

Oracle® DIVAnet

安全指南

2.0 版

E74312-01

2016 年 3 月

Oracle® DIVAnet
安全指南

E74312-01

版權 © 2016, 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
本書適用對象	5
文件輔助功能	5
1. 簡介	7
1.1. 產品簡介	7
1.1.1. DIVAnet ClientAdapter 服務	7
1.1.2. DIVAnet ManagerAdapter 服務	7
1.1.3. DIVAnet DbSync 服務	7
1.1.4. DIVAnet 使用者介面 (DIVAnetUI)	7
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. 盡可能使用最低權限原則	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	8
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. DIVAnet 伺服器	11
2.1.1.2. 資料庫	11
2.1.1.3. DIVArchive 來源、目的地和存檔媒體	11
2.1.1.4. 組態檔和設定值	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. 建議的部署技術	12
2.2.1. DIVAnet 安裝	12
2.2.2. 連線到 DIVArchive	12
2.2.3. 保護磁碟系統	13
2.3. 安裝後組態	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
- 3.4. 設定 **SSL/TLS** 16
 - 3.4.1. 私密金鑰存放區 17
 - 3.4.2. 公用金鑰存放區 17

- A. 安全部署檢查清單 19**

前言

Oracle DIVAnet 安全指南包含 Oracle DIVAnet 產品的相關資訊並說明應用程式安全的一般原則。

本書適用對象

本指南的適用對象是所有使用 DIVAnet 安全功能，以及進行 DIVAnet 安全安裝與組態的人員。

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 Oracle DIVAnet 2.0 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 DIVAnet 可對多個分散式 Oracle DIVArchive 系統的存檔內容提供統一的檢視。Oracle 的 DIVArchive 是具有擴充性的內容儲存管理系統，支援存檔至磁帶櫃和磁碟系統。DIVAnet 可協助在各個 DIVArchive 網站之間以及從客戶「來源和目的地」伺服器與磁碟之間移動內容。它會執行與災害復原、內容分配、存取控制、效能，以及內容可用性之目的相關的工作。

DIVAnet 包含下列主要元件：

1.1.1. DIVAnet ClientAdapter 服務

應用程式從屬端會使用 DIVArchive API 或 DIVAnet GUI 連線到 **DIVAnet ClientAdapter** (DIVAnet ClientAdapter 服務)。此 DIVAnet 服務接受來自應用程式的 Web 與通訊埠連線並會處理要求。系統會在已安裝 DIVArchive 和 DIVAnet 的網站，且對於已安裝應用程式的網站來說屬於本機的每個網站上，都設定 **ClientAdapter**。

1.1.2. DIVAnet ManagerAdapter 服務

DIVAnet ManagerAdapter Service (DIVAnet ManagerAdapter 服務) 的作用是在 DIVAnet 和 Oracle DIVArchive Manager 之間提供橋接器功能。它必須設定成由其他 DIVAnet 系統來提供遠端存取。

1.1.3. DIVAnet DbSync 服務

DIVAnet DbSync Service (DIVAnet DbSync 服務) 負責同步化來自多個 DIVArchive 網站的資產資訊，以及將資訊儲存在 DIVAnet 資料庫中。**DbSync** 以遠端方式和多個網站上的 **ManagerAdapter** 服務進行通訊，以同步化已存檔的物件資訊。**DbSync** 通常和 **ClientAdapter** 一起部署。**DbSync** 服務和 **ClientAdapter** 兩者會要求將存取導向至 DIVAnet 資料庫。

1.1.4. DIVAnet 使用者介面 (DIVAnetUI)

DIVAnetUI 是一個 GUI 應用程式，可供使用者監督 DIVAnet 要求以及在多個 DIVArchive 網站檢視、複製和刪除 DIVAnet 資產 (DIVA 存檔的物件)。無論是透過

API 或透過 UI 本身發出的要求，所有 DIVAnet 層次的要求都可加以監督。您還可以檢視所有已設定 DIVArchive 網站的資產資訊，無論該資產是否透過 DIVAnet 存檔。DIVAnetUI 提供靈活的方式查詢要求資訊和資產資訊。

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 DIVAnet 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

DIVAnet 預設使用下列 TCP/IP 連接埠：

- *tcp/9801* 是 DIVAnet **ClientAdapter** 所使用的預設 **WebService** (Web 服務) 連接埠
- *tcp/7101* 是 DIVAnet **ClientAdapter** 所使用的預設 API 通訊埠連接埠 (您可以設定其他連接埠)
- *tcp/9800* 是 DIVAnet **ManagerAdapter** 所使用的預設 **WebService** (Web 服務) 連接埠

注意:

所有這些連接埠並非都需要向外部公開，並且會以組態和使用狀況為基礎。

1.2.3. 盡可能使用最低權限原則

DIVAnet 服務不應該以 *admin* 或 *SuperUser* 身分執行。使用不同的作業系統使用者 (用來管理應用程式以外的使用者) 執行服務有助於整體系統安全。防火牆必須將連接埠限制為僅必要的連接埠。DIVAnet 包含存取控制功能 (「[存取控制](#)」中提供簡短描述)，用來將使用者和系統限制為盡可能的最低權限。

1.2.4. 監督系統活動

您必須監督系統活動，以判斷 DIVAnet 的運作情況以及 DIVAnet 是否記錄任何不尋常的活動。請檢查位於 *\$DIVANET_HOME/Program/log/* 資料夾中的記錄檔。

1.2.5. 將安全資訊保持在最新狀態

您可以在下列位置存取各種軟體產品的數種來源安全資訊和警示：

<http://www.us-cert.gov>

將安全資訊保持在最新狀態的首要方法是執行最新版的 DIVAnet 軟體。

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。請考量要保護的資源類型，然後決定提供的安全層級。

使用 DIVAnet 時，您必須保護下列資源：

2.1.1.1. DIVAnet 伺服器

DIVAnet 安裝在附加至一或多個磁碟 (可能是直接連接至 DIVAnet 系統的本機或遠端磁碟) 的伺服器上。單獨存取這些磁碟 (不是透過 DIVAnet) 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

DIVAnet 系統是使用資料庫軟體和資料資源所建立。資料通常位於連接到 DIVAnet 系統的本機或遠端磁碟上。單獨存取這些磁碟 (不是透過 DIVAnet) 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 來源、目的地和存檔媒體

DIVAnet 在滿足其要求的過程中會使用 DIVArchive 來源和目的地以及 DIVA 存檔系統 (磁碟或磁帶)。未經授權單獨存取這些伺服器磁碟和系統媒介 (這些通常是由 DIVArchive 系統控制) 會有安全風險。作為 DIVAnet 複製作業之暫時資料存放區的 **Source/Destinations** (來源/目的地) 應該限制存取，而且您應該考量將這些 **Source/Destinations** (來源/目的地) 單獨專用於 DIVAnet 作業，同時還要確保透過信任的網路進行加密或起始傳輸。

2.1.1.4. 組態檔和設定值

DIVAnet 系統組態設定值必須受到保護，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。讓非管理作業系統使用者可寫入組態檔會造成安全風險。

2.1.2. 必須防止哪些人存取資源？

一般而言，前節所述的資源必須受到保護，以防止被設定系統上的任何非管理員使用者存取，也要防止透過 WAN 或 FC 光纖來取這些資源的其他外部系統所存取。

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 DIVAdirector 作業以外的存取資料) 甚至資料損毀 (錯誤地刪除資產，或者以正常權限以外的方式寫入磁碟或磁帶)。

2.2. 建議的部署技術

本節描述安全基礎架構元件的安裝與組態。

如需安裝 DIVAnet 的相關資訊，請參閱「DIVAnet 2.0 文件庫」中的 *Oracle DIVAnet Guide*，網址為：

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

安裝和設定 DIVAnet 時，請考量以下各點。

2.2.1. DIVAnet 安裝

您應該只安裝需要的 DIVAnet 元件。例如，如果您計畫只從系統執行 **DIVAnetUI**，請於安裝期間在要安裝的元件清單中取消選取 **DIVAnet Services** (DIVAnet 服務)。安裝之後若要變更預設的 DIVAnet 安裝目錄權限和擁有者，必須考量變更所帶來的安全影響。

2.2.2. 連線到 DIVArchive

Oracle 建議您在 DIVArchive Manager 系統上安裝 **ManagerAdapter** 元件，以提升系統安全性。如果不需要外部存取 DIVArchive Manager 連接埠，建議您使用防火牆軟體封鎖連接埠。此外，一般而言，允許外部網路存取 **DIVAnet DbSync WebService** (DIVAnet DbSync Web 服務) 連接埠並非必要。

如果您透過 WAN 連線到遠端 DIVArchive 執行處理，請確定是透過信任的網路進行連線。此外，連線到網站時，請考量使用 *SSL/TLS* 來連線到遠端網站的 **ManagerAdapter** 連接埠。

2.2.3. 保護磁碟系統

使用「FC 分區」拒絕來自不需要存取透過「光纖通道」連線之 DIVAnet 磁碟的任何伺服器，讓這些伺服器無法存取 DIVAnet 磁碟。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。

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。您必須透過限制只有在信任網域內的系統才能夠對 SAN RAID 磁碟進行管理存取，來防止磁碟受到外部存取。此外，請變更磁碟陣列上的預設密碼。

2.3. 安裝後組態

安裝 DIVAnet 的任何部分之後，請完成[附錄 A, 安全部署檢查清單](#)中的「安全檢查清單」。

第 3 章 安全功能

若要避免潛在的安全威脅，操作 DIVAnet 的客戶必須關心系統的認證和授權。

只要正確地組態且遵循[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 - 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

DIVAnet 服務可以使用多種方法執行認證：

- **SSL / TLS 憑證** - 當 DIVAnet 對遠端 DIVAnet 服務建立外送連線時，DIVAnet 會查詢憑證信任存放區。這有助於確保 DIVAnet 連線到真正的 DIVAnet 服務。若要建立從 DIVAnet **ClientAdapter** 到 DIVArchive 執行處理的安全連線，您必須使用識別為 **WebServices** (Web 服務) 的 `<ConnectionType>` 來透過 **ManagerAdapter** 進行連線。
- **存取規則** - 從技術的角度看，存取規則是一種存取控制形式，可根據內送 IP 位址篩選內送連線。對於協助確保只有獲得核准的系統，才擁有適當的 DIVAnet 服務存取權，此功能不可或缺。

警告：

DIVAnet 服務使用資料庫密碼作為其組態的一部分。密碼需要在安裝之後立即變更，而且之後每隔 180 天 (最少) 都要加以變更。完成變更後，您必須將密碼以離線方式儲存在安全場所，並且在「Oracle 客戶服務部」需要時可立即取得。

3.3. 存取控制

您可以建立存取規則，限制特定使用者或系統可以在分散式存檔系統中執行的作業。存取規則能夠以下列方式執行：

- **ClientAdapter /MultiDiva** 模式 - 限制可執行的 DIVAnet 要求類型。
- **ManagerAdapter** - 限制可加以執行以滿足 DIVAnet 要求的 DIVArchive 要求類型 (可能是遠端系統的要求)。

存取規則會影響從 **DIVAnetUI** 或者從 API 通訊埠連線 (可能是由 MAM 或自動化系統所起始) 起始的要求。

DIVAnet 要求可以在 DIVAnet 層次或 DIVArchive 層次執行存取規則。在 DIVAnet 層次，**ClientAdapter** 會在收到要求的位置處理該要求。在 DIVArchive 層次，遠端 **ManagerAdapter** 會處理所發出的 DIVArchive 要求以滿足 DIVAnet 要求。

Oracle 建議您建立符合應用程式需求的最嚴格規則集。例如，如果只有管理員才需要執行全域刪除，請確定拒絕其他人員存取該功能。如果系統使用者群組僅需要存取有限的「來源與目的地」清單，請確定那些使用者只能針對那些特定的「來源與目的地」發出要求。

請同時考量用來滿足要求的網站。例如，如果本機網站上的使用者不需要在不是本機網站的來源或目標網站執行複製 (如果使用 DIVAnet 便可能發生這種情況)，請在 **ClientAdapter** 組態中設定這些規則。

最後，請考量您要從要求中全面排除的特定建構。例如，如果您不需要處理只有「物件名稱」(沒有類別) 的物件，請排除類別空白的所有要求。

此外，每個 **ClientAdapter WorkflowProfile** 都包含可由指派給 **WorkflowProfile** 之要求進行處理的有效訊息清單。在 **MultiDiva** 模式中，這可以提供方法排除處理特定訊息 (包括資訊訊息)。

Oracle 建議您從 *AccessRules.xml.ini* 檔案中定義的預設規則開始 (即使您沒有定義自己的存取規則)。如需「DIVAnet 存取控制」功能的詳細資訊，請參閱 *Oracle DIVAnet Guide*，網址為：

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

3.4. 設定 SSL/TLS

DIVAnet 的憑證資料位於兩個地方：用於在本機系統上代管之 Web 服務的私密金鑰存放區，以及用於驗證遠端方式呼叫之 Web 服務的公用金鑰存放區。您可以使用 **Java Keytool Utility** (Java 金鑰工具公用程式) 來變更金鑰存放區密碼以及新增和刪除憑證。

請參閱下列以瞭解建立金鑰存放區的詳細資訊：

<http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore>

只有 DIVAnet Web 服務連線才使用 *SSL/TLS*。在此版本中，使用 DIVArchive API 通訊埠連線到 DIVArchive 或 DIVAnet 將不會使用 *SSL/TLS*。

3.4.1. 私密金鑰存放區

DIVAnet 私密金鑰憑證資料儲存在：

```
$DIVANET_HOME/Program/divanet/lib/diva129.jks
```

此金鑰存放區中只能有一個憑證。此憑證用於由此 *\$DIVANET_HOME* 目錄執行之服務所代管的 Web 服務。建議您使用新憑證取代隨附的憑證，並且對您網路中的每個 DIVAnet 網站使用不同的憑證。

您必須變更此金鑰存放區的密碼。將密碼資訊儲存在名為 *\$DIVANET_HOME/Program/divanet/lib/diva129.properties* 的新檔案中，並將此檔案設成只有 DIVAnet 服務才能夠讀取，且系統的一般使用者不可讀取。請使用下列檔案格式：

```
keystorePassword=[newpassword]
```

3.4.2. 公用金鑰存放區

有時候又稱為信任存放區，此資料位於：

```
$DIVANET_HOME/Java/lib/security/cacerts2
```

此憑證資料用於外送 Web 服務呼叫 (包括 **DIVAnetUI**)。可將多個公用金鑰載入到此金鑰存放區。

如果您已經在 DIVAnet 私密金鑰存放區新增新的自行簽署的憑證，請使用金鑰工具公用程式匯出憑證。可呼叫此網站上之 **WebServices** (Web 服務) 的所有應用程式 (DIVAnet 服務、DIVAnetUI 等) 接著應該將匯出的憑證新增至本身的公用金鑰存放區。

附錄 A. 安全部署檢查清單

1. 替指派為 DIVAnet 管理員或服務角色的 Administrator 和所有其他作業系統帳號，設定更安全的密碼。其中包括：
 - *divanet*，Oracle 使用者 ID (若有使用)
 - 任何磁碟管理帳號
2. 請勿使用本機管理員作業系統帳號，請改為視需要將角色指派給其他使用者帳號。
3. 對每個 DIVAnet 安裝使用網站特定憑證，以及對 Oracle 資料庫和私密金鑰存放區定義更安全的密碼。對 Oracle 資料庫使用者登入設定更安全的密碼。
4. 在每個 DIVAnet 系統上安裝防火牆軟體並套用預設 DIVAnet 連接埠規則。將 DIVAnet API 通訊埠 (*tcp 7101*) 的存取限制為需要使用防火牆規則進行存取的 IP。使用 DIVAnet 的存取規則執行此步驟。
5. 定期安裝作業系統和 DIVAnet 更新，因為它們包含安全修正程式。
6. 安裝防毒軟體，同時排除 DIVAdirector 處理作業和儲存體的檢查 (基於效能考量)。
7. 最佳做法指示透過實體或「FC 分區」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。此安全措施有助於避免意外覆寫重要資料，造成資料遺失意外的發生。
8. 設定一組適當的 DIVAnet 組態和資料庫的備份。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，應包括一些原則。備份應受到和 DIVAnet 磁碟相同程度的保護。
