Oracle® DIVAdirector

Security Guide

Release 5.4

E86635-01

May 2017

ORACLE®

Oracle DIVAdirector Security Guide, Release 5.4

E86635-01

Primary Author: Lou Bonaventura

Contents

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, explains the general principles of application security, and includes the following information:

Product Overview

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

DIVAdirector Web

The web module of DIVAdirector provides a Web based UI interface, enabling you 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, Oracle Partial File Restore, and Delete on items added to *Work Bins* or *Shot Lists*. It also gives you 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 Transcode Service

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

DIVAdirector TaskManager Service

The DIVAdirector TaskManager Service is a Windows Service 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 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.

Keeping Software Up To Date

Stay current with the DIVAdirector release that you run. You can find current releases of the software for download at the Oracle Software Delivery Cloud:

`https://edelivery.oracle.com/`

Restricting Network Access to Critical Services

DIVAdirector uses the following TCP/IP ports:

- `tcp/8080` for the HTTP server

For DIVAdirector releases later than 5.4, three additional ports are needed as follows:

- `tcp/9444` for DIVA Enterprise Connect Service integration
- `tcp/9876` for DIVAtranscode Service integration
- `tcp/6543` for DIVAdirector API Service integration

> **Note:** The port numbers listed are current for this release.

Run as `admin` user and use Principle of Least Privilege where Possible

DIVAdirector provides a default *SystemAdmins* group with an `admin` user, whose password will be changed on the first log in. The `admin` password will be reset on the first log in. Beyond that, the `admin` user follows the same password rules as all other users. The `admin` user can then create other users with different group permissions for access and operations.

All passwords automatically expire every 90 days. Users are prompted for new passwords after successfully logging in after this expiration occurs.

After a password change has been made, the passwords must be stored in a safe location (offline recommended) where they can be made available for Oracle Support if needed.

Creating Users, Groups, and Organizations

DIVAdirector uses individual user profiles who's permissions and access rights are based on the group they belong to. These groups have a range of permissions related to different functional areas of the application and specific custom metadata permissions. Similarly, the group's LDAP and SMTP configuration are governed by their Organization, and metadata permissions are inherited from them. *See the Oracle DIVAdirector Administrator's Guide for configuration details*.

Monitoring System Activity

DIVAdirector uses a centralized logging framework for system events. Log files for individual components can be found in the `\logs` subdirectory for that component. For example, the TaskManager specific logs can be found in `C:\Program Files (x86)\DIVAdirector 5\TaskManager\logs`. The API logs are located in the `C:\Program Files (x86)\DIVAdirector 5\Api\log` folder.

You can also observe a live view of the entire system by configuring an appropriate `log4net` viewer, and component `log4net.config` file.

Keeping Up To Date on Latest Security Information

You can access several sources of security information. See `http://www.us-cert.gov` for security information and alerts for a large variety of software products.

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

2

Secure Installation

This chapter outlines the planning process for a secure installation, describes several recommended deployment topologies for the systems, and includes the following information:

Understanding 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 disks 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 level non-administrator users. In general, these settings are protected automatically by operating system level administrative users. Making the configuration files writable to non-administrative operating system 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`
- `DIVAdirector Database\pg_hba.conf`
- `DIVAdirector Database\postgresql.conf`

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 where data is accessed outside of normal DIVAdirector operations, to data corruption when there is writing to disk or tape outside of normal permissions.

Installing and Upgrading Custom Certificates

By default, DIVAdirector will install a generic `DD5` certificate for securing connections. During installation you are presented the option to upload your own certificate. Your certificate must be approved by a certificate authority. If you want to upgrade your certificate after installation, run the *Oracle DIVAdirector Certificate Utility* and follow the prompts to import the new certificate.

Securing the Connection to Oracle DIVA Enterprise Connect

Connections to Oracle DIVA Enterprise Connect (DIVAEC) can, and should, be secured using the certificate provided by the DIVAEC installer (see the *Oracle DIVA Enterprise Connect Installation, Configuration, and Operations Guide*, and the *Oracle DIVA Enterprise Connect Security Guide* for details). This certificate must be installed into the *Local Machine – Trusted Root Authority*, and you must place a reference to it in the Windows `hosts` file under `C:\Windows\System32\drivers\etc\hosts`. After you enter the information in the `hosts` file, you must set the following keys to the provided host name:

Configuration Files:

```
C:\Program Files (x86)\DIVAdirector 5\www\Web.config

C:\Program Files (x86)\DIVAdirector
5\TaskManager\Oracle.DIVAdirector.TaskManager.exe.config
```

Key to Modify:

```
<add key="DIVArchiveApiUrl" value="https://<new host
```

```
name>:9444/diva/service/rest/2.2/DIVArchiveWS_REST" />
```

PostgreSQL SSPI Pass-Through Authentication Setup

You can set up *PostgreSQL SSPI Pass-Through Authentication* after DIVAdirector is upgraded if you are using the same domain user account to run all DIVAdirector services, the IIS application pool, and PostgreSQL. This configuration removes the need to have plain text user names and passwords in the connection strings.

Follow the instructions at https://wiki.postgresql.org/wiki/Configuring_for_single_sign-on_using_SSPI_on_Windows to enable SSPI for PostgreSQL.

After you complete the instructions, you must update the configuration files for each of the following DIVAdirector services. You must modify the configuration files in the following default locations:

Oracle DIVAdirector Web Service

```
C:\Program Files(x86)\DIVAdirector 5\www\Web.config
```

Oracle DIVAdirector TaskManager

```
C:\Program Files (x86)\Divadirector
5\TaskManager\Oracle.DIVAdirector.TaskManager.exe.config
```

Oracle DIVAdirector API

```
C:\Program Files (x86)\Divadirector 5\Api\Oracle.DIVAdirector.Api.exe.config
```

Oracle DIVAdirector Annotation Import Service

```
C:\Program Files (x86)\Divadirector
5\Tools\DDServices\DIVADirectorServices.exe.config
```

In each of the services the key will be the same:

```
<connectionStrings>
   <add name="DIVAdirectorContext"
connectionString="Server=localhost;Database=DIVAdirector;User
Id=postgres;Password=MANAGER;" providerName="Npgsql"
    />
</connectionStrings>
```

You must modify the connection string parameter as follows:

```
connectionString="Server=localhost;Database=DIVAdirector;Integrated
Security=true;Include Realm=true;"
```

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.

This chapter includes the following information:

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.

TLS 1.2

TLS 1.2 is implemented for Oracle DIVAdirector API, and the DIVAdirector Web Interface. This has been accomplished by upgrading the framework to .Net 4.6.2, which uses TLS 1.2 by default.

Hashing Algorithm Specifics

DIVAdirector now uses the PBKDF2 algorithm with an injectable hashing function which is currently set to SHA512. Salts are randomized, provided on a per password basis, and the iteration count is progressive (based on year) with a minimum of 10000 hashing iterations. Passwords are stored with their hash and iteration count in the

database with a history of previous passwords to ensure that the complexity requirements are met. The old MD5 hashing algorithm still exists within the code base exclusively to provide a path to reset passwords using the new algorithm.

Securing Proxy Storage, IIS, and PostgreSQL Connections

Customers are required to use a domain account for securing connections to remote proxy storage, IIS, and PostgreSQL. The installer still creates a `dd5-user` account by default. However, this account must be changed immediately using the steps outlined in the *Oracle DIVAdirector Installation Guide*. There are two reasons for this change:

- It centralizes and simplifies the operating system permissions required to perform application tasks.
- It is required to configure PostgreSQL to use SSPI connections.

Updating PostgreSQL Connection Strings

You can set up *PostgreSQL SSPI Pass-Through Authentication* after DIVAdirector is upgraded if you are using the same domain user account to run all DIVAdirector services, the IIS application pool, and PostgreSQL. This configuration removes the need to have plain text user names and passwords in the connection strings.

Follow the instructions at https://wiki.postgresql.org/wiki/Configuring_for_single_sign-on_using_SSPI_on_Windows to enable SSPI for PostgreSQL.

After you complete the instructions, you must update the configuration files for each of the following DIVAdirector services. You must modify the configuration files in the following default locations:

Oracle DIVAdirector Web Service

```
C:\Program Files(x86)\DIVAdirector 5\www\Web.config
```

Oracle DIVAdirector TaskManager

```
C:\Program Files (x86)\Divadirector
5\TaskManager\Oracle.DIVAdirector.TaskManager.exe.config
```

Oracle DIVAdirector API

```
C:\Program Files (x86)\Divadirector 5\Api\Oracle.DIVAdirector.Api.exe.config
```

Oracle DIVAdirector Annotation Import Service

```
C:\Program Files (x86)\Divadirector
5\Tools\DDServices\DIVADirectorServices.exe.config
```

In each of the services the key will be the same:

```
<connectionStrings>
   <add name="DIVAdirectorContext"
connectionString="Server=localhost;Database=DIVAdirector;User
Id=postgres;Password=MANAGER;" providerName="Npgsql"
    />
</connectionStrings>
```

You must modify the connection string parameter as follows:

```
connectionString="Server=localhost;Database=DIVAdirector;Integrated
Security=true;Include Realm=true;"
```

You can secure your connections using SSL as follows:

```
connectionString="Server=localhost;Database=DIVAdirector;Integrated
Security=true;Include Realm=true; SSL Mode=Require;"
```

Archive Page Source/Destination File Viewer

Due to security concerns with the implementation of the file viewer on the **Archive** page, a new feature allows the manipulation of files on connected sources. To secure these connections DIVadirector authenticates user log ins, group configuration allows only specific access, and session timeouts log out unattended sessions.

Removal of Flat File Export Feature

Flat File Export allowed users to export database tables into `csv` files and download them through the Web Interface. The option to export database tables as flat files through the DIVAdirector interface has been removed due to security concerns. Oracle is currently reexamining use cases for this functionality to determine whether to re-implement it in a different form on a per use case basis in such a way that you are not exposed to the same risk.

A

Secure Deployment Checklist

1. Set strong passwords for the Administrator and any other operating system accounts that have any DIVArchive, DIVAdirector, administrator, or service roles assigned to them.
2. Do not use a local administrator operating system account but rather assign roles as needed to other user accounts.
3. Set a strong password for the DIVAdirector Administrator user. Change the password immediately from the default installed password to a strong password. You will be prompted to do this automatically when you first log in.

   Note: A password recovery feature is available to users on the log on screen if they forget their password.

4. Install a firewall on the system and apply the default DIVAdirector port rules.
5. Install operating system and DIVAdirector updates on a periodic basis because they include security patches.
6. Install antivirus, and exclude the DIVAdirector processes and storage for performance reasons.