a successful access is completed and this amount of time has passed since the connection was set to Out of Order.	1.0 (minute)
COMPONENT_SIZE_CONVERSION_TO_KB_RULE	Number	When an element is successfully transferred to tape or disk, the Actor reports the size of the element in bytes. This value is then converted to KB before it is saved to the database. The conversion may be one of three possible values: 1—KB = (bytes / 1024) + 1 2—KB = bytes/1024, but if (KB < 1) then KB = 1 3—KB = Math.ceil(bytes/1024)	3
DIVAMANAGER_MAX_EXCLUDED_INSTANCES	Number	Maximum number of instances excluded from a job that are logged as an event.	3

Parameter	Parameter Type	Description	Default
LOGGING_TRACE_LEVEL	DEBUG, INFO, WARN, ERROR, FATAL	<p>Defines the level of information written to the respective log files as follows:</p> <ul style="list-style-type: none"> <li>• <b>DEBUG</b>—All messages within the Manager are logged. Log files grow rapidly.</li> <li>• <b>INFO</b>—Information, Warning, Error, and Fatal messages are logged.</li> <li>• <b>WARN</b>—Warning, Error, and Fatal messages are logged.</li> <li>• <b>ERROR</b>—Error and Fatal messages are logged.</li> <li>• <b>FATAL</b>—No messages are logged unless the Manager stops unexpectedly.</li> </ul>	INFO
DIVAMANAGER_MAX_SPAN_SEGMENTS	Number	<p>DIVA will attempt to span the file across 2 or more tapes if no more writable tapes with enough free space are available to archive a file.</p> <p>This setting defines the maximum number of tapes that the Object will span. This setting will completely disable spanning if set to 1 or below. If a span case arises, the Manager retries the job with a new tape using the old Worst Fit algorithm, and the first tape in the attempted span will be marked full. If the second attempt fails, the job will terminate.</p>	0 (segments)
DIVAMANAGER_MAX_DATABASE_CONNECTION_ATTEMPTS	Number	The maximum number of allowable attempts to connect to the database.	10000
DIVAMANAGER_MIN_DATABASE_CONNECTION_PERIOD	Number	The minimum period (in milliseconds) between connection attempts.	1000 (milliseconds)
DIVAMANAGER_MAX_FOLDERS_IN_ARCHIVE	Number	The maximum number of folders allowed in an Archive job. Performance degradation can occur for values greater than 10000. The maximum value is 10000.	10000
DIVAMANAGER_COMPLEX_VIRTUALOBJECT_THRESHOLD	Number	The maximum number of files allowed before an Object is classified as a Complex Object. The maximum value is 10000.	1000

Parameter	Parameter Type	Description	Default
COPY_ONLY_FROM_DISK_INSTANCE_WHEN_POSSIBLE	Boolean	Controls instance selection for Copy and CopyAs jobs when the Destination Server is tape. Copy jobs always check if a disk instance can be used as the Source Server of a copy. If the required resources for a disk to tape transfer are not available, a tape to tape transfer may be used if this parameter is set to false. When set to true the job will wait for the resources to use the disk instance as the Source Server. This parameter is re-loadable in SERVICE mode.	true
COMPONENT_SIZE_CONVERSION_TO_KB_RULE	Number	This is the Object Size Conversion Rule. Use one of the following rules to convert an Object component size from Bytes to Kilobytes: 1—KB = (bytes/1024) + 1 2—KB = bytes/1024, but if (KB < 1) then KB = 1 3—KB = Math.ceil(bytes/1024)	3
COPY_ONLY_FROM_DISK_INSTANCE_TIMEOUT	Time in Minutes	Tape instance is available for a Tape to Tape transfer. After this time, either a disk or tape instance may be selected as the Source Server of a copy to tape.	15 (minutes)
DIVAMANAGER_RESTORE_QOS	CACHE_ONLY, DIRECT_ONLY, DIRECT_AND_CACHE, CACHE_AND_DIRECT, NEARLINE_ONLY, NEARLINE_AND_DIRECT	This identifies the default Quality of Service for Restore jobs.	NEARLINE_AND_DIRECT
NTH_PROGRESS_MESSAGE	Number	The number of progress messages sent to client apps. Every Nth progress message will be sent. The N=100 progress message is always sent.	5—implies send every fifth progress message to all GUIs.

Parameter	Parameter Type	Description	Default
DIVAMANAGER_TIME_TO_WAIT_FOR_GRACEFUL_SHUTDOWN	Minutes	The time to allow for a graceful shutdown to complete.	1440 (one day)
ABORT_ARCHIVES_ON_EMPTY_FILES	true or false	If true the Manager terminates an Archive job if it contains an empty file or folder.	false
TAPE_FULL_ON_SPAN_REJECTED	Boolean	If true, the Manager will mark a tape full when a span occurs but spanning is disabled.	false
DIVAMANAGER_RETRY_ON_SPAN_REJECTED_ALGORITHM	1 = Prefer empty tapes 2 = Prefer used tapes with less remaining space 3 = Prefer tapes with more remaining space	The tape selection retry algorithm to use when a span is rejected.  The Manager enables configuring the retry logic when spanning is disabled, but an Object is too large to fit on the selected tape. By default, the Manager retries with an empty tape, but you can alternatively retry with a used tape with most or less remaining space.	1

## Settings for Logging

The following table describes the Logging settings in the manager.conf file:

Parameter	Parameter Type	Description	Default
LOGGING_TRACE_LEVEL	DEBUG, INFO, WARN, ERROR, FATAL	Defines the level of information written to the respective log files as follows: <ul style="list-style-type: none"> <li>• DEBUG—All messages within the Manager are logged. Log files grow rapidly.</li> <li>• INFO—Information, Warning, Error, and Fatal messages are logged.</li> <li>• WARN—Warning, Error, and Fatal messages are logged.</li> <li>• ERROR—Error and Fatal messages are logged.</li> <li>• FATAL—No messages are logged unless the Manager stops unexpectedly.</li> </ul>	INFO
LOGGING_MAXFILESIZE	Kilobytes or Megabytes	When the log file reaches this size, a new file is generated and the old one renamed with appropriate time and date stamps. Older log files are subsequently compressed automatically into zip files at one hour intervals.	10 MB
LOGGING_LIFETIME	Hours	This setting defines how long to maintain trace service and zipped log files before deleting them.	50

## Configuring Job Priorities

Each job submitted to the Manager is placed in the Manager transfer queue. Job priorities enable DIVA to differentiate between important jobs, such as Restore jobs, over less important events. For example, tape repacks, and so on.

The job priority is a number from zero to one hundred with zero being the lowest priority and one hundred being the highest. The job priority is typically specified when you submit the job (either from the DIVA web app or the DIVA Client API). You can also alter the priority after you submit the job using the Change Priority command.

The default job priority for each job type is preset within DIVA. You can override the default priorities (at your discretion) using the following procedure:

1. Navigate to the %DIVA\_HOME%\Program\conf\manager folder.
2. Rename the managerpriority.conf.ini file to managerpriority.conf.
3. Edit the managerpriority.conf file using a plain text editor (for example, Notepad or Notepad++) to set the desired values for each job type.
4. You must reload the Manager configuration using the reload option or restart the Manager for the new settings to take effect.

Regardless of the configured job priority, the Manager will (by default) periodically increment the priority of every job already the job queue. This prevents a condition where a low job priority can be continually overridden by higher priority jobs and never executed.

You can disable this feature by setting the `DIVAMANAGER_UPDATE_PRIORITIES_PERIOD` parameter in the Manager configuration file to 0. You must then reload the Manager configuration or restart the Manager.

## Rerouting Destinations (`restore_translations.conf`)

To simplify production workflows, you can configure DIVA to automatically override the original Destination Server specified in a Restore, Partial File Restore, or N-restore job based on the Object Collection and original Destination Server. This is called Destination Rerouting. Typically, you use this function to enable selective transcoding based on an Object Collection.

You configure Destination Rerouting by editing the `restore_translations.conf` file. The file is located in the `%DIVA_HOME%\Program\conf\manager` folder with the Manager configuration file.

The `restore_translations.conf` file is delivered with an `.ini` extension. You must remove the `.ini` extension for this file to be considered by the Manager.

All re-routing entries must be in the following format:

```
DT_Number=Destination_1;Category_1;TranslatedDestination_1
```

The following list describes these parameters:

### **DT\_Number**

This must be the first string in the line and start with `DT_Number`. The Number can be any value unique among all entries. For example, `DT_0`, `DT_1`, `DT_2`, and so on. Up to three hundred entries are supported.

### **Destination\_1**

The Destination Server in a Restore job for this rule to apply.

### **Category\_1**

If the Object Collection of the job also matches the Destination Server will be re-routed.

### **TranslatedDestination\_1**

This is the new Destination Server for the Restore job.

The following example describes how to configure rerouting a destination:

- A video server accepts clips with Format1
- The archive contains clips with both Format1 and Format2



- Format 1 Objects are in Collection 1 (Cat1)
- Format 2 Objects are in Collection 2 (Cat2)

You configure this example as follows:

1. Define a Source Server (Source1) that points to the video server with no restore transcode options.
2. Define another Source Server (Source2) that points to the video server with options to transcode to Format1.
3. Create a restore\_translations.conf file containing the following line:

```
DT_0=Source1;Cat2;Source2
```

When an Object with the Collection Cat2 is restored to Destination Server Source1, re-route it to Destination Server Source2 instead. In this manner, the automation can always use Source1 as the Destination Server in the job.

Objects having a format of Format1, which are directly compatible with the video server, will be restored to Source1 without transcoding.

Objects having a format of Format2 and a Collection of Cat2 match the configuration line and are rerouted to Source2. Source2 has options to transcode them to Format1 when restoring.

## Manager Control

Manager control and management functions are performed from a command prompt on Windows platforms using the manager.bat batch file. The executable is located in the %DIVA\_HOME%\Program\Manager\bin folder.

### Installing and Removing the Manager Service in Windows

You must first install the Manager as a system service on new systems. You can accomplish this using the install (or -i) and uninstall (or -u) command line switches as follows:

#### manager install

This (or manager -i) installs the Manager service set by the SERVICE\_NAME parameter defined in manager.conf. If this parameter is undefined, the service is installed as Manager.

#### manager uninstall

This (or manager -u) removes the Manager service set by the SERVICE\_NAME parameter defined in manager.conf.

In the Windows Services applet, confirm that the Manager service is installed correctly. If you must change the service name, uninstall the existing service before editing the manager.conf file. Then reinstall the service after changing the service name.

The default path to the manager.conf file is %DIVA\_HOME%\Program\conf\manager.

You can identify a specific configuration in the command line if you require using an alternate file using the `-conf` or `-f` switch as follows:

```
manager install -conf [configuration file]
manager uninstall -conf [configuration file]
```

## Manager Service Management

You can manage the Manager Service using the following command line switches after the service is installed:

### **manager start**

This switch starts the Manager service (if stopped).

### **manager stop**

This switch stops the Manager service (if running).

### **manager shutdown**

This switch finishes currently jobs and stops accepting new jobs, then it stops the Manager service (if running).

### **manager restart**

This switch stops and subsequently starts the Manager service.

### **manager reload**

Some changes in the Manager configuration files take effect after reloading the Manager. This switch reloads the `manager.conf`, `managerpriority.conf`, and `restore_translations.conf` files from the default path (`%DIVA_HOME%\Program\conf\manager`).

Use the following command to reload the Manager using a different configuration file:

```
manager reload -conf [configuration file]
```

### **manager status**

This switch displays the current status of the Manager service (running or not running).

### **manager dump**

This switch requests a system dump from the Manager service.

### **manager version**

This switch (or `manager -v`) displays the Manager service release information and then exits.

### **manager help**

This switch (or `manager -h`) display all command line options and then exits.

## Manager Activity Logging

The Manager keeps detailed logs of its operations and stores them in the %DIVA\_HOME%\Program\log\manager folder. The logs are used for troubleshooting and diagnostics purposes, and may be requested by Technical Support.

The logging settings in manager.conf determine the level and quantity of information captured in each log file. If you must alter the settings, you can make the changes effective immediately using the manager reload command, or (in DIVA) change them dynamically from the DIVA web app. See the DIVA Operations Guide on the DIVA Technical Support site for detailed information.

Class-level logging is supported through the manager.classLog.properties file. Any class set to one of the following values will log at the specified logging level:

- TRACE
- DEBUG
- INFO
- WARN
- ERROR
- FATAL

New statical data is generated every five minutes that lists various Manager performance related metrics, and collected in a statistics folder.

After logs have reached the size defined by LOGGING\_MAXFILESIZE in manager.conf they are renamed with date and timestamps, compressed (zipped), and a new file is started (named manager.trace). The manager.trace file is the log file currently being written to by the Manager.

## Confirming System Connectivity

After the Manager has been successfully configured and launched you must check that the Manager can successfully be connected to by other DIVA clients (for example, the DIVA web app). Also, the Manager itself must be able to connect to the configured Actors and, if installed, Robot Managers.

### Confirming Remote Client to Manager Connectivity

This short test establishes whether the Manager is configured correctly and accepting remote connections from clients:

1. Launch the DIVA web app from a remote client (that is, not on the same host computer as the Manager).
2. Click the Menu Orb on the top left of the DIVA web app.
3. Click Connect.
4. Enter the IP Address and TCP Port of the Manager in the Connect to the Manager dialog box.

5. Click Connect.
6. A successful connection will be indicated by a Connected status in the DIVA web app notification area (at the bottom of the screen).

## Manager to Actors Connectivity Confirmation

This short test establishes whether the Manager can connect to all Actors in the system. This test assumes all Actors have been configured correctly and are online.

With the DIVA web app still open, click the Actors icon in the Home tab on the icon bar to display the Actors view.

Confirm that the Manager has established a connection to all configured Actors, and troubleshoot if necessary.

## Confirming Manager to Robot Manager Connectivity

This short test establishes whether the Manager can connected to each configured Core Robot Manager. This test assumes the following:

- All Core Robot Manager are configured correctly.
- Each Core Robot Manager is running.
- All Managed Storage are loaded with tapes.
- Any library management software (for example, ACSLS) is running, and the library is set to Online.
- Manual operation has been confirmed successfully with the Core Robot Manager Client Tools.

Use the following procedure to confirm connectivity:

1. Click the Tapes icon on the Home tab to display the Tapes view.
2. Take note of the ACS and LSM number for each tape to test each particular library.
3. Right-click a tape for each ACS and LSM to test and click Eject Tape from the resulting menu.
4. Click the Manager icon on the Home tab to display the Manager Current Jobs view.
5. Double-click the Eject Tape job entry to check if an error was encountered during job execution.

## Initiating Manager Failover

---

**Caution: The procedures in this section are critical and sensitive. They should only be performed under the control of Technical Support.**

---

The following steps are required to failover a Manager to the Backup when the database is still accessible on the original Manager:

1. Ensure all contents of the DIVA folder from main Manager exist in the Backup Manager (particularly the correct .conf files). If they do not exist move the .conf files to the Backup Manager.

---

**Caution: Make sure to confirm the Backup Manager has the correct DIVA binary files including major/minor version, patches, and proper database version. Always keep a backup of the original DIVA folders if making any file changes.**

---

2. Confirm all services are installed, for example WFM, Manager, Backups, SPM, Postgres, and so on, on the Backup Manager machine. If not, the services must be installed before proceeding. Ensure the services are at the same version and patch level as the main Manager.
3. Stop all services and export the database from the original Manager. Contact Telestream Support if the database is not accessible due to failure.
4. Create a new DIVA user on the Backup Manager using the -notable option, then import the database to the Backup Manager and verify the count of archived Objects is correct from the Original Manager to the Backup Manager. This can be done with the following query in SQL;  

```
SELECT COUNT(*) AO_VIRTUALOBJECT_NAME from  
DP_ARCHIVED_VIRTUALOBJECTS;
```

Contact Telestream Support if you need assistance exporting and importing the database.
5. Change the Backup Manager IP to the Original Manager IP by first applying a placeholder IP on the Original Manager.
6. Confirm the configuration is valid in the manager.conf, robotmanager.conf, spm.conf, and all disk and file paths in the configuration are accessible from the Backup Manager machine.
7. Enable and start all services and confirm Backup Manager is running as anticipated; monitor activities.

## Configuring the DIVA REST API Gateway

Use the following procedure to configure and start the REST API related services, so that the DIVA web app becomes accessible:

1. Open the  
%DIVA\_HOME%\Program\conf\restapi\_dataservice\application.properties file and confirm that the Data Source parameter settings match the database settings used in the installer.
2. Save the changes and close the file.
3. Navigate to %DIVA\_HOME%\Program\RestApi and run the menu.bat file to install the REST API services.

4. The listed services can be selected individually, or select option 5 to install and start all services (option 5 is recommended).
5. Open the Windows Services panel (services.msc) and confirm that the services were installed and are running.

---

**Note:** If the REST API Data Service is not running, change the IP Address in the application.properties file to 127.0.0.1, save the file, then restart the service.

---

Open your browser and navigate to the Manager's IP address using secure port 8765 (https://nnn.nnn.nnn.nnn:8765). Log in the first time to the DIVA web app using *sysadmin* and *changeit*.

---

**Note:** When you log in to DIVA the first time, create a new user immediately, so that the sysadmin account is not being used for configuration and viewing DIVA functions. Also, Telestream strongly recommends you change the password for sysadmin.

---

## Accessing the DIVA Web App

The DIVA web app is installed as part of the DIVA installer. It is hosted by the REST API Gateway. Installing the Manager and the REST API Data services will automatically set it up.

For DIVA to function properly the following must be installed:

- Notification Service: Required for the Running Jobs page to display Job Status in real-time.
- RestAPI Data service: Required for login to DIVA web app.
- Manager: Required by everything else in DIVA web app.

By default, the Manager expects the DIVA Web App SPA files under the DIVA/Program/DIVAWebUI folder. You can modify it (although it is not necessary) in Manager's configuration file.

## Navigation Menu

The DIVA web app is accessible at <https://127.0.0.1:8765/DIVAWebUI>. Log in the first time with user name sysadmin and password changeit. Be sure to change the password the first time you log in.

The application navigation menu will be displayed on the left-hand side. DIVA Web App section icons are permanently displayed, and full navigation details are revealed when you hover the mouse over them. Sub-items are revealed when the user clicks on an item. You can pin the full menu by clicking the hamburger button on the top banner.

## Back-end Support

The DIVA web app requires only a running Manager and Data Service. You need to update `api.server.port` in the `manager.conf` file to update the DIVA web app server port. The default port is set to 8765. You must update the `api.dataservice.url` in the `manager.conf` file if you change the data service address and/or port.

The manager only supports https, so port 8765 will point to a secure URL where you can access the DIVA web app interface at `https://xxx.xxx.xxx.xxx:8765/DIVAWebUI` where `xxx.xxx.xxx.xxx` is the DIVA web app server IP address. For example, `https://127.0.0.1:8765/DIVAWebUI`.

## Importing the License

DIVA requires a license. The Manager will not start without a valid license in the database. The license can be imported as part of the DIVA installer if you create the license before DIVA is installed. If DIVA is already installed, a license can be imported via the *Import License* page in the DIVA web app. In addition to enabling the Manager, the license includes a set of options that are necessary to enable the associated features in DIVA.

To import a license using the DIVA web app, do the following:

1. Navigate to *Configuration > User Management > License > Import License*.
2. Enter the Importer's name in the *Importer* text box.
3. Enter the reason for importing this license in the *Importer Reason* text box.
4. Click *Choose File* under the *License File Content* heading and locate the license file to import.
5. Enter the Manager IP Address in the *Manager Address* text box.
6. Enter the Manager port number in the *Manager Port* text box.
7. Turn on *Notify Manager After Import* using the slide button.
8. To import the license, click *Save* at the bottom of the screen.

## Database Backup Configuration

### Backup Service (BKS) Overview

The backup process as a whole is comprised of two types of services, DIVA Backup Service (BKS) and one or more DBAgents.

BKS facilitates the scheduling, storage, archiving, and monitoring of database backups within the DIVA ecosystem.

BKS controls command execution, DIVA archives, synchronization, and configuration. Backup configurations are agnostic of the data contained within them such that the

solution can be applied to any type of application database that does not have a backup solution, assuming the routines to do so are implemented.

---

**Note:** RabbitMQ is used as the messaging service between the BKS and DBAgent. If this service is offline or has problems, backups get stalled. Once the issue is resolved, restarting the BKS and DBAgent services resumes the normal processing.

---

Replication locations may be configured through the BKS. These locations associate a path, DBAgent, and the databases managed on a given server. The paths configured can be either a local path or an 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 and credentials 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:** 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:

```
<Path to the backup location>\Backups\<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 that are configured to replicate that database. 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 `DB_BackupArchives`. This only occurs after every full backup, after which a cleanup task will delete any archives that exceed the retention period.

---

**Caution: Manual restorations that involve pulling archives from tape should be performed only by Telestream Technical Support personnel.**

---



The backup service configuration files are located here:  
%DIVA\_HOME%\Program\conf\backup\_service\BackupService.settings.json.

---

**Note:** It is **strictly required** to use the BKS 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 BKS to remote backup servers.

## Configuring BKS

To configure BKS, do the following:

1. Browse to *Configuration > Services > Database Backup*.
2. Set options as desired.

---

**Note:** It's possible to configure BKS directly in the configuration file. However, this could allow invalid configuration values. Telestream strongly recommends configuring through the BKS REST API, which prevents invalid configuration values.

---

## DBAgent

The DBAgent Service performs database-specific tasks, backup, restore, fail-over, and schema initialization. DBAgent monitors the progress of these tasks, and reports disk usage. You can install and configure any number of DBAgents, but only one per server or container. This supports multi-server installations and automates access control. The DBAgent also exposes a REST API. The backup service calls this REST API to check the status of a backup, and to monitor disk space for configured mount points. The backup service also calls this REST API to initiate backups, restores, and fail-overs.

DBAgent configuration requires only the space monitoring and backup location. The majority of the configuration resides in the BKS. By default, mount point configuration monitors the backup location, the C, E, and F drives as expected by the default DIVA installation. You can configure DBAgent to monitor additional locations if necessary, and to trigger alerts to DIVA when those locations approach their space limits.

DBAgent creates a state file in the log directory for a given database job. Backup-job state files are stored in the BackupHistory directory. Restore-job state files are in the RestoreHistory directory. DBAgent actively updates these files as the backup or restore progresses to completion. These files are used to gather statuses about a given action. The state files include a full log of the action itself and any files that have been created as a result of the backup process.

## Backup Initiator

A command-line backup initiator is included in the bin installation folder. This program is a wrapper for the DBAgent API. This performs backups, restores, and fail-overs when

the web interface is unavailable. The command-line initiator offers 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

## Backup Timing

Priority, start and end times for backing up databases to tape are defined by `ArchivePriority`, `ArchiveWindowStart`, and `ArchiveWindowEnd`. Descriptions of these settings follow.

## ArchivePriority Settings

`ArchivePriority` defines the priority of the archive job. Allowed values are: Min, Low, Normal, High or Max; as well as any integer value between 0 and 100.

## ArchiveWindowStart Settings

`ArchiveWindowStart` defines the archive start timestamp. The default value is 00:00:00.

## ArchiveWindowEnd Settings

`ArchiveWindowEnd` defines the archive end timestamp. The default value is 23:59:59.

## 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

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 exist, 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.

---

## BKS Recommended Practices

The following are recommended practices for BKS:

- BKS must be installed on the same server as the Backup Manager, Actor, 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 incremental backups should be performed every 15 minutes.
- 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.
- When restoring a backup, it is mandatory to have the full backup as well as the first following the incremental minimum.

## BKS Installation and Configuration

The details for BKS installation and configuration follow.

### BKS Software Installation

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.

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 system is called Backup System 1 (required)
- Which system is called Backup System 2 (required)
- Which additional systems 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
<code>-log</code>	Path to log directory. Default: <code>..\..\log\backup_service</code>
<code>-conf</code>	Path to configuration directory. Default: <code>..\..\conf\backup_service</code>
<code>-httpport</code>	Port to listen for http connections. Default: 1876
<code>-httpsport</code>	Port to listen for https connections. Default: 1877
<code>-certpath</code>	Path to certificate located on disk.
<code>-user</code>	Username to install the service under. Blank entries will be installed as LocalSystem.
<code>-path</code>	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.

## BKS Configuration

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

`$DIVA_HOME\Program\conf\backup_service\BackupService.settings.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 DIVA 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 configured 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
}
```

## BKS and DBAgent Removal

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
```



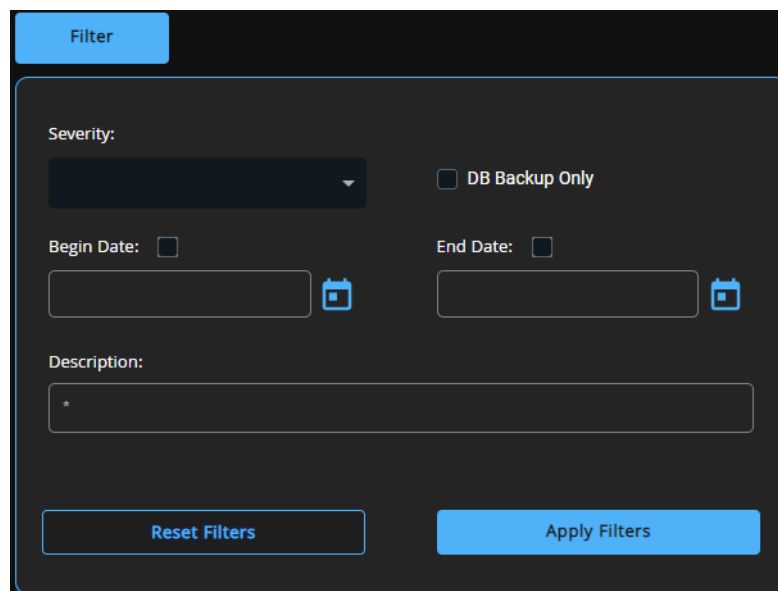
`db_agent.bat uninstall`

## The DIVA Backup Service (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 be 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

## The Actor

The Actor is the data mover between devices in the network. It supports the data transfer between many different types of devices and handles transcoding operations with Telestream transcoding software (optional). All Actor operations are initiated and

coordinated by Manager. One or more Actors can be configured to be controlled by a single Manager.

Each Actor runs as a Windows service and automatically starts and begins accepting connections from Manager when the Actor host is started. Actor services on each host may be managed from the Windows services dialog box.

## Actor Configuration Overview

The Actor runs on Windows. The Actor runs as a standalone server application. The Manager connects to each Actor as a client application.

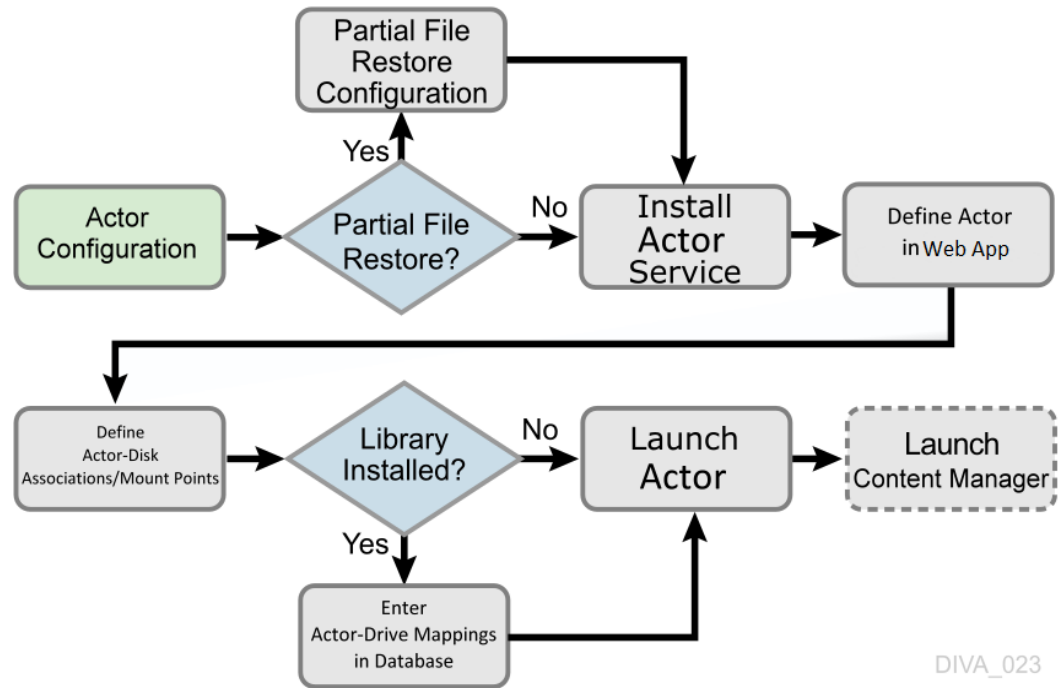
The Actor is installed in the %DIVA\_HOME%\Program\Actor\bin\ folder. The Actor's configuration files are located separately in the %DIVA\_HOME%\Program\conf\Actor\ folder. At the system level, the location and capabilities of each Actor are defined in the DIVA web app.

Find Name and Port settings in the configuration file. All other Actor settings are located in the DIVA Web App under Actor Advanced and Partial Restore Settings pages of the Actor area of the System page. Some settings are only available In Engineering Mode.

You must notify the Actors of any changes to the configuration by clicking on Notification, Notify Actors while connected to the Manager. The Actors must be running and connected to the Manager to receive the notifications.

Configure Actor settings on the Actor Settings Entry screen. Click + on the top right of the Actor Settings area to create and configure an Actor, or double-click the Actor you want to edit to access the settings screen.

The following figure is the workflow for installing an Actor:



DIVA\_023

## Actor Executables

Descriptions of the Actor executable files follow.

- `%DIVA_HOME%\Program\Actor\bin\ActorService.exe command [option]`

Executes commands for the Actor Service. Appending the `-conf` (or `-f`) option after one of the following commands specifies a specific configuration file to load settings from. The ActorService.exe command parameters are as follows:

- `install (-i)`

Installs the Actor as a system service.

- `uninstall (-u)`

Removes the Actor service.

- `debug (-d)`

Starts the Actor in console mode.

- `version (-v)`

Displays the Actor version information and then exits.

- `help (-h)`

Displays help information and then exits.

- `%DIVA_HOME%\Program\Actor\bin\scandrive.exe`

Identifies the tape drives in the system. There are no command-line parameters.

- `%DIVA_HOME%\Program\Actor\bin\TapeReadingUtility.exe`  
Opens the Tape Reading Utility, which enables manually reading the tape drives in the system. There are no command-line parameters.
- `%DIVA_HOME%\Program\Actor\bin\VideoAnalyser.exe`  
Opens the Video Analyzer Utility. This utility displays the internal structure of a video format by dropping video files to the appropriate top tab for that file type (for example, drop a MOV file on the MOV tab, an AVI file on the AVI tab, and so on). File information is displayed in the lower window panes. There are no command-line parameters.

## Local Actor Configuration File (actor.conf)

The Actor configuration file contains the Service Name and Port parameters. Remove the .ini extension from the actor.conf.ini file and edit the file with a plain text editor (for example, Notepad or Notepad++) to insert the Service Name and Port number as described in the following table.

Parameter	Parameter Type	Description	Default
DIVAActor_PORT	TCP Port Number	TCP Port Number for the Actor to listen on for incoming jobs. If running more than one Actor on the host, the TCP Port Number must be unique for each Actor.	9900
SERVICE_NAME	Name	The DIVAActor_SERVICE_NAME parameter specifies the name of the Actor and the service during installation. This is required if you install two or more Actors on a single Windows host computer because both cannot have the same Actor Service Name. If this parameter is not defined or commented out, the Service Name defaults to the Host Name of the Actor computer and will be <i>DivaAct Host_Name</i> .	

## Actor Service Installation and Removal

You can use the actorservice.exe executable in the Actor bin directory to install (or uninstall) the Actor as a service from a Windows command-line prompt.

By default, the Actor Service uses the actor.conf file located in `%DIVA_HOME%\Program\conf\actor` folder to define the Service Name. If you are installing multiple Actors on a single host, you must create additional Actor

configuration files and specify them to the service to create unique instances for each Actor (see [Actor Service Management Functions](#) for more information).

Use the following commands to install or uninstall the Actor Service from the Windows command line:

#### **actorservice -i**

Installs the Actor Service using the SERVICE\_NAME parameter defined in actor.conf. If this parameter is undefined, then the service is installed as Actor—Host\_Name.

#### **actorservice -u**

Removes the Actor Service using the SERVICE\_NAME parameter defined in actor.conf. If this parameter is undefined, then the service to be removed is Actor—Host\_Name.

## Actor Service Management Functions

When installing or uninstalling additional Actor Services on the same host, you must specify the path to each Actor's configuration file for each instance. You add the `-conf` (or `-f`) command switches when installing the service as follows:

```
actorservice {-i|-u} {-conf|-f} {Path and file name}
```

The following examples install the Actor services for two different Actors on the same host computer. You use the `-u` command switch (instead of `-i` to install) to uninstall these same Actor services.

Check the services applet after installation to verify that each Actor Service was installed correctly.

For example, use the following command to install the Actor defined by the SERVICE\_NAME in the actor1.conf configuration file:

```
actorservice -i -conf C:\DIVA\Program\conf\actor\actor1.conf
```

Use the following command to install the Actor defined by the SERVICE\_NAME in the actor2.conf configuration file:

```
actorservice -i -conf C:\DIVA\Program\conf\actor\actor2.conf
```

The following additional command options are also available for the Actor Service:

#### **actorservice debug**

Starts the Actor Service in console mode. This is used for troubleshooting.

#### **actorservice version**

Displays the Actor Service software release information. You can also use the `-v` switch instead of `version`.

#### **actorservice help**

- Displays all command line options.

## Actor Launch

Windows Actors no longer start automatically with Windows. The Actor Services are managed through the Windows Services applet, from a Windows command line.

The Actor Service can be located in the Windows Services applet, right-click the name, and then select the desired management function (Start, Stop, Restart, and so on) from the context menu.

---

**Note:** The quotation marks in the following commands must be used when specifying a Windows service with spaces in the name.

---

You can restart an Actor from a Windows command line using the following command sequence:

```
net stop "Actor"  
net start "Actor"
```

If a SERVICE\_NAME is specified in the actor.conf file (for multiple Actors on a single computer), then an Actor can be restarted from a Windows command line using the following command sequence:

```
net stop "Actor -SERVICE_NAME"  
net start "Actor -SERVICE_NAME"
```

---

**Tip:** Create a Windows batch file containing these commands and place it on the desktop for easy access.

---

## Actor Definition and Declaration

Each Actor must be declared in the DIVA Database. You declare the Actors in the Actors area in the DIVA web app. The Actors area has three tabs: Actor settings, Actor Advanced settings, and Partial File Restore settings.

### Actor Settings

This tab includes general Actor definition settings such as Actor name, IP address, port, Network, and so on. Descriptions of the Actor settings follow.

#### Name

This is the name of the Actor associated with the Partial File Restore options. This value is automatically filled in from the Actor settings. If you modify the name here, or in the Actor Settings Screen, it will be modified in both places.

#### IP Address

This is the IP address of the Actor.

#### Port

This is the port number the Actor listens on for commands.

**Prod. System**

This parameter identifies the Network where the Actor is in use.

**Site**

This parameter identifies the physical location of the Network.

**Max Drive Operations**

This is the maximum number of simultaneous jobs to and from drives that this Actor can perform. You can use this parameter to distribute jobs and bandwidth among all Actors.

**Max Server Operations**

This is the maximum number of simultaneous jobs to and from servers from the Servers configuration that this Actor can perform. You can use this parameter to distribute jobs and bandwidth among all Actors.

**Max Disk Operations**

This is the maximum number of simultaneous transfers to and from disks (both read and write) that this Actor can perform. You can use this parameter to distribute jobs and bandwidth among all Actors.

**Max Stage Operations**

This is the maximum number of staging job that an Actor is allowed to run at the same time.

**Max Bridge Operations**

This is the maximum number of concurrent jobs using DIVA Bridge that an Actor is allowed to run at the same time.

**Verify Tape**

This parameter defines whether tapes are verified.

**Direct Restore**

This parameter defines whether this Actor can be used for direct restores to a Source or Destination Server.

**Cache Restore**

The Actor is permitted to perform cache restores to a Source or Destination Server. You must disable this option if this Actor has no local cache storage for the temporary storage of the DIVA Object during a transfer.

**Copy To Tape Group**

This parameter defines whether this Actor can be used for Copy To Tape Group jobs. You can use this option to isolate specific Actors involved in critical operations from mass Copy To Tape Group jobs, such as those from the DIVA SPM option.

**Associative Copy**

This parameter defines whether this Actor can be used for Associative Copy jobs.

**Repack**

This parameter defines whether this Actor can be used for tape repack jobs. You must set this to N if the Actor has no local cache for temporary storage during the repack operation. Because tape repacking is a lengthy operation, you can also use this setting to dedicate an Actor solely to repack jobs by disabling the other options (except Delete) and disabling repack on the other Actors.

**Delete**

This parameter defines whether this Actor can be used for jobs that involve deleting DIVA Objects from a disk. You can use this option to isolate an Actor from mass deletion jobs (for example, jobs issued from the SPM option).

**Direct Archive**

This parameter defines whether this Actor can be used for direct Archive jobs.

**Cache Archive**

This parameter defines whether this Actor can be used for cache Archive jobs. You must disable this option if this Actor has no local cache storage for the temporary storage of the DIVA Object during a transfer.

**First Utilization Date**

This is the date the Actor was first put into use.

**Actor Advanced Settings**

This tab includes advanced settings such as read and write block sizes, tape unit timeout, Quantel, QuickTime and FTP settings.

Advanced Actor parameters are displayed, configured and edited on the Actor Advanced Setting page in the Actors Panel of the DIVA web app. To configure or edit advanced Actor parameters, double-click the Actor you want to edit to access the settings screen.

The following list describes the parameters on the Actor Advanced Settings Entry screen:

**Name**

This is the name of the Actor associated with the Partial File Restore options. This value is automatically filled in from the Actor settings. If you modify the name here, or in the Actor Settings Screen, it will be modified in both places.

**Tape Test Unit Ready Timeout (s)**

The time in seconds to wait for a drive to become ready after a tape is mounted. If the drive is not ready within this period, the drive is considered to be not responding.

**Profile Read Block Size (B)**

The FTP block size used for transfers on profile video servers when reading. The default value (1500) is the best block size to use with GVG profile servers. This value



may be different when using other servers. Possible values are between 1500 and 262,144 bytes.

### **Profile Write Block Size (B)**

The FTP block size used for transfers on profile video servers when writing. The default value (32,768) is the best block size to use with GVG profile servers. This value may be different when using other servers. Possible values are between 1500 and 262,144 bytes.

### **Quantel Rename Clips**

Automatically rename clips when restoring them to Quantel.

- Setting this to N disables this feature. This is the default setting.
- Setting this to Y renames files using the first part of the Object name (before the comma) truncated. This is Omnibus renaming.

### **QT Self-contained Threshold (MB)**

When performing a QuickTime Partial File Restore, the Actor must determine if a clip is self-contained, or not based on the size of the input file. This parameter is a limit in MB. When this limit is exceeded, the Actor considers the clip to be self-contained. The unique objective of this parameter is to prevent the Actor from loading a large self-contained clip into memory. Values range from 10 MB through 100 MB.

### **Disk FTP Passive Mode**

FTP data connections are, by default, created in Active mode. The DIVA FTP client connects from a random unprivileged port (greater than port 1023). Then it immediately starts listening to the port and sends a PORT command to the FTP server.

When you set this parameter to Y, data connections are created in Passive mode rather than Active mode. In Passive mode the DIVA FTP client sends a PASV command to the FTP server and the server creates socket, not the client.

### **Disk FTP Block Size (KB)**

This parameter defines how much data the Actor attempts to send and receive using a single system call during FTP transfers.

For example, if the Actor internal buffer size is set to 2 MB, and this parameter is set to 32768 bytes, 64 system calls are required to write a single buffer to a data socket.

### **Disk FTP Socket Window Size (B)**

This parameter adjusts the normal buffer size allocated for output and input buffers. This parameter is internally used to set the send and receive buffers for FTP-managed disk types.

## **Partial File Restore Settings**

The Partial File Restore parameters are located in the DIVA database. These options provide additional parameters to the Actor for specific partial file restore formats.

The following table describes the Partial File Restore parameters available in the DIVA database.

The following list describes the partial file restore settings.

Parameter	Value or Type	Job Option	Description	Default
Name	String		This is the name of the Actor associated with these Partial File Restore options. This value is automatically filled in from the Actor settings. If you modify the name here, or in the Actor settings screen, it will be modified in both places.	
QT Ignore Start Timecode	N (disabled) Y (enabled)	-PfrQtIgnoreStartTimecode	If this setting is enabled, Partial File Restore will ignore the SOM value of the original clip and process TCIN and TCOUT as if it starts from 00:00:00:00.	N
QT Omneon First Frame Handling	IGNORE RESET UPDATE	-PfrQtOmneonFistfrmHandling	Specifies how the Actor handles the first frame of a QuickTime clip: <ul style="list-style-type: none"> <li>• IGNORE: Partial Files Restore will ignore this field. The value found in the original clip will remain unchanged in the restored clip.</li> <li>• RESET: Partial File Restore will reset the value of this field to zero.</li> <li>• UPDATE: Partial File Restore will increment this value using the frame count from which the partially restored file begins.</li> </ul>	RESET

Parameter	Value or Type	Job Option	Description	Default
AVI Ignore Start Timecode	N (disabled) Y (enabled)	-PfrAvilgnoreStartTimecode	If this setting is enabled, Partial File Restore will ignore the SOM value of the original clip and process TCIN and TCOUT as if it starts from 00:00:00:00.	N
EVS MXF Ignore Start Timecode	N (disabled) Y (enabled)	-PfrEvsMxflgnStartTimecode	If this setting is enabled, Partial File Restore will ignore the SOM value of the original clip and process TCIN and TCOUT as if it starts from 00:00:00:00.	N
GXF Timecode Reference	Integer	-PfrGxfTimecodeRef	This setting specifies how the time code SOM reference is to be derived for a GXF Partial File Restore job. The options are defined by the following values: <ul style="list-style-type: none"> <li>• The Objects start time codes are ignored. TCIN and TCOUT must be relative to 00:00:00:00.</li> <li>• SOM is derived from the first field number of the MAP packet (default).</li> <li>• SOM is derived from the time code at Mark In from the UMF packet.</li> </ul>	1

Parameter	Value or Type	Job Option	Description	Default
GXF Progressive Timecode Translation	N (disabled) Y (enabled)	-PfrGxfProgTimecodeTrans	Partial File Restore is expecting TCIN and TCOUT to be in conformance with the frame rate of the archived clip by default. For example, if the frame rate of the clip is 29.97fps NTSC (or 25fps for PAL), the frame count of TCIN and TCOUT can be comprised between 0 and 29 (25 if it is PAL).  HD formats have progressive frame rates (23.976, 24, 29.97, 30, 59.94, 60). For automations, the actual frame rate of the clip can be unknown. When this parameter is set to Y (enabled), DIVA considers that TCIN and TCOUT are PAL or NTSC timecodes and translates these timecodes according to the actual frame rate of the archived clip.	N
LXF Ignore Start Timecode	N (disabled) Y (enabled)	-PfrLxfIgnoreStartTimecode	If this setting is enabled, Partial File Restore will ignore the SOM value of the original clip and process TCIN and TCOUT as if it starts from 00:00:00:00.	N

Parameter	Value or Type	Job Option	Description	Default
MXF Partial Restore Dictionary File	Path and File Name	-PfrMxfPrDictFile	<p>This parameter must point to the name and location of the MXF dictionary file. The dictionary is normally distributed with the Actor installation in the %DIVA_HOME%\Program\Actor\bin folder. The default dictionary file name is mxf_file.bin.</p> <p>Set this parameter to %DIVA_HOME%\Program\Actor\bin\mxf_file.bin.</p> <p>Where %DIVA_HOME% is the root path of your DIVA installation for the Actor (typically C:\Diva).</p>	
MXF Timecode From Source Package	N (disabled) Y (enabled)	-PfrMxfTimecodeFrmSrcPkg	If you set this parameter Y (enabled), the time code track used to locate the in and out points will be the one from the source package. Otherwise, timecode will be sourced from the Material Package.	N
MXF Timecode Value To Switch Package	-1 (no switch) 0 (switch)	-PfrMxfTCValuetoSwitchPkg	If the SOM value found in the MXF package specified by the parameter MXF Timecode From Source Package is equal to this value, the Actor will automatically look for the SOM in the other MXF Package. The default value of -1 avoids switching from one package to the other.	-1

Parameter	Value or Type	Job Option	Description	Default
MXF Enforce Closed Header	N (disabled) Y (enabled)	-PfrMxfEnforceClosedHeader	If this parameter is set to Y (enabled) the extraction will fail if the metadata in the header is not closed. If set to N (disabled), the Actor will attempt to find closed metadata in the footer partition.	Y
MXF Run In Processor	File Name	-PfrMxfRunInProcessor	If this parameter is defined it must contain the name of the RunInProcessor.dll. In this case, the run-in processor will be used to read and create run-ins. For example: RUN_IN_PROCESSOR=R unInProcessor.dll.	
MXF Ignore Start Timecode	N (disabled) Y (enabled)	-PfrMxfIgnoreStartTimecode	If this parameter is set to Y (enabled), MXF Partial File Restore will ignore all start time code values of the original clip and TCIN and TCOU (SOM and EOM) is processed as if the original clip starts at 00:00:00:00. This option overrides the MXF TIMECODE FROM SOURCE PACKAGE parameter.	N
MXF Use Omneon Dark Meta	N (disabled) Y (enabled)	-PfrMxfUseOmneonDarkMeta	Certain Omneon MXF clips have their start time code located in a Dark Metadata Set. By default the MXF Partial File Restore does not pay attention to this field. Set this parameter to Y if you want the MXF Partial File Restore to manage this field.	N

Parameter	Value or Type	Job Option	Description	Default
MXF Use BMX Library (instead of MOG SDK)	N (disabled) Y (enabled)	-PfrMxfUseBMXLibrary	The use of either MOG SDK or BMX can be selected from the DIVA web app under Configuration > Actor Settings, by setting the Use BMX Library parameter to Y.	N
MXF Serialize Depth First	N (disabled) Y (enabled)	-PfrMxfSerializeDepthFirst	If this parameter is set to Y (enabled) the MXF Partial File Restore serializes the Metadata Sets of the partially restored clip using a depth-first approach. This option is recommended when the Destination Server is a QUANTEL ISA gateway. If it is set to N (disabled), the MXF Partial File Restore serializes the Metadata Sets with no ordering.	N
MXF Generate Random Index Pack	N (disabled) Y (enabled)	-PfrMxfGenerateRip	RIP (Random Index Pack) is an optional small structure located after an MXF file that contains file offset information for each partition in the file (when present). You can set this parameter to N (disabled), for incompatible servers (for example, SONY XDCAM).	Y

Parameter	Value or Type	Job Option	Description	Default
MXF Number of Frames Per Body Partition	Integer between 50 and 250.	- PfrMxfFramesPerBodyPartition	This parameter defines the number of frames per partition in the output file. Only values between 50 and 250 are valid. If a value greater than 250 is entered, the MXF Partial File Restore will use 250. If the entered value is less than 50, it will use 50. This parameter is rounded automatically by the Actor to align body partitions on GOP boundaries.	250
MXF Update TC Track Origin	N (disabled) Y (enabled)	-PfrMxfUpdateTctrackOrigin	When the video essence is MPEG2 LGOP, Partial File Restore will use the origin field of each track to be frame accurate. The origin specifies GOP precharge frames. Your video server may use a different implementation or interpretation of this field. If this parameter is set to Y (enabled), the Origin field is modified in all tracks. If this parameter is set to N (disabled), the Origin field is modified in all tracks except the timecode track.	N



Parameter	Value or Type	Job Option	Description	Default
MXF Tolerance on TCOUT	Integer between 0 and 250.	-PfrMxfTcoutTolerance	This parameter can be set to indicate a tolerance on the TCOUT supplied to a Partial File Restore job. This tolerance value is 0 by default, but it you can set it to a specific number of frames. If the supplied TCOUT is beyond the end of the clip, but not too far out (within the tolerance), DIVA will perform the Partial File Restore until the end of the clip instead of reporting and invalid TCOUT.	0
MXF Duration From Footer	N (disabled) Y (enabled)	-PfrMxfDurationFromFooter	When the duration of the input clip is -1 in the header partition, the MXF Partial File Restore loads the footer partition in to obtain the correct value. Some older clips may not have a correct RIP after the file, and the footer partition may not be accessible.  If you set this value to N (disabled), the MXF Partial File Restore does not load the footer partition and performs a blind Partial File Restore, if TCIN and TCOUT are valid.	Y

Parameter	Value or Type	Job Option	Description	Default
MXF Maximum Queue Size	Integer between 0 and 200.	-PfrMxfMaxQueueSize	The maximum size (in MB) that the extractor can queue before producing an error (to avoid running out of memory).	200
Seachange Ignore Start Timecode	N (disabled) Y (enabled)	-PfrSealgnoreStartTimeCode	If you set this parameter to Y (enabled), SeaChange Partial File Restore ignores the start time code value of the original clip and processes TCIN and TCOU as if it starts from 00:00:00:00. The configuration of the MXF parser is also required for MXF. However, because this is a SeaChange clip, it ignores the MXF Ignore Start Timecode in this workflow.	N
MPEG2 Transport Stream Ignore Start Timecode	N (disabled) Y (enabled)	-PfrTslgnoreStartTimeCode	If you set this parameter to Y (enabled), the MPEG2 transport stream Partial File Restore ignores the start time code value of the original clip, and processes TCIN and TCOU as if it starts from 00:00:00:00.	N
MPEG2 Program Stream Ignore Start Timecode	N (disabled) Y (enabled)	-PfrPSlgnoreStartTimeCode	If you set this parameter to Y (enabled), MPEG2 transport stream Partial File Restore ignores the start timecode value of the original clip and processes TCIN and TCOU as if it starts from 00:00:00:00.	N

## Actor to Drive Connections

The Data Transfer component of the drives must be configured for use with the Actors separate from the Tape Drive Control configuration for the Robot Manager. You must logically configure of each drive in the Actor-Drive configuration in the database.

The Actors-Drives area is located on the Drives page. The area displays the current Actor-Drive associations including the Actor Name, Drive Number, and Library location. If a drive is connected to multiple Actors through a SAN, the Actor-Drive mapping must be repeated for each Actor accessing this drive.

You can combine the Drive Operations settings and the Actor Capability settings to dedicate a drive to a particular set of Actors for specific operations. For example, tape repacking.

To edit the parameters, double-click the Actor Name in the Actors-Drives area to open the Add new row in Actors-Drives Connections dialog box. Click the + button on the top of the area to add a Actors-Drives connection.

Two options are available on the Add new row in Actors-Drives Connections dialog box as follows:

### Actor

Select the Actor the drive is connected to from the list. Only Actors already defined in the Actors area of the System page are listed.

### Drives

Select the logical drive in the relevant library for this mapping. Only drives defined in the Drives area of the Drives page are listed. You can select one or more drives using the check boxes. Multiple selections are only available when adding an association, not while editing an existing one.

When you select a different Actor, the drives available for configuration are displayed. If all drives have already been configured for the selected Actor, the Drives list is not available and indicates there are no drives available for the selected Actor.

## Core Proxy Actor Definitions

---

**Note:** This feature is only supported for disk and Server based jobs.

---

The user must first define an Actor with a UDP port to configure a Proxy Actor. The UDP port allows a regular Actor to message a Proxy Actor using the connection-less protocol. In the following figure, Actor *diva8024\_actor1\_9901* is configured as a Proxy Actor with UDP port 10001. The TCP port is irrelevant for a Proxy Actor.

You must configure the link between the Actor and Proxy Actor to notify Manager that this Actor is a Proxy by adding an Data-Proxy Actor Connection.

After configuration, Manager is now aware that Actor `diva8024_actor0_9900` can see Proxy `diva8024_actor1_9901`. This means that any remote resources only visible to the Proxy Actor can now be accessed using the regular Actor.

The Actor configuration file corresponding to the proxy must also be updated with the UDP port. In this example, the Actor configuration file for `diva8024_actor1_9901` (the Proxy Actor) only requires a UDP port.

```
DIVAActor_PORT=UDP/10001
```

If you want to specify both a TCP and UDP port, then you must use `DIVAActor_PORT2` as shown here:

```
DIVAActor_PORT=9901
```

```
DIVAActor_PORT2=UDP/10001
```

You can now configure a remote disk that is not connected to a regular Actor and still archive to that disk if a Proxy Actor is connected to that disk.

---

**Note:** The Manager does not directly connect to a Proxy Actor. It can only directly communicate with a regular Actor. A Proxy Actor exclusively communicates with a regular Actor.

---

## Resource Selection and Manager-Actor Communication

The Manager selects what regular Actor to use to satisfy a job based on the resources that Actor can directly or indirectly (via a proxy) access. If multiple proxies are configured for a single Actor, the decision of which proxy to use is based primarily on the load on that Actor.

The Manager does NOT directly connect to a proxy. It can only directly communicate with a regular Actor. A proxy exclusively communicates with a regular Actor.

## Actor and Tape Clones

In addition to configuring Clone Tape Groups, Actors and Source Tapes must be enabled for cloning. By default, all Source Tapes are enabled for cloning. However, a Source Tape will be disabled for automatic cloning if a read failure occurs during a clone job. The user will have to manually re-enable the Source Tape for automatic cloning by setting the corresponding Tape State in the DIVA web app.

If a write error occurs during a clone job, the Source Tape is unaffected and can still be used for writing content. If the Clone Tape is bad and cannot be used, the existing clone link must be removed, and then either manually invoke the clone or use the automated clone scheduler to invoke it. On invocation, the clone job will select a new tape from the Clone Tape Group.

See the DIVA Operations Guide on the DIVA Technical Support site for details on tape selection, manual cloning, and automatic cloning processes.

## Actor Activity Logs

Actors log all activities during normal operations. The log files are named actor.log, or actor\_SERVICE\_NAME.log. The files are stored in the %DIVA\_HOME%\Program\log\actor folder.

Each Actor also provides additional logging functions for some specific functionalities implemented in shared libraries that are considered as part of actor. For example, the Object Storage client interface, FTP servers, and Partial File Restore. Core enables logs by default, and they are unique for each server type. They provide detailed logging information from that protocol to the standard Actor log file.

These files are useful in diagnosing transfer errors with either drives or servers, and particularly for debugging the configuration when a Source or Destination Server has been added. Technical Support may job these logs when providing assistance.

## Configuring SMTP Messages

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, configure DIVA to connect to an SMTP mail provider.

To enable e-mail notifications, do the following:

1. Open the DIVA 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 mis-configured 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 DIVA 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.

## The Metadata Database

This section describes configuration of the Core Metadata Database and includes the following information:

- [Metadata Database Configuration](#)
- [Metadata Database Sizing](#)
- [MDDDB \(Flat File Metadata Database\) to MDS \(Metadata Service\) Migration](#)
- [Metadata Database Failure Scenarios](#)

## Metadata Database Configuration

You must set the following two parameters on the Manager Setting page of the DIVA web app to enable Complex Object workflows and Metadata Database backups:

## Enable Metadata Database

Select this check box to enable use of the Metadata Database.

## Metadata Database Location

Enter an empty directory path that exists in the file system in the Metadata Database Location field.

---

**Note:** Changes made to these parameters require you to restart the Manager and Backup Service. When it is necessary to change the Metadata location, you must confirm that you have copied all of the Metadata files from the old location to the new location.

---

Technical Support **highly recommends** that you store the Metadata Database files on a RAID disk array. The Metadata Database should not be on a standard disk due to decreased performance and the real-time backup functionality that a RAID array affords the system.

Metadata Database files stored on a standard disk are vulnerable to data loss if a single disk failure occurs until the information is replicated with the DIVA Backup Service. Storing the Metadata Database files on a RAID array isolates the data from these types of failures.

## Metadata Database Sizing

---

**Note:** MongoDB, in its default configuration, can use up to half the available RAM minus 1GB on the server on which it is installed. You have to plan the location of MDS MongoDB installation accordingly.

---

You can use the following formula as a rough guide to determine the minimum disk space required to support the Metadata Database:

$$(100 + \text{avg\_path\_file\_name\_size}) * 1.15 * \text{avg\_number\_component\_files} * \text{number\_virtual\_objects}$$

When planning, enough Metadata Database disk space should be allocated to ensure expected, or unexpected, growth of your environment. You must allocate the same disk space for the Metadata Database on all of the remote backup systems.

### Example:

**avg\_path\_file\_name\_size = 60**

this/nested/subdir01/As\_The\_World\_Turns\_24fps\_scenes1-10.avi

**avg\_number\_component\_files = 200,000**

This is the average number of files and folders within the Complex Object.



## num\_objs = 50,000

This is the number of Complex Objects to be archived.

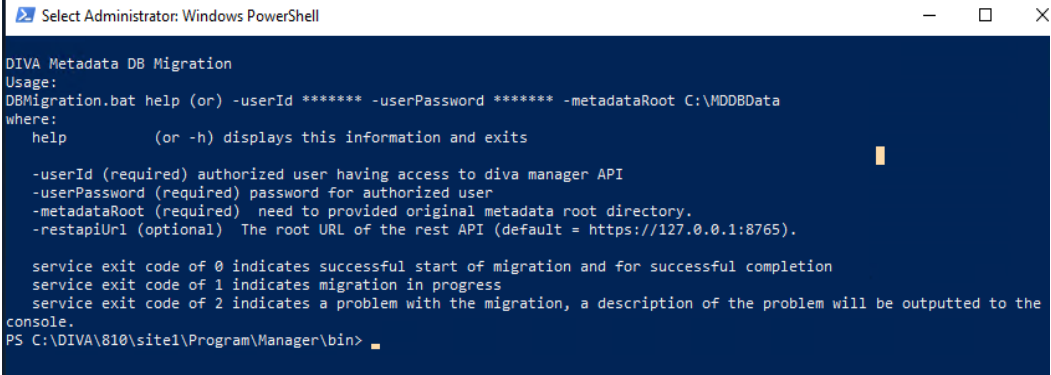
In this example, the recommended minimum disk space allotment would be for a Metadata Database size of approximately 1.67 TB.

## Mddb (Flat File Metadata Database) to MDS (Metadata Service) Migration

If Mddb Migration failed during a DIVA upgrade using the DIVA Installer and retrying did not work due to MDS and Rest API services being incorrectly installed, migration can be performed manually using `~/DIVA/Program/Manager/bin/DBMigrate.BAT`.

Remember the folder that contains the Mddb database files (that is, the Complex Objects Metadata Database Location setting in DIVA Database) before upgrade. This setting is removed automatically during a database upgrade to 9.0 and later.

If you enter `DBMigrate.BAT` without arguments, or with the `-h` parameter, you will see the following:



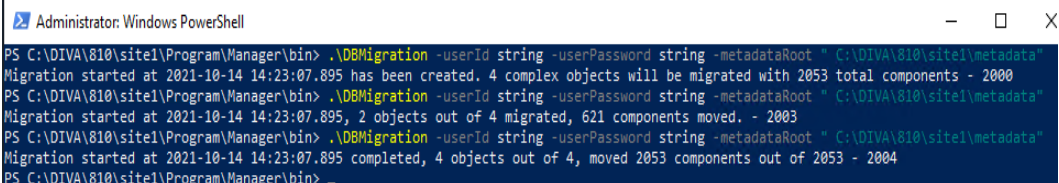
```
Select Administrator: Windows PowerShell
DIVA Metadata DB Migration
Usage:
DBMigrate.bat help (or) -userId ***** -userPassword ***** -metadataRoot C:\MddbData
where:
  help          (or -h) displays this information and exits
  -userId (required) authorized user having access to diva manager API
  -userPassword (required) password for authorized user
  -metadataRoot (required) need to provided original metadata root directory.
  -restapiUrl (optional) The root URL of the rest API (default = https://127.0.0.1:8765).

  service exit code of 0 indicates successful start of migration and for successful completion
  service exit code of 1 indicates migration in progress
  service exit code of 2 indicates a problem with the migration, a description of the problem will be outputted to the
  console.
PS C:\DIVA\810\site1\Program\Manager\bin>
```

For example:

```
DBMigrate -userId [REST API user name] -userPassword [password]
-metadataRoot "C:\DIVA\metadata"
```

Migration begins the first time this is executed. Subsequent calls provide the current status until complete, as shown here:



```
Administrator: Windows PowerShell
PS C:\DIVA\810\site1\Program\Manager\bin> .\DBMigrate -userId string -userPassword string -metadataRoot "C:\DIVA\810\site1\metadata"
Migration started at 2021-10-14 14:23:07.895 has been created. 4 complex objects will be migrated with 2053 total components - 2000
PS C:\DIVA\810\site1\Program\Manager\bin> .\DBMigrate -userId string -userPassword string -metadataRoot "C:\DIVA\810\site1\metadata"
Migration started at 2021-10-14 14:23:07.895, 2 objects out of 4 migrated, 621 components moved. - 2003
PS C:\DIVA\810\site1\Program\Manager\bin> .\DBMigrate -userId string -userPassword string -metadataRoot "C:\DIVA\810\site1\metadata"
Migration started at 2021-10-14 14:23:07.895 completed, 4 objects out of 4, moved 2053 components out of 2053 - 2004
PS C:\DIVA\810\site1\Program\Manager\bin>
```

The first call created the migration and returned 2000. The next call shows two of four Objects migrated and returned 2003. This indicates the migration is still in progress. A

typical migration will show this response many times. The final call shows the migration is complete with a return of 2004.

Calling the script in this way does not show the exit codes of 0, 1 or 2. To see these exit codes create a batch file as follows to make the call:

```
call DBMigration -userId string -userPassword string -metadataRoot  
"C:\DIVA\810\site1\metadata"  
echo ERRORLEVEL %ERRORLEVEL%
```

## Troubleshooting

This topic describes basic troubleshooting methods.

### Metadata Database Failure Scenarios

This section describes possible Metadata Database failures and resolutions.

The typical Core Metadata Database backup configuration backs up the database and transfers the backup files to remote systems (as defined in the configuration) every 15 minutes. Technical Support recommends having at least two remote backup systems for redundancy.

#### Identifying Failure Scenarios, Causes, and Resolutions

The following are examples of possible failure scenarios. Each scenario includes the method of detection, the cause of the failure, a description of the failure, and recovery procedures. Contact Technical Support if you require additional assistance to resolve any of these issues.

---

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

---

### Scenario 1: Metadata Database Storage Disk Failure

A disk failure is identified on the Main Manager because no more Complex Objects can be archived into the DIVA system. Only Delete jobs are possible on existing Complex Objects. DIVA is still operational for archiving non-complex Objects.

New Metadata files created for Complex Objects archived since the last successful backup, up until the disk failure, are not available immediately. However, they can be recovered from the AXF file.

A disk failure is identified on one of the backup systems because the Metadata Database files created by a new Archive job since the disk failure are backed up only to one backup system, instead of all identified backup systems.

The method of detection for this failure is that a Complex Object job fails with the error Internal error: metadata database error. Metadata Database Backup Failure events are logged in the Manager Event Log.

The possible causes of this failure include the following:

- RAID controller failures
- Power surges
- External process errors
- Disk volume reconstruction error if the RAID was previously rebuilt

Even though Technical Support recommends storing the Metadata Database on a RAID disk, disk failure scenarios cannot be totally eradicated, and the unlikely chance of Disk Failure still exist.

Use the following procedure to attempt recovery from disk failure on the Main Manager:

1. Stop the Manager and Backup Service.
2. Replace the failed disk.
3. Navigate to the Manager Setting page in the DIVA web app and confirm that the Metadata Database Location setting is pointing to the replaced disk.
4. Start the Manager and Backup Service.
5. Copy all of the Metadata files from a backup system to the Metadata Database Location on the replaced disk.
6. Confirm no Complex Objects are lost.
7. The Metadata files of Complex Objects archived since the last successful backup, and before the disk failure, are not immediately available. However, they are recoverable from the AXF file. Recovery from AXF files is not supported in this DIVA release; contact Technical Support for assistance.

Use the following procedure to attempt recovery from disk failure on one of the backup systems. The system can be operational if the backups made to other backup systems were successful.

1. Replace the failed disk.
2. Copy all Metadata files from the second Backup System and Main Manager System to the folder identified in the Metadata Database Location on the replaced disk.

## Scenario 2: Metadata Database File Corruption

No operations or jobs are possible on Complex Objects whose Metadata files are corrupted, except Delete Object jobs, until it is restored. A Metadata file modified by any external source (other than DIVA) after it is backed up will not affect its backup copies in the backup systems.

You can identify when a Metadata Database file becomes corrupted because Complex Object jobs fail with the following error:

```
Internal error: metadata database error:  
Message: Metadata file read error.
```

The possible causes of this failure include the following:

- External process errors
- The file is modified manually by mistake

Use the following procedure to attempt recovery from a corrupt Metadata Database file. If the corruption occurred after the Metadata file is backed up, the Metadata file can be restored from one of the backups servers.

1. Execute the *FindMetadataFile.bat* utility located in the %DIVA\_HOME%/programs/utilities/bin folder on the Main Manager System.  
This utility prints out the location of the Metadata file with its file name inside the specified Metadata Database Location, and accepts the database connection parameters and the Complex Object name and Collection as parameters.
2. Locate the file with the file name and path printed from the utility in the Metadata Database backup location on one of the backup servers.
3. Replace the Metadata file on the Main Manager System in the configured Metadata Database Location with the copy from the backup server.

If the corruption occurred before the Metadata file was backed up, the Metadata file is not immediately available. However, it is recoverable from the AXF file. Recovery from AXF files is not supported in this DIVA release; contact Technical Support for assistance.

### Scenario 3: Lost or Manually Deleted Metadata Database File

Metadata deleted by any external source other than DIVA after it is successfully backed up does not affect its backup copies on the backup systems.

You cannot perform any operations or jobs on Complex Objects whose Metadata file is corrupt, except Delete Object, until the Metadata file is restored.

You can identify when a Metadata Database file is lost or deleted because Complex Object jobs fail with the following error message:

```
Internal error: metadata database error:  
Message: get: Error opening metadata for objectname/category, db  
error=Error file not found.
```

The possible causes of this failure include the following:

- External process errors
- The file was manually deleted by mistake

If the file is lost after the Metadata File is backed up, the Metadata File can be restored from one of the Backup Servers. Use the following process to attempt recovery from a lost or deleted Metadata Database file:

1. Execute the *FindMetadataFile.bat* utility located in the %DIVA\_HOME%/programs/utilities/bin folder on the Main Manager system.  
This utility prints out the location of the Metadata file with its file name inside the specified Metadata Database Location, and accepts the database connection parameters and the Complex Object name and collection as parameters.
2. Locate the file with the file name and path printed from the utility in the Metadata Database backup location on one of the backup servers.
3. Replace the Metadata file on the Main Manager System in the configured Metadata Database Location with the copy from the backup server.

If the file was lost before the Metadata file was backed up, the Metadata file is not immediately available. However, it is recoverable from the AXF file. Recovery from AXF files is not supported in this DIVA release; contact Technical Support for assistance.

## Scenario 4: Failure to Backup Metadata Database to All Backup Systems

Failure to back up the Metadata Database to all backup systems results in all Complex Objects archived after this failure not being backed up. You must resolve this failure as soon as possible because the DIVA system is at risk of data loss.

You can identify this error when a Metadata Database Backup Failure is logged in the Manager Event Log.

The possible causes of this error are as follows:

- Network errors
- The backup systems are offline
- The Backup Service has failed

Use the following referenced resolutions to attempt correction of this issue:

### Network Errors

Resolve the network error.

### Backup System Offline

Start, or restart, the Backup System.

### Backup Service Failure

Restart the Backup Service and collect the logs for investigation.

After the problem is resolved, all of the Backup Systems sync automatically, and the missing Metadata files are backed up during the process. There is no data recovery required for this scenario.

## Scenario 5: Failure of the Metadata Database Backup to One Backup System

In this scenario, the Metadata Database fails to back up to (only) one of the Backup Systems. However, the back ups to other Backup Systems continue successfully.

You can identify this error when a Metadata Database Backup Failure is logged in the Manager Event Log.

The possible causes of this error are as follows:

- Network errors
- The Backup System where the error occurred is offline

Use the following referenced resolutions to attempt correction of this issue:

### Network Errors

Resolve the network error.

### Backup System Offline

Start, or restart, the Backup System.

After the problem is resolved, all of the Backup Systems sync automatically, and the missing Metadata files are backed up during the process. There is no data recovery required for this scenario.

### Manager Will Not Start

When the Manager starts it checks the following parameters. The Manager will not start if any combination of these parameters is incorrect. Confirm the Enable Metadata Database parameter is configured correctly, and the Metadata Database Path is a valid path that is not empty.

### Backup Service Will Not Start

The DIVA Backup Service is designed to terminate execution immediately after attempting to start if it is configured incorrectly. This behavior can be caused by any of the following reasons:

- The configuration file is missing.
- The database connection information is incorrect, or the database is not running.
- The BACKUP\_SERVICE\_MANAGE\_METADATA\_BACKUPS parameter is set to Y (Yes, or enabled) in the Configuration file, but not enabled under the Manager Settings panel in the DIVA web app.
- The BACKUP\_SERVICE\_MANAGE\_METADATA\_BACKUPS parameter is set to Y (Yes, or enabled) in the Configuration file, but the Metadata Database Location is not set, or set to an invalid directory under the Manager Settings panel in the DIVA web app.
- The BACKUP\_SERVICE\_MANAGE\_METADATA\_BACKUPS parameter is set to Y (Yes, or enabled) in the Configuration file, and the Metadata Database Backup is enabled under the Manager Settings panel in the DIVA web app, but the Metadata Database Location is not set, or set to an invalid directory.
- BACKUP\_SERVICE\_MANAGE\_DATABASE\_BACKUPS and BACKUP\_SERVICE\_MANAGE\_METADATA\_BACKUPS parameters are set to N (No, or disabled) in the Configuration file.
- RMANRecoverWindow.bat is not in the bin folder for the Backup Service.

## Troubleshooting and Failovers

### 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 patch (if available) and restart the Manager
3. Upgrade the DIVA installation
  - Instance Failure
4. Restart the Postgres instance
5. 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.

```

Mode                LastWriteTime         Length Name
-----
d-----            1/5/2023  12:27 AM
-a-----            1/5/2023  12:27 AM      16777216 archive_status
Starting service: postgresql-x64-14...
sc start postgresql-x64-14

SERVICE_NAME: postgresql-x64-14
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT           : 0xea60
        PID                : 512
        FLAGS               :

Service: running.
True
Creating 500MB space reservation file...
File F:\DO_NOT_DELETE_-_WAL_LOGS_SPACE_RESERVE is created

Cleaning up...
*****
Logs for this installation can be found at:
C:\_scripts\2022-12-07 Postgres14_64bit_windows\log
*****
Press any key to close this window...

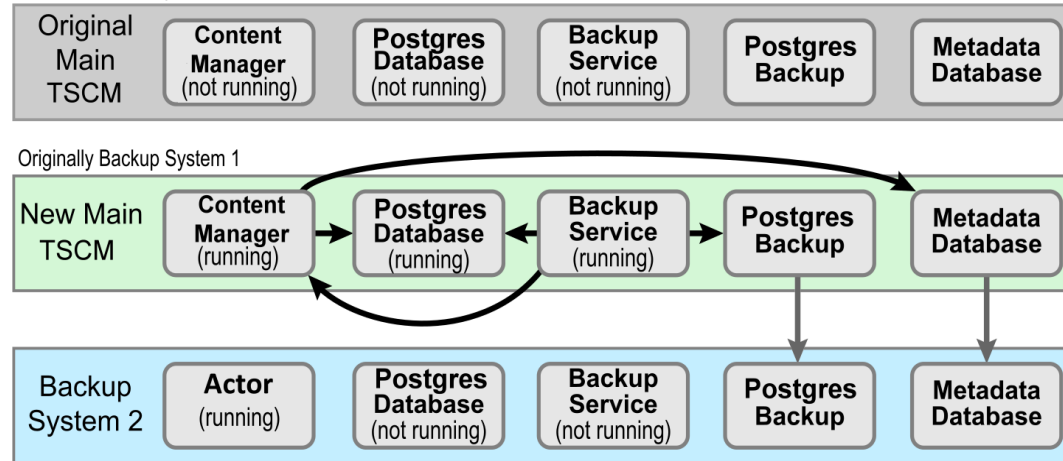
```

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.

Offline and Non-Operational



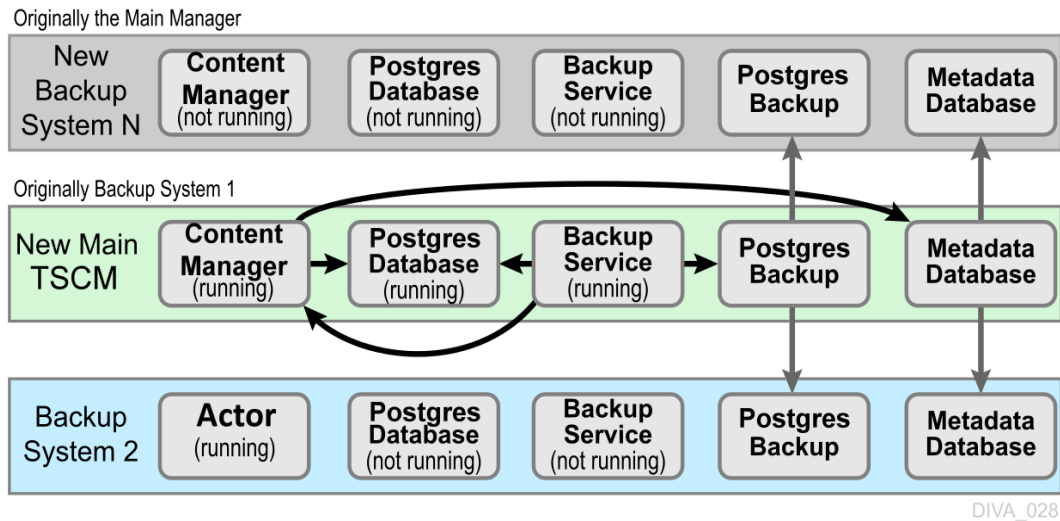
DIVA\_027

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 DIVA 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.

- 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:

- Add the configuration in a new database profile and install a DBAgent on that standby server.
- 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.

# System Maintenance and Monitoring

This chapter describes starting and stopping DIVA, involving specific, ordered processes.

## Topics

- [The DIVA Launch Process](#)
- [Stopping DIVA](#)
- [Backup Service Warnings and Notifications](#)
- [Failover Procedures](#)
- [Job Monitoring](#)
- [System Information and Log Collection Tool](#)

## The DIVA Launch Process

To start the DIVA system, start the hardware first, then start the software in the sequence as described in the following sections.

### Starting DIVA Hardware

Perform the following steps in sequence to start all of the DIVA hardware components. Wait for initialization of each hardware component to complete before moving to the following step.

1. Confirm that all required devices are installed. If they are not installed, they must be installed before proceeding any further.
  - a. Managed Storage and Drives
  - b. SAN RAID Arrays
  - c. Fiber Channel Switches
  - d. Networking Devices
  - e. Terminal Concentrator
  - f. Graphical Front End Hosts (DIVA web app)
  - g. Library DIVA Host
  - h. External Direct Attached Devices
  - i. DIVA Hosts
  - j. Actor Hosts
2. Power on the Managed Storage and Drives.
3. Power on the SAN RAID Arrays.
4. Power on the Fiber Channel Switches (if installed).
5. Power on the Networking Devices.
6. Power on the Terminal Concentrator (if installed).
7. Power on the Graphical Front End Hosts (DIVA web app).
8. Power on the Library DIVA Host (if installed).
9. Power on External Direct Attached Devices.
10. Power on DIVA Hosts.

In installations where two DIVA Hosts are installed, it may be required to always start the Main DIVA first, and then the Alternate (or Backup) DIVA at a later time. Consult with your Telestream Installer to determine if this is applicable to the installation.
11. Power on the Actor Hosts.

Hardware start is complete if everything powered on successfully.

## Starting DIVA Software

The following steps describe the required order that the software components of a DIVA system must be launched. Some software components may be set to launch automatically when the host is started (for example, the Actor Service).

---

**Note:** Some DIVA Windows Services may be disabled, or set to be launched in manual mode, due to the configuration and settings done by Professional Services during the installation.

---

Perform the following steps in sequence to start all of the DIVA software components:

1. Confirm that all required components are installed. If they are not installed, they must be installed before proceeding any further.
  - a. REST API Gateway
  - b. Discovery service
  - c. Library Robot Controller
  - d. Library
  - e. Manager
  - f. Backup Service
  - g. DIVA Connect
  - h. VACP Converter
  - i. SPM (Storage Policy Manager)
  - j. WFM (Watch Folder Monitor)
2. Launch the Library Control software.
  - a. ACSLS
  - b. PCS
  - c. SDLC
3. Launch the Robot Managers.
4. Launch the Actors.
5. Launch Manager.
6. Launch DIVA Connect.

You can start the following services independently:

  - Robot Managers
  - Actors
  - Metadata Service (MDS)
  - Manager
  - Proxy service
7. Launch the VACP Converter.
8. Launch SPM.
9. Launch WFM.

Software start is complete if everything initialized successfully.

## Stopping DIVA

DIVA is stopped in the reverse order from starting the system. Shut down the software first and then the hardware. The following sections describe the required procedure to fully shut down DIVA.

## Shutting Down the Software

To ensure that jobs currently still in progress are not prematurely terminated by shutting down the DIVA system, it is recommended the DIVA be stopped first, because any jobs currently active are completed before DIVA completes shut down.

See [Stopping DIVA](#) for DIVA shut down procedures. When the DIVA is shut down all operations are ceased. It is not necessary to stop other software components before shutting down the host computer where they are installed.

## Shutting Down the Hardware

Use the following procedure (in sequence) to shut down all DIVA-related equipment and devices:

1. Shut down the DIVA Host.
2. Shut down the Actor Hosts.
3. Power off all External Direct Attached Devices.
4. Power off Graphical Front End Hosts.
5. Power off Terminal Concentrator (if installed).
6. Shut down the Library Manager Host (if installed)
7. Power off Network Devices.
8. Power off Fiber Channel Switches (if installed).
9. Power off SAN RAID Arrays (if installed).
10. Power off Library and Drives.

Hardware shut down is complete if everything powered off successfully.

## Backup Service Warnings and Notifications

In DIVA the Backup Service error and warning dialog boxes are no longer displayed in the DIVA web app.

## Failover Procedures

---

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

---

The following steps are required to fail over a DIVA to the Backup when the database is still accessible on the original DIVA:

## Scenario 1—Failover with Multiple BKS Installations (Recommended)

Use the following procedure to fail-over using multiple BKS installations. This is the recommended scenario.

1. Stop all services on the Primary site (if available).
2. Start the BKS and DBAgent and related databases on the Failover site.  
If backups are enabled on the fail over site, you should disable them by setting the Enabled flag in the configuration file. This ensures that there are no backup operations competing with your failover command.

```
"DatabaseBackup": {  
  "Enabled": false, <=== UPDATE  
  "FullBackupInterval": {  
    "executionPeriod": 0,  
    "timeOfDay": "12:00:00",  
    "instancesInPeriod": null  
  },  
  "IncrementalPeriod": 15,  
  "FullBackupFileRetention": 10,  
  "FullBackupArchiveRetention": 30,  
  "ArchiveMediaGroup": "",  
  "PermanentRetentionPeriod": 180,  
  "ArchiveSourceName": "",  
  "BackupExecutionTimeout": 120,  
  "RestoreExecutionTimeout": 120,  
  "StatusPollingPeriod": 3,  
  "StatusReportingInterval": 1440  
}
```

3. Initiate the failover command (This must be done for each database):

**From the API: <https://localhost:1877>:**

- a. Select `PUT /Backup/failover/{name}` and click Try It Out.'
- b. Enter the database profile name for the source.
- c. Enter the failover profile name as the target.
- d. Enter a date if you are recovering from a specific time, or leave the field empty if you would like the latest backup file used.
- e. Click Execute.



---

**Note:** The API does not wait for status before returning. To see the status of the job you can use the `GET /Backup/status/{name}` endpoint with the name of the target profile.

---

**From the Initiator.exe:**

- a. Select the Failover option.
- b. Select the option for your failover. It looks similar to  
`<profile name> ? <profile name failover>`.
- c. Select a time to failover from.
- d. Wait for the operation to complete.

After the databases have been failed over, start other services and verify they are running as expected.

Enable the database backups in the configuration file that you disabled in an earlier step.

---

**Note:** To fail back, the same steps are run replacing the source and target database profiles. No files need to be transferred, all of this is done by the BKS.

---

## Scenario 2—Failover from a Single BKS Instance

Use this procedure to failover using a single BKS installation. See the DIVA Database and BKS Installation, Configuration and Operations book for configuration details.

1. Verify the DBAgent and the databases needed are up on the Failover server and that all services that use the database are offline.
2. Disable backups.  
If backups are enabled on the failover site, you should disable them by setting the Enabled flag in the configuration file. This ensures that there are no backup operations competing with your failover command.
3. Remove the primary databases from the managed primary location and add the failover databases to the managed databases for the failover location.

```
"LocationSettings": {  
  "Locations": [  
    {  
      "Name": "Primary",  
      "Primary": true,  
      "Enabled": true,  
      "Location": "H:\\divaback",  
      "AgentUrl": "https://localhost:1878/",  
      "Type": "Local",  
      "ManagedDatabases": [], <=== UPDATE  
      "BackupReplication": [  
        "MetadataDatabaseFailover",  
        "OracleDatabaseFailover"  
      ],  
    },  
  ],  
}
```

```

        "SourceName": "",
        "User": "",
        "Password": ""
    },
    {
        "Name": "Secondary",
        "Primary": false,
        "Enabled": true,
        "Location": "\\<path to divaback on failover>",
        "AgentUrl": "https://<failover server ip>:1878/",
        "Type": "Local",
        "ManagedDatabases": [
            "MetadataDatabaseFailover", <=== UPDATE
            "OracleDatabaseFailover" <=== UPDATE
        ],
        "BackupReplication": [
            "MetadataDatabase",
            "OracleDatabase"
        ],
        "SourceName": "",
        "User": "",
        "Password": ""
    }
]
}

```

**4. Initiate the failover from the API or Initiator.exe:**

**From the API: <https://localhost:1877>:**

- a. Select PUT /Backup/failover/{name} and click Try It Out.'
- b. Enter the database profile name for the source.
- c. Enter the failover profile name as the target.
- d. Enter a date if you are recovering from a specific time, or leave the field empty if you would like the latest backup file used.
- e. Click Execute.

---

**Note:** The API does not wait for status before returning. To see the status of the job you can use the GET /Backup/status/{name} endpoint with the name of the target profile.

---

**From the Initiator.exe:**

- a. Select the Failover option.
- b. Select the option for your failover. It looks similar to  
<profile name> ? <profile name failover>.
- c. Select a time to failover from.
- d. Wait for the operation to complete.

**5. Enable the database backups in the configuration file that you disabled earlier.**

---

**Note:** To fail back, perform the above setups replacing the source and target databases and change which databases are being managed.

---

## Job Monitoring

During normal operations, periodic monitoring of the Errors column in the DIVA web app's Jobs or Job History view for warnings and/or errors is necessary.

An orange exclamation mark indicates that the job had recoverable errors.

A red exclamation mark indicates that the job had an irrecoverable error and was terminated.

The current state of a job can be viewed in the DIVA web app under the Content Management > Job History page in the STATE column.

Contact Telestream (see [Telestream Contact Information](#)) for additional assistance when required.

## Job Warnings

A warning status indicated on a job signifies that an unexpected error occurred during the jobs execution, but the job was still completed.

The following are three example Scenarios:

An I/O error occurred when reading an object from tape. However, there was a second instance of the object on another tape. DIVA attempted to use the second instance and this time the object transferred successfully. The tape from the first restore attempt must be investigated. If multiple events of this type occur across multiple tapes, establish whether they all relate to a specific tape drive. If the errors are severe, DIVA will automatically mark the drive Out of Order.

An object is being transferred to a disk array. Because multiple disks can be assigned to an array, an unexpected I/O error may have occurred with one of the disks in the array. DIVA automatically selects another disk from the array to transfer the object to, and this attempt is successful. The disk where the I/O error occurred is marked Out of Order by DIVA and not used again. The offline disk must be examined for the cause of the error.

An object is being archived to tape and a write error occurs with the selected tape. DIVA attempts to use another tape and drive to fulfill the job. The tape from the first write attempt is marked Read-Only, and not used for additional archive jobs.

## Initiating a Cluster Failover

---

**Note:** Clusters are not supported in this DIVA release.

---

Use the following procedures if a cluster fails to initiate:

1. Check that the backups are synced on the Active Node and Backup DIVA Core.
2. Stop all DIVA Services from the Microsoft Cluster on the Active Node.
3. On the Active Node, run `SELECT COUNT(*) AO_OBJECT_NAME from DP_ARCHIVED_OBJECTS;`

4. Create an export of the current database from the Active Node.
5. Stop the DB Services on the Active Node from the Microsoft Cluster Core.
6. Start the DB Services on the Backup DIVA Core server.
7. Recover the database from the backups. Contact Telestream (see [Telestream Contact Information](#)) if you require assistance recovering the database.
8. Start the DIVA Services on the Backup DIVA Core and run some tests to confirm functionality.

When all testing is successful, stop all Backup DIVA Core services, and restart all services from the Microsoft Cluster Core. Verify all operations are functioning normally.

## System Information and Log Collection Tool

The Customer Information Collection Tool is a utility feature used by Telestream Support and Development teams to collect information on the client's DIVA system to analyze and diagnose issues uncovered in the field. This utility is included in the DIVA delivery, but is only intended to be used by Telestream personnel.

The tool receives all customer information required for support investigations including log files, dump files, and client environment information. It receives information from all client sites in a uniform manner, and retains detailed client issue information with the originator's contact information. The tool also notifies the Telestream Development Team as soon as information is transferred to the development facility, where it is stored permanently for future issue resolution as necessary.

The CollectSysInfo.bat file enables collecting the required information to send to the Telestream Support and Telestream Development teams for issue resolution. Execute the batch file using the following command and parameters:

```
%DIVA_HOME%\Program\Utilities\bin\CollectSysInfo.bat [parameter value]
```

Example:

```
%DIVA_HOME%\Program\Utilities\bin\CollectSysInfo.bat -EXMODULES VACP, AMCommunicator -AFTERDATE 09/25/2016 -MACHINES 172.16.3.45,172.16.3.46 -DBTYPE conf -CUST -CUSTOMER1
```

The main CollectSysInfo.bat command parameters are as follows:

- **-EXMODULES [MODULE\_NAMES]**  
Excludes the specified module from collection logs and configuration files. Using **-EXMODULES ALL** excludes all of the modules and only collect the Core Database dump. The default is collecting all modules.
- **-AFTERDATE [MM/DD/YYYY]**  
Collects logs only on or after the specified date. The default is collecting all available logs.

- `-MACHINES [IP:host_name,IP:host_name,and so on]`  
Collects the logs from any additional computers identified. Multiple host names are identified in a comma separated list. The default is to only collect logs for the current system where the script is running.
- `-DBTYPE [FULL|CONF]`  
Collects a full Core Database dump, or just a configuration dump. The default is collecting a full database dump.
- `-CUST [CUSTOMER_NAME]`  
The name of the customer where the logs are collected. The customer name is truncated if it is longer than 13 characters. There is no default value for this optional parameter. If it is not supplied as an argument the script prompts you to enter the Customer Name during execution.

There are also several internal parameters for the script. Each of the internal parameters has a default value that can be overridden by specifying a custom value using the script options.

**Example:**

```
%DIVA_HOME%\Program\Utilities\bin\CollectSysInfo.bat -EXMODULES
VACP, AMCommunicator -AFTERDATE 09/25/2016 -MACHINES
172.16.3.45,172.16.3.46 -DBTYPE conf -CUST CUSTOMER1 -DIVALOC
C:\INSTALL\DIVA
```

The additional script parameters are as follows:

- `-DIVALOC`  
The DIVA installation path for all computers from where the script is collecting logs. The default value is `%DIVA_HOME%`.
- `-REMOTEDIVA`  
The DIVA installation location if additional computers are specified using the `-MACHINES` parameter. The path set in this parameter must be shared within the network. The default value is `\\RemoteSystem\C$\DIVA`.
- `-DUMPPATH`  
The location where the script generates and outputs the .7z zip file. The default value is `H:\`.
- `-POSTGRESLOGIN`  
The Core Postgres Database user name and its connection details.
- `-CYGWIN`  
The Cygwin installation path. Default: `C:\cygwin\bin`.
- `-SEVENZIP`  
The 7z zip tool installation path. Default: `C:\Program Files\7-Zip\7z.exe`.
- `-TEMPDIR`  
The temporary directory where the script copies the logs and configuration files. This folder is created automatically at the beginning of the script execution and

subsequently deleted after the script completes execution. The script fails execution if the path set in this parameter already exists. Default: H:\supportinfo.

# Frequently Asked Questions

In general, refer to the documentation for the specific component for Frequently Asked Questions about that particular component. Contact Technical Support for any additional questions not covered here. This chapter includes some basic examples from those documents and answers the following questions:

## Topics

- [DIVA Installation Questions and Answers](#)
- [Database Backup Questions and Answers](#)

## DIVA Installation Questions and Answers

### **What Happened to DIVA Command?**

DIVA Command has been replaced by the DIVA web app.

### **What if the Customer Information Collection Tool does not work?**

Confirm that CygWin and the 7z archive programs are installed correctly. If the CygWin or the 7z programs are not installed, the Customer Information Collection Tool will stop running and display one of the following error messages:

```
Error: Cygwin environment could not be located at "...". Please check the configuration or reinstall Cygwin environment if necessary.
```

```
Error: 7Z archiver could not be located at "...". Please check the configuration or reinstall 7Z archiver if necessary.
```

### **Should all operating systems be kept up to date with critical updates?**

Technical Support recommends applying all critical updates to all computers because some may include security updates. Windows operating system updates and patches are not tested by Telestream.

### **Should operating systems be kept up to date with optional updates?**

Optional operating system updates are not necessary in the DIVA environment and are not tested by Telestream. However the decision to apply optional updates is left to your System Administrator.

### **Are there any operating system updates that should not be installed?**

Technical Support is not currently aware of any operating system updates that impact DIVA functionality or operations. However, operating system updates and patches are not tested by Telestream.

### **Should the servers be restarted with any frequency?**

No, restarting the servers will cause downtime for the system and possibly cause data corruption if a process is executing when the server is restarted. Only restart a server when absolutely necessary and perform a normal system shutdown.

---

**Caution: Do not just power off the computer unless absolutely necessary. Data and/or database corruption or loss could occur if normal shutdown procedures are not followed. See the DIVA Operations Guide on the DIVA Technical Support site for proper shutdown procedures.**

---

### **Should any services be restarted with any frequency?**

No, restarting the services will cause downtime for the system and possibly cause data corruption if a process is executing when the service is restarted. Only restart a service when absolutely necessary.

### **Should any vendor applications be restarted with any frequency?**

No, only restart a vendor application when absolutely necessary.

### **Should vendor applications always be updated to the latest version?**

No, only update vendor applications to benefit from new functionality or for bug fixes.

### **Where are vendor-specific logs located?**

The vendor-specific log files are located in the %DIVA\_HOME%\Program\log folder.

### **How far back in time do the logs go?**

The log file retention period is configurable in the DIVA configuration file. Contact Technical Support for more information. The log files are retained as follows by default:

- DIVA Manager, DIVA Connect: fifty hours
- Actor, Robot Manager, Storage Policy Manager, Avid Transfer Manager Communicator, Avid Archive Manager Communicator: 10 days
- Watch Folder Monitor: variable based on size

### **What is the suggested log backup frequency?**

The log files do not require backup.



**Are there any special considerations regarding maintenance and backup of vendor servers and systems?**

Technical Support only supports the DIVA software. You must contact the server supplier for any hardware issue. You must keep Technical Support in the loop for any issues on the DIVA solution (for example, loss of a RAID disk, failover to the backup manager, and so on).

**Are there special considerations related to recovering from a server failure when the server is part of the vendor solution?**

As previously mentioned, you must keep Technical Support in the loop if issues are encountered.

**When a Metadata file is manually deleted from Main Manager System, is it also deleted from all backup systems?**

Manually deleted Metadata files are not propagated to any backup systems.

**How do I recover when a Complex Object's Metadata File is lost on the Main Manager System and all backup systems?**

You can restore Metadata files from tape or disk. The feature to restore Metadata files from tape or disk is not currently available in this DIVA release. Contact Technical Support for assistance.

**How do I locate a Complex Object's Metadata inside the Metadata Database?**

Contact Technical Support for assistance.

**How do I estimate the size for the Metadata Database location?**

See [Metadata Database Sizing](#) for detailed information.

**Where do I configure the location of the Metadata Database?**

The location of the Metadata Database is configured using the Complex Objects Metadata Location parameter in the Manager Setting panel in the DIVA web app.

**What information is stored in the Metadata Database file?**

All file details including file names, folder names, location, size, checksums, etc.

**Is the information stored in the Metadata Database irreplaceable or mission critical?**

Technical Support always recommends having at least two backup copies of the Metadata Database. Use the DIVA Backup Service to back up the Metadata Database. In a worst case scenario, use the Archive eXchange Format Explorer (AXF) to recover the Object from tape if the Metadata Database file of a particular Object is lost.

**Why is this information not being stored in the existing Database?**

The amount of Metadata information is huge. Complex Objects are supported up to 1,000,000 files. Currently, the Database in use does not have any scalability features to support Complex Object workflows.

**What are the space requirements for the Metadata Database and data? Does it depend on the quantity of Objects, the complexity of those Objects, or something else?**

See [Metadata Database Sizing](#) for detailed information.

**What if a customer has, for example, 1,000,000 Objects, each with 100,000 files?**

The Metadata Database is very scalable and can handle this amount with no issues.

**What are the consequences of the Metadata Database becoming inoperable, corrupt, or missing? Will data loss, performance loss, or something else occur?**

You will not be able to process Complex Object jobs if the database becomes inoperable. You can restore from one of the backup copies if the database becomes corrupt, or is missing.

**What are the consequences of the Metadata Database running out of available storage space? Will data loss, performance loss, or something else occur?**

In this case you will not be able to process any Complex Object jobs. See [Metadata Database Sizing](#) for detailed information.

**What tools exist for testing or verifying the integrity of the Metadata Database? Are the tools automatic, invoked manually, or can either method be used?**

Currently there are no tools that exist to check the database integrity. Contact Technical Support if you need assistance.

**What tools exist for backing up the Metadata Database? Are the tools automatic, invoked manually, or can either method be used?**

Always use the DIVA Backup Manager Service to back up the Metadata Database.

**What tools exist for recovering the Metadata Database if loss or corruption occurs? What is the procedure to execute recovery, and is any of the recovery automatic?**

See [Metadata Database Failure Scenarios](#) for the complete procedure.

**Can the location of the Metadata Database backups be configured?**

Yes, you can configure the backup location. See [Installing Metadata Database Installation \(Optional\)](#) for DIVA Backup Service installation and configuration procedures.

# Database Backup Questions and Answers

## **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 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 the DIVA User Guide 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 the DIVA User Guide 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. Refer to the DIVA User Guide for complete procedures.