Oracle® DIVArchive

安全指南

发行版 7.5

E86531-01

2016 年 11 月

ORACLE

Oracle® DIVArchive
安全指南

E86531-01

目录

前言

《Oracle DIVArchive 安全指南》包括了有关 DIVArchive 产品的信息并说明了一般性的应用程序安全原则。

目标读者

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

1.1. 产品概述

Oracle DIVArchive 是一个分布式内容存储管理系统。DIVArchive 包括以下重要组件：

1.1.1. Oracle DIVArchive Manager

DIVArchive Manager 是 DIVArchive 系统的主要组件。所有归档操作都由 DIVArchive Manager 控制和处理。操作请求是由发起方应用程序通过 DIVArchive 客户机 API 发送的。作为一个可购买的选件，DIVArchive 还支持主要和备份 DIVArchive Manager。有关 DIVArchive 的更多信息，请参见 DIVArchive 软件发行版 7.4 客户文档库，网址为：

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

1.1.2. Oracle DIVArchive Actor

DIVArchive Actor 是生产系统中设备之间的数据移动程序。它支持在许多不同类型的设备之间传输数据以及通过 Telestream 转码软件处理转码操作（可选）。

所有 Actor 操作都是由 DIVArchive Manager 发起和协调的。一个 DIVArchive Manager 可以配置和控制一个或多个 Actor。

1.1.3. DIVArchive Robot Manager

虽然 DIVArchive 只能用来管理磁盘存储，但是可以通过添加一个或多个磁带库来进一步扩展存储容量。在这些情况下，DIVArchive Robot Manager 模块为 DIVArchive Manager 提供了一个中间软件层来与许多不同类型的磁带库进行交互。它通过 TCP/IP 连接到 DIVArchive Manager。DIVArchive Robot Manager 使用到磁带库本身的直接接口（经由本机 SCSI 或基于光纤通道的 SCSI）或者通过到生产商自己的磁带库控制软件的中间以太网连接来连接到磁带库。

1.1.4. DIVArchive 备份服务

为确保可靠性并同时监视 Oracle 数据库和元数据数据库备份，引入了 DIVArchive 备份服务。

DIVArchive 备份服务组件是作为标准 DIVArchive 系统安装的组成部分安装的。此组件通常与 DIVArchive Manager 和 Oracle 数据库安装在同一服务器上。DIVArchive 备份服务允许通过其配置文件配置预订的备份。DIVArchive 备份服务管理并监视整个备份过程。

DIVArchive 备份服务现在能够通过电子邮件发送对数据库和元数据数据库文件进行备份期间出现的问题。要利用此功能，必须对 DIVArchive 进行配置以连接到某个 SMTP 邮件提供程序。电子邮件通知是通过 DIVArchive 配置实用程序在 "Manager Setting" 选项卡下配置的。

有关安装和配置 DIVArchive 备份服务的信息，请参见 DIVArchive 7.4 客户文档库，网址为：

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

1.1.5. Oracle DIVArchive Avid Connectivity

DIVArchive 的 Avid Connectivity 用于以特定的视频格式将归档数据传送到或传送出 DIVArchive，并实现对单个剪辑或一系列剪辑的归档和检索。AMC 和 TMC 相关组件随主要 DIVArchive 安装一起安装。对于 AMC 和 TMC 的某些插件，需要额外进行安装。

1.1.6. DIVArchive Drop Folder Monitor (DFM)

DIVArchive Drop Folder Monitor (DFM) 可以自动监视在最多 20 个本地文件夹或 FTP 文件夹（或其组合）中新创建的文件。支持每个 DIVArchive 对象一个文件或多个文件（在 FTP 文件夹中）。当识别出新文件（或 FTP 文件夹）时，DFM 会自动向 DIVArchive 发出一个归档请求以对新文件或文件夹进行归档。在这些文件成功归档后，它们将自动从源中删除。

1.1.7. DIVArchive SNMP

DIVArchive 简单网络管理协议 (Simple Network Management Protocol, SNMP) 代理和管理信息库 (Management Information Base, MIB) 支持通过第三方监视应用程序使用 SNMP 协议对 DIVArchive 及其子系统的活动和状态进行监视。DIVArchive SNMP 仅在 Windows 环境中受支持。

1.1.8. DIVArchive Storage Plan Manager (SPM)

DIVArchive Storage Plan Manager (SPM) 能够根据 SPM 配置中定义的规则和策略对归档中的材料自动进行迁移和生命周期管理。

SPM 组件还用来触发从 SPM 受管理阵列中删除材料（根据磁盘空间水位标志）。

1.1.9. DIVArchive 迁移服务

DIVArchive 包括了一项嵌入式迁移服务。它是一项全新且独立的内部（对 DIVArchive 而言）服务，可以帮助用户预订并运行在 DIVArchive 系统内不同介质之间迁移内容的作业。您可以使用控制 GUI 或命令行客户机。

1.1.10. DIVArchive VACP

VACP（Video Archive Command Protocol，视频归档命令协议）是由 Harris Automation 开发的一种用于连接到归档系统的协议。DIVArchive 有其自己的用于与 DIVArchive Manager 进行通信的 API，该 API 与 VACP 不兼容。

1.1.11. DIVArchive 控制 GUI

可以使用 DIVArchive 控制 GUI（Graphical User Interface，图形用户界面）来监视、控制和管理 DIVArchive 中的操作。可以同时运行多个 DIVArchive GUI 并将其连接到同一 DIVArchive 系统。

1.1.12. DIVArchive 配置实用程序

可以使用 DIVArchive 配置实用程序来配置 DIVArchive 系统。配置实用程序虽然主要用于配置 DIVArchive，但也可以用于执行一些操作功能。

1.1.13. DIVArchive 访问网关

访问网关允许从单台计算机操作多个独立的 DIVArchive 系统以及与之进行交互。它是用于内容分发的全局解决方案。到镜像站点的自动文件复制为本地分发、备份和灾难恢复提供了一种清晰简单的方法，其中涉及安全性、带宽控制和校验和验证。网络将受到监视，并且 DIVAnet 将确保内容的最终交付。

1.1.14. DIVArchive 本地删除

本地删除是一项服务，它监视在本地 DIVArchive 系统（例如 DIVAlocal）与一个（或多个）远程 DIVArchive 系统（例如 DIVAdr）之间执行的对象复制功能。当对象成功复制到远程 DIVArchive 系统后，它会标记为可以从本地 DIVArchive 系统中删除。

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所需的基本原则。

1.2.1. 使软件保持最新

使运行的 DIVArchive 的版本保持最新。可以在 Oracle Software Delivery Cloud 上找到供下载的最新软件版本，网址为：

https://edelivery.oracle.com/

1.2.2. 限制对关键服务的网络访问

DIVArchive 使用以下 TCP/IP 端口：

- DIVArchive Robot Manager 使用 *tcp/8500*
- DIVArchive Manager 使用 tcp/9000
- DIVArchive 备份服务使用 tcp/9300
- DIVArchive 访问网关使用 tcp/9500
- DIVArchive Actor 使用 *tcp/9900*
- DIVArchive 迁移服务使用 tcp/9191

1.2.3. 以 DIVA 用户身份运行并尽可能使用最小特权原则

请勿使用管理员（或 Root）操作系统用户帐户运行 DIVArchive 服务。您必须始终使用名为 DIVA 的专用操作系统用户（或组）来运行所有 DIVArchive 服务。

DIVArchive 控制 GUI 提供了三个固定的用户角色（管理员、操作员和用户）。管理员和操作员帐户需要密码来获取访问权限。您必须在配置实用程序中为管理员和/或操作员指定密码，然后才能使用这些角色。

可以在安装和配置期间为管理员和操作员帐户创建密码。之后密码必须每隔 180 天更改一次（最低要求）。如果必要，必须将密码提供给 Oracle 技术支持。

1.2.4. 监视系统活动

监视系统活动以确定 DIVArchive 的运行情况以及是否正在记录任何异常活动。请检查位于安装目录下 */Program/log/* 中的日志文件。

1.2.5. 密切关注最新安全信息

您可以访问安全信息的多个来源。有关各种软件产品的安全信息和警报，请参见：

http://www.us-cert.gov

及时解决最新安全问题的主要方式是运行最新版本的 DIVArchive 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 DIVArchive 时，将保护以下资源：

2.1.1.1. 主数据磁盘

存在用来构建 DIVArchive 系统的数据磁盘和高速缓存磁盘资源。它们通常是连接到 DIVArchive 系统的本地或远程磁盘。对这些磁盘的独立访问（而非通过 DIVArchive）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. 数据库磁盘、元数据磁盘和备份磁盘

存在用来构建包含复杂对象的 DIVArchive 系统的数据库磁盘、元数据磁盘和备份磁盘资源。它们通常是连接到 DIVArchive 系统的本地或远程磁盘。对这些磁盘的独立访问（而非通过 DIVArchive）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 磁带

允许独立访问在其中写入数据的磁带（通常位于由 DIVArchive 系统控制的磁带库中）是一个安全风险。

2.1.1.4. 导出磁带元数据

通过导出操作创建的磁带元数据转储包含数据和元数据。必须对此数据和元数据权限进行限制，以便仅管理员（或 Root）操作系统帐户或者 DIVA 操作系统用户（或组）在例行导出或导入活动期间具有这些权限。

2.1.1.5. 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 DIVArchive 系统配置设置。使配置文件可由非管理操作系统用户进行写入会带来安全风险，因此，必须对这些文件权限进行限制，以便仅管理员（或 Root）操作系统帐户或者 DIVA 操作系统用户（或组）具有这些权限。

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 网状结构网络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 DIVArchive 操作之外访问数据）、数据损坏（在没有正常权限的情况下写入磁盘或磁带）等。

2.2. 建议的部署拓扑结构

本部分介绍了如何安全地安装和配置基础结构组件。有关安装 DIVArchive 的信息，请参阅 DIVArchive 7.4 客户文档库，网址为：

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

在安装和配置 DIVArchive 时，请考虑以下要点：

2.2.1. 独立的元数据网络

对于 DIVArchive 服务组件彼此之间的连接、到元数据数据库的连接，以及来自其客户机的连接，请提供未连接到任何 WAN 的独立 TCP/IP 网络和交换机硬件。由于元数据通信是使用 TCP/IP 实现的，因此，从理论上讲，可能会存在对此通信的外部攻击。配置单独的元数据网络降低了此风险并且还提供了增强的性能。如果独立的网络不可行，则至少拒绝从外部 WAN 和网络中任何不受信任的主机到 DIVArchive 端口的通信。请参见限制对关键服务的网络访问。

2.2.2. FC 区域划分

使用 FC 区域划分方式拒绝访问从不需要访问 DIVArchive 磁盘的任何服务器通过光纤通道连接的这些磁盘。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。

2.2.3. 保护 SAN 磁盘配置访问

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。

2.2.4. 安装 DIVArchive 软件包

首先，仅安装您需要的那些 DIVArchive 服务。例如，如果您不打算从某个系统运行 GUI 或配置实用程序，则在安装过程中请在要安装的组件列表中取消选中这些组件。必须对默认 DIVArchive 安装目录权限和属主进行限制，以便仅管理员（或 Root）帐户或者 DIVA 操作系统用户（或组）具有这些权限。

2.2.5. DIVArchive 磁带安全

阻止对由 DIVArchive 系统控制的磁带库内的 DIVArchive 磁带的外部访问。对 DIVArchive 磁带的未经授权访问可能会危害或毁坏用户数据。

2.2.6. 备份

使用 DIVArchive 备份服务设置并执行数据库备份。必须对备份转储权限进行限制，以便仅管理员（或 Root）操作系统帐户或者 DIVA 操作系统用户（或组）具有这些权限。

2.3. 安装后配置

安装任何 DIVArchive 之后，执行附录 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 DIVArchive 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－确保只有经过授权的个人才会被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

DIVArchive 控制 GUI 提供了三个固定的用户角色（管理员、操作员和用户）。管理员和操作员帐户需要密码来获取访问权限。您必须在配置实用程序中为管理员和/或操作员指定密码，然后才能使用这些角色。

管理员和操作员帐户密码必须每隔 180 天（或更短时间）更改一次。如果必要，必须将密码提供给 Oracle 技术支持。

3.3. 访问控制

DIVArchive 中的访问控制划分为三个角色。管理员和操作员帐户需要密码来获取访问权限。您必须在配置实用程序中为管理员和/或操作员帐户指定密码，然后才能使用这些角色。

用户－在建立到 DIVArchive Manager 的连接后，控制 GUI 将仅允许用户监视 DIVArchive 操作，以及从数据库中检索数据。这称为用户角色。在用户角色模式下，并非所有向 DIVArchive 发出命令的功能都可访问，这考虑到了需要进行监视但不允许向 DIVArchive 发送命令的情况。

管理员－要向 DIVArchive 发出请求（例如归档或恢复请求），或者要从磁带库弹出磁带，则必须切换到管理员角色。管理员角色受密码保护。必须在配置实用程序中为此角色指定密码，然后才能使用此角色。有关更多信息，请参阅 Oracle DIVArchive 7.4 客户文档库，网址为：

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

操作员和高级操作员－除了用户角色权限以外，操作员角色还提供了对 Object Transfer 实用程序的访问权限，并且需要在配置实用程序中配置的密码，才能使用此角色。控制 GUI 中的操作员和高级操作员角色现在可以选择启用请求优先级取消和更改权限。这些选项在配置实用程序的 Manager Configuration 面板中定义。默认情况下，禁用此选项。

附录 A

附录 A. 安全部署核对表

1. 为管理员（或 Root）或者分配有 DIVArchive 管理员或服务角色的任何其他操作系统帐户设置强密码，包括：
   - DIVA、Oracle 用户 ID（如果在使用）
   - 任何磁盘阵列管理帐户
2. 请勿使用本地管理员操作系统帐户。根据需要为其他用户帐户分配角色。
3. 为控制 GUI 的管理员和操作员设置强密码。您必须在配置实用程序中为这些角色指定密码，然后才能使用。
4. 为 Oracle 数据库登录名设置强密码。
5. 在每个系统上安装防火墙并应用默认的 DIVArchive 端口规则。限制对 DIVArchive API (*tcp/9000*) 的访问，仅允许需要使用防火墙规则进行访问的 IP 访问。
6. 定期安装操作系统和 DIVArchive 更新，因为它们包含安全更新。
7. 安装防病毒软件并排除 DIVArchive 进程和存储（出于性能考虑）。
8. 最好的做法是以物理方式或通过 FC 区域划分对 FC 磁盘和 FC 磁带机进行隔离，以使磁盘和磁带设备不共享相同的 HBA 端口。对于受管理磁盘，应当只有 DIVArchive Actor 能够访问磁盘和磁带机。此安全做法可帮助防止由于意外覆写磁带或磁盘而造成的数据丢失事件。
9. 为 DIVArchive 配置和数据库设置一组合适的备份。备份属于安全范畴，用于恢复意外丢失或由于某些类型的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 DIVArchive 磁带和磁盘那样保护备份。