

Oracle® DIVArchive
Security Guide
Release 7.4
E73115-01

June 2016

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
1 Overview	
Product Overview	1-1
Oracle DIVArchive Manager	1-1
Oracle DIVArchive Actor	1-1
DIVArchive Robot Manager	1-1
DIVArchive Backup Service	1-2
Oracle DIVArchive Avid Connectivity	1-2
DIVArchive Drop Folder Monitor (DFM)	1-2
DIVArchive SNMP	1-2
DIVArchive Storage Plan Manager (SPM)	1-2
DIVArchive Migrate Service	1-3
DIVArchive VACP	1-3
DIVArchive Control GUI	1-3
DIVArchive Configuration Utility	1-3
DIVArchive Access Gateway	1-3
DIVArchive Local Delete	1-3
General Security Principles	1-3
Keep Software Up To Date	1-3
Restrict Network Access to Critical Services	1-4
Run as DIVA User and use Principle of Least Privilege where Possible	1-4
Monitor System Activity	1-4
Keep Up To Date on Latest Security Information	1-4
2 Secure Installation	
Understand Your Environment	2-1
Which resources need to be protected?	2-1
Primary Data Disk	2-1
Database Disk, Metadata Disk, and Backup Disks	2-1
DIVArchive Tapes	2-1
Export Tape Metadata	2-1
Configuration Files and Settings	2-2

From whom are the resources being protected?.....	2-2
What will happen if the protections on strategic resources fail?	2-2
Recommended Deployment Topologies	2-2
Separate Metadata Network.....	2-2
FC Zoning.....	2-2
Safeguard SAN Disks Configuration Access	2-2
Install the DIVArchive Package	2-3
DIVArchive Tape Security	2-3
Backups.....	2-3
Postinstallation Configuration	2-3

3 Security Features

The Security Model.....	3-1
Authentication	3-1
Access Control.....	3-1

A Secure Deployment Checklist

Preface

Oracle's DIVArchive Security Guide includes information about the DIVArchive product and explains the general principles of application security.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of DIVArchive.

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.

This chapter provides an overview of the DIVArchive product and explains the general principles of application security.

Product Overview

Oracle's DIVArchive is a distributed content storage management system. DIVArchive consists of the following major components:

Oracle DIVArchive Manager

The DIVArchive Manager is the main component in a DIVArchive System. All archive operations are controlled and handled by the DIVArchive Manager. Operation requests are sent by initiator applications through the DIVArchive Client API. As a purchasable option, DIVArchive also supports Main and Backup DIVArchive Managers. For more information about DIVArchive, see the DIVArchive Software Release 7.4 Customer Documentation Library at:

<https://docs.oracle.com/en/storage/#csm>

Oracle DIVArchive Actor

The DIVArchive Actor is the data mover between devices in the production system. It supports the data transfer between many different types of devices and handles Transcode operations with Telestream Transcoding Software (optional).

All Actor operations are initiated and coordinated by the DIVArchive Manager. A single DIVArchive Manager can configure and control one or more Actors.

DIVArchive Robot Manager

Although you can use DIVArchive to only manage disk storage, storage capacity can be further expanded by adding one or more tape libraries. In these cases, the DIVArchive Robot Manager module provides an intermediate software layer for the DIVArchive Manager to interact with many different types of tape libraries. It is connected to the DIVArchive Manager through TCP/IP. The DIVArchive Robot Manager interfaces to the library by using either a direct interface to the library itself (through native SCSI or SCSI over Fibre Channel), or through an intermediate Ethernet connection to the manufacturer's own library control software.

DIVArchive Backup Service

To ensure reliability and monitoring of both the Oracle Database and Metadata Database backups, the DIVArchive Backup Service was introduced.

The DIVArchive Backup Service component is installed as an integral part of the standard DIVArchive System installation. The component is typically installed on the same server as the DIVArchive Manager and Oracle Database. The DIVArchive Backup Service allows for configuration of scheduled backups through its configuration file. The DIVArchive Backup Service manages and monitors the entire backup process.

The DIVArchive Backup Service now incorporates the ability to send out emails of issues arising from the process of backing up the Database and Metadata Database files. To take advantage of this feature, DIVArchive must be configured to connect to an SMTP mail provider. The email notifications are configured through the DIVArchive Configuration Utility under the Manager Setting Tab.

For information about installing and configuring the DIVArchive Backup service, see the DIVArchive 7.4 Customer Documentation Library at:

<https://docs.oracle.com/en/storage/#csm>

Oracle DIVArchive Avid Connectivity

The purpose of the Avid Connectivity with DIVArchive is to transfer archival data to and from DIVArchive in specific video formats and enable archiving and retrieval of single clips or a sequence of clips. The AMC and TMC related components are installed along with the main DIVArchive installation. Additional installation is required for certain plugins for both AMC and TMC.

DIVArchive Drop Folder Monitor (DFM)

The DIVArchive Drop Folder Monitor (DFM) provides automatic monitoring of newly created files in up to 20 local folders or FTP folders (or combinations thereof). One file or multiple files (in FTP-folders) per DIVArchive Object are supported. When a new file (or FTP folder) is identified, DFM issues an archive request automatically to DIVArchive to archive the new file or folders. Once these files are successfully archived, they are then automatically deleted from the source.

DIVArchive SNMP

The DIVArchive Simple Network Management Protocol (SNMP) Agent and Management Information Base (MIB) support status and activity monitoring of DIVArchive and its subsystems through a third party monitoring application over the SNMP protocol. DIVArchive SNMP is only supported in Windows environments.

DIVArchive Storage Plan Manager (SPM)

The DIVArchive Storage Plan Manager (SPM) provides automatic migration and life cycling of material within the archive based on the rules and policies defined in the SPM configuration.

The SPM component is also used to trigger deletion of material from SPM managed arrays (based on disk space watermarks).

DIVArchive Migrate Service

DIVArchive includes an embedded migration service. It is a new and separate internal (to DIVArchive) service which helps users to schedule and run jobs to migrate content between different media inside of a DIVArchive system. You can use the Control GUI or command line client.

DIVArchive VACP

VACP (Video Archive Command Protocol) is a protocol developed by Harris Automation for interfacing to an Archive System. DIVArchive has its own API for communicating with the DIVArchive Manager, which is not compatible with VACP.

DIVArchive Control GUI

You use the DIVArchive Control GUI (Graphical User Interface) to monitor, control, and supervise operations in DIVArchive. Several DIVArchive GUIs can be running and connected to the same DIVArchive System at the same time.

DIVArchive Configuration Utility

You use the DIVArchive Configuration Utility to configure a DIVArchive System. Although used primarily for configuration of DIVArchive, some operational functions are also performed from the Configuration Utility.

DIVArchive Access Gateway

Access Gateway allows the operation and interaction of multiple independent DIVArchive systems from a single computer. It is the global solution for content distribution. Automated file replication to mirror sites provides a clean and easy method for local distribution, backup, and disaster recovery with security, bandwidth control, and checksum verification. Networks are monitored and DIVAnet ensures final delivery of content.

DIVArchive Local Delete

Local Delete is a service that monitors object replication functions between a local DIVArchive System (for example, DIVAlocal) and one (or more) remote DIVArchive Systems (for example, DIVAdr). Once the object has been successfully replicated to the remote DIVArchive System, it is flagged as eligible for deletion from the local DIVArchive System.

General Security Principles

The following sections describe the fundamental principles that are required to use any application securely.

Keep Software Up To Date

Stay current with the version of DIVArchive that you run. You can find current versions of the software for download at the Oracle Software Delivery Cloud:

<https://edelivery.oracle.com/>

Restrict Network Access to Critical Services

DIVArchive uses the following TCP/IP ports:

- DIVArchive Robot Manager uses tcp/8500
- DIVArchive Manager uses tcp/9000
- DIVArchive Backup Service uses tcp/9300
- DIVArchive Access Gateway uses tcp/9500
- DIVArchive Actor uses tcp/9900
- DIVArchive Migrate Service uses tcp/9191

Run as DIVA User and use Principle of Least Privilege where Possible

Do not run DIVArchive services using an Administrator (or Root) operating system user account. You must always run all DIVArchive services using a dedicated operating system user (or group) named DIVA.

The DIVArchive Control GUI provides three fixed user profiles (Administrator, Operator, and User). The Administrator and Operator accounts require a password to obtain access. You must assign an Administrator and (or) Operator password in the Configuration Utility before using these profiles.

You create passwords during installation and configuration for both the Administrator and Operator accounts. The passwords must be changed every 180 days (minimum) thereafter. Passwords must be made available for Oracle Support if needed.

Monitor System Activity

Monitor system activity to determine how well DIVArchive is operating and whether it is logging any unusual activity. Check the log files located in the installation directory under `/Program/log/`.

Keep Up To Date on Latest Security Information

You can access several sources of security information. For security information and alerts for a large variety of software products, see:

<http://www.us-cert.gov>

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

Secure Installation

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

Understand Your Environment

To better understand security needs, the following questions must be asked:

Which resources need to be protected?

You can protect many of the resources in the production environment. Consider the type of resources that you want to protect when determining the level of security to provide.

When using DIVArchive, protect the following resources:

Primary Data Disk

There are Data disk and Cache Disk resources used to build DIVArchive systems. They are typically local or remote disks connected to the DIVArchive systems. Independent access to these disks (other than by DIVArchive) 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 DIVArchive systems with complex objects. They are typically local or remote disks connected to the DIVArchive systems. Independent access to these disks (other than by DIVArchive) 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.

DIVArchive Tapes

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

Export Tape Metadata

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

Configuration Files and Settings

DIVArchive 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 (or group).

From whom are the resources being protected?

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

What will happen if the protections on strategic resources fail?

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

Recommended Deployment Topologies

This section describes how to install and configure an infrastructure component securely.

For information about installing DIVArchive, refer to DIVArchive 7.4 Customer Documentation Library at:

<https://docs.oracle.com/en/storage/#csm>

Consider the following points when installing and configuring DIVArchive:

Separate Metadata Network

For connection between DIVArchive services components with one another, Connection to 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 by 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 DIVArchive ports from the external WAN and any untrusted hosts on the network. See [Restrict Network Access to Critical Services](#).

FC Zoning

Use FC zoning to deny access to the DIVArchive disks connected through fibre 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. You must 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 DIVArchive Package

First, install only those DIVArchive services that you require. For example, if you do not plan to run the GUI or Configuration Utility from a system uncheck them in the list of components to be installed during installation. The default DIVArchive installation directory permissions and owners must be restricted to only the Administrator (or Root) account, or the DIVA operating system user (or group).

DIVArchive Tape Security

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

Backups

Set up and perform database backups using the DIVArchive 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 (or group).

Postinstallation Configuration

After installing any of the DIVArchive, go through the security checklist in [Appendix A](#).

Security Features

To avoid potential security threats, customers operating DIVArchive must be concerned about authentication and authorization of the system.

These security threats can be minimized by proper configuration and by following the postinstallation checklist in [Appendix A](#).

The Security Model

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

- Authentication - Ensures that only authorized individuals are granted access to the system and data.
- Authorization - Access control to system privileges and data. This feature builds on authentication to ensure that individuals get only appropriate access.

Authentication

The DIVArchive Control GUI provides three fixed user profiles (Administrator, Operator and User). The Administrator and Operator accounts require a password to obtain access. You must assign an Administrator and (or) Operator password in the Configuration Utility before using these profiles.

Both the Administrator and Operator account passwords must be changed every 180 days (or before). Passwords must be made available for Oracle Support if needed.

Access Control

Access control in DIVArchive is divided into three profiles. The Administrator and Operator accounts require a password to obtain access. You must assign an Administrator and (or) Operator account password in the Configuration Utility before using these profiles.

User - After the connection to the DIVArchive Manager is established, the Control GUI will only allow the user to monitor DIVArchive operations, and retrieve data from the database. This is known as the User Profile. Not all functions that issue commands to DIVArchive are accessible while in the User profile mode, enabling situations where monitoring is required but no commands are permitted to be sent to DIVArchive.

Administrator - To issue requests to DIVArchive, such as archive or restore requests, or to eject a tape from a library, you must change to the Administrator Profile. The Administrator Profile is password protected. The password for this profile must be assigned in the Configuration Utility before using the profile. For more information, refer to the Oracle DIVArchive 7.4 Customer Documentation Library at:

<https://docs.oracle.com/en/storage/#csm>

Operator - In addition to User Profile permissions, the operator profile provides access to the Object Transfer Utility and requires a password configured in the Configuration Utility before using the profile.

Secure Deployment Checklist

1. Set strong passwords for Administrator (or Root) and any other operating system accounts that have any DIVArchive administrator or service roles assigned to them, including:
 - DIVA, Oracle 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. Set a strong password for Administrator and Operator for the Control GUI. You must assign a password for these profiles in the Configuration Utility before use.
4. Set a strong password for the Oracle database login.
5. Install a firewall on every system and apply the default DIVArchive port rules. Restrict access to DIVArchive API (`tcp/9000`) to IP's that need access using firewall rules.
6. Install operating system and DIVArchive updates on a periodic basis since they include security updates.
7. Install Anti-virus and exclude the DIVArchive processes and storage (for performance reasons).
8. 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 DIVArchive 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.
9. Set up an appropriate set of backups of the DIVArchive configuration and database. Backups are part of security and provide a way of restoring data lost either accidentally, or through some type of breach. Your backup should include some policy while being transported to an offsite location. Backups need to be protected to the same degree as DIVArchive tapes and disk.

