Installation and Administration Guide

Release: 9.4

Revision: 1

January 14, 2025 | 1401251005|

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, 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, 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, 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.

intoPIX and Fraunhofer. Notice under 35 U.S.C. §287(a): This product or service includes JPEG XS compliant features that are covered by patents in the United States and in other jurisdictions owned by intoPIX SA (“intoPIX”) and/or Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung E.V. (“Fraunhofer”) and listed at HYPERLINK "http://www.jpegxspool.com"www.jpegxspool.com. Additional patents may be pending in United States and elsewhere.

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.

MediaInfo. 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.

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.

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 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: EN 55032, IEC/EN 61000-3-2, IEC/EN 61000-3-3, FCC Part 15 Subpart B, ICES-003, VCCI 32-1, AS/NZS CISPR 32

Electromagnetic Immunity: EN 550535

Safety: IEC 62368-1, EN 62368-1, CSA C22.2 No. 62368-1-14, UL 62368-1

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.

Contents

Getting Started 14

System Administrators 14
Media Managers 14
Users 15
Questions to Consider 15

DIVA Components 17

DIVA Architecture 17
Hardware Components 18
- Storage Devices 18
- Storage Connection 19
- System Component Interconnectivity 19
- Network Devices 19

Software Components 19
- Software Component Relationships 20
- Actors and Proxy Actors 20
- Actor and Manager (Single Computer) 21
- Analytics 21
- Backup Service (BKS) 21
- DBAgent 21
- DIVA 22
- DIVA Connect 22
- DIVA REST API 22
- DIVA Web App 22
  - Accessing the DIVA Web App 23
  - Navigation Menu 23
  - Back-end Support 23
- Drop Folder Manager (DFM) (Legacy) (Optional) 23
  - Supported Functionalities 24
- Drop Folder Monitor (DFM) 24
  - Supported Functionalities 24
- Manager 24
- Metadata Database Service (MDS) 25

Migration Service (MGS) 25
Notification Service 25
Proxy Service 25
Recover Damaged Tape Utility (RDTU) 25
Robot Manager 26
Rosetta 26
SNMP Agent (Optional) 26
Storage Policy Manager (SPM) 26
Video Archive Communications Protocol (VACP) (Optional) 26
Workflow Service Module (Optional) 27
Other Components 27

Security Guidelines 28

Security Overview 28
Installation planning 29
The Installation Environment 29
Which Resources Need to be Protected? 29
Excluded Roles 30
Impacts of Protection Failures 30
Recommended Deployment Topologies 30
Separate Metadata Network 30
Fiber Channel Zoning 31
Safeguard SAN Disks Configuration Access 31
Install the DIVA Package 31
Tape Security 31
Backup Production Databases 31
Security Model 31
Authentication 32
Authorization 32
Tape Group Encryption 32
SSL Authentication and Secure Communications 32
DIVA User Management 32
Viewing DIVA User Roles 32
LDAP Authentication 33
Internal Communication Security 34
Secure Sockets Layer and Authentication 34
External Certificate Authorities 35
Security Tools 35
DIVA REST API Security Changes 36
Secure Deployment Checklist 37

DIVA Installation and Setup 39

Preparing to Install DIVA 39
Software Component Distribution 39
Downloading the Tooling, DIVA, and DB Installers 41
Third-Party Database Engines 41

Postgres Installation and Configuration 41
Prerequisites 42
Installing Postgres DB 42
Running the Postgres Manager (`pgadmin`) 43
Uninstalling Postgres 43
Elasticsearch Installation and Configuration 43
Installing Elasticsearch 43
Troubleshooting an Elasticsearch Installation 44
Uninstalling Elasticsearch 44
MongoDB Installation and Configuration 45
Installing MongoDB 45
Uninstalling MongoDB 46
TIKA Installation and Configuration 46
Installing TIKA 47
Uninstalling TIKA 47
Uninstalling the Oracle Database Server in Windows 47
DIVA 48
DIVA Components 48
Installing and Configuring DIVA 49
Database Schema (Optional) 53
DIVA Appliance (Optional) 53
DIVA Demo (Optional) 53
Manually Creating the Database User and Schema 54
Configuration While Manager is Running 55
Upgrading DIVA 55

Post-Installation Configuration 57

Post-Installation Configuration Overview 57
Module Configuration Files 59
Importing the DIVA License 59
Metadata Database (MDS) Module 60
Prerequisites 60
Installing the Metadata Database 60
Metadata Database Configuration 61
Metadata Database Sizing 61
MDDB (Flat File Metadata Database) to MDS (Metadata Service) Migration 62
Troubleshooting the Metadata Database 63
Metadata Database Failure Scenarios 63
Scenario 1: Metadata Database Storage Disk Failure 63
Scenario 2: Metadata Database File Corruption 64
Scenario 3: Lost or Manually Deleted Metadata Database File 64
Scenario 4: Failure to Backup Metadata Database to All Backup Systems 65
Scenario 5: Failure of the Metadata Database Backup to One Backup System 66
Actor Module 66
Prerequisites 66
Configuring Actors 67

Installing the Actor 67
Actor Executables 68
Additional Actor Batch Files 68
Local Actor Configuration File (`actor.conf`) 68
Actor Service Installation and Removal 69
Actor Service Management Functions 69
Actor Launch 70
Actor Definition and Declaration 70
Actor Settings 70
Actor Advanced Settings 72
Actor to Drive Connections 84
Proxy Actor Definitions 84
Resource Selection and Manager-Actor Communication 85
Actor and Tape Clones 85
Actor Activity Logs 86
Analytics Service Module 86
Prerequisites 86
Installing, Uninstalling, and Operating the Analytics Service on Windows 86
Configuring the Analytics App 87
Backup Service (BKS) Module 87
Configuring BKS 88
DBAgent 89
Backup Initiator 89
Backup Timing 90
Workflows 90
Archive Workflow 90
Restore Workflow 91
BKS Recommended Practices 92
BKS Installation and Configuration 92
BKS Software Installation 92
BKS Configuration 95
BKS and DBAgent Removal 96
Backup Service Logged Events 96
Complex Objects 97
Prerequisites 97
Configuring REST API Gateway 98
Manager Module 98
Prerequisites 98
Manager Configuration 99
Manager Configuration 99
Tape Import Batch File 100
Basic Settings 100
Database Settings 100
Settings for Logging 100
Configuring Job Priorities 101
Installing and Removing the Manager Service 101
Manager Service Management 103
Manager Activity Logging 104

Confirming System Connectivity 104
Confirming Remote Client to Manager Connectivity 105
Confirming Manager to Actors Connectivity 105
Confirming Manager to Robot Manager Connectivity 105
Rerouting Destinations (Optional) 106
Drop Folder Monitor (DFM) 107
Migration Service Module (MGS) (Optional) 107
Prerequisites 107
Installing, Uninstalling, and Operating MGS on Windows 108
Configuring the Migration Service 108
Migration Service API Documentation 108
MGS License 108
MGS Log File 109
Dedicated mgs_diva Postgres Database 109
Notification Service Module 109
Prerequisites 109
Proxy Service Module (Optional) 110
Prerequisites 111
Installing, Uninstalling, and Running the Proxy Service Module on Windows 111
Workflow Service Module (WFS) (Optional) 112
Prerequisites 113
Installing the Workflow Initiator Service 113
Uninstalling the Workflow Initiator Service 114
Upgrading from DIVA 9.3 to DIVA 9.4 114
The WFS Configuration File 115
The WFS Log File 115
MTE Transcoder 115
Workflow Engine Selection 115
VACP Converter (Optional) 116
Starting the VACP Converter 116
Ports for DIVA stack services and Third-Party DBs 117

Notifications: SNMP and Email 119

Configuring the SNMP Agent 119
Starting and Stopping the SNMP Service 120
Configuring Email Notifications 121
Configuring SMTP Messages 121

DIVA Configuration with Manager Running 124

Manager Restart Versus Manager Configuration Reload and Notify 125
Updates in the Manager Configuration 125
Updates in the DIVA Web App System Page 127
Networks Area 127
Sites Area 127
Servers Area 128

Actors Area 128
Transcoders Area 129
Updates in the DIVA Web App Robots Page 129
Robot Managers Area 129
Media Compatibility Area 130
Robot Managers-ACS Area 130
Updates in the DIVA Web App Disks Page 130
Arrays Area 130
Disks Area 130
Actor-Disk Connections Area 131
Object Storage Accounts Area 131
Updates in the DIVA Web App Drives Page 131
Drives Area 132
Managed Storage Area 132
Drive Properties Area 132
Actor-Drives Area 132
Updates in the Diva Web App Tapes Page 132
Updates in the DIVA Web App Sets, Tape Groups & Media Mapping Page 133
Updates in the DIVA Web App Analytics App Page 133
Updates in the DIVA Web App Storage Plans Page 133
Updates in the DIVA Web App Slots Page 133

System Operation, Maintenance and Monitoring 134

DIVA Launch Process 134
Starting DIVA Hardware 134
Starting DIVA Software 135
Stopping DIVA 137
Shutting Down the Software 138
Shutting Down the Hardware 138
Backup Service Warnings and Notifications 138
Backup Service Will Not Start 138
Failover Procedures 139
Scenario 1—Failover with Multiple BKS Installations (Recommended) 139
Scenario 2—Failover from a Single BKS Instance 140
Job Monitoring 142
Job Warnings 143
DIVA System Failure Scenarios and Recovery Procedures 143
Non-fail-over Scenarios 143
Failover Scenarios 144
Failover Procedures 144
Database Service Failover 146
Initiating Manager Failover 147

Frequently Asked Questions 149

DIVA Installation Questions and Answers 149
Database Backup Questions and Answers 153

Getting Started

This guide describes installation, configuration, and use of the DIVA system. It assumes a working knowledge of the Windows operating system, networking, RAID, tape drives, and fiber channel technologies.

Topics

- System Administrators
- Media Managers
- Users
- Questions to Consider

System Administrators

Before the DIVA Professional Services engineer arrives, confirm that you've installed and configured everything required to run DIVA. The DIVA Professional Services engineer can then put the necessary DIVA software on your server(s).

For basic installation information, see *DIVA Components* and *DIVA Installation and Setup*.

For specific server and network configurations, see *Supported Environments*.

Media Managers

Media Managers should work with users to determine the types of media they'll use with DIVA, and the additional DIVA products needed to complete the environment. Media Managers should work also with System Administrators, Telestream Sales, or Telestream Technical Support to identify the types of hardware to be used. Hardware could include, for example, servers, tape drives, disk arrays, and cloud accounts.

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 which DIVA components are best suited for their daily use. Leave the technical aspects to the System Administrators, but ask users what they need to fulfill their daily operations. User input on media formats, archival operations, restore operations, and other specific tasks is valuable for creating a successful, functional environment.

Questions to Consider

These questions help administrators decide which components, both hardware and software, to include in 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?
- Will end users have different roles when using the DIVA Web App?
- Will migration of older TAPE technology to a newer one be required?

- To how many remote locations will the DB backups be copied?
- Will DB Backups to tape or to cloud storage be required?

Note: In this guide, references to the name of a view in the user interface use the same spelling and capitalization as the name of the view; italicized to indicate the word is the name of the view. For example, to search for the *JOBS* view by name, you can enter capital letters; for example, "JOBS."

Note: For a list of changes made to DIVA for this release, see the *DIVA Release Notes* for this release.

DIVA Components

This chapter describes the main components of the DIVA system.

Topics

- DIVA Architecture
- Hardware Components
- Software Components
- Other Components

DIVA Architecture

DIVA is an integrated archive solution composed of several hardware and software components. A DIVA system uses a combination of software modules. The modules can run on a single computer, or can be distributed across different systems.

The DIVA architecture allows the integration of many different types of servers and technologies. For example, broadcast video servers, storage area networks, and enterprise tape-group managed storage. DIVA supports interoperability among systems, helping to ensure long-term accessibility to valued content, and keeping up with evolving storage technologies.

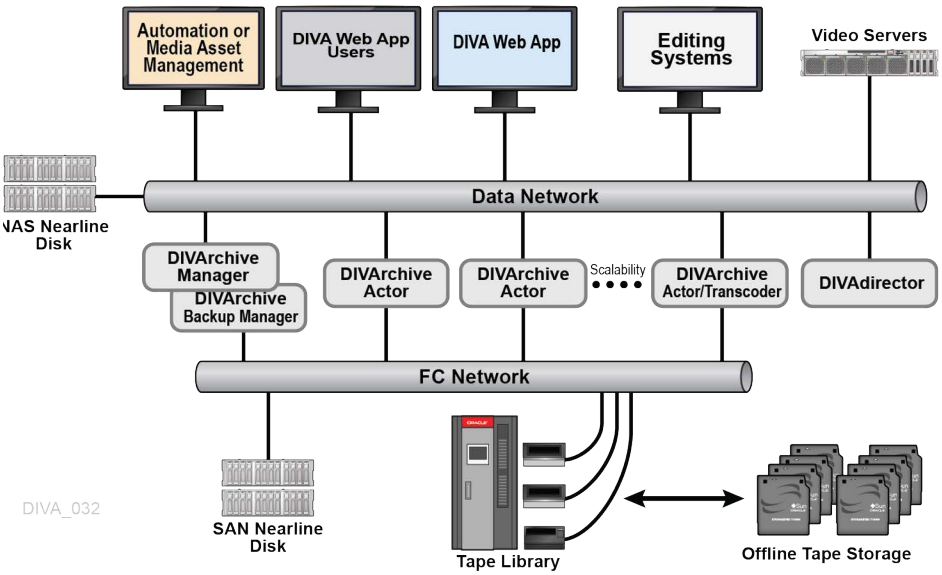
The installation of DIVA varies from site to site. The exact configuration of your specific DIVA platform is not covered in this guide. For details on your specific DIVA System installation and configuration, consult with your System Administrator, Telestream Professional Services, or Telestream Technical Support.

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

Note: The initial DIVA release is a Windows-only release; there is no Linux support at this time.

As you read through DIVA documentation, refer to the DIVA Glossary in the *DIVA User Guide* as needed.

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.



Hardware Components

Multiple hardware components are required to install the software components and together comprise a complete archiving system. The following sections describe the main system components.

Storage Devices

DIVA performs operations among different types and formats of storage devices. Some examples follow.

- RAID sets store data on hard disk drives.
- Tape Managed Storage automates storage on magnetic tapes. The tape library includes robotics, tape drives, and a set of tapes stored in the tape library.
- Tape drives can either be SCSI attached to the Actors, or through a Fiber Channel interface. When connected to a Fiber Channel Switch, they can be shared by multiple Actors. Sharing of resources among the Actors is controlled and coordinated by DIVA. The Fiber Channel Switch provides the connectivity between the Actors and any tape drives that are connected to it.
- Object Storage with on-premise or cloud-based hosting.
- For a list of environments supported by DIVA archiving, see *Supported Environments*.

Storage Connection

SAN, NAS, 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

System Component Interconnectivity

On the data path, a DIVA solution is connected on the storage side to the tape group library, or object storage, or shared disks, or any combination of these. On the source and target side, DIVA is connected to the video servers, NLE, or file servers.

Network Devices

The connections between the DIVA system components are achieved through a 10/100BaseT or Gigabit Ethernet hub or switch.

Software Components

DIVA software includes the following components:

- Actor
- Analytics Service
- APIs (Various)
- API Translation Service for Kumulate (Rosetta)
- Avid Connectivity

  For information, see *Avid Connectivity and Tools* in the *DIVA User Guide*.
- Backup Service (BKS)
- DIVA C++ API (deprecated in favor of DIVA REST API)
- DIVA Connect (Optional)

  For information, see *DIVA Connect 4.0*.
- DIVA REST API (recommended and used by DIVA)
- DIVA Java API (deprecated in favor of DIVA REST API)
- DIVA Web App
- DataBase Agent Service
- Drop Folder Manager (DFM) (legacy) (optional)
- Drop Folder Monitor (DFM) (optional)
- Manager

- Metadata Service (MDS)
- Migration Service
- Proxy Actor
- Proxy Service
- Robot Manager
- SNMP Agent
- Storage Policy Management
- VACP Converter
- Workflow Service Module (WFS)
- WS API (deprecated in favor of DIVA REST API)

Note: For a list of DIVA components that shows where they are typically installed, and whether they are mandatory or optional, see *Software Component Distribution* in the *DIVA Installation and Administration Guide*.

Third-party control software may also be provided by the library manufacturer to control the library robotics. The name of the software depends on the type and brand of the library used in the DIVA solution.

Software Component Relationships

A client-server link between two components doesn't necessarily mean that the server software must be started before the client. For example, the Manager to Actor connection. Each Actor acts as a server and the Manager initiates a client connection to the Actor. However, an Actor can be launched after the Manager is running since the Manager will attempt to reconnect to the Actor at periodic intervals.

Note: DIVA can run independently of the DIVA Web App. You can launch DIVA any time after the Manager starts running. This applies to all DIVA modules except when noted otherwise.

Actors and Proxy Actors

The DIVA Actors make all types of data transfers, such as Archive, Restore, Copy, and Repack.

Dedicated Windows or Linux servers can host the Actor component. Alternatively, you can install the Actor software directly on a production server.

Proxy Actors enable remote resources not visible to regular Actors to become visible and usable to regular Actors through a Proxy. A Proxy Actor is simply an Actor that acts on behalf of another Actor. In the most common case, a Proxy Actor reads or writes from a remote resource at the request of a regular Actor. DIVA tells a regular Actor

where it can find a proxy that will give it access to a needed remote resource through a new link between an Actor and its Proxy Actor.

See *Actor Module*.

Actor and Manager (Single Computer)

Systems running both Actor and Manager functions on a single computer. This configuration should try to be avoided for performance reasons, and is only usable for entry level configurations.

Analytics

The DIVA Analytics application is a utility that collects operational statistics from the DIVA system to monitor and maintain the archive's subcomponents (servers, media, drives, tapes, and so on). Analysis of these statistics allows both proactive and reactive maintenance of the DIVA system.

See *Workflow Service Module (WFS) (Optional)* and *Changes made in this page are effective immediately. Telestream strongly recommends you stop SPM before altering any settings on this page.*.

Backup Service (BKS)

The DIVA Backup Service (BKS) is responsible for backing up the DIVA Postgres database, the MongoDB Metadata database, and Elasticsearch.

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

See Backup Service (BKS) Module.

DBAgent

The DBAgent Service is a sub component of the Backup Service that performs database-specific tasks (that is, backups and restores), monitors their progress, and reports disk usage. Database maintenance functionality can easily be added if necessary, but only the specific backup tasks are currently implemented.

See the Database and BKS documentation on the DIVA Support Portal for detailed information.

Note: DBAgent Service User and Password are optional.

DIVA

DIVA is the generic product name of the DIVA Software and Components stack. You can install DIVA on Windows. As a purchasable option, DIVA also supports Main and Backup systems. To implement redundancy and high availability in the Active / Standby model, you can use a Backup DIVA system with the DIVA Backup Service.

DIVA Connect

DIVA Connect provides a unified view of archived digital media files across multiple, distributed DIVA systems and the cloud. It facilitates the moving of content back and forth among DIVA sites, and from customer servers and disks. DIVA Connect assists with disaster recovery, content distribution, access control, performance, and content availability.

DIVA REST API

The DIVA REST API detailed documentation is included in DIVA as HTTP documentation; this is accessible directly from within the REST API. The Swagger documentation for the REST API services is accessible at `https://localhost:8765/api-docs`.

A new Gateway and Discovery service are used in DIVA versions 9.0 and later.

Only the API configuration settings of the Discovery and Gateway services may be changed. No other settings should be changed and are present for ease of development and testing.

Telestream recommends using the REST API rather than the previous existing APIs (that is, DIVA Enterprise Connect, DIVAS, Java and C++). Although all previous APIs remain available, the REST API offers new and enhanced features. It is integrated into the DIVA Manager and is required by the DIVA Web App to function.

DIVA Web App

The DIVA Web App is a software GUI utility that connects to DIVA. You can use the DIVA Web App for configuring, monitoring and managing the DIVA system. You can operate multiple DIVA Web App instances simultaneously from any computer that has TCP/IP connectivity. The DIVA Web App is browser-based and platform-independent.

Note: The DIVA Web App replaces the legacy, Java-based, DIVA Control GUI and Configuration Utility. The DIVA Web App also replaces DIVA Command, which was introduced in early versions of DIVA 8.

Accessing the DIVA Web App

The DIVA Web App is installed by the DIVA installer. It is hosted by the REST API Gateway. Installing the Manager and REST API Data services automatically sets up the DIVA Web App.

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 the DIVA Web app.
- Manager: Required for general use of the DIVA Web app.

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

Navigation Menu

The DIVA Web App is accessible at https://127.0.0.1:8765. Log in the first time with the user name `sysadmin` and the default password. Be sure to change the password the first time you log in.

The DIVA Web App displays the navigation menu on the left-hand side. Hovering your cursor over a navigation button displays full navigation details. Click a navigation button to reveal sub-items.

Back-end Support

The DIVA Web App requires, among other services, a running Manager and Data Service.To update the DIVA Web App server port, update `api.server.port` in the `manager.conf` file. The default port is set to 8765. If you change the data service address, port, or both, update the `api.dataservice.url` in the `manager.conf` file.

The manager supports only https, so port 8765 points 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`.

Drop Folder Manager (DFM) (Legacy) (Optional)

Note: For documentation of the legacy Drop Folder Manager see the DIVA User Guide.

Drop Folder Manager (DFM) allows users and third-party applications to deliver content for archiving by copying related files to a folder, an FTP server, or a CIFS share.

Drop Folder Manager supports drop folder configuration and monitoring from the DIVA Web App. DFM archives multi-file objects without an MDF file. For information

about configuring and using Drop Folder Manager, see the chapter, *Drop Folder Manager (Legacy)* in the *DIVA User Guide*.

Supported Functionalities

- DFM supports local disks and SMB network shares (SMB 3 is required).
- DFM can't extract the content of dropped AXF
- DFM supports long path names
- DFM works on Windows but not on Linux

Drop Folder Monitor (DFM)

Note: Starting in DIVA 9.4, Drop Folder Monitor (DFM) replaces the legacy Drop Folder Manager. The DIVA Drop Folder Monitor allows users and third-party applications to submit content for archiving by copying related files to a folder, an FTP server, or a CIFS share.

DFM provides automatic monitoring of newly-created files in up to 20 local folders, FTP folders, or a combination of the two. DIVA supports one or more files in FTP folders per object.

Drop Folder Monitor (DFM) can archive multi-file objects without a configured MDF file. You can configure the Drop Folder Monitor (DFM) from the DIVA Web App.

For information about configuring and using Drop Folder Monitor, see the chapter *Drop Folder Monitor (DFM)* in the *DIVA User Guide*.

Supported Functionalities

- Drop Folder Monitor supports local disks and SMB network shares (SMB 3 required)
- Drop Folder Monitor can't extract the content of dropped AXF
- Drop Folder Monitor supports long path names
- Drop Folder Monitor currently runs on Windows but not on Linux

Manager

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

Running the DIVA software component requires at least one instance of the Manager application, and the library control software that controls the robotics. The server hosting the Manager application features a mirrored (RAID1) configuration for the data disk where the databases, and all essential data, are stored.

Because the Manager is essential to the operations of the archive system, Telestream recommends you also configure a Backup Manager. In case of failure, a failover can allow moving DIVA operations from the Main Manager to the Backup Manager.

Note: Telestream hasn't tested Microsoft Cluster Manager. nor clustering. with the current version of DIVA.

Metadata Database Service (MDS)

To effectively operate with large volumes of files and folders and other metadata, DIVA stores the metadata separately from the Postgres database in the DIVA Metadata Database. The DIVA Metadata Database is also used to store the information for Complex Objects. As such, it replaces the FBM (Flat file Based Metadata Database or MDDB) that was used in DIVA Core releases up to 8.1.

A dedicated Windows Service called Metadata Database Service is used to control storing and retrieving information from the Metadata Database.

Migration Service (MGS)

The Migrate Service is installed as part of the DIVA Suite's standard installation. It is located in the `%DIVA_HOME%\Program\MigrationService\` folder, and runs as a Windows Service.

See *Migration Service Module (MGS) (Optional)*.

Notification Service

The notification service is based on a message broker that is used to communicate and exchange information between the components of DIVA. DIVA uses the RabbitMQ Notification Service.

See *Notification Service Module*.

Proxy Service

The Proxy Service handles proxy generation of source clips for te objects archived in DIVA. It triggers Transcode Archive job requests based on rules to select the Objects needing proxies.

See *Proxy Service Module (Optional)*.

Recover Damaged Tape Utility (RDTU)

Recover Damaged Tape Utility (RDTU) recovers object instances that reside on a damaged tape. The utility can recover instances that have valid copies on other available media (that is, internal tape or a connected disk array) within a local or remote

DIVA system. There are no command line parameters. The settings and configurations are defined in the `rdtu-conf.xml` configuration file.

Robot Manager

Although you can use DIVA to only manage disk storage or cloud storage, storage capacity can be further expanded by adding one or more tape Managed Storage. In these cases, the Robot Manager module provides an intermediate software layer for DIVA to interact with many different types of tape Managed Storage. Robot Manager connects to DIVA through TCP/IP.

Rosetta

Rosetta emulates both the XML & REST APIs of Flashnet so that a DIVA system will appear to an end-user as a Flashnet system, focusing on API usage by Avid MAM plugins for Flashnet.

This allows restoring content archived through Rosetta, as well as content archived to a Flashnet system that was migrated to DIVA.

The DIVA Web App allows this functionality to be enabled or disabled, and configuring some behavior of the system (Mapping of values, or entry of default values to use).

SNMP Agent (Optional)

The SNMP (Simple Network Management Protocol) Agent and MIB (Management Information Base) supports status and activity monitoring of DIVA and its subsystems to a third party monitoring application through the SNMP protocol.

Storage Policy Manager (SPM)

The SPM (Storage Policy Manager) software component provides object life cycle management (interacting with DIVA), and is typically installed on the same computer as DIVA. For example, an archived object can reside on a specific medium the first day, and migrate (over time) to a different medium according to your established policies and rules.

See the Storage Policy Manager documentation on the DIVA Support Portal for detailed information.

Video Archive Communications Protocol (VACP) (Optional)

The Video Archive Communications Protocol is developed by Harris Automation Solutions and used by some automation systems for interfacing to an archive system. DIVA has its own API for communicating with the Manager, which is not compatible with VACP.

To provide interoperability without the need to redevelop the archive interface at the automation level, this module is provided to act as an interface to convert VACP commands from the attached automation system to DIVA API commands on computers that have TCP/IP connectivity to DIVA.

See *VACP Converter (Optional)*.

Workflow Service Module (Optional)

The Workflow Initiator service enables a robust integration between DIVA and Telestream Vantage, and between DIVA and a large variety of encoders.

Other Components

Other systems and components interacting with the DIVA system include the following:

- The applications controlling the archive operations either to move objects to the archive or to retrieve objects from the archive, and to obtain information about the archive systems or objects stored within the archive. These applications are referred to as Archive Initiators. Examples of an Archive Initiator are Broadcast Automation Systems, or MAM (Media Asset Management) applications.
- The production servers are where objects (for example, video files) are produced or from where they are broadcast. For example, a video server is a production server. Production servers can be the source of the objects to archive or the destination of the objects to retrieve from the archive.
- The production network is typically a high-speed LAN connecting the production servers together to allow object transfer between the servers. It also allows the connection of the Actors that are either attached directly to the high-speed network or through a gateway device provided by the production server manufacturer.

Security Guidelines

This chapter provides security guidelines for DIVA.

Topics

- Security Overview
- Installation planning
- DIVA User Management
- LDAP Authentication
- Internal Communication Security
- Secure Deployment Checklist

Security Overview

Keep data security as a high priority when configuring and using DIVA. Important tips for maintaining data security follow. To maintain high data security, check your system for the following:

Up-To-Date Software. Stay current with the version of DIVA that is being run. Current versions of the software are available for download at: https://www.telestream.net/telestream-support/content-manager/support.htm

Restricted 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, or permissions, restricted, on a per server basis.

DIVA Services Running as a DIVA User. Don't run as an administrator. You can use the default operating-system user with the user name *diva*.

Don't run DIVA services using an administrator (or root) operating-system admin account. Run DIVA services using a dedicated operating-system user.

Regular Monitoring. Monitor system activity to determine how well DIVA is operating, and whether DIVA logs any unusual activity. Check the log files located in the installation directory under `%DIVA_HOME%/Program/log/`.

See *System Operation, Maintenance and Monitoring*.

Up-To-Date Security Information. The primary way to keep up to date on security matters is to run the most current release of the DIVA software.

For security information and alerts for a large variety of software products, see https://www.cisa.gov/.

Anti-Virus Software. Install and run anti-virus software. For best performance, exclude the DIVA Program directory, the DIVA Windows Services, and storage managed by DIVA.

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.

Note: Be sure to change the password from the default in both the INI file and in the MDS configuration file.

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

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. You must restrict access to this data and metadata to only the Administrator (or root) operating system account, or to 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.

Excluded Roles

In general, you must protect the resources described in the previous sections 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.

Impacts of Protection Failures

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), and encryption of production data by malware.

Recommended Deployment Topologies

This section focuses on security concerns. Consider the following points when installing and configuring DIVA.

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 Storage Plan Manager (SPM), stop the corresponding Windows Service, and uninstall it or set to Manual Start.

You must restrict the default DIVA installation directory permissions and owners to only the Administrator (or root) account, or to the DIVA operating-system user.

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.

See Backup Service (BKS) Module.

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 User Management

All accounts require a password to obtain access.

Passwords are created during installation and configuration for the `sysadmin` account. Telestream recommends that you change the passwords at least every 180 days thereafter. Passwords must be made available for Telestream Support if requested.

You must assign account passwords in the DIVA Web App before using these profiles.

Note: Each DIVA component uses its own dedicated user name and password to connect to the main application. These are stored in DIVA database and shouldn't be changed.

To configure DIVA user profiles with the DIVA Web App, browse to *Configuration* > *User Management* > *User Accounts*.

Viewing DIVA User Roles

To view a visual list of what actions are allowed or not allowed for each Role, do the following:

1. Connect to the DIVA Web App.
2. Browse to *Configuration* > *User Management* > *Role Permissions*.

The DIVA system provides five fixed user Roles as follows:

System Administrator (`sysadmin`)

The System Administrator uses the `sysadmin` Role to log into the DIVA Web App. This Role allows access to all functions of the DIVA Web App. Use the `sysadmin` Role only when making additions, deletions, or changes to the DIVA system.

Caution: Telestream strongly recommends changing the default `sysadmin` password during DIVA installation and configuration.

Administrator (`admin`)

To issue jobs--such as archive or restore jobs--to DIVA, or to eject a tape from a library, use the `admin` Role. You must assign the password for the Administrator profile before using the `admin` Role.

Advanced Operator (`advoperator`)

You can use the `advoperator` Role to enable privileges for canceling and changing the priority of jobs. The options are defined in the DIVA Web App. By default, this Role is disabled.

Operator (`operator`)

You can use the `operator` Role to enable privileges for canceling and changing the priority of jobs. By default, the `operator` Role is disabled.

User (`user`)

This is the most restrictive Role. After the connection to the Manager is established, the DIVA Web App allows the User only to monitor DIVA operations. A User doesn't have access to all functions that issue commands to DIVA. Users can monitor DIVA operations, but can't send most commands to DIVA.

LDAP Authentication

You can authenticate DIVArchive with LDAP authentication instead of authenticating against the DIVA database.

To configure LDAP authentication via the DIVA Web App, do the following:

1. Browse to *Configuration* > *User Accounts* > *LDAP Configuration*.
2. To enable LDAP, drag the *Enabled LDAP* slider to the right.
3. Enter field values, as follows:

- Limit the *Base DN*, *Bind DN*, *Group Membership*, each *Host* and the *Logon* attribute to 1000 characters.
- Default the *Logon* attribute to *cn*.
- Default the group membership attribute to *member*.
- Set the password between 10 and 128 characters.
- Set the port between 0 and 65535. The default is 389.

- Set the connect timeout between two and 120 seconds. The default is five seconds.
- All parameters are mandatory.

4. Keep the following considerations in mind:

- There is a single collection of settings used to define the LDAP configuration in DIVArchive.
- You can specify the hosts containing the main and backup LDAP servers in order of priority by specifying a comma-delimited list of servers; for example, 10.1.1.1,10.1.1.2.
- In addition, you can specify the port; for example 389.
- DIVArchive uses the fully-qualified socket address, for example 10.1.1.1:389, to contact the associated LDAP server.

Note: Encryption is not supported.

- To connect to the server, DIVArchive requires a Bind DN and password. Anonymous queries are not supported. The Base DN (Distinguished Name) is the base path from which queries are performed on an LDAP server. DIVArchive uses it to query for user groups.
- The *Logon* attribute is the key used to identify the user in queries. On login, the user name is specified as a value for the login attribute, for example *cn*, to locate the user on the LDAP server. Similarly, DIVArchive uses the group membership as a key in queries to identify the user group, for example, *member*.
- User groups are converted to roles using the Role Mapping; for example, *Administrators: admin* where Administrators is the group and admin is the usual DIVArchive role.
- DIVArchive ignores this configuration unless LDAP authentication is enabled.

5. When LDAP authentication is enabled, make sure of the following:

- Disable the *Add User* button in Configuration/ User Management. A tooltip gives the reason why the user is not allowed to create new users.
- Configure 'Edit User' to allow only changing the Connect timeout. DIVArchive derives the additional information from LDAP.

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_HOME%\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_HOME%\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_HOME%\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/DIVAWebUI/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 reports an SSL Handshake Timeout if attempting to connect to the non-secure port.

SSL and Authentication

DIVA consist of services in Java C++ 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 services (DIVA Web App, Migration Utility, Actor, SPM, DFM, 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.
4. Set a strong password for `sysadmin` and any new user created in 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 software, and exclude the DIVA Program directory, the DIVA windows services, and storage managed by DIVA, 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. Set up BKS DB backup to tape.
12. 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

- Preparing to Install DIVA
- Downloading the Tooling, DIVA, and DB Installers
- Third-Party Database Engines
- DIVA

Preparing to Install DIVA

Before installing DIVA, do the following:

1. Make sure DIVA supports your system environment, and that your system meets the minimum hardware, software, and hard-drive partition requirements for DIVA.

   See *Supported Environments*.

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, and whether they are optional or mandatory to configure for a working DIVA stack.

Component	Location	Mandatory/ Optional
Actors	Actor servers	Mandatory: at least one Actor service
Archive Manager Communicator (AMC)	Actor servers	Optional
Backup Service (BKS)	Main and Backup Manager and Actor servers	Mandatory
DIVA Connect	Main and Backup Manager servers	Optional
Drop Folder Manager (DFM) (legacy)	Actor servers	Optional
Drop Folder Monitor (DFM)	Actor servers (bundled as part of Actor service)	Optional
Managers	Main and Backup Manager servers	Mandatory
Metadata Database	Main and Backup Manager servers	Mandatory
Metadata Service (MDS)	Main and Backup Manager servers	Mandatory
Postgres Database	Main and Backup Manager servers	Mandatory
Proxy Service	Main and Backup Manager servers	Mandatory
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.	Optional
Rosetta	Main and Backup servers	Optional
SNMP Agent	Main and Backup Manager servers	Optional
Storage Policy Manager (SPM)	Main and Backup Manager servers	Mandatory
Transfer Manager Communicator (TMC)	Actor servers	Optional
VACP Services	Main and Backup Manager servers	Optional
Workflow Service (WFS)	Main and Backup Manager servers	Optional

Note: When a component is installed on the Main Manager and on the Backup Manager servers, stop the corresponding Windows Service and set it to Manual on the server that is not providing the service. Typically, when the Main Manager server is

functional, the standby DIVA Modules on the Backup Manager server should be stopped.

Downloading the Tooling, DIVA, and DB Installers

1. Download all required DIVA Core installers from https://dynamic.telestream.net/downloads/diva.asp?prodid=diva.
2. Download the latest version of pgAdmin from https://www.pgadmin.org/download/.
3. Unzip the downloaded zip files.

Third-Party Database Engines

Before installing DIVA, install these database engines: Postgres DB, Elasticsearch, and MongoDB.

Postgres Installation and Configuration

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 large-scale configurations.

Caution: Before you install the Postgres Database, if you have to migrate data out of the existing DIVA 8.X Oracle database into the new DIVA 9.X Postgres one, contact Telestream Sales.

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

Caution: Telestream doesn't support direct modification of this database by customers.

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 database. This is commonly known (and will be referred to in this document) as the DIVA database (or just simply as the database).

For details about changes that can be made to the system configuration dynamically while the Manager is running, see *DIVA Configuration with Manager Running*.

The information stored in the DIVA database should be stored on a RAID-1 array to prevent data loss if a single disk fails.

To confirm disk partitioning and recommended block sizes before proceeding, see *Supported Environments*.

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*.

Installing Postgres DB

To install Postgres DB, do the following:

1. Download the Postgres installer from https://dynamic.telestream.net/downloads/diva.asp?prodid=diva.

Note: The Postgres installer is not included in the DIVA installer. The Postgres installer is installed via a dedicated package.

---

2. Unzip the Postgres zip file.
3. Open a Windows command line.
4. Run `install.bat`, and provide the following settings:

- [1] 1=Standard database
- C: for Postgres Home
- [2] 2=E:\pg_data, F:\pg_data

  This maps the legacy way of creating partitions with ORACLE for DIVA Core 8.X, therefor making the upgrade process from existing DIVA Core 8.X easier. It also allows for a clear separation between DIVA Core Postgres DB Data, and DIVA Core Postgres redo WAL logs.
- Database Memory Target is computed automatically by the installation script.

  For values, see *Minimum Partition Sizing for a Server Hosting Databases*.
- Password: Contact Telestream Support for the default password.
- Database Mount Points: The default and recommended option is 2 (2 = E:\pg_data, F:\pg_wall)
- Suggested Database User Processes: The default and recommended option is 300.

  When installation is done, the installer displays the following:

  ```
  Logs for this installation can be found at: <Location of DIVA Postgres installation binary>\log.
  ```

  The database engine is now installed and ready for the schema to be inserted.

5. To execute the installation press ENTER.

   When the installation has completed the Windows command prompt displays the results.

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

Running the Postgres Manager (`pgadmin`)

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 the 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.

To run the Postgres Manager, do the following:

1. Export the existing database contents or ensure you have a valid backup.
2. Browse to `C:\Program Files\PostgreSQL\pgAdmin 4\bin\`
3. Run `pgAdmin4.exe`.

Note: Since the Postgres Manager is a tool used often, Telestream recommends creating a desktop shortcut to `pgAdmin4.exe`.

4. Obtain the Postgres Manager default password from Telestream Support.

Uninstalling Postgres

To uninstall the Postgres Manager, do the following:

1. Browse to `<Location of DIVA Postgres installation binary>`.
2. Run `uninstall.bat`.

   On completion, the uninstaller displays the following:

   ```
   Postgres Database Uninstall completed successfully. Press any
   key to continue.
   ```

Elasticsearch Installation and Configuration

Installing Elasticsearch

Prerequisites

- Avoid white spaces in the directory tree where you copy the installation binaries.
- Ensure DIVA_JAVA_HOME is removed. See *Troubleshooting an Elasticsearch Installation*.

To install Elasticsearch, do the following:

1. Download the ElasticSearch installation bundle from https://dynamic.telestream.net/downloads/diva.asp?prodid=diva.
2. Run `InstallElasticSearchNoSSL.bat`.
3. Enter the path to the directory where the Elasticsearch indexes should be stored.

   By default the Elasticsearch binaries are installed on `C:\ElasticSearch` and the data are stored on: `S:\ElasticSearchData`.

   Telestream recommends using a dedicated partition for `ElasticSearchData`.

   See also *Minimum Partition Sizing for a Server Hosting Databases*.

Note: A Java installation package is bundled in the Elasticsearch installer. This ensures that Elasticsearch is running with the correct Java version.

4. Check Windows Services to confirm that this service is running: `Elasticsearch 7.10.2 (elasticsearch-service-x64).`

Troubleshooting an Elasticsearch Installation

An Elasticsearch installation might fail, for example in a case where DIVA 8.x previously had been installed. You can resolve this issue by deleting DIVA_JAVA_HOME from your Windows System Variables. To delete DIVA_JAVA_HOME, do the following:

1. Launch *Windows System Properties*.
2. Click the *Environment Variables* button.

   Windows opens the *Environment Variables* window.
3. In the *System variables* pane, select DIVA_JAVA_HOME.
4. Click *Delete*.
5. Click *OK*.

Uninstalling Elasticsearch

Caution: Starting from DIVA 9.3, legacy DIVA Protect data has migrated from the DIVA Database into the Elasticsearch Database. Therefore, deleting the Elasticsearch dataset erases the data used for computing DIVA Analytics. Ensure you have a valid Elasticsearch backup before proceeding with deletion.

To uninstall Elasticsearch, do the following:

1. Ensure you have a valid backup of the Elasticsearch data set.
2. Delete the Windows Service for Elasticsearch.
3. Delete the directory `S:\ElasticSearchData`.

   As mentioned earlier, this deletes the production data set.
4. Delete the directory `ElasticSearch` on the `C:` drive.

MongoDB Installation and Configuration

Installing MongoDB

Unlike postgres and ElasticSearch, which have their own dedicated installation packages, MongoDB engine is installed and configured by the DIVA Core main installer.

When performing a fresh DIVA installation, check the box for *Metadata Database*.

To Install MongoDB and set up instance and service, from outside the DIVA Installer, run the DIVA Core Metadata Service Command Line Interface, as follows:

- Run `metadata_service.bat [command] [options]` with any of the following commands:

Parameter	Option	Definition
`metadata_service.bat`		
	`install (or -i)`	`To install the module as a system service`
	`-log`	`Path to log directory. Default: ..\..\log\metadata_service`
	`-conf`	`Path to configuration directory. Default:..\..\conf\metadata_service`
	`-httpport`	`Port to listen for http connections. Default: 1776`
	`-httpsport`	`Port to listen for https connections. Default: 1777`
	`-dburl`	`Url for DB connection. Default: mongodb://127.0.0.1:27017/Core`
	`-certpath`	`Path to certificate located on disk.`
	`uninstall (or -u)`	`To remove the executable as a system service`
	`start`	`Starts the module`
	`stop`	`Stops the module if it is currently running`

Parameter	Option	Definition
	`restart`	`Stops and subsequently starts the module`
	`status`	`Determines whether or not the module is running`
`installdb`		`Installs MongoDB`
	`-datadir`	`Path to the data directory to store the MongoDB database.` `Default: H:\MDDB`
	`-port`	`Port for MongoDB to listen on. Default: 27017`
`upgradedb`		`Upgrades existing MongoDB installation`
`uninstalldb`		`Uninstalls MongoDB if installed locally.`
	`version (or -v)`	`Display the module version information and exits`
	`help (or -h, or -?)`	`Displays this information and exits`

Uninstalling MongoDB

DIVA Installer doesn't support uninstalling MongoDB.

To uninstall MongoDB manually, use the scripts provided in each DIVA component. To uninstall MongoDB, do the following:

- Run `metadata_service.bat uninstalldb`.

Note: For security purposes, this uninstall script doesn't remove the MongoDB dataset. Ensure there is a valid dataset backup before proceeding with un-installation.

See also *Installing the Metadata Database*.

TIKA Installation and Configuration

TIKA is a third-party tool that extracts metadata and text from over a thousand different file types, such as PPT, XLS, and PDF. All of these file types can be parsed, making TIKA useful for such uses as search-engine indexing and content analysis.

Installing TIKA

To install TIKA, do the following:

1. Download the bundled installer from the Telestream site.
2. Unzip the installer.
3. Run `InstallTika.bat`.

   The TIKA installer installs TIKA.
4. Check the list of WIndows Services to make sure the TIKA service is in the running state.

Uninstalling TIKA

To uninstall TIKA, do the following:

- Run `UninstallTika.bat`.

  The TIKA uninstaller uninstalls TIKA.

Uninstalling the Oracle Database Server in Windows

Caution: Uninstalling the DIVA Oracle Database should be done only after the data was migrated from Oracle DB to Postgres DB, and after acceptance tests confirm the DIVA upgrade and production-data migration was done correctly.

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

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

1. Stop all running DIVA services.
2. Export the existing database contents.

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.

DIVA

The following sections describe installation of the DIVA system. If you need assistance, contact Technical Support.

Notes: The Postgres Database must be available for DIVA before installation. See *Postgres Installation and Configuration*, and Backup Service (BKS) Module.
Before upgrading from DIVA 8.3 to DIVA 9.x on a system with cloud storage, you must confirm that the cloud array and its associated disk have the same name. DIVA supports only a single disk per cloud array.
It is possible to have multiple arrays using the same cloud account.
In this case, use the Configuration utility to convert this manually after the upgrade is complete. Otherwise, the DIVA Web App won't display the cloud array settings correctly.

DIVA Components

The DIVA Core 9 installer installs the following Windows Services:

- DIVA Connect REST API Adapter
- DIVA Core Analytics
- DIVA Core Backup Service
- DIVA Core DB Agent
- DIVA Core Metadata Service
- DIVA Core Migration Service
- DIVA Core REST API Data Service
- DIVA Core REST API Discovery
- DIVA Core REST API Gateway
- DIVA Core Rosetta
- DIVArchive Actor
- DIVArchive Drop Folder Manager (DFM)
- DIVArchive Hole Punch Server
- DIVArchive Manager
- DIVArchive Robot Manager
- DIVArchive VACP
- MongoDB Set 0
- RabbitMQ

Postgres installer is not bundled and must be installed separately. See *Postgres Installation and Configuration*.

ElasticSearch installer is not bundled and must be installed separately. See *Elasticsearch Installation and Configuration*.

Note: Starting from DIVA 9.0:
Telestream has replaced Control GUI with DIVA Web App.
Telestream has replaced Configuration Utility with DIVA Web App.
Telestream has removed OracleClient and Database schema files.
DB schema files are re-factored into DBAgent/Packages folder.
DBAgent Service User and Password are optional.

Installing and Configuring DIVA

To install DIVA, do the following:

1. Open the Command line.
2. Run the DIVA installer, for example, `DIVACore_x.x.x.exe`.

   The DIVA installer opens the *Choose Install Location* dialog.
3. Browse to the desired folder location for the binaries, and select it.

   The default and recommended value is `C:\DIVA`. This location is referred to as `%DIVA_HOME%`.

   All binaries for DIVA modules are installed in this directory. However, you can configure and start, as windows services, only the binaries needed on a given server.

   See *Software Component Distribution*.
4. Click *Next*.

   The DIVA installer opens the *Install or Upgrade* dialog.
5. Select the *Install* check box for an initial installation.
6. Click *Next*.

   The DIVA installer opens the *Metadata Database (MDDB) Settings* dialog.
7. Select locations for *MDDB Data Folder* and *MDDB Port*

   Mongodb stores its data in the *MDDB Data Folder*. The default data folder is `H:\MDDBData`. If the `H:` drive doesn't exist, the default data folder is `C:\MDDBData`.

   MDDB Port: by default it is 27017 (Note: if you change this port, DIVA services that use this port still default to 27017; so you must change those service configurations too.)
8. Click *Next*.

   The DIVA installer opens the *Choose Components* dialog.

9. Do one of the following:
   - To install DIVA on the Main Manager or on a Backup Manager server, check the boxes for the components you want to install. Include *Metadata Database* and *Notification Service*.
   - To install an actor service don't select *Metadata Database* or *Notification Service*.

   See also *Notification Service Module*.

Note: Checking the box for *DIVA Demo* automatically checks all the components required for the DIVA Demo.
See also DIVA Demo (Optional) and *Notification Service Module*.

10. Click *Next*.

    The DIVA installer opens the *Notification Service Settings* dialog.

11. Click *Next*.

    The DIVA installer opens the *Install DIVA DB User/Schema* dialog.

Note: This option requires postgres DB to be installed and setup properly. The DIVA installer installs the DIVA DB schema and user to that database.

12. Fill the fields as desired.

    The following table provides field descriptions.

Field	Description
DB User	The user that's created in postgres for the DIVA Core database. Legacy value = diva
DB Password	The corresponding user password. Postgres user password must not contain any URL-like characters. This breaks the connection string such that the `pg_basebackup.exe` doesn't recognize the port. The password is passed to the connection string in this format: `$"postgres://{postgres.User}:{postgres.Password}@{hostname}:{port}";`
DB Master Password	The master user (postgres) password when you install Postgres DB. It must be the same as the one provided during Postgres DB engine installation.
DB Name	The DIVA Core database schema's name that is created in Postgres. Telestream recommends using the 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 an unique DB Name and user. Legacy value = diva

Field	Description
License File Path	The Location and name of the DIVA Core 9 license. Note: DIVA Core 8.X licenses are not compatible with DIVA Core 9.X installer.
DB Agent BasePath	This is the folder where DIVA DB Agent will store DB backups and redo logs.
DBA Service User	The user name to run DBAgent service. If DBAgent needs to access network shares to copy backup files to and from, and ensure the user has the appropriate rights. If the User and Password fields are empty strings, the DIVA installer proceeds using LocalSystem. If either field is filled in, it validates the credentials and use the specified account for DBAgent. When credential validation fails, this pops up an error message. NOTE: DBAgent Service User and Password are optional.
DBA Service Pass	The password for the user to run DBAgent service. Refer to details for DBA Service User.

13. Click *Next*.

    If you selected the DIVA Appliance component, the DIVA installer opens the *Setup an Appliance DIVA System* dialog.

    See *DIVA Appliance (Optional)*.

16. (Optional) In the DIVA Demo dialog, enter field values as desired. If you selected the DIVA Demo component, the DIVA installer opens the DIVA Demo dialog.

    See *DIVA Appliance (Optional)*.

17. Click *Install*.

    The DIVA installer extracts the binaries, configuration files, log files and any required dependencies to `%DIVA_HOME%`, and displays a message indicating a successful installation.

    The DIVA installer opens the *Installation Complete* dialog.

18. Click *Close*.

    There's no need to start the DIVA Web App at this stage.

19. Install the DIVA Database user when running the DIVA installer. In Windows, this is a check box.

20. While installing the database user, make sure to import the license.

    The Manager Service won't start until the license is imported using the DIVA Web App after installation.

21. Configure the basic, essential, Manager settings to get the Manager Service operational.

22. Configure the DIVA REST API.

23. Start the DIVA Web App and log in under the `sysadmin` account.
24. Create a DIVA Web App user.

    This is done so the `sysadmin` account isn't being used, in day to day operations, 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` can't manage users.

    c. To save the new user, click *Save*.

    The user now appears in the *Users* list.
25. Log out of the DIVA Web App.
26. Log back in with the user account just created (not the `sysadmin` account).
27. Configure the Network Servers, and so on, until you have DIVA fully installed and configured.

    See the operating-system-specific sections for detailed instructions.

Note: Use the DIVA Web App to select most of the DIVA configuration settings and options.
For intensive archive operations, use a broadcast-automation or media-asset-management (MAM) system, rather than the DIVA Web App.

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 (typically `diva`)
- **DB Password:** Schema User's password
- **DB Master Password:** Password of the postgres system account user, defined when you install Postgres
- **DB Name:** Name of the schema. Unlike Oracle, we recommend using the same value as the schema user. If you want to install more than one schema on the same Postgres DB, each schema must have an unique DB Name and user.
- **License File Path:** Path to the DIVA license file
- **DB Agent Base Path:** This is the folder where DIVA stores DB Backups.
- **DBA Service User:** The user name to run DBAgent service. If left empty, DBAgent service is installed using Local System.
- **DBA Service Pass:** The password for the user to run DBAgent service

  If the DB Agent File Path doesn't exist, DIVA displays the following error message: *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 won't 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 the storage simulator is installed. This includes DIVA managed and unmanaged storages, disk arrays, one simulated tape library, and so on.

The installation logs are available in:

```
%DIVA_HOME%\Program\log\diva_upgrade\diva_upgrade.trace.log
```

Manually Creating the Database User and Schema

1. From the command line, navigate to the `%DIVA_HOME%/Program/Database/Diva/Install` directory.
2. Execute `create_diva_user.bat` (Windows), which creates the given DIVA database user and its associated tables.

   Usage:

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

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

Parameter	Option	Definition
`syspasswd`		Password of the Postgres sys account.
`username`		Username to create
`userpasswd`		Associated user password
`postgres_connection`		Postgres service name or connection string (such as IP_ADDRESS:PORT/ POSTGRES_SERVICE_NAME).
`DIVA|SYS`		Use either TSCM or SYS to reset the respective password in the password file.
`new_password`		New password
`current_password`		If there is no current database password, then enter the new password for this parameter.
	`-useronly`	Only creates the database user and no database objects.

Parameter	Option	Definition
	`-tablesonly`	Only creates the database objects for the given user.
	`-custom_tablespaces`	• Use of custom tablespaces -`tables_tablespace`: tablespace for tables -`indexes_tablespace`: tablespaces for indexes -`temp_tablespace`: database temp tablespace
	`-postgrespwd`	Option to reset/generate password file.

Configuration While Manager is Running

You can complete most changes to the configuration while the Manager is running. There are a small number of configuration changes that require a restart of the Manager to become effective.

The DIVA Web App dynamically updates DIVA with changes you make to the Jobs, Job Properties, and Migration pages. Click the Refresh button on other pages to ensure that updates are sent to DIVA.

You can run the DIVA Web App through a web browser (Telestream recommends Chrome) on any computer that has TCP/IP connectivity to the database, and connectivity to the DIVA REST API on port 8765. In some cases, a network firewall between the two can prevent a connection.

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.

Upgrading DIVA

Use this procedure only to upgrade DIVA from version 9.0 or later, not from earlier versions.

Caution: If you want to upgrade to DIVA 9.X from an earlier version of DIVA, contact Telestream Sales.

1. Open the Command line.
2. Run the DIVA installer, for example, `DIVACore_x.x.x.exe`.

   The DIVA installer opens the *Install or Upgrade* dialog.

   To upgrade DIVA from a previous version, select *Upgrade*.

3. Open the *DIVACore Setup* dialog.
4. In the *Destination Folder* field, browse to or enter the path to the destination folder. Click *Next*.
5. From the list in the *Select components to install field*, choose the options to install, as desired.
6. Click *Next*.

   DIVA displays dialogs for the options selected.

See *Database Schema (Optional)*.

Post-Installation Configuration

This chapter describes DIVA configuration after installation.

Topics

- Post-Installation Configuration Overview
- Metadata Database (MDS) Module
- Actor Module
- Analytics Service Module
- Backup Service (BKS) Module
- Complex Objects
- Configuring REST API Gateway
- Manager Module
- Drop Folder Monitor (DFM)
- Migration Service Module (MGS) (Optional)
- Notification Service Module
- Proxy Service Module (Optional)
- Workflow Service Module (WFS) (Optional)
- VACP Converter (Optional)
- Ports for DIVA stack services and Third-Party DBs

Post-Installation Configuration Overview

Configuring DIVA modules usually consists of the following steps:

- Identifying whether the module should or shouldn't be installed on a given server
  See also *Software Component Distribution*.
- Locating the configuration file for that module

- Editing and configuring the parameters in this file that are required to ensure correct connectivity to third-party components; for example the Postgres database, the Mongo database, the Elasticsearch database
- Install and configure the parameters in this file that are required to ensure correct connectivity to other modules within DIVA
- Install the Windows DIVA module service
- Start the Windows DIVA module service
- Check the logs of the DIVA module service

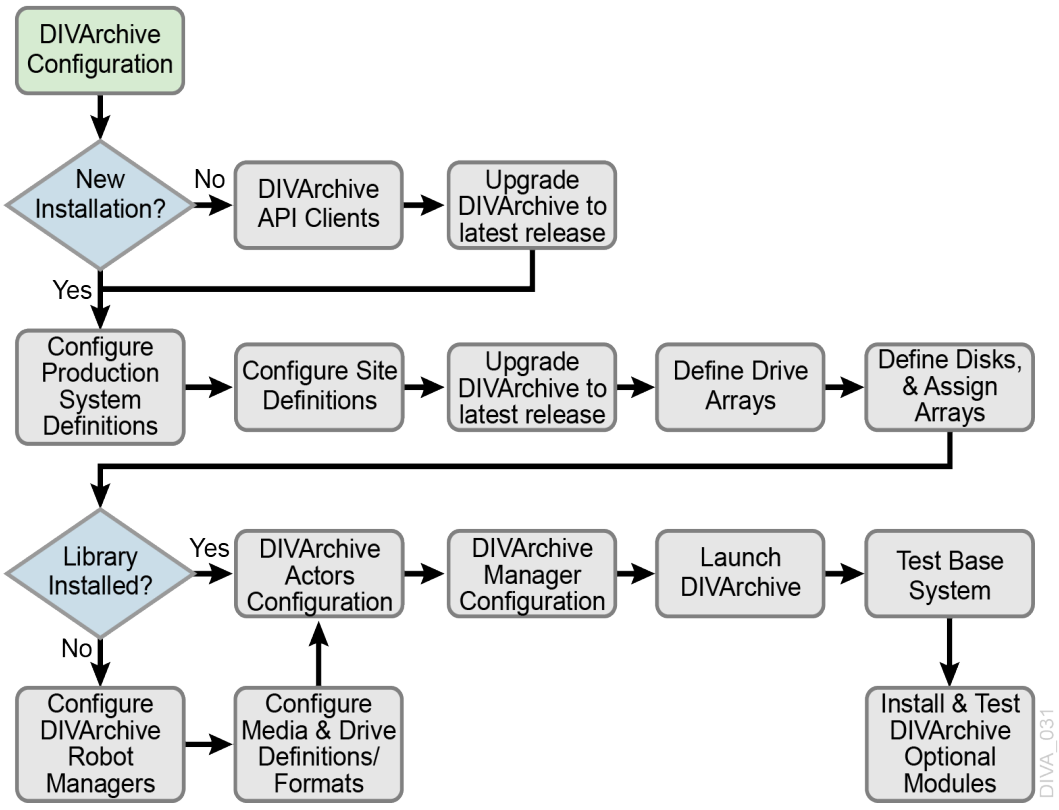
There are many interrelated components in a DIVA System. The following figure shows the basic configuration workflow.

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 Postgres, the Metadata Database, MongoDB, and the Elasticsearch Database.

> For more information on how to do such backups, see Backup Service (BKS) Module.

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



Module Configuration Files

Note: Except when specifically mentioned, Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing 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 filename extension. Some DIVA modules use an XML- or JSON- based file rather than a text file for their configuration. Those cases are noted where applicable.

DIVA centralizes all module configuration files in `%DIVA_HOME%\Program\conf`. The configuration files are typically updated with additional or changed settings in newer releases of the software. A new or patch release of DIVA has the new releases of the `CONF` files appended with an `INI` extension. For example, the Manager Configuration file is named `manager.conf.ini`. Remove the `INI` extension after the installation is complete and the new configuration file updated.

You can open and edit each configuration file with any plain-text editor, for example, Windows Notepad or Notepad++. Most configuration files contain descriptions of the supported variables.

Importing the DIVA License

DIVA requires a license. The Manager doesn't start without a valid license in the database.

If you obtain the license before installing DIVA for the first time, the DIVA installer can import the license. If you have a licensed copy of DIVA installed before you install a new version of DIVA, you can import the license from the earlier version via the *Import License* page in the DIVA Web App.

The license enables the Manager, which is necessary for enabling many of the features of DIVA. Also, the license enables the list of features and options specific to your DIVA system.

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.

Note: DIVA Web App now updates the system health as follows: 30 days before the license expires, DIVA Web App displays license health as Warning (yellow). One week before the license expires, DIVA Web App displays license health as Error (red).

Metadata Database (MDS) Module

This section describes the manual installation and configuration of the Metadata Database.

Note: If you used the DIVA Installer and selected the Metadata Database option, the steps described in this section have already been executed on your server.

Prerequisites

- RabbitMQ service, installed, running, and accessible
- MongoDB service installed, running, and accessible
- Elasticsearch service installed, running, and accessible
- DIVA Core Data Service installed, running, an accessible, for authenticating API commands.

Installing the Metadata Database

To install the service, do the following:

1. Run `cmd.exe` as administrator.
2. Change directory to the `%DIVA_HOME%\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 `M:\MDDBData`. If `M:` drive doesn't exist, the default is `C:\MDDBData`.
- **MDDB Port:** the default is 27017.

Note: If this port is changed, DIVA services that use this port to connect to MDDB still default to 27017; so you must 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. This shows the Swagger documentation page for the Metadata Service.

See also *MongoDB Installation and Configuration*.

Metadata Database Configuration

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure metadata, browse to *Configuration* > *Services* > *Metadata*.

Technical Support highly recommends that you store the Metadata Database files on a RAID disk array. The Metadata Database shouldn't be installed 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.

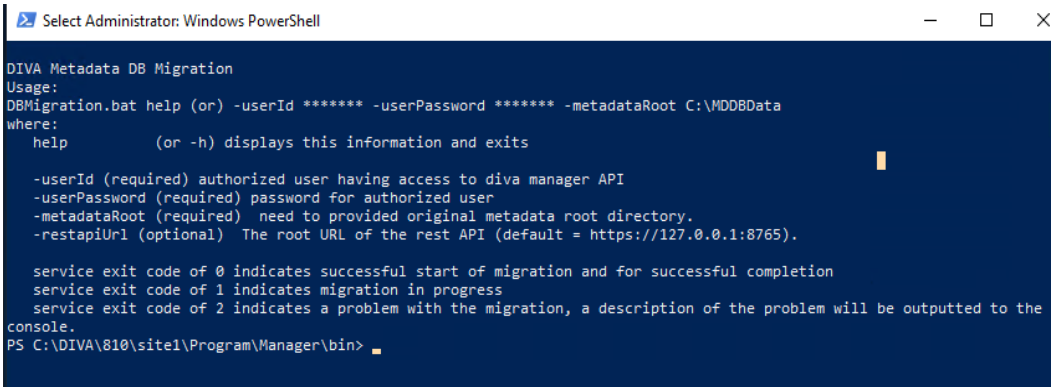
MDDB (Flat File Metadata Database) to MDS (Metadata Service) Migration

Note: This step is needed if you are upgrading from a DIVA 8.x version to DIVA 9.x, and if the data from MDDB Flat File was not already imported into MongoDB.

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.

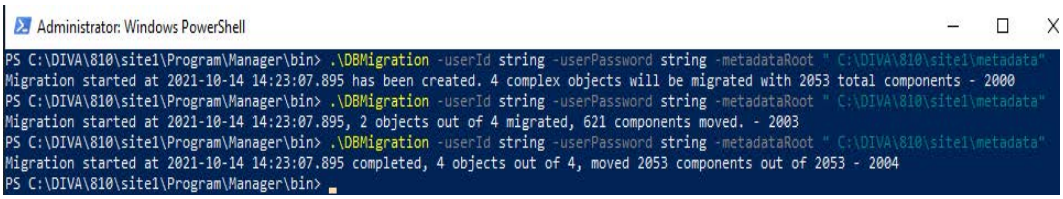
If you enter `DBMigrate.bat` without arguments, or with the `-h` parameter, you see the following:



For example:

```
DBMigration -userId [REST API user name] -userPassword [password]
-metadataRoot "%DIVA_HOME%\metadata"
```

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



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
"%DIVA_HOME%\810\site1\metadata"

echo ERRORLEVEL %ERRORLEVEL%
```

Troubleshooting the Metadata Database

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.

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.

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. Stop the DIVA Metadata Service, and MongoDB Service. Edit the `C:\Program Files\MongoDB\Server\5.0\bin\ mongod0.cfg` configuration file and check that the path variables are pointing to the correct locations.
4. Start the MongoDB and DIVA Backup Service.
5. Using BKS, restore a valid backup of the Metadata Database to the production location.
6. Confirm that no Object Metadata and no Complex Objects have been 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.

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. Using BKS, restore a valid backup of the Metadata Database to the production location.

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. Using BKS, restore a valid backup of the Metadata Database to the production location.

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.

Actor Module

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.

Prerequisites

- None

Configuring Actors

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

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure Actors, in the DIVA Web App, do the following:

1. Browse to *Configuration* > *Resources* > *System Settings* > *Actors*.

   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.
2. Find Name and Port settings in the configuration file.

   All other Actor settings are located in the DIVA Web App under Actor Settings, Advanced and Partial Restore Settings pages of the Actor area of the System page.
3. Make sure the Actors are running and connected to the Manager.
4. To notify the Manager of any changes to the configuration, click

   Notify > *Notify Manager*.

   Manager sends a notification to each Actor. The notification contains the new Actor configuration.

Note: To receive the notifications, the Actors must be running and connected to the Manager.

5. To create and configure an Actor, click + on the Actor Settings area, or, to edit an Actor, double-click the Actor you want to edit.

   The DIVA Web App opens the settings page.
6. Configure the Actor settings on the *Actor Settings Entry* page.

See *Actor Definition and Declaration*.

Installing the Actor

To install an Actor, do the following:

1. Set the Actor name and port in the Actor configuration file.
2. Install the Actor service.

   See *Actor Executables*.
3. In the DIVA Web App, define the Actor in the system configuration.
4. Define Actor-disk, and Actor-drive associations as needed.
5. Notify the Manager.

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.

Additional Actor Batch Files

`%DIVA_HOME%\Program\Actor\bin\scandrive.bat` 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. This 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.

Note: To receive the notifications, the Actors must be running and connected to the Manager.

For additional commands, see *Actor Executables*.

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.

Note: Descriptions of the parameters, parameter types, and default settings are contained in the `actor.conf` file. You can read the contents of this file in a web browser.

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 %DIVA_HOME%\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 %DIVA_HOME%\Program\conf\actor\actor2.conf
```

For details on additional commands, see *Actor Executables*.

Actor Launch

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 preforming 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.

Job Options

The partial restore parameters can be overridden at the Job level by adding these job options to the Partial File Restore job request.

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: • IGNORE: Partial Files Restore will ignore this field. The value found in the original clip will remain unchanged in the restored clip. • RESET: Partial File Restore will reset the value of this field to zero. • UPDATE: Partial File Restore will increment this value using the frame count from which the partially restored file begins.	RESET

Parameter	Value or Type	Job Option	Description	Default
AVI Ignore Start Timecode	N (disabled) Y (enabled)	-PfrAviIgnoreStartTimecode	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)	-PfrEvsMxfIgnStartTimecode	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: • The Objects start time codes are ignored. TCIN and TCOUT must be relative to 00:00:00:00. • SOM is derived from the first field number of the MAP packet (default). • SOM is derived from the time code at Mark In from the UMF packet.	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	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. Set this parameter to `%DIVA_HOME%\Program\Actor\bin\mxf_file.bin`. Where `%DIVA_HOME%` is the root path of your DIVA installation for the Actor.	
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=RunInProcessor.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 TCOUT (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)	-PfrMxfUpdateTctrackOrgin	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)	-PfrSeaIgnoreStartTimecode	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 TCOUT 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)	-PfrTsIgnoreStartTimecode	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 TCOUT as if it starts from 00:00:00:00.	N
MPEG2 Program Stream Ignore Start Timecode	N (disabled) Y (enabled)	-PfrPSIgnoreStartTimecode	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 TCOUT 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.

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.

Analytics Service Module

To publish analytics data, a DIVA micro-service sends the data to a RabbitMQ queue. The Analytics Service monitors the queue, parses the messages and stores them in an Elasticsearch index. The Analytics Service provides endpoints for querying the data in Elasticsearch. You can view much of this data via the Analytics charts in the DIVA Web App. Since the data are kept in the Elasticsearch, you can also display the data in Kibana custom charts.

Prerequisites

- RabbitMQ service, installed, running, and accessible.
- Elasticsearch service installed, running, and accessible.
- To authenticate API commands: the DIVA Core Data Service installed, running, and accessible.
- To import legacy data: Postgres installed, running, and accessible.

Note: Reading the legacy analytics events out of DIVA into the Elasticsearch depository is done once.

Installing, Uninstalling, and Operating the Analytics Service on Windows

1. Open the command line.
2. For descriptions of relevant parameters and options, enter `analytics.bat -h, or analytics.bat help.`
3. Run `analytics.bat [parameter] [options].`

Configuring the Analytics App

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure Analytics, in the DIVA Web App, browse to *Configuration* > *Services* > *Analytics*.

For information about using the DIVA Analytics charts, see the topic, *Analytics Charts*, in the *DIVA User Guide*.

Backup Service (BKS) Module

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.
NOTE: DBAgent Service User and Password are optional.

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`.

Caution: You must use the BKS as soon as a Metadata Database is configured on the DIVA system. This is mandatory for DIVA versions 9.2 and later.

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 are incrementally replicated by the BKS to remote backup servers.

Configuring BKS

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure BKS, do the following:

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

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 DIVA 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.

Note: DBAgent Service User and Password are optional.

Backup Initiator

A command-line backup `initiator.exe` is included in the `DIVA\Program\BackupService\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 exists, or is deleted, and will contain records for both regular archives and gold archives.

Restore Workflow

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

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

```
<Location Path>\Restore\FromArchive\…
```

3. If not, BKS checks the archive ledger to determine if any archive on the list can be restored to the above location for the job to proceed.

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

Manual Restoration

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

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

BKS Recommended Practices

The following are recommended practices for BKS:

- BKS must be installed on the same server as the Main Manager and DIVA database.
- At least two backup systems are always required to store backups. Actor computers can serve dual purposes and be used as both backup computers and Actor computers.
- Postgres incremental backups should be performed every 15 minutes.
- Metadata Database 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, the Metadata Database, and Elasticsearch database must be stored on RAID disk arrays.
- 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.You must install the component on the same server as the Manager and the 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

To install BKS and DBAgent, do the following:

1. Open the Command line.
2. Run `backup_service.bat [parameter] [options]`, with one of the following parameters:

Parameter	Option	Definition
`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.

You can add any of the options described in the following table:

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

3. *Run* `db_agent.bat [parameter] [options]`, *with* one of the following parameters:

Parameter	Option	Description
`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.

Parameter	Option	Description
	`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.

You can add any of the options described in the following table.

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 DIVA Web App 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.

DIVA API Settings

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

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

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
```

Note: DBAgent Service User and Password are optional.

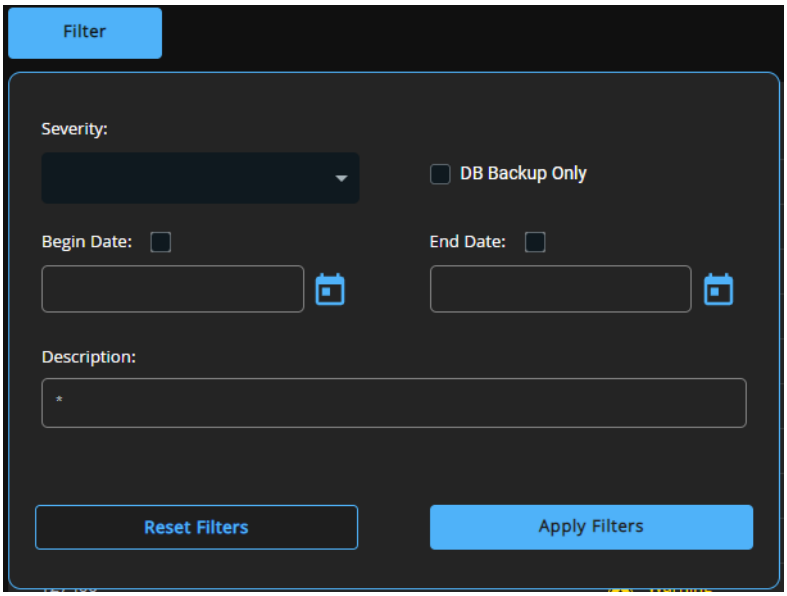
Backup Service Logged Events

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

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

Events in the *Troubleshooting* > *Logged Events* panel may be filtered using the filter check boxes and fields to display specific types of entries being viewed. The following

figure shows that the screen can been filtered to show only Warning, Error, Critical, or Information by using the pull-down menu and clicking the Filter button.



The following table describes the different warning and error notifications.

Message Type	Code	User Message	Posted to Manager
SUCCESS	0	Completed successfully	Yes, informational
RUN	1	Running	No, internal only
ERROR	2	Failure: Refer to the backup service logs for more details.	Yes, error

Complex Objects

By default, Objects archived with more than 1,000 files are considered Complex Objects. Set this value with the `DIVAMANAGER_COMPLEX_OBJECT_THRESHOLD` parameter in the `manager.conf` file. 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.

Prerequisites

- IP address of the Manager server is known.

Configuring REST API Gateway

To configure and start the REST API related services, so that the DIVA Web App becomes accessible, do the following:

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 as `sysadmin` with the default password.

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`.

Manager Module

The Manager is the main component in a DIVA system. The Manager controls all archive operations. 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. You can turn the Manager on or off through the Windows Services utility.

Prerequisites

- RabbitMQ service, installed, running, and accessible.
- Postgres installed, running, and accessible.
- A valid DIVA license is available.

Manager Configuration

The static configuration file for DIVA is `diva.conf`. You can leave most of the settings in `manager.conf` at their default values. You can monitor the operations of DIVA through the DIVA Web App.

Manager Configuration

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

Appending the -conf (or -f) option after one of the above commands specifies a specific configuration file to load settings from. For example:

```
%DIVA_HOME%\Program\manager\bin\manager.bat start -conf con-
fig_file_name.conf
```

`Manager.conf.ini` is the static configuration file for the Manager. You must remove the `INI` extension for it to be recognized by the Manager.

Note: You can find up-to-date details for configuration parameters on the Module Confluence page.

Note: Descriptions of the parameters, parameter types, and default settings are contained in the `manager.conf.ini` file. You can read the contents of this file in a web browser.

The `manager.conf` configuration file contains the following groups of settings;

- DIVA Manager Basic Settings
- DIVA Manager Logging
- DIVA REST API Options
- DIVA Service Options

To configure the general settings for the Manager, in the DIVA Web App, browse to *Configuration* > *Resources* > *General Settings*.

Caution: Don't modify any of the values in the DIVA Service Options section without guidance from Telestream Technical Support. This manual doesn't cover DIVA Service Options settings.

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.

You can make most of the customizations in the configuration file effective immediately using the restart command-line switch.

Caution: Restarting the Manager can disrupt a live Network. Follow the proper procedures for stopping and restarting the Manager.

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 DIVA Manager Basic Settings, 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.

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

Tape Import Batch File

`ImportTapes.bat` imports tapes into a Tape Group.

Basic Settings

To start successfully, the Manager requires correct parameter values for all the basic settings except `SERVICE_NAME`, which is optional. These settings define how other DIVA software components and DIVA REST 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.

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. You can view the definitions for the options in the `manager.conf.ini` file.

Settings for Logging

You can view the settings for logging in the `manager.conf.ini` file.

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 100 with zero being the lowest priority and 100 being the highest. The job priority is typically specified when you submit the job (either from the DIVA Web App or the DIVA REST 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.

Installing and Removing the Manager Service

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

The `manager.bat` file enables running DIVA as a service or using a console window.

Run `manager.bat` using the following command and parameters:

```
%DIVA_HOME%\Program\manager\bin\manager.bat [parameter] [options]
```

The following table describes each of the `manager.bat` parameters.

Parameter	Description
`install` (`-i`)	Installs DIVA as a system service.
`uninstall` (`-u`)	Removes the DIVA service.
`start` `Example: manager.bat start`	Starts DIVA.

Parameter	Description
`stop` `Example: manager.bat stop`	Stops DIVA immediately if it is running.
`graceful_shutdown` `Example: manager.bat graceful_shutdown`	Stops DIVA after all currently-running jobs have terminated. Ignores any new jobs.
`restart` `Example: manager.bat restart`	Stops and then starts DIVA.
`reload` `Example: manager.bat reload`	Requests that the current service reloads its settings.
`status` `Example: manager.bat status`	Determines whether the service is running and displays the status.
`dump` `Example: manager.bat 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.

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 parameters after the service is installed:

Parameter	Option	Description
`manager start`		This starts the Manager service (if stopped).
`manager stop`		This stops the Manager service (if running).
`manager shutdown`		This finishes currently jobs and stops accepting new jobs, then it stops the Manager service (if running).
`manager restart`		This stops and then starts the Manager service.
`manager reload`		Some changes in the Manager configuration files take effect after reloading the Manager. This parameter reloads the `manager.conf`, `managerpriority.conf`, and `restore_translations.conf` files from the default path `%DIVA_HOME%\Program\conf\manager`.
`manager reload`	`-conf [configuration file]`	Use this parameter and option to reload the Manager using a different configuration file.
`manager status`		This displays the current status of the Manager service (running or not running).

Parameter	Option	Description
`manager dump`		This requests a system dump from the Manager service.
`manager version` (or `manager -v`)		This displays the Manager service release information and then exits.
`manager help` `(or manager -h)`		This displays all command-line parameters 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.

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. Log in as the `sysadmin` user.
3. Check that you are not receiving Manager connection-error notifications in the upper-right corner of the DIVA Web App.

Confirming Manager to Actors Connectivity

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. To confirm Manager to Actors connectivity, do the following:

1. In the DIVA Web App, browse to *Resource Management* > *Actors*.

   A green led displayed next to each Actor indicates a successful connection between that Actor and the main Manager.
2. 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. In the DIVA Web App, browse to *Resource Management* > *Tapes*.
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. To view the Manager Current Jobs, browse to *Content Management* > *Jobs*.
5. To see whether an error was encountered during job execution, double-click the *Eject Tape* job entry.

Rerouting Destinations (Optional)

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. It can simplify production workflows. For example, you can 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.

Drop Folder Monitor (DFM)

Note: Starting in DIVA 9.4, Drop Folder Monitor replaces the legacy Drop Folder Manager. The DIVA Drop Folder Monitor (DFM) allows users and third-party applications to submit content for archiving by copying related files to a folder, an FTP server, or a CIFS share.

Drop Folder Monitor (DFM) is a DIVA service executed by an actor.

Migration Service Module (MGS) (Optional)

If there is no need to process migration tasks, you don't need to install this module.

Telestream recommends installing the Migration service (MGS) on the same server as the one running the Main Manager and DIVA database. Technically, you can install the Migration service on any server of the DIVA system.

The Migration service module creates migration jobs for DIVA, and schedules them for processing.

The Migration service has a dedicated database called `MGS`.

The Migrate Service configuration file is a YML file. There are no specific configuration parameters to change in that file.

The 3 components that provide migration of tapes are:

- Migration Service
- Manager
- DIVA Web App

Prerequisites

- Postgres service installed, running, and accessible

Installing, Uninstalling, and Operating MGS on Windows

1. Open the Command line.
2. Run `migration_service.bat [parameter] [options]`.

`migration_service.bat` describes the commands and options as follows:

Parameter	Description
`install (or -i)`	Installs the module as a system service.
`uninstall (or -u)`	Removes the executable as a system service.
`start`	Starts the module.
`stop`	Stops the module if it is currently running.
`help (or -h)`	Displays this information and exits.

Configuring the Migration Service

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure the Migration service, in the DIVA Web App, browse to *Migrations*.

Note: The DIVA Web App displays the *Migration* tab only if the Migration Tool is enabled in the DIVA license.

Migration Service API Documentation

The Migration service API is fully documented in Swagger (v3) along with each DTO for consumption.

See https://127.0.0.1:8765/webjars/swagger-ui/index.html?urls.primaryName=migration.

MGS License

MGS retrieves an active license from the data service on startup. If the feature isn't enabled in the license, or if the data service is not running when MGS is started, all MGS endpoints respond with *HTTP 403*.

Once an active license is successfully read from the data service, MGS enables all endpoints for 24 hours. then, MGS reads the license from the data service again.

MGS Log File

To ease tracing progress of TAPE Migration in Operation as well as troubleshooting, Manager logs all events and tasks related to migration of a tape via `CopyTape` to a dedicated file:

```
%DIVA_HOME%\Program\log\manager\diva_manager\manager.copy-tape-trace.log
```

```
MGS logs are located here:
%DIVA_HOME%\Program\log\migration_service
```

Dedicated mgs_diva Postgres Database

MGS creates and upgrades its own DB schema on service startup via DBAgent service. MGS accesses DBAgent via the RestAPI gateway using the user and password configured in the MGS `application.yml` file.

MGS DB schema parameters are configured in the MGS `application.yml` file.

- `DBName` is parsed from the JDBC url connection string: `datasource: {url: 'jdbc:postgresql://localhost:5432/mgs_diva'`
- `DBUserName` is configured as `username parameter: username: mgs_diva`
- `DBUserPassword` is ignored. If configured in application.yml, `DBUserPassword` won't be used. `DBUserPassword` comes from the scrambled password file created as `pkpwd`. This file must be created before the DBAgent service will run.

Notification Service Module

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

Note: You must install one Notification Service per DIVA system. Telestream recommends that you install the Notification Service on the Main Manager.

Prerequisites

- DIVA installer was run and there is a %DIVA_HOME% folder.

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.

`Install_rabbitmq.bat` and `uninstall_rabbitmq.bat` aren't meant to be used by regular users. Support and admin users may edit these files to understand how RabbitMQ was installed or uninstalled.

The install_rabbitmq.bat batch file requires Erlang installer to be placed inside the `%DIVA_HOME%` folder; this script does not work as delivered. The DIVA installer also doesn't 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 %DIVA_HOME%`.

Note: `Uninstall_rabbitmq.bat` also uninstalls Erlang runtime. After it is uninstalled, you can't reinstall it by running `install_rabbitmq.bat` unless you have a copy of Erlang installer in the `%DIVA_HOME%` 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. The DIVA installer creates a default admin user (username wsuser and default password): 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.

Proxy Service Module (Optional)

If there are no proxies needed on the DIVA platform, installing this module isn't necessary.

Running on Windows, the Proxy Service Module generates and manages additional metadata files. These include proxy files, thumbnails, and technical metadata files that you can extract from a transcoder engine.

The Manager executes `TranscodeArchive` requests to generate the desired proxy, thumbnails, and technical metadata files. The Manager can store these metadata on a proxy array. A proxy array is a disk array dedicated to storing proxy objects and making the files accessible via HTTP.

The Proxy Service Module detects whether objects from DIVA require proxies, based on the Proxy Service configuration. The Proxy Service Module generates proxy objects in the background, and detects when an object requires proxy or metadata generation. The Proxy Service Module analyzes the technical metadata and communicates them to the metadata service so that they are searchable. You can filter objects requiring proxy or metadata generation in various ways, for example by category name, object name, or object age.

The Proxy Service Module sends objects needing proxies to Vantage, and Vantage creates the proxies. Vantage then sends these proxies, which persist in proxy tables, to MDS proxies metadata.

The Proxy Service Module can run in the background automatically, or it can run on a schedule.

The DIVA Web App communicates with the Proxy Service Module through the DIVA REST API.

Note: Telestream recommends configuring modules, wherever possible, through the DIVA Web App, not by directly editing configuration files.

To configure Proxy Service Module, browse to *Configuration* > *Resources* > *Proxy Storage*.

Prerequisites

- RabbitMQ service, installed, running, and accessible.
- DIVA license with Metadata feature.

Installing, Uninstalling, and Running the Proxy Service Module on Windows

To install the Proxy Service Module on Windows, do the following:

1. Open the Command line.

2. Run `proxy.bat [parameter] [options]`.

   `Proxy.bat` describes the commands and options as follows:

Parameter	Option	Description
`install (or -i)`		Installs the module as a system service.
	`-log`	Path to log directory. Default: `..\..\log\proxy`
	`-conf`	Path to configuration directory.
	`-httpport`	Port to listen for http connections. Default: 1976
	`-httpsport`	Port to listen for https connections. Default: 1977
	`-certpath`	Path to certificate located on disk.
	`-user`	Username to install the service under. Blank entries are installed as LocalSystem.
	`-pass`	Password for the provided user.
`uninstall (or -u)`		Removes the executable as a system service.
	`start`	Starts the module.
	`stop`	Stops the module if it is currently running.
	`restart`	Stops and then starts the module.
	`status`	Determines whether or not the module is running.
	`version (or -v)`	Displays the module version information, and exits.
	`help (or -h, or -?)`	Displays this information and exits.

Workflow Service Module (WFS) (Optional)

The Workflow Initiator service enables a robust integration between DIVA and Telestream Vantage, and between DIVA and a large variety of encoders.You can define Workflow Engines in the WFS configuration. The configuration file hold the details of how to work with the Vantage API. The micro-service provides a REST API to create, read, update, and delete these configurations. It also provides a REST API to submit tasks to a workflow engine for execution.This monitors the status of executing tasks and allows the status to be retrieved, either via the REST API or through notifications which are posted to RabbitMQ.

The workflow initiator service also enables you to cancel and delete submitted tasks.

To install the Workflow Initiator service run the respective command line interfaces described below.

Prerequisites

- RabbitMQ service, installed, running, and accessible.
- Postgres service installed, running, and accessible.
- To authenticate API commands: the DIVA Core Data Service installed, running, and accessible.

Installing the Workflow Initiator Service

The default installation for DIVA installs the Workflow Initiator service on the primary server.

To install the Workflow Initiator Service on Windows, run `workflow.bat [parameter] [options]` with the parameters and options in the following table:

Parameter	Option	Description
install (or -i)		Installs the module as a system service.
	-log	Path to log directory. Default: ..\..\log\workflow
	-conf	Path to configuration directory. Default: ..\..\conf\workflow
	-httpport	Port to listen for http connections. Default: 2376
	-certpath	Path to certificate located on disk.
	-user	Username to install the service under. Blank entries will be installed as LocalSystem
	-pass	Password for the provided user.
uninstall (or -u)		To remove the executable as a system service
start		Starts the module

Parameter	Option	Description
stop		Stops the module if it is currently running
restart		Stops and then starts the module
status		Determines whether or not the module is running
version (or -v)		Display the module version information and exits
help (or -h, or -?)		Displays this information and exits

Uninstalling the Workflow Initiator Service

To uninstall, the Workflow Initiator Service, run `workflow.bat uninstall`.

Upgrading from DIVA 9.3 to DIVA 9.4

The Workflow Engine Service is introduced in DIVA 9.4. Therefore, when upgrading from DIVA 9.3 to 9.4 and later:

- WFS is installed automatically on the server where the Manager is installed.
- WFS is installed using database settings that come from `manager.conf` of the manager service.
- On a server with no manager, WFS isn't installed by DIVA installer, but can be installed manually.
- Transcoders configured in DIVA 9.3 are migrated to the WFS workflow database as workflow engines.
  - This happens only if WFS is installed on the Manager server sharing the same database user and password as the database used by Manager.
  - If WFS is installed using a database user different from the ones Manager uses, there is no migration of transcoder settings to the WFS.
- When upgrading from DIVA 9.4 to future releases, WFS is upgraded like other regular DIVA services.
  - The DIVA installer copies over the older WFS configuration file, and uses it in the new WFS after upgrade.

WFS defaults to any new setting fields introduced in newer versions. This is the standard behavior for all DIVA micro-services.

The WFS Configuration File

To modify your WFS configuration, don't make changes directly in the `Workflow.settings.json file`. You can make most changes through the DIVA Web App. The Workflow Service configuration file is generated with default settings that allow access to the database and RabbitMQ, assuming they are installed on the same server, with default credentials.

By default the configuration file is location here:
`(Root of DIVA)\Program\conf\analytics\Workflow.settings.json`.

Field descriptions are contained in the `Workflow.settings.json` file itself. You can read the contents of this file in a web browser.To configure WFS using the DIVA Web App, see *Configuring Workflow Service Module (WFS)* in the *DIVA User Guide*.

The WFS Log File

Note: Use the DIVA Web App to select most of the DIVA configuration settings and options.
For intensive archive operations, use a broadcast-automation or media-asset-management (MAM) system, rather than the DIVA Web App.

Log file tracing level is controlled by the `Logging` section in the configuration file. By default, the log file is located here:
`(Root of DIVA)\Program\log\workflow\Workflow.log`.

MTE Transcoder

Use the Telestream MTE Transcoder to generate proxies for AAF source clips. For help installing and configuring MTE on your DIVA Stack, contact Telestream Support.

Workflow Engine Selection

A workflow engine is selected based on two engine properties; the configured workflow task queue size and performance. The configured queue size determines the number of workflow tasks that can be queued by an engine. The performance is an integer rating assigned to the engine. An engine with no tasks is selected before an engine with tasks. If all engines aren't processing any tasks, no preference is given to any engine, so any workflow engine may be selected. If all engines are processing tasks, an engine with a higher performance rating is selected over an engine with a lower performance rating, and an engine with more queue slots available is selected over an engine with less queue slots available. The calculation runs as follows:
<Performance> * 50 + (<Configured Queue Size> - <# tasks in Queue>)
where <Configured Queue Size> = # of task slots.

VACP Converter (Optional)

Video Archive Command Protocol (VACP) is a protocol developed by Harris Automation for interfacing with an archive system. The DIVA REST API is not compatible with VACP. The VACP Converter module converts VACP commands from the attached automation system to DIVA REST API commands.

The VACP Converter requires a successful connection to DIVA. With DIVA running, start the service manually, either through the Windows Services component, or from the command line.

Starting the VACP Converter

To start the VACP Service from the command prompt, do the following:

1. Open a Windows command prompt.
2. To start the VACP Service, enter `net start "VACP Converter"` at the command prompt. The quotation marks are required for services with spaces in their service name.
3. To stop the VACP Service, enter `net stop "VACP Converter"` at the command prompt. The quotation marks are required for services with spaces in their service name.

The `VACPService.exe` file enables you to run the VACP Converter as a service. Execute the file using the following command and parameters:

```
%DIVA_HOME%\Program\VACP\VACPService.exe command [options]
```

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

Parameter	Description
`install (-i)`	Installs the VACP module as a system service.
`uninstall (-u)`	Removes the VACP module service.
`debug (-d)`	Starts the VACP module in console mode.
`version (-v)`	Displays the version information and then exits.
`help (-h)`	Displays help information and then exits.

Ports for DIVA stack services and Third-Party DBs

The following tables list known TCP ports used by DIVA 8.x, DIVA 9.X stack versions, and third-party components.

When a new module or port is added, DIVA specifies the applicable version. These are the default port values. You can change them via each module's configuration files.

Table 1. TCP Ports for DIVA Modules

Port Number	Module Name	Applicable from DIVA Version
1777	Metadata Service - MDS	8.2
1877	Backup Service - BKS	8.2
1878	DBAgent	8.2
1977	SPM	8.3
2077	Proxy	9.2
2177	Analytics	9.3
2277	Rosetta	9.3
2377	WFS	9.4
8000	Manager - MGR	7.x
8043	Migration Service - MGS http	9.2
8044	Migration Service - MGS https	9.2
8199	Rosetta	9.3
8500	RobotManager - RM	7.x
8765	REST API Gateway	8.x
9900	Actor	7.x
11000	Rosetta	9.3
12443	Manager/Data Service	8.X then replaced by port 13443 in 9.x
13443	Manager/Data Service	9.x
17443	DIVA Connect	2.x

Table 2. TCP Ports for Third-Party Tools

Port Number	Module Name	Applicable from DIVA Version
2047	MTE	9.4
5432	Postgres	9.0
8676	Vantage	8.x
8761	Eureka Discovery Service	7.x
9200	Elasticsearch	9.2
9998	Tika	9.2
15674	RabbitMQ	8.2
27017	MongoDB	8.2

Notifications: SNMP and Email

This chapter describes the different notification capabilities available in DIVA.

Topics

- Configuring the SNMP Agent
- Configuring Email Notifications

Configuring the SNMP Agent

The Simple Network Management Protocol (SNMP) Agent, and the Management Information Base (MIB) support third-party status and activity monitoring of DIVA.

The SNMP agent is integrated with the Windows SNMP Service. The Windows SNMP service starts automatically when the server is started.

The SNMP Agent provides DIVA SNMP information to a monitoring application. The monitoring application automatically connects to DIVA when you start DIVA.

To configure the SNMP Service to monitor DIVA, do the following:

1. Make sure Microsoft SNMP Services is installed on the computer where DIVA is installed.
   a. On the server, navigate to *Windows Key* > *Administrative Tools* > *Server DIVA*.
   b. Click *Manage* > *Add Roles and Features*.
   c. On each of the next four views, click *Next*.
   d. Verify the SNMP Services are listed.

      If the SNMP Service is not listed in the services window, use the following procedure to add the service:

   e. On the server, navigate to *Windows Key* > *Administrative Tools* > *Server DIVA*.

f. Click *Manage* > *Add Roles and Features*.

g. When you get to the view showing services that can be installed, select *SNMP Service* and click *Add Feature*.

h. Click *Next* > *Install*.

i. After installation is complete, return to the Windows Services view and click Refresh to refresh the display.

The services list now includes the SNMP Service.

2. Stop the SNMP Service and SNMP Trap Service.
3. Navigate to the SNMP installation folder.

   `%DIVA_HOME%\Program\SNMPAgent\bin`
4. Confirm this folder contains the `DivaApi.dll` file. If not, contact Telestream Support.
5. Enter the correct DIVA connection information in the `config.txt.ini` file.

   Also, set the POLLING_RATE to 60 (to poll for jobs every 60 seconds), and remove the INI from the end of the file name when saving the edited file.
6. Open the appropriate registry file and edit pathname so that it points to the SNMP path being used.

   For example, `%DIVA_HOME%\Program\SNMPAgent\bin\divasnmpagt.dll`.
7. Double-click the registry file that was just edited to install the SNMP registry keys.
8. Start `Regedit` and using the registry information in the registry file, navigate to each registry key and make sure the path in the registry is as displayed in the registry file.
9. Open the SNMP Service properties and edit the following parameters:
   - On the Traps tab, enter *public* in the Community Name field and add the IP address of the computer where traps are viewed (for example, the computer where the MIB browser is installed).
   - On the Security tab, confirm the Send authentication trap and Accept SNMP packets from any host check boxes are selected.
   - In the Accepted community names field, add *public with READ ONLY rights*.
10. Click *Apply*.
11. Start the SNMP service. Do not start the SNMP Trap service.

Starting and Stopping the SNMP Service

To control the SNMP service through the Windows command prompt, do the following):

1. Open a Windows command prompt.
2. Do one of the following:

- To start the SNMP Service, enter *net start* `"SNMP Service"` at the command prompt. The quotation marks are required for services with spaces in their service name.

- To stop the SNMP Service, enter `net stop "SNMP Service"` at the command prompt. The quotation marks are required for services with spaces in their service name.

Configuring Email Notifications

To configure email notifications, the notification frequency, and the time before the first email is sent, do the following:

1. Browse to *Configuration* > *Resources* > *General Settings* > *SMTP Notifications*.
2. To enable email notifications, drag the slider for *Enable Email Notification* to the right.
3. Select the type of database backup notification desired from the *Database Backup Notification* drop-down list.
4. Enter your system values into the fields for *(SMTP) Outgoing Mail Host* and *(SMTP) Outgoing Mail Port*.
5. If your email host requires authentication, drag the slider for *(SMTP) Outgoing Mail Required Authentication* to the right, and enter your system values into the fields *Account Name (Full Email Address)*, *Account Password*, *DIVA System Administrator Email Address*, *Email Subject*, and *Notification Email Recipients (Comma Delimited)*.
6. To save your settings, click *Save All Changes*.

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. Browse 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.

DIVA Configuration with Manager Running

The Manager and other DIVA Modules read their configuration parameters from the configuration files, on startup.

To make configuration changes, use the DIVA Web App, except where otherwise noted. Configuration changes persist in the DIVA database or in the corresponding module configuration files.

To force Manager or SPM modules to read updated configuration parameters, click the Notification button at the top right of the web interface, and select the module to notify.

The DIVA Web App notifies other modules, such as BKS, Proxies, and MDS, of the updated configuration parameters as soon as you save the configuration changes.

This chapter describes the changes to the DIVA configuration that become effective while the Manager is running, those changes that require a software component, and those changes which require you to restart the Manager.

Topics

- Manager Restart Versus Manager Configuration Reload and Notify
- Updates in the Manager Configuration
- Updates in the DIVA Web App System Page
- Updates in the DIVA Web App Robots Page
- Updates in the DIVA Web App Disks Page
- Updates in the DIVA Web App Drives Page
- Updates in the DIVA Web App Sets, Tape Groups & Media Mapping Page
- Updates in the DIVA Web App Analytics App Page
- Updates in the DIVA Web App Storage Plans Page
- Updates in the DIVA Web App Slots Page

Manager Restart Versus Manager Configuration Reload and Notify

The are operational differences when running the Manager `restart`, `reload`, or `notify` commands.

When running Manager `restart`:

- All ongoing operations and jobs processing in DIVA are aborted.
- Remote access to DIVA from the DIVA-Web-App-connected end users are degraded until the Manager is back online.
- Remote access to DIVA from third-party applications using the DIVA APIs, particularly the DIVA REST API, are degraded until the Manager is back online.

When reloading a Manager configuration, or when running Manager `notify` via the DIVA Web App:

- Queued jobs are paused until the new configuration changes are applied.
- Remote access to DIVA from the DIVA-Web-App-connected end users is fully operational.
- Remote access to DIVA from third-party applications using the DIVA APIs, particularly the DIVA REST API, is fully operational. Incoming job requests are queued until the new configuration changes are applied.

Updates in the Manager Configuration

If a parameter in the `manager.conf` file is changed, the following list identifies the requirements for the change to take effect.

Use the Manager `restart` command for these parameter changes to take effect:

- SERVICE_NAME (also effective after reinstall)
- DIVAMANAGER_NAME
- DIVAMANAGER_SECURE_PORT
- DIVAMANAGER_DBHOST
- DIVAMANAGER_DBPORT
- DIVAMANAGER_DBSID
- DIVAMANAGER_DBUSER
- DIVAMANAGER_MAX_CONNECTIONS
- DIVAMANAGER_TYPICAL_VIRTUALOBJECT_SIZE
- DIVAMANAGER_CAPACITY_LOW_WATER_MARK
- DIVAMANAGER_STOP_IMMEDIATELY_FOR_REPACK
- DIVAMANAGER_TIME_TO_WAIT_FOR_GRACEFUL_SHUTDOWN

- DIVAMANAGER_DISMOUNT_AFTER
- DIVAMANAGER_UPDATE_PRIORITIES_PERIOD
- DIVAMANAGER_PING_INTERVAL
- DIVAMANAGER_ETC_FEATURE
- DIVAMANAGER_ETC_CONFIDENCE_LEVEL

See *Manager Service Management*.

Use the manager reload command, as mentioned in the `manager.conf.ini` file, for these parameter changes to take effect:

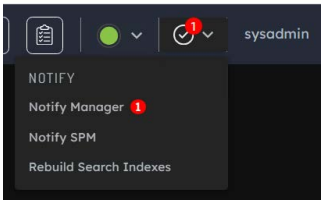
- DIVAMANAGER_TO_LOWER
- DIVAMANAGER_MAX_SIMULTANEOUS_REQUESTS
- DIVAMANAGER_MAX_INACTIVE_REQUESTS
- DIVAMANAGER_MAX_SPAN_SEGMENTS
- DIVAMANAGER_MAX_VIRTUALOBJECTS_FOR_REPACK
- DIVAMANAGER_MAX_DELAY_BETWEEN_SCHEDULER
- DIVAMANAGER_SCHEDULER_AFTER_INACTIVITY
- DIVAMANAGER_EXPORT_ROOT_DIR
- DIVAMANAGER_MAX_RESTORE_SERVERS
- DIVAMANAGER_MAX_EXPORT_TAPES
- DIVAMANAGER_MAX_EXPORT_ELEMENTS
- DIVAMANAGER_MAX_FILES_IN_ARCHIVE
- DIVAMANAGER_MAX_FILES_IN_PARTIAL_RESTORE
- USE_IMPROVED_BEST_WORST_FIT_ALGORITHM
- DIVAMANAGER_SITE_SUPPORT_ENABLED
- DIVAMANAGER_CACHE_QOS_USE_DISK
- DIVAMANAGER_PRIORITY_TIER
- DIVAMANAGER_OVERWRITE_POLICY
- DIVAMANAGER_OVERWRITE_OVERRIDE
- ATTEMPT_ACCESS_TO_OFFLINE_DISK
- CHANGE_DISK_STATE_ON_ERROR
- MANAGER_ACTOR_DISK_RETRY_NUMBER
- DISK_STATUS_POLLING_RATE
- DISK_BUFFER_SPACE
- DISK_CONNECTION_STATE_RESET_DELAY
- DIVAMANAGER_MAX_EXCLUDED_INSTANCES
- DIVAMANAGER_REQUEST_SCHEDULING_QUEUE_SIZE

- DIVAMANAGER_API_TASK_QUEUE_SIZE
- DIVAMANAGER_MAX_CONCURRENT_REQUESTS
- DIVAMANAGER_MIN_DB_CONNECTION_LIMIT
- DIVAMANAGER_MAX_DB_CONNECTION_LIMIT
- DIVAMANAGER_INITIAL_DB_CONNECTION_LIMIT
- DIVAMANAGER_INACTIVITY_TIMEOUT
- DIVAMANAGER_SIZE_OF_STATEMENT_CACHE
- DIVAMANAGER_DEFAULT_ROW_PREFETCH
- DIVAMANAGER_FAILOVER_ENABLED
- DIVAMANAGER_NUM_RS_SOLUTIONS_TO_EVALUATE
- DIVAMANAGER_DBSERVICENAME
- ABORT_ARCHIVES_ON_EMPTY_FILES (reloadable in service mode)
- TAPE_FULL_ON_SPAN_REJECTED (reloadable in service mode)

Updates in the DIVA Web App System Page

These topics describe updates made in the various areas on the System page.

When you make configuration changes through the DIVA WEB App that require the manager to be notified, the *Notify* button becomes active. To notify the Manager of the changes, click the *Notify* button toward the upper-right, then click *Notify Manager*.



Networks Area

If one of these parameters or actions in the Networks area of the Systems page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Network Name

Sites Area

If one of these parameters or actions in the Sites area of the Systems page is changed, Manager must be notified for the changes to take effect.

- Add

- Delete
- Site Name
- Is Main Site
- Comments

Servers Area

If one of these parameters or actions in the Systems page Servers panel is changed, Manager must be notified for the changes to take effect.

The following changes take effect only after notifying the Manager, and only after currently-running jobs are complete.

- Add
- Delete
- Source Server Name
- IP Address
- Source Server Type
- Network
- Site
- Connect Options
- Root Path)
- Max Throughput
- Max Accesses You must not make changes to this parameter while there are active job because it could lead to the job being terminated.
- Max Read Accesses You must not make changes to this parameter while there are active job because it could lead to the job being terminated.
- Max Write Accesses You must not make changes to this parameter while there are active job because it could lead to the job being terminated.

Actors Area

If one of the following parameters or actions in the Actors area of the Systems page is changed, Manager must be notified for the changes to take effect.

Before the change becomes effective on several of the parameters or actions, the actor must be disconnected.

The following changes take effect only after notifying the Manager, and only after currently-running jobs are complete.

- Add
- Delete
- Actor Name

- IP Address
- Port
- Network
- Site
- Max Drive Operations
- Max Server Operations
- Max Disk Operations
- Direct Restore
- Cache Restore
- Copy to Tape Group
- Associative Copy
- Repack
- Delete
- Direct Archive
- Cache Archive

Transcoders Area

If one of the following parameters or actions in the Transcoders area of the Systems page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Transcoder Name
- Transcoder Type
- Transcoder Port
- Working Directory
- Executable Path
- Performance

Updates in the DIVA Web App Robots Page

The following sections describe updates made in the various areas on the Robots page.

Robot Managers Area

If one of the following parameters or actions in the Robot Managers area of the Robots page is changed, Manager must be notified for the changes to take effect.

Before the change becomes effective on several of the parameters or actions, the Robot Manager must be disconnected.

- Add
- Delete
- Robot Manager Name
- Address (must disconnect Robot Manager first and Notify Manager)
- Port (must disconnect Robot Manager first and Notify Manager)
- Site

Media Compatibility Area

If an entry is deleted in the Media Compatibility area of the Robots page, Manager must be notified for the changes to take effect.

Robot Managers-ACS Area

If an entry is deleted in the Robot Managers-ACS area of the Robots page, Manager must be notified for the changes to take effect.

Updates in the DIVA Web App Disks Page

The following sections describe updates made in the various areas on the Disks page.

Arrays Area

If one of the following parameters or actions in the Arrays frame of the Disks page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Array Name
- Description

Disks Area

If one of the following parameters or actions in the Disks area of the Disks page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Disk Name
- Array
- Site
- Status

- Min Free Space

Actor-Disk Connections Area

If one of the following parameters or actions in the Actor-Disk Connections area of the Disks page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Disk
- Actor
- Interface
- Mount Point
- Max Throughput
- Access
- Used For

Object Storage Accounts Area

If one of the following parameters or actions in the Object Storage Accounts area of the Disks page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Account Name
- Login
- Password
- URL
- Proxy
- Service Name
- Identity Domain
- Threads Per Transfer
- Type
- Vendor

Updates in the DIVA Web App Drives Page

The following sections describe updates made in the various areas on the Drives page.

Drives Area

If one of the following parameters or actions in the Drives area of the Drives page is changed, the noted action must be performed for the changes to take effect.

- Delete (Notify Manager)
- Serial Number (Notify Manager)
- Status (Notify Manager)
- Enabled Operations (Notify Manager)
- Used (manager restart)
- Installation Date (no action required, effective immediately)
- Last Upgrade Date (no action required, effective immediately)
- Last Cleaning Date (no action required, effective immediately)

Managed Storage Area

If one of the following parameters or actions in the Managed Storage area of the Drives page is changed, Manager must be notified for the changes to take effect.

- Delete
- Name
- Serial Number
- Status

Drive Properties Area

If one of the following parameters or actions in the Drive Properties area of the Drives page is changed, Manager must be notified for the changes to take effect.

- Add (through syncDB)
- Delete

Actor-Drives Area

If one of the following parameters or actions in the Actor-Drives area of the Drives page is changed, Manager must be notified for the changes to take effect.

- Add
- Delete
- Actor
- Drive

Updates in the Diva Web App Tapes Page

If one of the following parameters or actions in the Tapes page is changed, the noted action must be preformed for the changes to take effect.

- Tape Properties (Notify Manager)
- Empty Ejected Tapes (no action required, effective immediately)
- Inserted Protected Tapes (no action required, effective immediately)
- Tape States (no action required, effective immediately)

Updates in the DIVA Web App Sets, Tape Groups & Media Mapping Page

Changes made in this page are effective as soon as they are applied. No manual update is necessary.

Updates in the DIVA Web App Analytics App Page

If one of the following parameters or actions in the Analytics App page is changed, the noted action must be performed for the changes to take effect.

- Configuration (Notify Manager)
- Event Definitions (can't be altered)
- Metric Definitions (no action required, effective immediately)

Updates in the DIVA Web App Storage Plans Page

Changes made in this page are effective immediately. Telestream strongly recommends you stop SPM before altering any settings on this page.

Updates in the DIVA Web App Slots Page

Changes made in this page are effective immediately. Telestream strongly recommends you stop SPM before altering any settings on this page.

System Operation, Maintenance and Monitoring

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

Topics

- DIVA Launch Process
- Stopping DIVA
- Backup Service Warnings and Notifications
- Job Monitoring
- DIVA System Failure Scenarios and Recovery Procedures

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

Start the DIVA hardware components in sequence. Wait for initialization of each hardware component to finish before starting the next component.

1. Confirm that all required devices are installed. If they are not installed, they must be installed before proceeding any further. The following devices are required:
   - Managed Storage and Drives
   - SAN RAID Arrays
   - Fiber Channel Switches
   - Networking Devices
   - Terminal Concentrator
   - Graphical Front End Hosts (DIVA Web App)
   - Library DIVA Host
   - External Direct Attached Devices
   - DIVA Hosts
   - 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, you might have to start the Main DIVA first, and the Alternate (or Backup) DIVA later. Consult with your Telestream Installer to determine if this is the correct procedure for your installation.
11. Power on the Actor Hosts.

Hardware start is complete if everything powered on successfully.

Starting DIVA Software

The following third-party database and messaging components should be started and available:

- Postgres DB
- MongoDB
- RabbitMQ
- Elasticsearch
- (Optional) TIKA Service

Start the software components in sequence. Some software components (for example, the Actor Service) may be set to start automatically when the host is started.

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

Start all of the DIVA software components in sequence.

1. To confirm that all required components are installed, check in Windows Services. All installed DIVA components that are set to *Automatic startup mode* should be running. If they aren't, install any missing services before proceeding.

   The following list of services is not exhaustive. The list for your system depends on the services installed by Telestream Professional Services.

   - DIVA Connect REST API Adapter
   - DIVA Core Analytics
   - DIVA Core Backup Service
   - DIVA Core DB Agent
   - DIVA Core Metadata Service
   - DIVA Core Migration Service
   - DIVA Core Proxy Service
   - DIVA Core REST API Data Service
   - DIVA Core REST API Discovery
   - DIVA Core REST API Gateway
   - DIVA Core Rosetta
   - DIVA Core SPM
   - DIVArchive Actor
   - DIVArchive DFM
   - DIVArchive Hole Punch Server
   - DIVArchive Manager
   - DIVArchive Robot Manager
   - DIVArchive VACP
2. Launch the Library Control software, in the following order:
   a. ACSLS
   b. PCS
   c. SDLC
3. Launch the Robot Manager(s).
4. Launch the Actor(s).
5. Launch the Manager.
6. Launch DIVA Connect.

7. (Optional) You can start any of the following services independently:
   - Actors
   - Backup Service
   - DBAgent
   - Manager
   - Metadata Service (MDS)
   - Proxy service
   - Robot Managers
8. Launch the VACP Converter.
9. Launch SPM.
10. Launch DFM.

    If everything initialized successfully, the software start is complete.
11. To confirm, log into the DIVA Web App.
12. Click the *System Health Status* button .

    DIVA opens the *SYSTEM HEALTH STATUS* drop-down menu.

    A green dot next to the name of a component indicates the component is working correctly.
13. If you don't see the list of all components used in your DIVA System, in the DIVA Web App, browse to *Configuration* > *User Management* > *User Settings* > *System Health* > *Monitored Service Statuses*; and select the services to monitor.

Stopping DIVA

Stop DIVA in the reverse order from starting the system. First, shut down the software; then the hardware. The following topics describe the correct procedure for fully shutting down DIVA.

Caution: Do not simply power off the server computer. Use the correct shutdown procedure. Data corruption, database corruption, or data loss could occur if you don't follow the correct shutdown procedure.

Note: Before stopping DIVA software, check that you have valid and recent full database backups for all DB engines (Postgres, MongoDB and Elasticsearch), both on the Primary Location and on copied-to-Backup Locations. Refer to BKS Module user documentation for more details.

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.

1. Shut down the Manager Host.
2. Shut down the Actor Hosts.

Shutting Down the Hardware

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

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

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, or contains errors.
  To confirm this, at a WIndows command prompt, run the following and check for displayed errors:
  `%DIVA_HOME%\Program\BackupService\lib>DIVACore.BackupService.exe`
- The database connection information is incorrect, or the database is not running.
- `RMANRecoverWindow.bat` is not in the bin folder for the Backup Service. This applies only if BKS is in charge of backing up an Oracle DB.

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.

Note: Since the DIVA stack is not operational at this stage, you might not be able to use the DIVA Web App to configure BKS. Instead, edit the BKS configuration file directly.

```
"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, you can start the other DIVA Services and verify that 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.

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 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.

To view the current state of a job in the DIVA Web App, browse to *Content Management* > *Job History*. View the *STATE* column.

For additional assistance, contact Telestream Support. See *Telestream Contact Information*.

Job Warnings

A warning status indicator on a job signifies that, though the job was completed, an unexpected error occurred during the job execution.

Three example scenarios follow:

- An I/O error occurred while reading an object from tape. However, there was a second instance of the object on another tape. DIVA used the second instance, and transferred the object successfully. You must examine the tape from the first restore attempt. 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 automatically marks the drive *Out of Order*.
- An unexpected I/O error may have occurred with one of the disks in a disk array while an object was being transferred to the array. DIVA automatically selects another disk from the array to transfer the object to, and this attempt is successful. DIVA marks the disk where the I/O error occurred *Out of Order*, and doesn't use that disk again. You must examine the offline disk for the cause of the error.
- A write error occurs with the selected tape while an object is being archived to the tape. DIVA archives the object to another tape to fulfill the job. DIVA marks the tape from the first write attempt *Read-Only*, and doesn't use the tape for additional archive jobs.

DIVA System Failure Scenarios and Recovery Procedures

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

Non-fail-over Scenarios

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

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

– Manager Failure

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

– Instance Failure

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.

Contact Technical Support if you require assistance, 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.

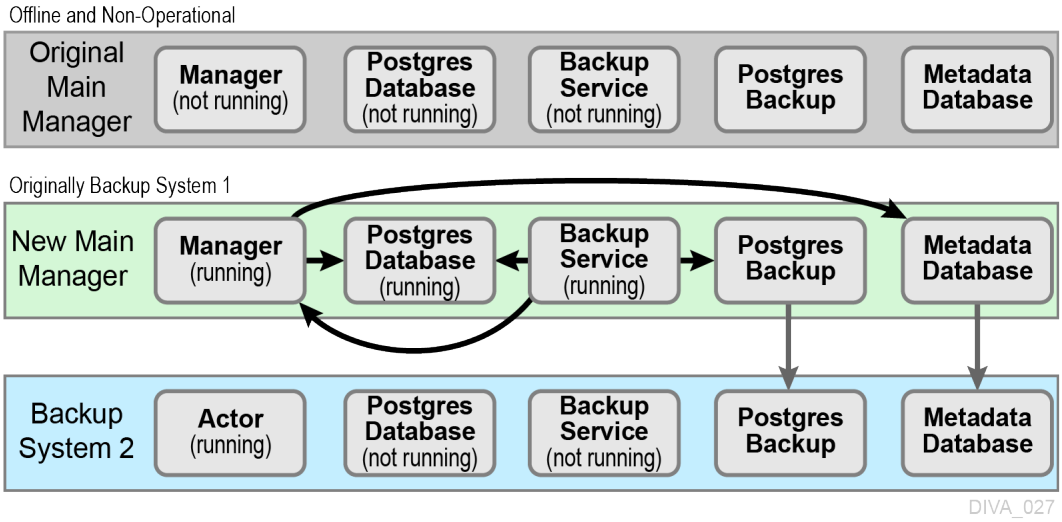
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/5/2023  12:27 AM                archive_status
-a----         1/5/2023  12:27 AM       16777216 00000001000000000000001
Starting service: postgresql-x64-14...
sc start postgresql-x64-14

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.



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.

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

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

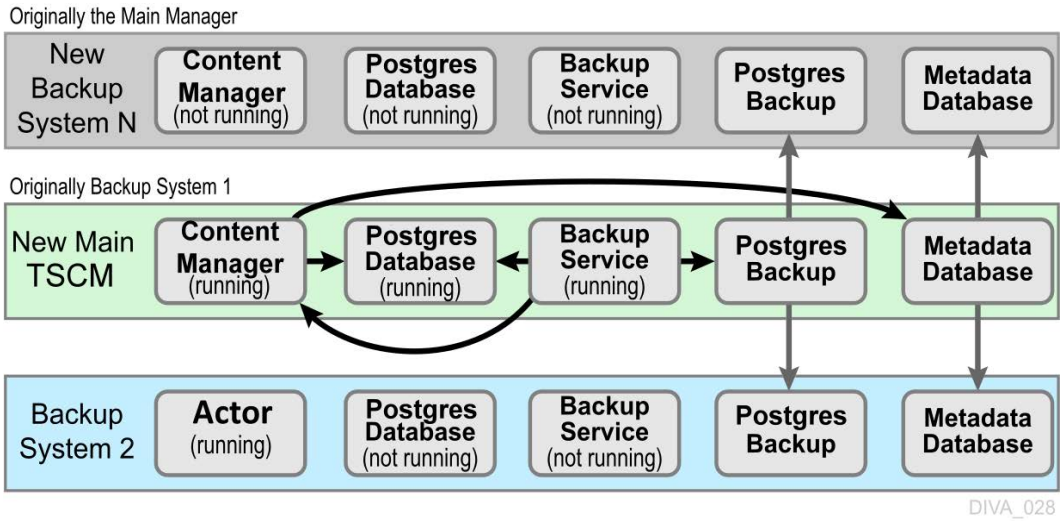
5. Start the Manager and backup service on the New Main Manager.

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

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

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

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



Database Service Failover

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

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

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

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

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

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

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

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

Use the following procedures to perform the fail-over:

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

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

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 from the Main Manager to the Backup Manager, 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 the 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.

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 questions not covered here.

Topics

- DIVA Installation Questions and Answers
- Database Backup Questions and Answers

DIVA Installation Questions and Answers

What happened to DIVA Command?

Telestream has replaced DIVA Command with the DIVA Web App.

What happened to the legacy Java DIVA Control GUI and the DIVA Configuration Utility?

Telestream has replaced them with the DIVA Web App.

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

Technical Support recommends applying all critical updates to all computers, because some updates include security updates. However, Telestream doesn't test Windows operating-system updates or patches.

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 causes downtime for the system. Also, if a process is running when a server is restarted, the restart can cause data corruption. Restart a server only when absolutely necessary, using the correct system shutdown procedure.

Caution: Do not simply power off the server computer. Use the correct shutdown procedure. Data corruption, database corruption, or data loss could occur if you don't follow the correct shutdown procedure.
See also *Stopping DIVA*.

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, or when instructed to do so by Telestream Support.

Should DIVA services or applications be restarted with any frequency?

No, restart a DIVA service or application only when absolutely necessary.

Where are DIVA service or application logs located?

The DIVA service or application log files are located in the `%DIVA_HOME%\Program\log` folder.

How far back in time do the logs go?

In most cases, you can customize the retention time in the configuration file for each module. As a general rule, you can check the parameter called `RetentionDays` in the corresponding module-configuration file. For assistance, contact Telestream Support.

The log files are retained as follows by default:

- DIVA Manager, DIVA Connect: 168 hours (7 days)
- Actor, Robot Manager, Storage Policy Manager, Avid Transfer Manager Communicator, Avid Archive Manager Communicator: 7 days
- Drop Folder Monitor (DFM): 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 DIVA servers and systems?

Technical Support supports only DIVA software. You must contact the server supplier for any hardware issue. Keep Technical Support in the loop for any issues on the DIVA solution (for example, loss of a RAID disk, or failover to the backup manager).

Are there special considerations related to recovering from a server failure when the server is part of the DIVA solution?

Keep Technical Support in the loop if issues are encountered.

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 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 (MDS)?

MDS Metadata Database is located in MongoDB. MongoDB is the database engine that the MDS Metadata Service connects to. The settings are located in MDS configuration file:

```
"Databases": [
      {
        "ProfileName": "MetadataDatabase",
        "DatabaseName": "Core",
        "DatabaseType": "MongoDB",
        "DatabaseVersion": "5.0",
        "ConnectionString": "mongodb://127.0.0.1:27017/
?replicaSet=rs0",
        "RootDirectory": "",
        "DataDirectory": null,
        "User": "MongoAdmin",
        "Password": "ECwyt273MiTostEsjHr+/
wrBS3UMc63DfNoaTn+wANw=",
        "CertPath": null,
        "Options": null
      },
```

Where do I configure the location of the Elasticsearch Database?

Elasticsearch is the DB engine that the Metadata Service (MDS) connects to. The settings are located in MDS configuration file:

```
{
        "ProfileName": "SearchDatabase",
        "DatabaseName": "Core",
        "DatabaseType": "ElasticSearch",
        "DatabaseVersion": "7.10.2",
        "ConnectionString": "http://localhost:9200/",
        "RootDirectory": "",
        "DataDirectory": null,
        "User": "ElasticAdmin",
        "Password": null,
        "CertPath": null,
        "Options": null
      }
```

What information is stored in the Metadata Database?

The Metadata Database file contains all file details, for example file names, folder names, location, size, and checksums. In addition to the information stored for Complex Objects, the Metadata Database also stores all the metadata created and associated with Objects stored in DIVA, for example DIVA Object metadata, metadata extracted from source clips, user-defined metadata, and attachments metadata.

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.

Why is this information not being stored in the existing Database?

All file lists, including Complex Objects are stored in MDS, up to 1,000,000 files. This is an enormous amount of data. DIVA runs searches against MDS metadata. The exclusion of the file lists from the primary database improves the performance of queries.

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 won't be able to access Objects Metadata information 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*.

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. If you need assistance, contact Technical Support.

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 the Metadata Database* for DIVA Backup Service installation and configuration procedures.

Database Backup Questions and Answers

What is the recommended frequency of database backups?

You can configure BKS settings. In the DIVA Web App, browse to *Configuration* > *Services* > *Database Backup*.

By default, DIVA Databases are automatically backed up for incremental changes every 15 minutes. You can set a new backup timing, in minutes, with the *Incremental Period (Minutes)* setting.

One full backup per database must be done daily, at the time defined in *Backup Time*.

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:\divaback`) 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 might 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:\divaback` folder. The files are synced to locations defined in the DIVA Web App *Configuration* > *Services* > *Database Backup* > *Locations* setting. This defines the path to replicate the DB backups to remote server locations.

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

By default, DIVA retains the backup files for the previous 10 days. You can customize the retention period for the database backup files via the DIVA Web App. Set the value for *Full Backup File Retention (Days)*.

How do I failover to a Backup System when the Main Manager System has failed?

For information about failover procedures, see *Failover Scenarios*.

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

Disk failures, or corruption, requires a failover from the Main Manager to the Backup Manager. For information about failover procedures, see *DIVA System Failure Scenarios and Recovery 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 Postgres Secure Backups and Metadata Backups?

Yes, the recovery-window setting applies to both backups and Elasticsearch 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. For information about storage requirements, see *General Storage Requirements*.