

Oracle® DIVArchive

安全指南

版本 7.3

E70868-01

2015 年 12 月

Oracle® DIVArchive
安全指南

E70868-01

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. DIVArchive Manager	7
1.1.2. DIVArchive Actor	7
1.1.3. DIVArchive Robot Manager	7
1.1.4. DIVArchive Backup Service	7
1.1.5. Oracle Avid Connectivity	8
1.1.6. DIVArchive Drop Folder Monitor	8
1.1.7. DIVArchive SNMP	8
1.1.8. DIVArchive SPM	8
1.1.9. DIVArchive Migrate Service	8
1.1.10. DIVArchive VACP	9
1.1.11. DIVArchive Control GUI	9
1.1.12. DIVArchive Configuration Utility	9
1.1.13. DIVArchive Access Gateway	9
1.1.14. DIVArchive Lynx Local delete	9
1.2. 一般安全原則	9
1.2.1. 將軟體保持在最新狀態	9
1.2.2. 限制對重要服務的網路存取	9
1.2.3. 以 DIVA 使用者身分執行並儘可能遵循以最低權限的原則	10
1.2.4. 監督系統活動	10
1.2.5. 將安全資訊保持在最新狀態	10
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、描述資料磁碟及備份磁碟	11
2.1.1.3. DIVArchive 磁帶	11
2.1.1.4. 匯出磁帶描述資料	11

2.1.1.5. 配置檔和設定值	12
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
2.2. 建議的建置拓樸	12
2.2.1. 區隔描述資料網路	12
2.2.2. FC 分區	12
2.2.3. 保護 SAN 磁碟配置存取	12
2.2.4. 安裝 DIVArchive 套裝軟體	13
2.2.5. DIVArchive 磁帶安全性	13
2.2.6. 備份	13
2.3. 安裝後配置	13
3. 安全功能	15
3.1. 安全模型	15
3.2. 認證	15
3.3. 存取控制	15
A. 安全建置檢查清單	17

前言

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

對象

本指南適用於使用 DIVArchive 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>。

第 1 章 簡介

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

1.1. 產品簡介

Oracle 的 DIVArchive 是一種分散式內容儲存管理系統。DIVArchive 的主要組成元件如下：

1.1.1. DIVArchive Manager

DIVArchive Manager 是 DIVArchive 系統中的主要元件。所有歸檔作業都是由 DIVArchive Manager 來控制與處理。作業要求是藉由啟動器應用程式透過 DIVArchive 用戶端 API 來傳送。在可購買選項中，DIVArchive 還支援主要和備份 DIVArchive Manager。如需關於 DIVArchive 的詳細資訊，請參閱 DIVArchive Software Release 7.3 Customer Documentation Library，網址為：

<https://docs.oracle.com/en/storage/#csm>

1.1.2. DIVArchive Actor

在生產系統中，DIVArchive Actor 是裝置之間移動資料的元件。它支援許多不同類型裝置之間的資料傳輸，以及處理遠距串流轉碼軟體的轉碼作業 (選擇性)。

所有 Actor 作業都是由 DIVArchive Manager 來起始與協調。單一 DIVArchive Manager 可配置與控制一或多個 Actor。

1.1.3. DIVArchive Robot Manager

雖然 DIVArchive 只能用來管理磁碟儲存體，但是可以藉由新增一或多個磁帶櫃來進一步擴充儲存容量。在這些情況下，DIVArchive Robot Manager 模組可提供 DIVArchive Manager 與許多不同類型磁帶櫃互動的中介軟體層。它主要透過 TCP/IP 連線至 DIVArchive Manager。DIVArchive Robot Manager 會使用磁帶櫃本身的直接介面 (透過原生 SCSI 或 SCSI over Fiber Channel)，或是透過製造商所擁有的磁帶櫃控制軟體的中介乙太網路連線，作為與磁帶櫃之間的介面。

1.1.4. DIVArchive Backup Service

為了確保 Oracle 資料庫和中繼資料資料庫備份的可靠性與監督，我們導入了 DIVArchive Backup Service。

DIVArchive Backup Service 元件會整合成為標準 DIVArchive 系統安裝的一部分來進行安裝。此元件通常會安裝在和 DIVArchive Manager 與 Oracle 資料庫相同的伺服器上。DIVArchive Backup Service 允許透過其配置檔來配置排定的備份。DIVArchive Backup Service 會管理與監督整個備份處理作業。

DIVArchive Backup Service 現在結合了在備份資料庫和描述資料資料庫檔案發生問題時，送出電子郵件的能力。若要使用此功能，必須將 DIVArchive 配置為連線至 SMTP 郵件提供者。電子郵件通知是透過 [Manger Setting] (Manger 設定) 頁籤下的 [DIVArchive Configuration Utility] (DIVArchive 配置公用程式) 來進行配置。

如需安裝與配置 DIVArchive Backup Service 的相關資訊，請參閱 DIVArchive Software Release 7.3 Customer Documentation Library，網址為：

<https://docs.oracle.com/en/storage/#csm>

1.1.5. Oracle Avid Connectivity

DIVArchive 中 Avid Connectivity 的用途是以特定視訊格式在 DIVArchive 來回傳輸歸檔資料，並且能夠歸檔與擷取單一片段或一連串片段。AMC 和 TMC 相關元件會隨著主要 DIVArchive 安裝一併安裝。AMC 和 TMC 的特定外掛程式則需要額外安裝。

1.1.6. DIVArchive Drop Folder Monitor

DIVArchive Drop Folder Monitor (DFM) 最多可自動監督 20 個本機資料夾或 FTP 資料夾 (或二者合計)。每一 DIVArchive Object 均支援一或多個檔案 (在 FTP 資料夾中)。識別出新的檔案 (或 FTP 資料夾) 時，DFM 便會向 DIVArchive 自動發出歸檔要求，以歸檔新的檔案或資料夾。順利將這些檔案歸檔之後，便會自動刪除來源中的這些檔案。

1.1.7. DIVArchive SNMP

DIVArchive 簡單網路管理協定 (SNMP) 代理程式和管理資訊庫 (MIB) 支援透過 SNMP 協定使用第三方監督應用程式來監督 DIVArchive 及其子系統的狀態和活動。

1.1.8. DIVArchive SPM

DIVArchive Storage Plan Manager (SPM) 根據 SPM 配置中定義的規則和原則，提供媒體的自動化移轉和自動化週期。

SPM 元件同時可用來觸發刪除 SPM 管理陣列中的內容 (根據磁碟空間浮水印)。

1.1.9. DIVArchive Migrate Service

DIVArchive 包含內嵌的移轉服務。這是新的個別內部 (對 DIVArchive 而言) 服務，可協助使用者排定與執行工作來移轉 DIVArchive 系統內不同媒體之間的内容。您可以使用 Control GUI 或命令行用戶端。

1.1.10. DIVArchive VACP

VACP (視訊歸檔命令協定) 是由 Harris Automation 所開發的協定，用來作為與歸檔系統之間的介面。DIVArchive 使用自己的 API 與 DIVArchive Manager (與 VACP 並不相容) 進行通訊。

1.1.11. DIVArchive Control GUI

DIVArchive Control GUI (圖形使用者介面) 的功用是在 DIVArchive 中進行監督、控制與管理作業。一個 DIVArchive 系統上同時可以執行與連線數個 DIVArchive GUI。

1.1.12. DIVArchive Configuration Utility

DIVArchive Configuration Utility 主要用來配置 DIVArchive 系統。雖然 Configuration Utility 主要是用來配置 DIVArchive，但是仍然可以從它執行某些操作功能。

1.1.13. DIVArchive Access Gateway

Access Gateway 允許從單一電腦與多個獨立 DIVArchive 系統進行作業與互動。它是全球性內容分配的解決方案。將檔案自動複製到鏡射站台，可以為安全地區域分配、備份、災害復原以及頻寬控制和總和檢驗驗證，提供一種清晰而簡單的方法。網路會受到監督，而 DIVAnet 可確保最終的傳遞內容。

1.1.14. DIVArchive Lynx Local delete

LYNXLocalDelete 是一種監督本機 DIVArchive 系統 (例如 LYNXlocal) 和一或多個遠端 DIVArchive 系統 (例如 LYNXdr) 之間物件複製功能的服務。順利將物件複製到遠端 DIVArchive 系統之後，就會將該物件標示為可以從本機 DIVArchive 系統刪除。

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 DIVArchive 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

DIVArchive 使用下列 TCP/IP 連接埠：

- DIVArchive Robot Manager 使用 tcp/8500
- DIVArchive Manager 使用 tcp/9000
- DIVArchive Backup Service 使用 tcp/9300

- DIVArchive Access Gateway 使用 tcp/9500
- DIVArchive Actor 使用 tcp/9900
- DIVArchive Migrate Service 使用 tcp/9191

1.2.3. 以 DIVA 使用者身分執行並儘可能遵循以最低權限的原則

所有 DIVArchive 服務均以 DIVA 使用者身分執行。DIVArchive Control GUI 提供三個固定的使用者設定檔 (Administrator、Operator 及 User)。Administrator 和 Operator 帳號需要密碼才能取得存取權。您可以隨時使用 DIVArchive Configuration 公用程式來變更 DIVArchive 系統安裝時所使用的預設密碼。若未變更預設密碼，可能會讓 DIVArchive 系統被惡意活動存取。在安裝與配置 **Administrator** 和 **Operator** 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

監督系統活動以判斷 DIVArchive 運作的情形，以及是否有任何不尋常活動的記錄。檢查位於安裝目錄中 /Program/log/ 下的記錄檔。

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>

持續保持安全的主要方法就是執行最新版本的 DIVArchive 軟體。

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 DIVArchive 時，請保護下列資源：

2.1.1.1. 主要資料磁碟

建立 DIVArchive 系統會使用資料磁碟和快取磁碟資源。這些磁碟通常是連線至 DIVArchive 系統的本機或遠端磁碟。單獨存取這些磁碟 (不是透過 DIVArchive 的方式) 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、描述資料磁碟及備份磁碟

建立含有複雜物件的 DIVArchive 會使用資料庫磁碟、描述資料磁碟和備份磁碟資源。這些磁碟通常是連線至 DIVArchive 系統的本機或遠端磁碟。單獨存取這些磁碟 (不是透過 DIVArchive 的方式) 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. DIVArchive 磁帶

允許對 DIVArchive 系統所控制、用來寫入資料之磁帶櫃中的磁帶進行單獨存取會造成安全風險。

2.1.1.4. 匯出磁帶描述資料

從匯出作業建立的磁帶描述資料傾印會包含資料和描述資料。這類資料和描述資料應受到保護，避免在例行匯出或匯入活動時被作業系統管理員以外的人存取。

2.1.1.5. 配置檔和設定值

DIVArchive 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。

2.1.2. 必須防止哪些人存取資源？

一般而言，前節所述的資源都必須受到保護，不受配置系統上的所有非管理員存取，或有問題的外部系統透過 WAN 或 FC 光纖的方法來存取這些資源。

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 (正常 DIVArchive 作業以外的存取資料) 甚至資料損毀 (正常權限以外的寫入磁碟或磁帶)。

2.2. 建議的建置拓樸

本節描述如何安全地安裝與配置基礎架構元件。如需安裝 DIVArchive 的相關資訊，請參閱 DIVArchive Software Release 7.3 Customer Documentation Library，網址為：

<https://docs.oracle.com/en/storage/#csm>

安裝與配置 DIVArchive 時，請考量下列各點：

2.2.1. 區隔描述資料網路

對於 DIVArchive 服務元件相互間的連線、對描述資料資料庫的連線以及來自其用戶端的連線，請提供沒有連線至任何 WAN 的其他 TCP/IP 網路和交換器硬體。因為描述資料流量是使用 TCP/IP 來實行，理論上外部有可能會攻擊此流量。配置不同的描述資料網路可降低此風險，同時可提供更好的效能。如果區隔網路不可行，請至少拒絕來自外部 WAN 以及網路上任何不信任主機的 DIVArchive 連接埠的流量。請參閱節 1.2.2, 「限制對重要服務的網路存取」。

2.2.2. FC 分區

使用 FC 分區可拒絕來自不需要存取這些磁碟之任何伺服器，對於透過光纖通道連線之 DIVArchive 磁碟的存取。最好使用不同的 FC 交換器，而且實際上只連線到需要存取的伺服器。

2.2.3. 保護 SAN 磁碟配置存取

SAN RAID 磁碟通常會透過 TCP/IP 或更典型的 HTTP 方式存取以進行管理。您必須限制只有信任網域中的系統才能對 SAN RAID 磁碟進行管理存取，保護磁碟不受外部存取。同時，變更磁碟陣列上的預設密碼。

2.2.4. 安裝 DIVArchive 套裝軟體

首先，僅安裝您所需要的 DIVArchive 服務。例如，如果您並未計畫從系統執行 GUI 或 Configuration 公用程式，請在安裝期間的元件清單中取消勾選這些元件。安裝之後若要變更預設的 DIVArchive 安裝目錄權限和擁有者，必須考量變更所帶來的安全影響。

2.2.5. DIVArchive 磁帶安全性

防止外部存取由 DIVArchive 系統控制之磁帶櫃中的 DIVArchive 磁帶。對 DIVArchive 磁帶的未授權存取可能會影響或損毀使用者資料。

2.2.6. 備份

使用 DIVArchive Backup 服務設定並執行資料庫備份。將備份傾印限制為只有作業系統層次管理員使用者才能存取。

2.3. 安裝後配置

安裝任何 DIVArchive 之後，請檢查[附錄 A, 安全建置檢查清單](#)中所列的項目。

第 3 章 安全功能

為了避免潛在的安全威脅，使用 DIVArchive 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。

3.2. 認證

DIVArchive Control GUI 提供三個固定的使用者設定檔 (Administrator、Operator 及 User)。Administrator 和 Operator 帳號需要密碼才能取得存取權。您可以隨時透過 DIVArchive Configuration 公用程式來變更安裝 DIVArchive 系統時所使用的預設密碼。若未變更預設密碼，可能會讓 DIVArchive 系統被惡意活動存取。在安裝與配置 Administrator 和 Operator 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。

3.3. 存取控制

DIVArchive 中的存取控制分為三個設定檔：

User - 與 DIVArchive Manager 建立連線之後，Control GUI 僅允許使用者監督 DIVArchive 作業，以及從資料庫擷取資料，這就是 User 設定檔。在 User 設定檔模式下，並無法存取對 DIVArchive 發出命令的所有功能。在需要監督但不允許傳送命令至 DIVArchive 的情形時，可以使用此設定檔。

Administrator - 若要對 DIVArchive 發出要求，例如歸檔、回復要求或是從磁帶櫃退出磁帶，您都必須變更為 Administrator 設定檔。Administrator 設定檔受到密碼保護。此設定檔的預設密碼為 diva，但是可以在 Configuration 公用程式中加以變更 (或可能已經變更)。如需詳細資訊，請參閱 DIVArchive Software Release 7.3 Customer Documentation Library，網址為：

<https://docs.oracle.com/en/storage/#csm>

Operator - 除了 User 設定檔權限之外，Operator 設定檔可提供對 Object Transfer Utility 的存取，此設定檔需要輸入和 Administrator 設定檔相同的密碼。

附錄 A. 安全建置檢查清單

1. 替 Administrator 和被指派 DIVArchive 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，包括：
 - DIVA - Oracle 使用者 ID (若有使用)
 - 任何磁碟陣列管理帳號
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 Administrator 和 Control GUI 的 Operator 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 [Tools] (工具) 底下的 [Configuration] (配置) 公用程式來進行這項操作。
4. 替 Oracle 資料庫登入帳戶設定更安全的密碼。將預設的 Oracle 資料庫使用者密碼從安裝的預設密碼改為其他密碼。
5. 在每個系統上安裝防火牆，並套用預設的 DIVArchive 連接埠規則。使用防火牆規則，將對 DIVArchive API (tcp 9000) 的存取限制為只有需要存取的 IP。
6. 定期安裝作業系統和 DIVArchive 更新，因為這些更新包含安全更新。
7. 安裝防毒軟體，並且不包括 DIVArchive 處理作業和儲存體的檢查 (基於效能考量)。
8. 最佳做法是透過實體或 FC 分區方式隔離 FC 磁碟和 FC 磁帶機，如此磁碟和磁帶裝置便不會共用相同的 HBA 連接埠。對於受管理的磁碟，應只有 DIVArchive Actor 能夠存取磁碟和磁帶機。此安全措施有助於避免意外覆寫磁帶或磁碟，造成資料遺失意外的發生。
9. 替 DIVArchive 配置和資料庫設定一組適當的備份。備份是安全的一部分，在意外或漏洞造成資料遺失時，可提供復原資料的方法。您的備份在傳輸到異地理位置時，應包括某些原則。備份應受到和 DIVArchive 磁帶與磁碟相同程度的保護。

