Oracle® DIVArchive

安全指南

版本 7.5

E86532-01

2016 年 11 月

ORACLE®

Oracle® DIVArchive
安全指南

E86532-01

內容

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、安全安裝及設定組態的相關人員。

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 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. Oracle 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 7.4 Customer Documentation Library，網址為：

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

1.1.2. Oracle 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，並且可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 可設定並控制一或多個 Actor。

1.1.3. DIVArchive Robot Manager

雖然您只能使用 DIVArchive 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 Fibre Channel)，或是透過製造商自有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 允許透過組態檔來設定排定的備份。DIVArchive Backup Service 會管理與監督整個備份處理作業。

DIVArchive Backup Service 現在能夠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。若要使用此功能，必須將 DIVArchive 設定為連線至 SMTP 郵件提供者。電子郵件通知是透過 [Manager Setting] (Manager 設定) 頁籤下的 [DIVArchive Configuration Utility] (DIVArchive 組態公用程式) 來進行設定。

如需安裝並設定 DIVArchive Backup Service 的相關資訊，請參閱 DIVArchive 7.4 Customer Documentation Library，網址為：

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

1.1.5. Oracle DIVArchive 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 (DFM)

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。DIVArchive SNMP 只在 Windows 環境中才有支援。

1.1.8. DIVArchive Storage Plan Manager (SPM)

DIVArchive Storage Plan Manager (SPM) 根據 SPM 組態中定義的規則和原則，提供歸檔內之內容的自動移轉和自動化週期。

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內容。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

您可以使用 DIVArchive Control GUI (圖形使用者介面) 來監督、控制並管理 DIVArchive 中的作業。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

您可以使用 DIVArchive Configuration Utility 來設定 DIVArchive 系統。雖然 Configuration Utility 主要是用來設定 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 Local Delete

Local Delete 是一種監督本機 DIVArchive 系統 (例如 DIVAlocal) 與一或多個遠端 DIVArchive 系統 (例如 DIVAdr) 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使用最低權限原則

請勿使用 Administrator (或 root) 作業系統使用者帳號來執行 DIVArchive 服務。您必須一律使用名為 DIVA 的專用作業系統使用者 (或群組) 來執行所有 DIVArchive 服務。

DIVArchive Control GUI 提供三個固定的使用者設定檔 (Administrator、Operator 以及 User)。Administrator 和 Operator 帳號需要密碼才能取得存取權。您必須先在 Configuration Utility 中指派 Administrator 和 (或) Operator 密碼，才能使用這些設定檔。

您需要在安裝和設定組態期間建立 Administrator 和 Operator 帳號的密碼。之後每隔 180 天 (最少) 必須變更這些密碼一次。密碼在需要時必須提供給「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。請查看位於安裝目錄中 */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。

2

第 2 章 安全安裝

本章概述安全安裝的規劃程序，並描述數種建議的系統部署拓樸。

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) 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惡意系統，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) 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惡意系統，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

允許對由 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。在進行例行匯出或匯入活動時，必須將此資料和描述資料的權限，限於 Administrator (或 root) 作業系統帳號或 DIVA 作業系統使用者 (或群組)。

2.1.1.5. 組態檔和設定值

DIVArchive 系統組態設定值必須受到保護，避免讓作業系統層次的非管理員使用者存取。讓非管理作業系統使用者可寫入組態檔會帶來安全風險，因此必須限制只有 Administrator (或 root) 作業系統帳號或 DIVA 作業系統使用者 (或群組) 才能具備這些檔案的權限。

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，以防止被設定系統上的任何非管理員存取，也要防止讓外部系統可透過 WAN 或 FC 光纖來存取這些資源。

2.1.3. 策略性資源的保護萬一失敗將發生什麼情況？

如果保護策略資源失敗，可能會導致不適當的存取 (亦即正常 DIVArchive 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)。

2.2. 建議的部署拓樸

本節描述如何安全地安裝並設定基礎架構元件。如需安裝 DIVArchive 的相關資訊，請參閱 DIVArchive 7.4 Customer Documentation Library，網址為：

`https://docs.oracle.com/en/storage/#csm`

安裝和設定 DIVArchive 時，請考量以下各點：

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。設定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。請參閱限制對重要服務的網路存取。

2.2.2. FC 分區

對於不需要存取 DIVArchive 磁碟的任何伺服器，請使用 FC 分區來拒絕讓這些伺服器透過光纖通道存取 DIVArchive 磁碟。最好使用不同的 FC 交換器，而且僅實際連接到需要存取的伺服器。

2.2.3. 保護 SAN 磁碟組態存取

SAN RAID 磁碟通常可以透過 TCP/IP 或更典型的 HTTP 來存取，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 Utility，請於安裝期間取消勾選元件清單中的這些元件。預設 DIVArchive 安裝目錄權限和擁有者必須只限制於 Administrator (或 root) 帳號或 DIVA 作業系統使用者 (或群組)。

2.2.5. DIVArchive 磁帶安全性

防止可從外部存取由 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。「備份傾印」的權限必須只限於 Administrator (或 root) 作業系統帳號或 DIVA 作業系統使用者 (或群組)。

2.3. 安裝後組態

安裝任何 DIVArchive 之後，請檢查附錄 A, 安全部署檢查清單中所列的項目。

3

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。

只要正確地設定組態且遵循附錄 A, 安全部署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 - 控制對系統權限和資料的存取。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。您必須先在 Configuration Utility 中指派 Administrator 和 (或) Operator 密碼，才能使用這些設定檔。

Administrator 和 Operator 帳號密碼每隔 180 天 (或之前) 必須變更一次。必須確保密碼在「Oracle 客戶服務部」需要時可立即取得。

3.3. 存取控制

DIVArchive 中的存取控制分為三個設定檔。Administrator 和 Operator 帳號需要密碼才能取得存取權。您必須先在 Configuration Utility 中指派 Administrator 和 (或) Operator 帳號密碼，才能使用這些設定檔。

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，此模式會啟用需要監督但不允許傳送命令至 DIVArchive 的環境。

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。您

必須先在 Configuration Utility 中指派此設定檔的密碼，才能使用此設定檔。如需詳細資訊，請參閱 Oracle DIVArchive 7.4 Customer Documentation Library，網址為：

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

Operator 和 *Advanced Operator* - 除了 User 設定檔權限之外，Operator 設定檔也提供對 Object Transfer Utility 的存取，但必須先在 Configuration Utility 中設定密碼，才能使用此設定檔。Control GUI 中的 Operator 和 Advanced Operator 設定檔現在可以選擇性地啟用權限，以取消與變更要求的優先順序。這些選項可在 Configuration Utility 的 Manager Configuration 面板定義。此選項預設為 *disabled* (停用)。

附錄 A

附錄 A. 安全部署檢查清單

1. 替 Administrator (或 root) 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，其中包括：
   - 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。視需要將角色指派給其他使用者帳號。
3. 替 Control GUI 的 Administrator 和 Operator 設定更安全的密碼。您必須先在 Configuration Utility 中指派這些設定檔的密碼，才能開始使用。
4. 對 Oracle 資料庫登入設定更安全的密碼。
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，同時排除 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，讓磁碟和磁帶裝置不共用相同的 HBA 連接埠。若為受管理的磁碟，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 組態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。