Oracle® DIVArchive

Security Guide

Release 7.6.1

E84062-02

December 2017

ORACLE

Oracle DIVArchive Security Guide, Release 7.6.1

E84062-02

Contents

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.

Related Documents

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

1

Overview

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 Oracle DIVArchive documentation set for this release located 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 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 Oracle DIVArchive documentation set for this release located 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 DFM (Drop Folder Monitor)

The DIVArchive DFM (Drop Folder Monitor) 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 (Simple Network Management Protocol)

The DIVArchive SNMP (Simple Network Management Protocol) Agent and MIB (Management Information Base) 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 SPM (Storage Plan Manager)

The DIVArchive SPM (Storage Plan Manager) 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 separate internal (to DIVArchive) service that 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

The 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 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

The 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/8000` for secure connections (this is the default), and `tcp/9000` to accommodate legacy versions of the DIVArchive API to connect to the DIVArchive 7.6 Manager.
- 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 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 release of the DIVArchive software.

2

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 operations contain data and metadata. This data and metadata permissions must be restricted to only the Administrator (or root) operating system account, or the DIVA operating system user (or 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 sections must be protected from all non-administrator access on a configured system, or from a rogue external system that can access these resources through the WAN or FC Fabric.

What will happen if the protections on strategic resources 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 more information, see the Oracle DIVArchive documentation set for this release located at `https://docs.oracle.com/en/storage/#csm`.

Consider the following points when installing and configuring DIVArchive:

Separate Metadata Network

For connections between DIVArchive services components, 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 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 the 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, then 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.

3

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 post-installation 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.
- Tape Group Encryption - Tape drive encryption securely supports bulk tape migration between DIVArchive systems.
- SSL Authentication and Secure Communications - DIVArchive 7.6 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.

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 and *Advanced 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. Both Operator and Advanced Operator profiles in the Control GUI can now optionally enable privileges for canceling and changing the priority of requests. The options are defined in the Manager Configuration panel of the Configuration Utility. By default, this option is *disabled*.

Tape Group Encryption

Starting with the DIVArchive 7.6 release, tape drive encryption securely supports bulk tape migration between DIVArchive systems.

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. 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.

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) and Authentication

DIVArchive 7.6 introduces SSL Certificate Authentication for authentication of services, and securing the internal and API communications in DIVArchive. Certificate authentication provides unique identification and secure communications for each DIVArchive service in a network.

DIVArchive 7.6 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.

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 (Secure Sockets Layer) certificates are signed by a recognized CA (Certificate Authority). 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.

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.

External Certificate Authorities

You can use external third party CAs (for example, VeriSign, Comodo, and so on) with DIVArchive. 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 certificate chain.

Security Tools

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

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

The tool is located in the `%DIVA_HOME%/security/bin` directory.

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 (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.

SSL (Secure Sockets Layer) and Authentication

DIVArchive consist of services in Java and C++. The format in how certificates and keys are represented are different in each. DIVArchive 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 DIVArchive 7.6 services (Control GUI, Configuration Utility, DBBackup, Migration Utility, Actor, SPM, DFM, SNMP, Robot Manager, RDTU, and Migration 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. Clients using the Java or 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 Controler (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 `%DIVA_API_HOME%/security` is added to the DIVArchive API installation structure as follows:

```
%DIVA_API_HOME%
    security
      conf
```

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

See the *Oracle DIVArchive Java API* documentation included with the API, and the *Oracle C++ API Programer's Guide* in the *Oracle DIVArchive Additional Features documentation* library for detailed information.

Secure Communication with Oracle Database

With DIVA 7.6.1, 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.

A

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.
10. Oracle strongly recommends using an external CA for additional security.