Oracle® DIVArchive Suite

Release Notes

Release 7.6.2

E84054-05

October 2018

This document provides product release information for the Oracle DIVArchive Suite releases 7.6.0, 7.6.1, and 7.6.2.

Read this documentation before installing and using Oracle DIVArchive.

Installing, Configuring, or Updating DIVArchive

Contact Oracle Support for assistance installing, updating, or configuring DIVArchive. The Oracle Support Contacts Global Directory can be found at:

`http://www.oracle.com/us/support/contact/index.html`

For more information, see the Oracle DIVArchive documentation set for this release located at `https://docs.oracle.com/en/storage/#csm`.

DIVArchive Options and Licensing

The following table identifies DIVArchive options and licensing metrics.

Part Number	Description	Licensing Metric
L101163	Oracle DIVArchive Nearline Capacity	Per TB
L101164	Oracle DIVArchive Archive Capacity	Per Slot
L101165	Oracle DIVArchive Actor	Per Server
L101166	Oracle DIVArchive Manager	Per Server
L101167	Oracle DIVArchive Partial File Restore	Per Wrapper
L101168	Oracle DIVArchive Avid Connectivity	Per Server
L101169	Oracle DIVArchive Application Filtering	Per Server

Part Number	Description	Licensing Metric
L101170	Oracle DIVArchive Storage Plan Manager (2 storage plans are included with a DIVArchive Manager License)	Per Server
L101171	Oracle DIVAnet	Per Server
L101172	Oracle DIVAdirector	Per User
L101918	Oracle DIVArchive Export / Import	Per Server
L101919	Oracle DIVArchive Additional Archive Robotic System	Per Tape Library
L101920	Oracle DIVArchive Automatic Data Migration	Per Server

Security

Oracle recommends keeping the operating system up to date with the latest security patches. However, Oracle cannot guarantee that all patches will operate correctly with DIVArchive because the operating system security patches are independent of the DIVArchive application.

You should determine the acceptable operating system security patch level for your environment. Contact Oracle Support for assistance in determining operating system patch level compatibility if necessary.

What’s New in Oracle DIVArchive Suite 7.6.2

DIVArchive 7.6.2 includes the following new features and enhancements:

New DIVArchive Installer

The 7.6.2 DIVArchive installer provides a better user experience by adding new features for both the Windows and Linux platforms. You can now install a new instance of DIVArhive or upgrade an existing installation using a single installer. You can also optionally install or upgrade the DIVArchive database schema using the same installer. If you choose to install or upgrade the database schema, the installer will prompt you for database credentials.

The option to install or upgrade specific components such as actors, manager, and so on has been removed. The installer will always install all DIVA components together. This will standardize the DIVArchive installation location going forward.

The installer will always backup the existing install location and database schema before upgrading. You can restore previous installations easily by copying files from the backup folder and running a command to restore the database schema.

Refer to the *DIVArchive Installation and Configuration Guide* for more details.

Support for Oracle Database Version

DIVArchive 7.6.2 supports both Oracle 11gR2 and 12cR1. This allows you to take advantage of the new DIVArchive installer to upgrade to the latest DIVA software without having to upgrade the Oracle database version.

New Partial Restore Support

MXF

MXF partial restore is now supported for Linux. BMX has replaced the MOG SDK library. For Linux, BMX will always be used.

For Windows, you can select either MOG SDK or BMX from the Config Utility under Advanced Actor Settings, by setting the Use BMX Library parameter to Y.

MXF DNxHR

DNxHR is a new codec from AVID for high and ultra high definition. This essence is supported by the MXF partial restore.

AVI FFV1

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

OCI Archive Storage Tier Support

DIVArchive now supports the archive storage tier for OCI accounts. A user may configure the archive storage tier for a DIVArchive array by specifying `-oracle_storage_class=ARCHIVE` as a storage option of the array connected to the OCI object storage account.

New Disk Cloud Source/Destination

A new type of source/destination has been added to allow the export of DIVArchive objects to a disk in the cloud instance.

Priority Setting for .mdf Metadata Files

During restores, DIVarchive can generate metadata files compatible with DFM (with .mdf extension). A new source/destination option has been added to specify the priority value:

```
-mdf_priority <VALUE>
```

Where VALUE is an integer comprised between 0 and 100. Default is 50.

Volume Tag Filtering Option

A new option has been added to the RobotManager configuration file in order to replace RM_SCSI_ENABLE_MEDIA_TYPE_DETECTION and RM_SCSI_MEDIA_TYPE_LEFT_DETECTION. This option defines a layout to filter out the label of a tape and media type from the volume tag returned by the library. The layout is a string of 8-10 characters indicating where the label and the media type are. It must contain these three characters only:

- **L** — the tape label/barcode considered into DIVArchive database
- **T** — used for media type detection
- **X** — ignored

Example: If the layout is set to LLLLLLTT, for a volume tag of ABC003L6, the RobotManager will detect L6 as the media type (LTO6) and report ABC003 as the label to DIVArchive.

When upgrading DIVArchive from a previous version, RobotManager will automatically upgrade its configuration following this matrix:

DETECTION_LAYOUT	TYPE_DETECTION	TYPE_LEFT_DETECTION
LLLLLLLL	0	N/A
LLLLLLTT	1	0
TTLLLLLL	1	1

What's New in Oracle DIVArchive Suite 7.6.1

DIVArchive 7.6.1 includes the following new features and enhancements:

Component Removal

DIVArchive Access Gateway (replaced by DIVAnet 2.x) has been removed from DIVArchive 7.6.1 update and are no longer included in future software distributions.

Operating System Support Enhancements

DIVArchive 7.6.1 (and later) includes support for Windows 2016 Server.

Secure Communication with Oracle Database

A new DIVAOracle package version 3-1-0 was created:

- Windows: OracleDivaDB_3-1-0_12_2_0_1_0_SE2_Windows_64-bit
- Linux: OracleDivaDB_3-1-0_12_2_0_1_0_SE2_OEL7_x86_64

This new package includes the following

1. Secure Oracle Database listener listening on port 1522, additional on top of the regular unsecured listener listening on port 1521.
2. Oracle Database wallet for storing the Trust Certificate and DIVADatabaseServer Certificates. During installation DIVADatabaseServer.jks holding the default DIVA_CA trust certificate and Default DIVADatabaseServer certificate is import into the Oracle Database wallet for enabling the secure communication.
3. This new package also creates a secure TNSNames LIB5SSL which enables any DIVA services to connect to the oracle database securely over SSL connecting to the new secure Oracle database listener listening on port 1522 using the TNSNames.

New Entry in TNSNames.ora:

```
LIB5SSL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCPS)(HOST = HOSTNAME)(PORT = 1522))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = LIB5.WORLD)
    )
  )
```

A new Configuration Parameter "DIVAMANAGER_DB_SECURE_CONNECT" was added to the Manager,Migrate,DBBackup configuration file to enable secure communication to database using Hostname/IPAddress and port. This parameter has no effect if using DIVAMANAGER_TNSNAME parameter in the configuration file.

Valid parameter values are:

- TRUE - When set to TRUE, the DIVAMANAGER_DBPORT in the Manager,Migrate,DBBackup configuration file must point to the secure port of the Oracle Database.
- FALSE (default)

The Configuration Utility and Control GUI also supports connecting securely to the database. SPMService can connect securely only using TNS names.

Drop Folder Manager

In DIVA 7.6.1, only one DFM service instance can be run from each installation of DIVArchive. If you need to run multiple DFM services at the same time, install and run each DFM service instance in its own DIVA folder.

DIVADBWallet

You can use DIVADBWallet (Windows - DIVADBWallet.bat or Linux - DIVADBWallet.sh) to update the Oracle Database Server wallet with the DIVADatabaseServer.jks changes after installing an external certificate authority using the DivaSecurityTool. Oracle Database Server wallet is created during Oracle Database Installation using DIVAOracle Database package OracleDivaDB_3-1-0_12_2_0_1_0_SE2_Windows_64-bit or OracleDivaDB_3-1-0_12_2_0_1_0_SE2_OEL7_x86_64 and later (see "Secure Communication with Oracle Database" above).

DIVADBWallet provides the following options that DIVA administrator can choose to perform.

Display DIVADBWallet

Displays the certificates information from Oracle Database Server wallet used by DIVArchive.

Update DIVADBWallet

Updates the Oracle Database Server wallet with the new DIVADatabaseServer.jks provided by the user. Use this option after installing an external certificate authority to communicate securely with the Oracle Database server.

Change DIVADBWallet password

Resets the password for Oracle Database Server wallet.

Oracle OCI Support Enhancements

DIVArchive 7.6.1 (and later) includes support for storing your data in Oracle Cloud Infrastructure (OCI).

New LTO Drive Support

DIVArchive 7.6.1 includes support for LTO-8 drives. The LTO-8 tapes have a higher capacity than the previous tapes; 12.8 TB native and 32 TB compressed. Data transfer rates are up to 472 MBps uncompressed, and 1180 MBps compressed.

The LTO-8 drives are backward compatible with LTO-7 tapes (Read and Write).

UUID Preservation

DIVArchive 7.6.1 enables the preservation of the original UUID of AXF objects during archive operations. You enable this option by selecting the ***Enable UUID Preservation*** check box on the **Manager Setting** tab in the Configuration Utility. Deselecting the check box disables this functionality.

The object you are attempting to archive must have a unique UUID. The request will fail if this setting is enabled and you attempt to archive an object that has the same UUID as an existing object.

AXF 1.1 Compliance

DIVArchive 7.6.1 includes an improved internal AXF format to support the latest AXF release. The latest AXF release includes official support for symbolic links and improved XML compliance. To validate XML files produced by DIVArchive, the file must have an extension of the XSD that includes the DIVArchive specific elements.

DIVArchive 7.6.1 continues support for earlier AXF releases as follows:

DIVArchive Release	AXF 0.9 Support	AXF 1.0 Support	AXF 1.1 Support
7.6	Read Only	Read and Write	Read and Write
7.3, 7.4, 7.5	Read Only	Read and Write	None

Read and write support for AXF 1.0 is required in some DIVAnet environments. For example, a DIVArchive 7.6.1 system could export an object to an earlier DIVArchive release if the format is set to AXF 1.0 instead of AXF 1.1.

In previous DIVArchive releases you chose between **AXF** or **LEGACY** formats in the Configuration Utility when adding tape groups or disk arrays. Starting with DIVArchive 7.6.1 you must select either **AXF_1.1**, **AXF_1.0**, or **LEGACY**.

DIVArchive 7.6.1 can archive the content of an AXF file from a Source/Destination if it is the only file in the list, and it has the `.axf` file name extension. DIVArchive 7.6 can still detect and read all versions of AXF files.

In the Actor-Manager communication, the `tapeFormat` and `instanceFormat` attributes can be **AXF**, **AXF_1.0**, or **AXF_1.1**. The version is only relevant for the writing device. During read operations the Manager can specify **AXF** and the Actor will automatically detect the format.

DIVArchive can archive the content of an AXF file from a Source/Destination if it is the only file in the list, and has the `.axf` extension. DIVArchive 7.6.1 can still detect and read all the versions of AXF files.

The `-axf` option for restore operations now supports additional parameters to specify the target AXF version. If you specify `-axf` or `-axf 1.1` in the request options, DIVArchive restores an AXF 1.1 compliant file. If you specify `-axf 1.0` in the request options, DIVArchive restores an AXF 1.0 compliant file.

What's New in Oracle DIVArchive Suite 7.6.0

DIVArchive 7.6.0 includes the following new features and enhancements:

EMC ECS (Elastic Cloud Storage) Integration

Instances stored on EMC Elastic Cloud Storage are local instances whose priority is lower than other types of local disk instances, but a higher priority than tape storage instances.

In DIVArchive 7.6.0 you can define Oracle ***Storage Class*** and ***Storage Location*** separately. If you require new cloud or local arrays in the future, you can specify all of these parameters as options. You can set the ***Media Priority*** of a source instance for a Restore, Oracle Partial File Restore, and Copy to Group requests, which enables restoring an instance stored on a local non-EMC ECS array with a higher priority than an instance on an EMC ECS array. If the priorities for the media are all the same, then the Manager decides which source instance is preferred during these requests.

Source Media Priority

The ***Source Media Priority*** determines which source instance is preferred (according to the media where the instance resides) during the instance selection process of a Restore, Partial File Restore, and Copy To Group request. Instances on media with a higher priority are preferred. Cloud instances are only copied or restored if all local instances are offline, or no local instances exist. This is an absolute condition independent of the ***Source Media Priority***.

The default priority value for all media is `50`. Also, when you upgrade from an earlier DIVArchive release, all media is assigned the default priority value (`50`).

See the *Oracle DIVArchive Operations Guide* in the *Oracle DIVArchive Core documentation* library for detailed information.

EMC ECS Object Store Integration

DIVArchive 7.6.0 supports local arrays that include disks with *Swift* interfaces, for example an EMC ECS Object Store. First, you define a disk and assign it to the EMC ECS array (like a local disk), and then you must define an Object Storage Account (formerly a Cloud Account). You can also specify a proxy server to use if your Oracle DIVArchive Actor cannot access the Object Storage Account directly. You can view the storage options on the **Home**, **Disks** screen in the DIVArchive Control GUI.

During an upgrade from an earlier DIVArchive release, all disk instances with an **Archive** or **Standard** Storage Class are updated with a storage option containing `-storage_location=CLOUD` and `-oracle_storage_class={ARCHIVE|STANDARD}`. All disk instances with a **None** Storage Class are updated with a storage option containing `-storage_location=LOCAL` and `-oracle_storage_class=NONE`. All Actor-Disk connections with **cloud** as the interface are updated to **Swift** for the interface.

> **Note:** Swift Source/Destination types do not support EMC ECS, GC (Genuine Checksum), VFA (Verify Following Archive), or VFR (Verify Following Restore) functions.

The APIs report storage options in the `getArraysList` call, and instances in the `getObjectInfo` and `getObjectDetailsList` calls.

See the *Oracle DIVArchive Installation and Configuration Guide* in the *Oracle DIVArchive Core documentation* library for detailed configuration information.

Tape Group Encryption

Starting with the DIVArchive 7.6.0 release, tape drive encryption securely supports bulk tape migration between DIVArchive systems. Group level encryption is enabled, disabled, or updated in the *Groups* view of the **Sets, Groups & Media Mapping** tab in the Configuration Utility.

After enabling encryption on a tape group, all additional tapes added to the group will also be encrypted. However, any existing tapes in the group remain unencrypted if encryption was previously disabled.

Enabling encryption on a tape group generates an encryption key, which is also encrypted. You can change the encryption key at any time by selecting **Update** from the ***Encryption*** options list on the *Edit Groups Entry* screen. You double-click the tape group from the list on the *Groups* view to display the *Edit Groups Entry* screen. Updating the encryption generates a new key. New tapes added to the group after the change will use the new encryption key. The existing tapes that were already encrypted will continue to use the original key. Therefore, tapes in the same tape group can have different encryption keys. You must notify the Manager of the change when updating the encryption key.

Disabling encryption (after it is already enabled) only affects additional tapes added to the group, and the existing tapes remain encrypted.

You can view the encryption status of the tape on the **Home**, **Tapes** screen in the Control GUI.

See the *Oracle DIVArchive Installation and Configuration Guide*, and the *Oracle DIVArchive Export/Import User's Guide* in the *Oracle DIVArchive Core documentation* library for detailed configuration, and export and import information.

SSL (Secure Sockets Layer) Authentication and Secure Communication

DIVArchive 7.6.0 introduces SSL (Secure Sockets Layer) Authentication for services, and to secure DIVArchive internal and API communications. Certificate authentication provides unique identification and secure communication for each DIVArchive Service in a network.

DIVArchive 7.6.0 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 DIVArchive services. Every DIVArchive service now has its own password protected private key and a SSL certificate signed by the `DIVA_CA` authority.

You can also use an external third party CA (for example, VeriSign, Comodo, and so on) to generate and sign your certificates.

See the *Oracle DIVArchive Installation and Configuration Guide* in the *Oracle DIVArchive Core documentation* library for detailed configuration information.

Security Tools

A new Security Tool is included in the DIVArchive 7.6,0 release as follows:

- Windows: `DivaSecurityTool.bat`
- Linux: `DivaSecurityTool.sh`

The tool is located in the `%DIVA_HOME%/security/bin` directory and provides the following functions:

Resetting Key Passwords

This tool enables resetting the Key password. All services must be restarted after changing the password.

Generating New Keys and Certificates

This tools enables generating new keys and certificates for all DIVArchive services. The new generated keys and certificates are signed by `DIVA_CA`.

Generating Certificate Signing Requests

This tool generates certificate signing requests for `DIVA_CA` to send to third party Certificate Authorities. The third party CA returns the signed `DIVA_CA` certificate and the third party's own certificate.

Installing External Certificate Authority

This tool installs the third party CA certificate into the DIVArchive installation.

See the *Oracle DIVArchive Installation and Configuration Guide* in the *Oracle DIVArchive Core documentation* library for detailed information about using these tools.

DIVArchive API Changes

The DIVArchive APIs include changes to establish secure communication with the Oracle DIVArchive Manager. The DIVArchive Manager is backward compatible with earlier Java, C++ and Web Services APIs to establish connections over regular sockets. The DIVArchive 7.6.0 (and later) Java and C++ API releases can establish Manager communications using secure, or unsecure, sockets.

The Java API includes new parameters added to the `SessionParameters` class to facilitate secure connections to the Manager Service.

Exporting and importing encrypted tapes is also available using the Java API.

See the *Oracle Java API Readme* in the *Oracle DIVArchive Additional Features documentation* library for the location of the Java API documentation.

The C++ API `DIVA_SSL_initialize` call is added to set the environment for secure communication with the Manager service. See the *Oracle DIVArchive C++ API Programmer's Guide* in the *Oracle DIVArchive Additional Features documentation* library for detailed information.

The Java and C++ APIs initiators both use the default keys and certificates under the `%DIVA_API_HOME%/lib/security` subfolder when connecting to the Manager.

Oracle DIVA Enterprise Connect connects to the Manager Service through the unsecure `tcp/9000` port. See the *Oracle DIVA Enterprise Connect Installation, Configuration, and Operations Guide* in the *Oracle DIVA Enterprise Connect documentation* library for detailed information.

The Manager Service is backward compatible with earlier releases of DIVAnet, Java API, C++ API, and Web Services API, and establishes the connection over regular sockets.

Dual Ports

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 DIVArchive services can only connect to secure ports. The control GUI will report an *SSL Handshake Timeout* if you attempt to connect to the non-secure port.

See the *Oracle DIVArchive Installation and Configuration Guide* in the *Oracle DIVArchive Core documentation* library for detailed information.

Object Storage Destinations

DIVArchive 7.6.0 enables restoring content to a destination, and archiving content from a source, linked to an Oracle Object Storage account. You can restore any type of object to these destinations. However, these destinations do not support symbolic links.

The ***Files Path Root*** for the destination must contain a value, and can contain an optional prefix. The value identifies the name for the target container. You use the optional prefix if you do not want to restore to the container root directory. The prefix must be separated from the container name using either `/` or `\`. For example, `container`, `container\folder`, and `container/subdir1/subdir2` are all valid paths.

You must define a **Swift** Source or Destination type to link to a Source or Destination to an Oracle Object Storage account. After you define a **Swift** destination, you can use the DIVArchive Object Transfer Utility (through the Control GUI) to browse the Oracle Object Storage account container's folder trees, and initiate Archive and Restore requests to the Source/Destinations. The OPC cloud OTU can also identify a manifest file and remove all file fragments in the manifest so that only a single manifest file is displayed.

See the *Oracle DIVArchive Installation and Configuration Guide*, and the *Oracle DIVArchive Operations Guide* in the *Oracle DIVArchive Core documentation* library, and the *Oracle DIVArchive Object Transfer Utility (OTU) User's Guide* in the *Oracle DIVArchive Additional Features documentation* library for detailed information.

Tape Compression

Tape compression is supported at the tape group level. You enable (or disable) tape compression on the *Groups* view in the Configuration Utility **Sets, Groups & Media Mapping** tab.

When tape compression is enabled, any empty tape assigned to the group will have compression enabled, and instances written to the tape will be compressed. Tapes assigned to the group before compression was enabled remain uncompressed, and instances written to the uncompressed tape will be uncompressed.

When exporting a tape, compression is tracked using the new `isCompressionEnabled` attribute. This attribute value can be either `true` or `false`.

To view all tapes with compression enabled, you must select the **Home**, **Tapes** icon in the Control GUI, and set the ***Compression*** filter to **Y**.

Restricted Use of Included Oracle Software Components

The Oracle database included with the DIVArchive system is limited to use only for the operation of the DIVArchive software.

Related Documents

For more information, see the Oracle DIVArchive documentation set for this release located at `https://docs.oracle.com/en/storage/#csm`.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Oracle DIVArchive Suite Release Notes, Release 7.6.2
E84054-05