Oracle® DIVAdirector

Security Guide

Release 5.3

E69746-01

December 2015

ORACLE®

Oracle DIVAdirector Security Guide, Release 5.3

E69746-01

Primary Author: Lou Bonaventura

Contents

Preface v

Audience v
Documentation Accessibility v

1 Overview

Product Overview 1-1
DIVAdirector Server 1-1
DIVAdirector Web 1-1
DIVAdirector Database 1-1
DIVAdirector Transcoder Service 1-1
DIVAdirector Task Manager Service 1-2
DIVAdirector API Service 1-2
General Security Principles 1-2
Keep Software up To Date 1-2
Restrict Network Access to Critical Services 1-2
Run as ADMIN user and use Principle of Least Privilege where Possible 1-2
Monitor System Activity 1-3
Keep Up To Date on Latest Security Information 1-3

2 Secure Installation

Understand Your Environment 2-1
Which resources need to be protected? 2-1
Primary Data Disk 2-1
Database Disk and Backup Disks 2-1
Configuration Files and Settings 2-1
From whom are the resources being protected? 2-2
What will happen if the protections on strategic resources fail? 2-2

3 Security Features

The Security Model 3-1

A Secure Deployment Checklist

Preface

Oracle's DIVAdirector Security Guide includes information about the DIVAdirector 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 DIVAdirector.

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.

1

Overview

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

Product Overview

Oracle DIVAdirector is a tool for interacting with existing Oracle DIVArchive systems. The User Interface (UI) is delivered graphically through a web browser. DIVAdirector consists of the following major components:

DIVAdirector Server

The DIVAdirector Server provides interfaces with DIVArchive through the C++ API for all operations which are requested by DIVAdirector Web. It also synchronizes discovered object info stored in DIVArchive into its own database. It monitors configured drop folders for proxies, metadata and for operations, and maintains history of all drop folders and UI operations.

DIVAdirector Web

The web module of DIVAdirector provides a Web-based UI interface, allowing users to search for discovered objects in DIVArchive, administer user access rights, add metadata for assets, play proxies of objects and perform operations such as restore, partial restore and delete, on items added to work bins or shot lists. It also provides users the ability to browse files locally and to archive content to the DIVArchive system.

DIVAdirector Database

DIVAdirector uses PostgreSQL to store all DIVArchive assets information, metadata, proxy info, user information, operation history, and configuration settings.

DIVAdirector Transcoder Service

The DIVAdirector Transcoder Service is a separate service that is called by DIVAdirector to transcode high resolution clips to low resolution proxies which are then shown within the DIVAdirector Web UI.

DIVAdirector Task Manager Service

The DIVAdirector Task Manager Service is a windows service application visible in the standard Services Control Manager dialog box. This application is responsible for executing potentially long-running tasks in a background process.

DIVAdirector API Service

This service exposes endpoints for common DIVAdirector functionality. Initially, only a small subset of DIVAdirector's logic will be contained in this service. The endpoints exposed through this service will continue to grow as functionality is gradually migrated away from DIVAdirector Web.

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 DIVAdirector 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

DIVAdirector uses the following TCP/IP ports:

- tcp/7680 for user interface commands
- tcp/8080 for the HTTP Server

For DIVAdirector releases later than 5.3.0, three additional ports are needed:

- tcp/9763 - DIVArchiveWS Service integration.
- tcp/9876 - DIVAtranscode Service integration.
- tcp/6543 - DIVAdirector API Service integration.

> **Note:** The port numbers listed above are current, however they are likely to change in the future.

Run as ADMIN user and use Principle of Least Privilege where Possible

DIVAdirector provides a default Super Admin user whose password should be changed after first login. Then this user can create other users with different group permissions for access and operations.

If the default password is not changed, it leaves the system accessible to possible malicious activity. The default password must be changed immediately after installation and configuration for the Super Admin account, and every 180 days (minimum) thereafter. Once the change has been made, you must store the passwords in a safe location, offline, where they can be made available for Oracle Support if needed.

Monitor System Activity

You can monitor system activity to determine how well DIVAdirector is operating. Logs are located at C:\Program Files (x86)\DIVAdirector 5\cmg-server and C:\Program Files (x86)\DIVAdirector 5\www\logs.

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 DIVAdirector 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 DIVAdirector, protect the following resources:

Primary Data Disk

There are proxy folders containing low resolution clips. They are primarily on local or remote disks connected to the DIVAdirector system. Independent access to these disks (not through DIVAdirector) 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 and Backup Disks

There are Database Disk and Backup Disk resources used to build DIVAdirector. They are typically local or remote disk connected to the DIVAdirector systems. Independent access to these disks (not through DIVAdirector) 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.

Configuration Files and Settings

DIVAdirector system configuration settings must be protected from operating system (OS) level non-administrator users. In general, these settings are protected automatically by OS level administrative users. Note that making the configuration files writable to non-administrative OS users presents a security risk. Sensitive files encompass all application configuration files contained in the installation directory including:

- www\Web.config
- Api\Oracle.DIVAdirector.Api.exe.config
- TaskManager\Oracle.DIVAdirector.TaskManager.exe.config
- cmgserver\cmgserver.ini

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 by means of 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 DIVAdirector operations) to data corruption (writing to disk or tape outside of normal permissions).

3

Security Features

To avoid potential security threats, customers operating DIVAdirector 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, "Secure Deployment Checklist".

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.

A

Secure Deployment Checklist

1. Set strong passwords for the Administrator and any other OS accounts that have any DIVArchive or DIVAdirector administrator or service roles assigned to them.
2. Do not use a local administrator OS account but rather assign roles as needed to other user accounts.
3. Set a strong password for the DIVAdirector Administrator user. Change the password right away from the default installed password to a strong password. You can do this from the DIVAdirector **Admin**, **Personal** settings screen.
4. Install a firewall on the system and apply the default DIVAdirector port rules.
5. Install OS and DIVAdirector updates on a periodic basis since they include security patches.
6. Install antivirus and exclude the DIVAdirector processes and storage for performance reasons.