Oracle® DIVAdirector

安全指南

发行版 5.3

E71128-01

2015 年 12 月

ORACLE®

Oracle® DIVAdirector
安全指南

E71128-01

目录

前言

《Oracle DIVAdirector 安全指南》包括 DIVAdirector 产品的相关信息并介绍了应用程序的一般安全原则。

目标读者

本指南的目标读者是要使用 DIVAdirector 的安全功能以及要安全可靠地安装和配置 DIVAdirector 的所有人。

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获得 Oracle 支持
购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

1

第 1 章 概述

本章概述了 DIVAdirector 产品并介绍了应用程序的一般安全原则。

1.1. 产品概述

Oracle DIVAdirector 是一款与现有 Oracle DIVArchive 系统交互的工具。用户界面 (User Interface, UI) 通过 Web 浏览器以图形方式提供。DIVAdirector 主要包括以下组件：

1.1.1. DIVAdirector 服务器

DIVAdirector 服务器通过 C++ API 为 DIVAdirector Web 请求的所有操作提供与 DIVArchive 的接口。它还将发现的对象存储在 DIVArchive 中的信息同步到自己的数据库中。它监视所配置的代理、元数据和操作的放置文件夹，并维护所有放置文件夹和 UI 操作的历史记录。

1.1.2. DIVAdirector Web

DIVAdirector 的 Web 模块提供基于 Web 的 UI 界面，用户可通过该界面搜索在 DIVArchive 中发现的对象，管理用户访问权限，添加资产元数据，播放对象的代理，以及对添加到材料箱或拍摄程序表中的项目执行恢复、部分恢复以及删除等操作。还支持用户在本地浏览文件，以及将内容归档到 DIVArchive 系统。

1.1.3. DIVAdirector 数据库

DIVAdirector 使用 PostgreSQL 存储所有 DIVArchive 资产信息、元数据、代理信息、用户信息、操作历史记录以及配置设置。

1.1.4. DIVAdirector 转码器服务

DIVAdirector 转码器服务是一个由 DIVAdirector 调用的单独服务，用于将高分辨率的剪辑转码为低分辨率的代理，然后剪辑就可以在 DIVAdirector Web UI 中显示。

1.1.5. DIVAdirector 任务管理器服务

DIVAdirector 任务管理器服务是一个 Windows 服务应用程序，可在标准的“服务控制管理器”对话框中查看。此应用程序负责在后台进程中执行可能长期运行的任务。

1.1.6. DIVAdirector API 服务

此服务为常用的 DIVAdirector 功能公开端点。最初，此服务只包含 DIVAdirector 逻辑的一小部分。随着功能逐渐迁出 DIVAdirector Web，通过此服务公开的端点将继续增加。

1.2. 一般安全原则

以下各节介绍了安全使用任何应用程序都需要遵守的基本原则。

1.2.1. 保持软件为最新版本

使运行的 DIVAdirector 的版本保持最新。可在 Oracle Software Delivery Cloud 上查找并下载最新的软件版本，网址为：

https://edelivery.oracle.com/

1.2.2. 限制对关键服务的网络访问

DIVAdirector 使用以下 TCP/IP 端口：

- tcp/7680 用于用户界面命令
- tcp/8080 用于 HTTP 服务器

高于 5.3.0 的 DIVAdirector 发行版还需要另外三个端口：

- tcp/9763－DIVArchiveWS 服务集成。
- tcp/9876－DIVAtranscode 服务集成。
- tcp/6543－DIVAdirector API 服务集成。

注意:

上面列出的端口号是最新的端口号，但是将来可能会更改。

1.2.3. 以 ADMIN 用户身份运行并尽可能使用最小特权原则

DIVAdirector 提供了默认的 Super Admin 用户，其密码应该在第一次登录后更改。然后，此用户可以创建对访问和操作具有不同组权限的其他用户。

如果默认密码未更改，系统就可能受到恶意行为的威胁。对于 Super Admin 帐户，需要在安装和配置后立即更改默认密码，之后至少每 180 天更改一次。在更改后，您必须将密码存放在一个安全的脱机位置，这样在需要时可以将其提供给 Oracle 技术支持。

1.2.4. 监视系统活动

可以监视系统活动进而确定 DIVAdirector 的运行状况。日志位于 C:/Program Files (x86)/DIVAdirector 5/cmg-server 和 C:/Program Files (x86)/DIVAdirector 5/www/logs。

1.2.5. 密切关注最新安全信息

可以从多个来源获取安全信息。有关各种软件产品的安全信息和警报，请访问：

http://www.us-cert.gov

及时解决最新安全问题的主要方式是运行最新版本的 DIVAdirector 软件。

2

第 2 章 安全安装

本章概述了安全安装的规划过程并介绍了建议系统使用的一些部署拓扑结构。

2.1. 了解环境

要更好地了解安全需求，必须回答以下问题：

2.1.1. 需要保护哪些资源?

您可以保护生产环境中的很多资源。确定要提供的安全级别时，请考虑要保护的资源的类型。使用 DIVAdirector 时，要保护以下资源：

2.1.1.1. 主数据磁盘

有一些包含低分辨率剪辑的代理文件夹。这些文件夹主要位于连接到 DIVAdirector 系统的本地或远程磁盘上。对这些磁盘的独立访问（不通过 DIVAdirector）会带来安全问题。这种外部访问可能来自试图读取或写入这些磁盘的恶意系统，也可能来自无意中对这些磁盘提供访问的内部系统。

2.1.1.2. 数据库磁盘和备份磁盘

有一些用作 DIVAdirector 基础的数据库磁盘和备份磁盘资源。这些资源通常位于连接到 DIVAdirector 系统的本地或远程磁盘上。对这些磁盘的独立访问（不通过 DIVAdirector）会带来安全问题。这种外部访问可能来自试图读取或写入这些磁盘的恶意系统，也可能来自无意中对这些磁盘提供访问的内部系统。

2.1.1.3. 配置文件和设置

必须防止操作系统 (operating system, OS) 级的非管理员用户访问 DIVAdirector 系统配置设置。通常情况下，只有 OS 级的管理用户可以访问这些设置，系统自动提供此保护。请注意，使配置文件对非管理 OS 用户可写存在安全风险。敏感文件涵盖安装目录中包含的所有应用程序配置文件，包括：

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

2.1.2. 要避免资源被哪些用户访问?

通常，必须阻止所有非管理员在已配置的系统上访问上一节中描述的资源，还必须阻止可以通过 WAN 或 FC 结构访问这些资源的外部恶意系统来访问这些资源。

2.1.3. 如果对战略性资源的保护失败，将会产生什么后果?

保护战略性资源失败会产生许多问题，包括非正常访问（即，在正常 DIVAdirector 操作之外访问数据）、数据损坏（在没有正常权限的情况下写入磁盘或磁带）等。

3

第 3 章 安全功能

要避免潜在的安全威胁，客户操作 DIVAdirector 时必须关注系统的验证和授权。

通过正确配置以及遵循附录 A, 安全部署核对表中的安装后核对表，可最大程度地减少这些安全威胁。

3.1. 安全模型

针对安全威胁提供保护的关键安全功能包括：

- 验证－确保仅为已授权的个人授予对系统和数据的访问权限。
- 授权－对系统特权和数据的访问控制。此功能基于验证构建，用于确保个人只获取相应的访问权限。

附录 A

附录 A. 安全部署核对表

1. 为管理员或任何分配有 DIVArchive 或 DIVAdirector 管理员或服务角色的其他 OS 帐户设置强密码。
2. 请勿使用本地管理员 OS 帐户，而应根据需要将角色分配给其他用户帐户。
3. 为 DIVAdirector 管理员用户设置强密码。立刻将安装的默认密码更改为强密码。可以通过 DIVAdirector **Admin**、**Personal** 设置屏幕执行此操作。
4. 在系统上安装防火墙并应用默认 DIVAdirector 端口规则。
5. 定期安装 OS 和 DIVAdirector 更新，因为其中包含安全修补程序。
6. 安装防病毒软件，出于性能原因，请将 DIVAdirector 进程和存储排除在监视范围之外。