Oracle® DIVAnet

安全指南

发行版 2.2

E86303-01

2017 年 1 月

ORACLE®

Oracle® DIVAnet
安全指南

E86303-01

目录

前言

《Oracle DIVAnet 安全指南》包括有关 Oracle DIVAnet 产品的信息，并介绍了应用程序安全性的一般原则。

目标读者

本指南的目标读者是要使用 DIVAnet 的安全功能以及要安全可靠地安装和配置 DIVAnet 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 Oracle DIVAnet 2.2 产品并介绍了应用程序安全的一般原则。

1.1. 产品概述

Oracle DIVAnet 提供了多个分布式 Oracle DIVArchive 系统中归档内容的统一视图。Oracle 的 DIVArchive 是可伸缩的内容存储管理系统，支持归档到磁带库和磁盘系统。DIVAnet 有助于内容在 DIVArchive 站点之间的来回移动以及从客户的源和目标服务器及磁盘移动。该系统可针对灾难恢复、内容分发、访问控制、性能和内容可用性需求来执行相关任务。

DIVAnet 主要包括以下组件：

1.1.1. DIVAnet ClientAdapter 服务

要使用 DIVArchive API 或者要使用 DIVAnet GUI 的应用程序客户机可连接到 **DIVAnet ClientAdapter** 服务。此 DIVAnet 服务接受来自应用程序的 Web 和套接字连接并处理请求。**ClientAdapter** 在具有对已安装 DIVArchive 和 DIVAnet 的站点为本地的应用程序的每个站点上进行配置。

1.1.2. DIVAnet ManagerAdapter 服务

DIVAnet ManagerAdapter 服务充当 DIVAnet 和 Oracle DIVArchive Manager 之间的桥接程序。它必须配置为通过其他 DIVAnet 系统提供远程访问。

1.1.3. DIVAnet DbSync 服务

DIVAnet DbSync 服务负责将来自多个 DIVArchive 站点的资产信息进行同步，并将信息存储在 DIVAnet 数据库中。**DbSync** 与多个站点上的 **ManagerAdapter** 服务进行远程通信以同步归档的对象信息。**DbSync** 通常与 **ClientAdapter** 一起部署。**DbSync** 服务和 **ClientAdapter** 均需要直接访问 DIVAnet 数据库。

1.1.4. DIVAnet 用户界面 (DIVAnetUI)

DIVAnetUI 是 GUI 应用程序，可以监视 DIVAnet 请求，以及查看、复制和删除多个 DIVArchive 站点中的 DIVAnet 资产（DIVA 归档对象）。可以监视 DIVAnet 级别的所有请求，无论这些请求是通过 API 发出的还是通过 UI 本身发出的。还可以查看

所有的已配置 DIVArchive 站点的资产信息，而不管资产是否通过 DIVAnet 进行归档。**DIVAnetUI** 提供了灵活的方式来同时查询请求信息和资产信息。

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 DIVAnet 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

默认情况下，DIVAnet 使用以下 TCP/IP 端口：

- *tcp/9801* 是由 DIVAnet **ClientAdapter** 使用的默认 **WebService** 端口
- *tcp/7101* 是由 DIVAnet **ClientAdapter** 使用的默认 API 套接字端口（您可以配置其他端口）
- *tcp/9800* 是由 DIVAnet **ManagerAdapter** 使用的默认 **WebService** 端口

> **注意：**
>
> 并非所有这些端口都必须向外部公开，应视配置和使用情况而定。

1.2.3. 尽可能使用最小特权原则

DIVAnet 服务不应以 *admin* 或 *root* 身份运行。使用不同的操作系统用户（而不是用于管理应用程序的用户）运行服务有助于总体系统安全。

DIVanet Linux 安装程序需要两个用户来完成 DIVAnet 安装－*diva* 和操作系统用户。管理员和操作员使用 *diva* 帐户安装和监视 DIVAnet。操作系统用户控制 DIVAnet 服务。

防火墙必须将端口限制为仅所需的那些端口。DIVAnet 包含用于将用户和系统限制为最小可能特权的访问控制功能（在访问控制中进行了简要介绍）。

1.2.4. 监视系统活动

必须监视系统活动以确定 DIVAnet 的运行情况以及是否正在记录任何异常活动。检查位于 *$DIVANET_HOME/Program/log* 文件夹中的日志文件。

1.2.5. 密切关注最新安全信息

可以访问各种软件产品的安全信息和警报的若干来源，网址为：

http://www.us-cert.gov

及时了解最新安全信息的主要方式是运行最新发行版的 DIVAnet 软件。

2

第 2 章 安全安装

本章概述了安全安装的规划过程，并介绍了几种推荐的系统部署拓扑。

2.1. 了解您的环境

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 DIVAnet 时，必须保护以下资源：

2.1.1.1. DIVAnet 服务器

DIVAnet 安装在连接到一个或多个磁盘（直接连接到 DIVAnet 系统的本地或远程磁盘）的服务器上。对这些磁盘的独立访问（不通过 DIVAnet）会带来安全风险。此类型的外部访问可能来自对这些磁盘进行读取或写入的恶意系统，也可能来自意外提供了对这些磁盘设备的访问权限的内部系统。

2.1.1.2. 数据库

存在用于构建 DIVAnet 系统的数据库软件和数据资源。数据通常存在于已连接到 DIVAnet 系统的本地或远程磁盘上。对这些磁盘的独立访问（不通过 DIVAnet）会带来安全风险。此类型的外部访问可能来自对这些磁盘进行读取或写入的恶意系统，也可能来自意外提供了对这些磁盘设备的访问权限的内部系统。

2.1.1.3. DIVArchive 源、目标和归档介质

在满足其请求的过程中，DIVAnet 使用 DIVArchive 源和目标以及 DIVA 归档系统（磁盘或磁带）。对这些服务器磁盘和系统介质（通常由 DIVArchive 系统控制）的无保证独立访问会带来安全风险。用作 DIVAnet 复制操作的临时数据存储的**源/目标**应该已限制访问，并且您应该考虑将这些**源/目标**专用于 DIVAnet 操作－并且还要确保传输得到加密或者源于可信网络。

2.1.1.4. 配置文件和设置

必须防止操作系统级的非管理员用户访问 DIVAnet 系统配置设置。通常，这些设置由操作系统级的管理用户自动保护。使配置文件对操作系统级的非管理用户可写会带来安全风险。

2.1.2. 要避免资源被哪些用户访问?

通常，必须阻止已配置系统上的所有非管理员访问上一节中介绍的资源，也必须阻止可以通过 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（错误地删除资产，或者在没有正常权限的情况下写入磁盘或磁带）等。

2.2. 推荐的部署技术

本节介绍安全基础结构组件的安装和配置。

有关安装 DIVAnet 的信息，请参阅 *DIVAnet 2.2* 文档库中的《*Oracle DIVAnet* 安装、配置和操作指南》，网址为：

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

安装和配置 DIVAnet 时，请考虑以下几点。

2.2.1. DIVAnet 安装

应该仅安装您需要的那些 DIVAnet 组件。例如，如果计划从客户机计算机仅运行 **DIVAnetUI**，请在安装期间在要安装的组件列表中取消选中 **DIVAnet Services** 复选框。完成安装后，在未考虑更改默认 DIVAnet 安装目录权限以及属主所带来的安全隐患的情况下，不应进行此类更改。

2.2.2. 连接到 DIVArchive

Oracle 建议将 **ManagerAdapter** 组件安装在 DIVArchive Manager 系统上以提高系统安全。如果不需要从外部访问 DIVArchive Manager 端口，则建议使用防火墙软件阻止该端口。此外，通常没有必要允许外部网络访问 **DIVAnet DbSync WebService** 端口。

如果通过 WAN 连接到远程 DIVArchive 实例，请确保通过可信网络进行连接。此外，请考虑将使用 *SSL/TLS* 的站点连接到远程站点的 **ManagerAdapter** 端口。

2.2.3. 保护磁盘系统

使用 FC 区域划分方式拒绝访问从不需要访问磁盘的任何服务器通过光纤通道连接的 DIVAnet 磁盘。最好使用独立的 FC 交换机，以便采用物理方式仅连接到需要访问磁盘的服务器。

通常可通过 TCP/IP（更典型的是 HTTP）访问 SAN RAID 磁盘执行管理操作。您必须将对 SAN RAID 磁盘的管理访问权限仅限定于可信域中的系统，以阻止对磁盘的外部访问。此外，请更改磁盘阵列的默认密码。

2.3. 安装后配置

安装 DIVAnet 的任何部分后，完成附录 A, 安全部署核对表中的安全核对表。

3

第 3 章 安全功能

要避免潜在的安全威胁，必须考虑由系统对操作 DIVAnet 的用户进行验证和授权。

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，用于确保个人只获取相应的访问权限。

3.2. 验证

DIVAnet 服务可以使用以下几种方法来执行验证：

- **SSL/TLS 证书**－当 DIVAnet 创建到远程 DIVAnet 服务的出站连接时，DIVAnet 会参照证书信任库。这有助于确保 DIVAnet 连接到真正的 DIVAnet 服务。要创建从 DIVAnet **ClientAdapter** 到 DIVArchive 实例的安全连接，必须使用标识为 **WebServices** 的 *`ConnectionType`* 通过 **ManagerAdapter** 进行连接。
- **访问规则**－虽然在技术上为访问控制的一种形式，但是访问规则可以基于入站 IP 地址来过滤入站连接。对于帮助确保只有经批准的系统才具有对 DIVAnet 服务的相应访问权限，此功能很有必要。

注意：

DIVAnet 服务将数据库密码用作其配置的一部分。在安装后必须立即更改密码，且之后每 180 天（最少）更改一次。进行更改后，必须将密码存储在一个安全的脱机位置，这样在需要时使其可供 Oracle 技术支持使用。

3.3. 访问控制

可以创建访问规则，以限制某些用户或系统可以在分布式归档系统中执行的操作。可以通过以下方式运行访问规则：

- **ClientAdapter/MultiDiva 模式**－限制可以执行的 DIVAnet 请求类型。

- **ManagerAdapter**－限制可以执行以满足 DIVAnet 请求（可能由远程系统请求）的 DIVArchive 请求类型。

访问规则可以影响从 **DIVAnetUI** 或者从 API 套接字连接（可能由 MAM 或自动化系统启动）启动的请求。

DIVAnet 请求可以具有在 DIVAnet 级别或 DIVArchive 级别上对其执行的访问规则。在 DIVAnet 级别上，**ClientAdapter** 处理在其中接收请求的请求。在 DIVArchive 级别上，远程 **ManagerAdapter** 处理发出的 DIVArchive 请求以满足 DIVAnet 请求。

Oracle 建议您创建满足应用程序要求的、限制性最强的规则集合。例如，如果只有管理员才需要执行全局删除，请确保拒绝他人访问该功能。如果一组系统用户仅需要访问源和目标的有限列表，请确保那些用户只能对那些特定的源和目标发出请求。

另请考虑用于满足请求的站点。例如，如果本地站点上的用户无理由执行其中源和目标站点都不是本地站点的副本（这可能会使用 DIVAnet），则在 **ClientAdapter** 配置中配置这些规则。

最后，请考虑您要全面排除的请求中的特定构造。例如，如果不需要仅具有对象名称（没有类别）的地址对象，则排除具有空白类别的所有请求。

此外，每个 ClientAdapter WorkflowProfile 都包含可以由分配给 WorkflowProfile 的请求处理的有效消息的列表。在 **MultiDiva 模式**下，这提供了一种将特定消息排除在处理之外的方法（包括信息性消息）。

Oracle 建议从 *AccessRules.xml.ini* 文件中定义的默认规则开始，即使您未定义自己的访问规则也是如此。有关 DIVAnet 访问控制功能的更多信息，请参阅《*Oracle DIVAnet* 安装、配置和操作指南》，网址为：

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

3.4. 配置 SSL/TLS

DIVAnet 在以下两个位置中包含证书数据：专用密钥库（用于在本地系统上托管的 Web 服务）和公共密钥库（用于验证远程调用的 Web 服务）。可以使用 **Java Keytool 实用程序**更改密钥库密码以及添加和删除证书。

有关创建密钥库的更多信息，请参阅以下内容：

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

只有 DIVAnet Web 服务连接才使用 *SSL/TLS*。在此发行版中，使用 DIVArchive API 套接字连接来连接到 DIVArchive 或 DIVAnet 将不使用 *SSL/TLS*。

3.4.1. 专用密钥库

DIVAnet 私钥证书数据存储在以下位置中：

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

恰好一个证书必须出现在此密钥库中。此证书用于从此 *$DIVANET_HOME* 目录运行的服务所托管的 Web 服务。建议将附带的证书替换为新证书，并将不同的证书用于网络中的每个 DIVAnet 站点。

必须更改此密钥库的密码。将密码信息存储在名为 *$DIVANET_HOME/Program/divanet/lib/diva129.properties* 的新文件中，并使此文件对 DIVAnet 服务可读（在 Linux 中，此用户为 *divanetsvc*），但是对系统的临时用户不可读（例如，Linux 中的 *diva* 用户）。对文件使用以下格式：

keystorePassword=newpassword

3.4.2. 公共密钥库

有时称为信任库，此数据位于以下位置：

$DIVANET_HOME/Java/lib/security/cacerts2

此证书数据在出站 Web 服务调用（包括 **DIVAnetUI**）中使用。可以将多个公钥装入到此密钥库中。

如果已将新的自签名证书添加到 DIVAnet 专用密钥库中，请使用 keytool 实用程序导出证书。然后，调用此站点上 **WebServices** 的所有应用程序（DIVAnet 服务、DIVAnetUI 等）应该将已导出的证书添加到自身的公共密钥库。

附录 A

附录 A. 安全部署核对表

1. 为管理员和已为其分配任何 DIVAnet 管理员或服务角色的任何其他操作系统帐户设置强密码。其中包括：
   - *diva*、*divanetsvc* 和 Oracle 用户 ID（如果在使用）
   - 所有磁盘管理帐户
2. 不要使用本地管理员操作系统帐户，而是根据需要将角色分配给其他用户帐户。
3. 对每个 DIVAnet 安装使用特定于站点的证书，并为 Oracle 数据库和专用密钥库定义强密码。为 Oracle 数据库操作系统登录设置强密码。
4. 在每个 DIVAnet 系统上安装防火墙软件并应用默认的 DIVAnet 端口规则。将对 DIVAnet API 套接字 (*tcp 7101*) 的访问限制为要求使用防火墙规则进行访问的 IP。按照 DIVAnet 的访问规则执行此步骤。
5. 定期安装操作系统和 DIVAnet 更新，因为它们包括安全修补程序。
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。
7. 最佳做法要求以物理方式或通过 FC 区域划分方式隔离 FC 磁盘和 FC 磁带机，以便磁盘和磁带设备不共享同一 HBA 端口。此安全做法可帮助防止由于意外覆写重要数据而造成的数据丢失事件。
8. 为 DIVAnet 配置和数据库配置一组相应的备份。备份属于安全范畴，用于恢复意外丢失或由于某些违规操作而丢失的数据。您的备份应包括有关传输至异地时的相关策略。应像保护 DIVAnet 磁盘那样保护备份。