Oracle® DIVAdirector

安全指南

版本 5.3

E71129-01

2015 年 12 月

ORACLE®

Oracle® DIVAdirector
安全指南

E71129-01

版權 © 2015, Oracle 和 (或) 其關係公司。保留一切權利。

本軟體與相關說明文件是依據含有用途及保密限制事項的授權合約所提供，且受智慧財產法的保護。除了授權合約中或法律明文允許的部分外，不得以任何形式或方法使用、複製、重製、翻譯、廣播、修改、授權、傳送、散佈、展示、演出、出版或陳列本軟體的任何部分。除非依法需要取得互通性操作 (interoperability)，否則嚴禁對本軟體進行還原工程 (reverse engineering)、反向組譯 (disassembly) 或解編 (decompilation)。

本文件中的資訊如有變更恕不另行通知，且不保證沒有任何錯誤。如果您發現任何問題，請來函告知。

如果本軟體或相關說明文件是提供給美國政府或代表美國政府授權使用本軟體者，則適用下列條例：

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.

本軟體或硬體是針對各類資訊管理應用的一般用途所開發。不適用任何原本就具危險性的應用上，包含會造成人身傷害風險的應用。如果您將本軟體或硬體應用於危險用途，則應採取適當的防範措施，包括保全、備份、儲備和其他措施以確保使用安全。Oracle Corporation 和其關係公司聲明對將本軟體或硬體應用於危險用途所造成之損害概不負任何責任。

Oracle 和 Java 是 Oracle 和 (或) 其關係公司的註冊商標。其他名稱為各商標持有人所擁有之商標。

Intel 和 Intel Xeon 是 Intel Corporation 的商標或註冊商標。所有 SPARC 商標的使用皆經過授權，且是 SPARC International, Inc. 的商標或註冊商標。AMD、Opteron、AMD 標誌與 AMD Opteron 標誌是 Advanced Micro Devices 的商標或註冊商標。UNIX 是 The Open Group 的註冊商標。

本軟體或硬體與說明文件可能提供第三方內容、產品和服務的存取途徑與資訊。除非您與 Oracle 之間的適用合約另有規定，否則 Oracle Corporation 和其關係公司明文聲明對第三方網站所提供的內容、產品與服務不做保證，且不負任何責任。除非您與 Oracle 之間的適用合約另有規定，否則 Oracle Corporation 和其關係公司對於您存取或使用第三方的內容、產品或服務所引起的任何損失、費用或損害亦不負任何責任。

內容

序言 5

對象 5
文件輔助功能 5

1. 簡介 7

1.1. 產品簡介 7
1.1.1. DIVAdirector 伺服器 7
1.1.2. DIVAdirector Web 7
1.1.3. DIVAdirector 資料庫 7
1.1.4. DIVAdirector Transcoder Service 7
1.1.5. DIVAdirector Task Manager Service 7
1.1.6. DIVAdirector API Service 8
1.2. 一般安全原則 8
1.2.1. 將軟體保持在最新狀態 8
1.2.2. 限制對重要服務的網路存取 8
1.2.3. 儘可能以 ADMIN 使用者身分執行，並採用最低權限原則 8
1.2.4. 監督系統活動 8
1.2.5. 將安全資訊保持在最新狀態 9

2. 安全安裝 11

2.1. 瞭解您的環境 11
2.1.1. 需要保護哪些資源？ 11
2.1.1.1. 主要資料磁碟 11
2.1.1.2. 資料庫磁碟和備份磁碟 11
2.1.1.3. 配置檔和設定值 11
2.1.2. 必須防止哪些人存取資源？ 12
2.1.3. 策略性資源的保護萬一失敗將發生什麼情況？ 12

3. 安全功能 13

3.1. 安全模型 13

A. 安全建置檢查清單 15

前言

「Oracle DIVAdirector 安全指南」包含 DIVAdirector 產品的相關資訊，以及應用程式安全性的一般原則。

對象

本指南適用於使用 DIVAdirector 安全功能、安全安裝及配置的相關人員。

文件輔助功能

如需 Oracle 對於輔助功能的承諾的相關資訊，請造訪 Oracle Accessibility Program 網站，網址為 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

取用 Oracle Support
已購買支援的 Oracle 客戶可以透過 My Oracle Support 使用電子支援。如需相關資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；或如果您在聽力上需要特殊服務，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

1

第 1 章 簡介

本章提供 DIVAdirector 產品的概覽，以及說明應用程式安全性的一般原則。

1.1. 產品簡介

Oracle DIVAdirector 是一種可與現有 Oracle DIVArchive 系統互動的工具。其使用者介面 (UI) 是透過 Web 瀏覽器以圖形方式提供。DIVAdirector 的主要組成元件如下：

1.1.1. DIVAdirector 伺服器

DIVAdirector 伺服器透過 C++ API 提供 DIVArchive 介面，以處理 DIVAdirector Web 要求的所有作業。同時會將在儲存於 DIVArchive 中發現的物件資訊同步到自己的資料庫。它會監督針對代理項目、描述資料以及作業所配置的捨棄資料夾，並維護所有捨棄資料夾和 UI 作業的歷史記錄。

1.1.2. DIVAdirector Web

DIVAdirector 的 Web 模組提供 Web 形式的 UI 介面，讓使用者能夠搜尋在 DIVArchive 中發現的物件、管理使用者存取權、新增資產的描述資料、執行物件的代理項目，以及對新增至工作筒 (work bin) 或分鏡表 (shot list) 的項目執行回復、部分回復及刪除等作業。它同時提供使用者本機瀏覽檔案以及將內容歸檔至 DIVArchive 系統的能力。

1.1.3. DIVAdirector 資料庫

DIVAdirector 使用 PostgreSQL 來儲存所有 DIVArchive 資產資訊、描述資料、代理資訊、使用者資訊、作業歷史記錄以及配置設定值。

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service 是由 DIVAdirector 呼叫的個別服務，用來將高解析度片段轉碼成為可在 DIVAdirector Web UI 中顯示的低解析度代理項目。

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service 是一個視窗服務應用程式，可在標準的「服務控制管理員 (SCM)」對話方塊中看到。此應用程式負責在背景處理作業中執行可能會長時間執行的工作。

1.1.6. DIVAdirector API Service

此服務會公開一般 DIVAdirector 功能的端點。此服務中一開始只會包含 DIVAdirector 邏輯的小型子集。隨著功能漸漸從 DIVAdirector Web 移轉過來，透過此服務公開的端點將會持續增加。

1.2. 一般安全原則

下列各節描述安全地使用任何應用程式所需的基本原則。

1.2.1. 將軟體保持在最新狀態

讓您執行的 DIVAdirector 保持在最新的版本。您可以在 Oracle Software Delivery Cloud 找到最新版本的軟體以進行下載：

https://edelivery.oracle.com/

1.2.2. 限制對重要服務的網路存取

DIVAdirector 使用下列 TCP/IP 連接埠：

- 使用者介面命令使用 tcp/7680
- HTTP 伺服器使用 tcp/8080

對於 DIVAdirector 5.3.0 以後的版本，另外還需要 3 個連接埠：

- DIVArchiveWS Service 整合使用 tcp/9763。
- DIVAtranscode Service 整合使用 tcp/9876。
- DIVAdirector API Service 整合使用 tcp/6543。

注意:

以上所列的都是目前使用的連接埠號碼，這些日後可能會有所變更。

1.2.3. 儘可能以 ADMIN 使用者身分執行，並採用最低權限原則

DIVAdirector 提供預設的 Super Admin 使用者，在首次登入之後應變更其密碼。然後此使用者便可針對存取權和作業，建立具有不同群組權限的其他使用者。

若未變更預設密碼，可能會讓系統被惡意活動存取。在安裝與配置 Super Admin 帳號之後，必須立即變更預設密碼，而且之後每隔 180 天 (至少) 都要加以變更。進行變更之後，您必須將密碼以離線方式儲存在安全的位置，以便在需要時可提供給「Oracle 客戶服務部」使用。

1.2.4. 監督系統活動

您可以監督系統活動以判斷 DIVAdirector 運作的情形。日誌位於 C:/Program Files (x86)/DIVAdirector 5/cmg-server 和 C:/Program Files (x86)/DIVAdirector 5/www/logs。

1.2.5. 將安全資訊保持在最新狀態

您可以存取數個安全資訊來源。如需各種軟體產品的安全資訊和警示，請參閱：

http://www.us-cert.gov

持續更新安全的主要方法就是執行最新版本的 DIVAdirector 軟體。

2

第 2 章 安全安裝

本章概述安全安裝的計畫程序，以及描述數種建議的系統建置拓樸。

2.1. 瞭解您的環境

為了更進一步瞭解安全需求，請考量下列問題：

2.1.1. 需要保護哪些資源？

您可以保護生產環境中的許多資源。請考量您想要保護的資源類型，然後決定提供的安全層級。使用 DIVAdirector 時，請保護下列資源：

2.1.1.1. 主要資料磁碟

這裡的代理資料夾內含低解析度片段。這些磁碟主要是連線至 DIVAdirector 系統的本機或遠端磁碟。單獨存取這些磁碟 (不是透過 DIVAdirector) 會造成安全風險。這類外部存取可能是來自讀取或寫入這些磁碟的有問題系統，或是來自意外提供對這些磁碟裝置存取功能的內部系統。

2.1.1.2. 資料庫磁碟和備份磁碟

建立 DIVAdirector 時，會使用資料庫磁碟和備份磁碟資源。這些磁碟通常是連線至 DIVAdirector 系統的本機或遠端磁碟。單獨存取這些磁碟 (不是透過 DIVAdirector) 會造成安全風險。這類外部存取可能是來自讀取或寫入這些磁碟的有問題系統，或是來自意外提供對這些磁碟裝置存取功能的內部系統。

2.1.1.3. 配置檔和設定值

DIVAdirector 系統配置設定必須受到保護，避免受到作業系統層次的非管理員使用者存取。一般而言，這些設定值會自動受到作業系統層次的管理使用者所保護。注意，讓非管理作業系統使用者可寫入配置檔會帶來安全風險。安裝目錄中包含的所有應用程式配置檔都屬於敏感檔案，包括：

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

2.1.2. 必須防止哪些人存取資源？

一般而言，前節所述的資源必須受到保護，所配置系統上的所有非管理員都不得存取，也不能讓有問題的外部系統透過 WAN 或 FC 光纖的方式存取這些資源。

2.1.3. 策略性資源的保護萬一失敗將發生什麼情況？

若保護策略資源失敗，可能會導致不適當的存取 (亦即正常 DIVAdirector 作業以外的存取資料) 甚至資料損毀 (以正常權限以外的方式寫入磁碟或磁帶)。

3

第 3 章 安全功能

為了避免潛在的安全威脅，使用 DIVAdirector 的客戶必須注意系統的認證和授權。

只要正確地配置且遵循附錄 A, 安全建置檢查清單中的安裝後檢查項目，即可將這些安全威脅降至最低。

3.1. 安全模型

提供保護防止安全威脅的重要安全功能如下：

- 認證 - 確保只有經過授權的個人才能夠存取系統和資料。
- 授權 - 對系統權限和資料的存取控制。此功能建立在認證上，以確保個人只能得到適當的存取權。

附錄 A

附錄 A. 安全建置檢查清單

1. 替 Administrator 和被指派 DIVArchive 或 DIVAdirector 管理員或服務角色的所有其他作業系統帳號設定更安全的密碼。
2. 請勿使用本機管理員作業系統帳號，而是將角色視需要指派給其他使用者帳號。
3. 替 DIVAdirector Administrator 使用者設定更安全的密碼。請立即將預設安裝的密碼變更為更安全的密碼。您可以從 DIVAdirector **Admin (管理)** 的 **Personal (個人化)** 設定值畫面進行這項操作。
4. 在系統上安裝防火牆，並套用預設的 DIVAdirector 連接埠規則。
5. 定期安裝作業系統和 DIVAdirector 更新，因為這些更新會包含安全更新。
6. 安裝防毒軟體，並且不包括 DIVAdirector 處理作業和儲存體的檢查 (基於效能考量)。