# OpenManage Integration for VMware vCenter 版本 5.3

## 安全配置指南

3 月 2021 年
Rev. A00

DELL EMC

## 注意、小心和警告

**注:** “注意”表示帮助您更好地使用该产品的重要信息。

**小心:** **“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。**

**警告:** **“警告”表示可能会导致财产损失、人身伤害甚至死亡。**

# 目录

# 图

# 表

# 1

# 前言

作为改进其产品线的一项措施，Dell EMC 会定期发布其软件和硬件的修订版。本文档中介绍的有些功能可能只受当前使用的部分软件或硬件版本支持。产品发行说明提供了有关产品功能的最新信息。

如果某个产品不能正常运行或其功能与本文档的描述不符，请与您的 Dell EMC 技术支持专业人员联系。本文档在发布时准确无误。要确保您使用的是本文档的最新版本，请转至 **https://www.dell.com/support**。

## 用途

本文档包含有关 OpenManage Integration for VMware vCenter (OMIVV) 的安全特性和功能的信息。

## 读者对象

本文档面向负责 OMIVV 安全管理的人员。

## 修订历史记录

下表呈现了本文档的修订历史。

**表. 1: 修订历史记录**

| 修订版 | 日期 | 说明 |
|---|---|---|
| A00_5.2.0 | 2020 年 10 月 | OpenManage Integration for VMware vCenter 5.2 安全配置指南的初始版本。 |
| A00_5.3.0 | 2021 年 3 月 | 在“验证和数据安全”主题中添加了 RESTful API 相关信息。 |

## 相关说明文件

OMIVV 的完整文档集可从 **https://www.dell.com/support** 获得。单击**浏览所有产品**，然后单击**软件** > **虚拟化解决方案**。单击 **OpenManage Integration for VMware vCenter** 访问下列说明文件：

- *OpenManage Integration for VMware vCenter 5.3 版用户指南*
- *OpenManage Integration for VMware vCenter 5.3 版发行说明*
- *OpenManage Integration for VMware vCenter 5.3 版兼容性表*
- *OpenManage Integration for VMware vCenter 5.3 版 API 指南*
- *OpenManage Integration for VMware vCenter 5.3 版安装指南*

您可以在 https://www.dell.com/support 上找到包括白皮书在内的技术资料。

# 2

# 本说明文件中使用的术语

**表. 2: 本说明文件中使用的术语**

| 术语 | 说明 |
|---|---|
| OMIVV | OpenManage Integration for VMware vCenter |
| OVF | 开放虚拟化格式 |
| HTTP | 超文本传输协议 |
| HTTPS | Hypertext Transfer Protocol Secure |
| NFS | 网络文件系统 |
| CIFS | 通用 Internet 文件系统 |
| OM MP | OpenManage Management pack for vRealize Operations |
| CMC | 机箱管理控制器(M1000e、FX、VRTX) |
| OME-M | OpenManage Modular Edition (MX7000) |
| iDRAC | Integrated Dell Remote Access Controller |
| SNMP | Simple Network Management Protocol |
| VM | 虚拟机 |
| TCP | Transmission Control Protocol |
| UDP | 用户数据报协议 |
| PEM | 隐私增强邮件 |
| RPM | Red Hat Package Manager |
| 操作系统 | 操作系统 |

# 3

# 部署模式

您可以在 VMware vCenter 环境中部署 OpenManage Integration for VMware vCenter (OMIVV) 作为 OVF。

**主题：**



## 开放式虚拟化格式 (OVF) 部署

如果您已有 VMware vSphere 虚拟机环境，建议您将 OMIVV 部署为开放式虚拟化格式 (OVF)。

OVF 部署模式包括预配置的捆绑包，其中包含 OMIVV 软件和 OMIVV 软件运行所依托的 Linux 操作系统。

OVF 环境还包括预配置的防火墙，该防火墙已针对 OMIVV 与受监测系统之间的通信要求进行调整。

OVF 使用 OVF 模板文件进行部署。有关将 OMIVV 部署为 OVF 的更多信息，请参见 **https://www.dell.com/support** 上提供的 *OpenManage Integration for VMware vCenter 5.3 安装指南*。

## 安全配置文件

OMIVV 具有用于安全 HTTP 访问的默认安全配置文件。为增强环境安全性，强烈建议替换证书颁发机构 (CA) 签名的证书。

# 4

# 产品和子系统安全性

**主题：**



## 安全控制图

OMIVV 使用 iDRAC 执行 PowerEdge 服务器的部署、资源清册和更新，并从 iDRAC 接收 SNMP 陷阱。

OMIVV 的用户界面是设备管理 Web 页面。OMIVV 插件 UI 从 VMware vCenter 客户端运行，并提供主机硬件监测和管理功能。

所有系统凭据均存储在 OMIVV 安全存储中。

下图显示了 OMIVV 安全控制图：

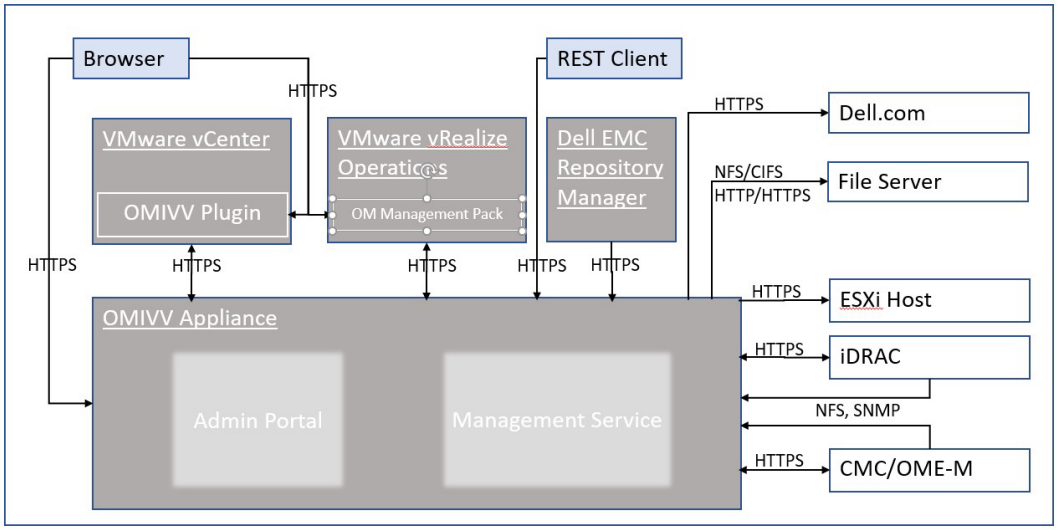


**图 1: 安全控制图**

# 验证

## 访问控制

访问控制设置可为资源提供保护，防止它们受到未经授权的访问。具有 VMware vCenter 中配置的适当角色和权限的 VMware vCenter 用户可以访问 OMIVV 插件页面。为 OMIVV 设备管理员帐户授予 OMIVV 管理控制台和 RESTful API 访问权限。

## 默认用户帐户

OMIVV 包括以下默认用户帐户：

- 本地用户帐户
- 只读用户帐户
- Root 帐户

### 本地用户帐户

OMIVV 提供了单个默认本地管理用户帐户。此内部帐户的用户名为 admin。

本地管理员只能访问 Dell EMC OMIVV 管理控制台中的所有操作。

首次部署 OMIVV 时，系统会提示您设置密码。按照屏幕上的说明设置密码。

### 只读用户帐户

OMIVV 提供单个默认本地只读用户帐户。只读帐户的用户名为只读。

管理员只能使用虚拟机远程控制台登录到 OMIVV。

在故障排除期间可以使用此帐户查看关键设备状态和日志。

首次部署 OMIVV 时，系统会提示您设置密码。按照屏幕上的说明设置密码。

### root 帐户

OMIVV 设备具有操作系统 root 帐户。

此默认帐户不可访问。技术支持团队使用 root 帐户调试字段问题。

## 外部用户帐户

当用户在 vCenter 上具有适当的角色和权限时，VMware vCenter 用户可以从 vCenter HTML5 客户端访问 OMIVV 插件用户界面元素。有关角色和权限的更多信息，请参阅所需的非管理员用户的权限 页面上的 13。

# 登录安全设置

## 失败的登录行为

OMIVV 包括了针对身份验证多次失败情况的安全设置。

## 本地用户帐户锁定

在连续 6 次尝试登录到本地用户帐户失败后，OMIVV 会将该用户暂时锁定一分钟。

# 自动会话超时

## 空闲浏览器会话超时

默认情况下，非活动状态超过 15 分钟，OMIVV 会话就会超时，同时会自动将您注销。

# 身份验证类型和设置注意事项

## vCenter 用户身份验证

OMIVV 依靠 vCenter 验证访问插件页面和处理 vCenter 操作的 RESTful API。插件页面和处理 vCenter 操作的 RESTful API 需要在注册过程中 Dell EMC 在 vCenter 上创建的权限。

## 注册新 vCenter 服务器

**前提条件**

您的 vCenter 帐户应具有创建用户所需的权限。有关所需权限的更多信息，请参阅所需的非管理员用户的权限 页面上的 13。

**关于此任务**

安装 OMIVV 后，您可以注册 OMIVV 设备。OMIVV 使用具有必要 vCenter 操作权限的管理员用户帐户或非管理员用户帐户。单个 OMIVV 设备实例可支持 15 个 vCenter 服务器（具有或不具有链接模式）和最多 2000 个 ESXi 主机。

如果您尝试注册超过 15 个 Vcenter，将显示以下错误消息：

您的许可证仅允许 <x> 个 Vcenter，并且它们均已注册。

要注册新 vCenter 服务器，请执行以下步骤：

**步骤**

1. 转至 https://<设备 IP 或主机名>。
2. 在 **vCenter 注册**页面的右窗格中，单击**注册新 vCenter 服务器**。
   此时将显示**注册新 vCenter** 页面。
3. 在**注册新 vCenter** 对话框中的 **vCenter 名称**下，执行以下任务：
   a. 在 **vCenter 服务器 IP 或主机名**框中，输入 vCenter 的 IP 地址或主机的 FQDN。
      Dell EMC 建议使用完全限定域名 (FQDN) 向 VMware vCenter 注册 OMIVV。对于所有注册，vCenter 的主机名必须可通过 DNS 服务器正确解析。建议您遵循以下建议的实践方法来使用 DNS 服务器：
      - 部署具有有效的 DNS 注册的 OMIVV 设备时，会分配静态 IP 地址和主机名。一个静态 IP 地址可确保在系统重新启动过程中，OMIVV 设备的 IP 地址保持相同。
      - 确保 OMIVV 主机名信息存在于 DNS 服务器的正向和反向查询区域中。
   b. 在**说明**框中，输入说明 - 可选。
4. 在 **vCenter 用户帐户**下，请执行以下步骤：
   a. 在 **vCenter 用户名**框中，输入管理员的用户名或具有必要权限的非管理员用户名。
   b. 在**密码**框中，输入密码。
   c. 在**验证密码**框中，再次输入密码。
   d. 选中**注册 vSphere 生命周期管理器**复选框。
      选中**注册 vSphere 生命周期管理器**复选框可让您使用 vCenter 7.0 及更高版本中的 vSphere 生命周期管理器功能。
5. 单击**注册**。
   如果 vCenter 注册失败，将显示以下错误消息：
   由于凭据错误，无法与给定的 vCenter 服务器 <x> 联系。检查用户名和密码。

### 结果

注册 vCenter 服务器后，OMIVV 注册为 vCenter 插件，“Dell EMC OpenManage Integration”图标出现在 vSphere Client 中，通过它可以访问 OMIVV 功能。

**注:** 对于 OMIVV 设备中的所有 vCenter 操作，OMIVV 使用已注册用户的权限，而不是登录到 VMware vCenter 的用户或 OMIVV 设备本地帐户的权限。例如，具有必要权限的用户 X 向 vCenter 注册 OMIVV，用户 Y 仅具有 Dell 权限。用户 Y 现在可以登录到 vCenter 并且可以从 OMIVV 触发固件更新任务。在执行固件更新任务时，OMIVV 使用用户 X 的权限将主机置于维护模式或重新引导主机。

**注:** 如果您想上传自定义证书颁发机构 (CA) 签名的至证书 OMIVV，请确保先上传新证书再注册 vCenter。如果您在注册 vCenter 后上传新的自定义证书，vSphere Client 会显示通信错误。要解决此问题，请先注销，然后再登录 vCenter。如果问题仍然存在，请重新启动 vCenter 服务器上的 vSphere Client 服务。

# 使用非管理帐户注册 vCenter 服务器

### 前提条件

您可使用 vCenter 管理员凭据或具有 Dell 权限的非管理员用户为 OMIVV 设备注册 vCenter 服务器。

### 关于此任务

要使具有必要权限的非管理员用户能够注册 vCenter 服务器，请执行以下步骤：

### 步骤

1. 创建角色或修改现有角色以使其具有所需权限。
   有关角色所需权限列表的更多信息，请参阅非管理员用户的所需权限。
   有关创建或修改角色以及在 vSphere Client (HTML-5) 中选择权限时所需的步骤，请参阅 VMware vSphere 说明文件
2. 将用户分配到新创建的角色后，您定义角色，然后选择角色权限。
   有关分配具有权限的角色的更多信息，请参阅 VMware vSphere 说明文件。
   具有所需权限的 vCenter 服务器非管理员用户现在可以注册和/或取消注册 vCenter、修改凭据或更新证书。
3. 使用具有必要权限的非管理员用户注册 vCenter 服务器。
4. 注册完成后，将 Dell 权限分配给步骤 1 中创建或修改的角色。请参阅将 Dell 权限分配给现有角色 页面上的 14。

### 结果

具有所需权限的非管理员用户可体验 Dell EMC 主机的 OMIVV 功能。

# 所需的非管理员用户的权限

向 vCenter 注册 OMIVV，非管理员用户必须具有以下权限：

通过非管理员用户向 OMIVV 注册 vCenter 服务器时，如果未分配以下权限，则会显示一条消息：

- 警报
  - 创建警报
  - 修改警报
  - 移除警报
- 分机
  - 注册扩展名
  - 注销扩展名
  - 更新扩展名
- 全局
  - 取消任务
  - 日志事件
  - 设置
- 运行状况更新提供程序
  - 注册
  - 注销

    - 更新
- 主机
    - CIM
        - CIM 交互
- Host.Config
    - 高级设置
    - 更改设置
    - 连接
    - 维护
    - 网络配置
    - 查询补丁程序
    - 安全配置文件和防火墙
- 资源清册
    - 将主机添加到群集
    - 添加独立主机
    - 修改群集
- 生命周期管理器：常规权限
    - 读取

    **注:** vSphere 生命周期管理器常规权限仅适用于 vCenter 7.0 及更高版本。
- 主机配置文件
    - 编辑
    - 查看
- 权限
    - 修改权限
    - 修改角色
- 会话
    - 验证会话
- 任务
    - 创建
    - 更新

**注:** 如果使用非管理员用户注册 vCenter 服务器以访问任何 OMIVV 功能，则非管理员用户必须具有 Dell 权限。有关查找 Dell 权限的更多信息，请参阅将 Dell 权限分配给现有角色 页面上的 14。

# 将 Dell 权限分配给现有角色

**关于此任务**

如果访问 OMIVV 的特定页面时没有向登录用户分配 Dell 权限，则显示错误 2000000。

您可以编辑现有角色以分配 Dell 权限。

**步骤**

1. 使用管理权限登录 vSphere Client (HTML-5)。
2. 在 vSphere Client (HTML-5) 中，展开**菜单**，然后单击**管理 → 角色**。
3. 从**角色提供程序**下拉列表中，选择 vCenter 服务器。
4. 从**角色**列表中，选择 **Dell 操作**，然后单击**权限**。
5. 要分配 Dell 权限，请编辑图标[ ]。
   此时将显示**编辑角色**页面。
6. 在左窗格中，单击 **Dell**，然后为所选角色选择以下 Dell 权限，之后单击**下一步**：
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting

有关 vCenter 内可用的 OMIVV 角色的详细信息，请参阅 Dell 操作角色 页面上的 15。

7. 编辑角色名称，然后输入所选角色的说明（如果需要）。
8. 单击**完成**。
   从 vCenter 中注销，然后重新登录。现在，具有必要权限的用户可以执行 OMIVV 操作。

# vCenter 用户安全

## 安全角色和权限

OpenManage Integration for VMware vCenter 以加密格式存储用户凭据。它不会向客户端应用程序提供任何密码，以避免任何不当请求。备份数据库使用自定义的安全短语进行完全加密，因此数据不会被滥用。

默认情况下，管理员组中的用户具有所有权限。管理员可在 VMware vSphere Web 客户端中使用 OpenManage Integration for VMware vCenter 的所有功能。如果您希望用户有管理产品的必要权限，请执行以下操作：

1. 创建具有必要权限的角色。
2. 使用该用户注册 vCenter 服务器。
3. 包括 Dell 操作角色和 Dell 基础架构部署角色。

### 数据完整性

OpenManage Integration for VMware vCenter、Administration Console 和 vCenter 之间的通信使用 HTTPS 完成。OpenManage Integration for VMware vCenter 生成一个用于在 vCenter 和设备之间进行受信通信的证书。它还在通信和 OpenManage Integration for VMware vCenter 注册之前，它还会验证和信任 vCenter 服务器的证书。

安全 Administration Console 会话具有 15 分钟闲置超时，并且只有在当前浏览器窗口和/或选项卡中时此会话才有效。如果您尝试在新窗口或选项卡中打开会话，则会提示一个安全错误，要求有效的会话。此操作还会阻止用户单击任何可能会攻击 Administration Console 会话的恶意 URL。


**图 2: 安全错误消息**

## 访问控制验证、授权和角色

为执行 vCenter 操作，OpenManage Integration for VMware vCenter 使用 vSphere 客户端的当前用户会话和 OpenManage Integration 的存储管理凭据。OpenManage Integration for VMware vCenter 采用 vCenter 服务器内置的角色和权限模型来授权用户在 OpenManage Integration 和 vCenter 托管对象（主机和群集）上执行的操作。

## Dell 操作角色

该角色包含权限/组以完成设备和 vCenter 服务器任务，其中包括固件更新、硬件资源清册、重新启动主机、将主机置于维护模式或创建 vCenter 服务器任务。

此角色包含以下权限组：

**表. 3: 权限组**

| 组名称 | 说明 |
|---|---|
| 权限组 - Dell.Configuration | 执行主机相关任务、执行 vCenter 相关任务、配置 SelLog、配置 ConnectionProfile、配置 ClearLed、固件更新 |
| 权限组 - Dell.Inventory | 配置资源清册、配置保修检索、配置只读 |

**表. 3: 权限组**

| 组名称 | 说明 |
| --- | --- |
| 权限组 - Dell.Monitoring | 配置监测、监测 |
| 权限组 - Dell. Reporting (Not used) | 创建报告、运行报告 |

## Dell 基础架构部署角色

该角色包含与虚拟机监控程序部署功能相关的权限。

此角色提供的权限为“配置主机凭据配置文件”、“分配标识”和“部署”。

**权限组 — Dell.Deploy-Provisioning**

配置主机凭据配置文件、分配标识、部署。

## 关于权限

OpenManage Integration for VMware vCenter 执行的每个操作均与权限相关联。以下部分列出了可用的操作和关联的权限：

- Dell.Configuration.Perform vCenter-related tasks
  - 退出和进入维护模式
  - 使 vCenter 用户组能查询权限
  - 注册和配置警报，例如，在事件设置页上启用/禁用警报
  - 将事件/警报发布到 vCenter
  - 在事件设置页上配置事件设置
  - 在事件设置页上恢复默认警报
  - 在配置警报/事件设置时检查群集的 DRS 状态
  - 在执行更新或其它配置操作后重新启动主机
  - 监测 vCenter 任务状态/进程
  - 创建 vCenter 任务，例如：固件更新任务、主机配置任务和资源清册任务
  - 更新 vCenter 任务状态/进程
  - 获得主机配置文件
  - 将主机添加到数据中心
  - 将主机添加到群集
  - 将配置文件应用到主机
  - 获得 CIM 凭据
  - 配置主机的兼容性
  - 获得兼容性任务状态
- Dell.Inventory.Configure ReadOnly
  - 在配置连接配置文件时，获得所有 vCenter 主机来构建 vCenter 树
  - 在选定此选项卡时，检查该主机是否是 Dell 服务器
  - 获得 vCenter 的地址/IP
  - 获得主机 IP/地址
  - 基于 vSphere 客户端会话 ID，获得当前 vCenter 会话用户
  - 获得 vCenter 资源清册树以按照树结构显示 vCenter 资源清册
- Dell.Monitoring.Monitor
  - 获得用于发布事件的主机名
  - 执行事件日志操作，例如：获得事件计数，或更改事件日志设置
  - 注册、注销和配置事件/警报 — 接收 SNMP 陷阱和发布事件
- Dell.Configuration.Firmware Update
  - 执行固件更新
  - 在固件更新向导页上加载固件存储库和 DUP 文件信息
  - 查询固件资源清册
  - 配置固件存储库设置
  - 配置暂存文件夹和使用暂存功能执行更新
  - 测试网络和存储库连接

- Dell.Deploy-Provisioning.Create Template
  - 配置硬件配置的配置文件
  - 配置虚拟机监管程序部署配置文件
  - 配置连接配置文件
  - 分配标识
  - 部署
- Dell.Configuration.Perform host-related tasks
  - 闪烁 LED、清除 LED
  - 启动 iDRAC 控制台
  - 显示和清除 SEL 日志
- Dell.Inventory.Configure Inventory
  - 在 Dell 服务器管理选项卡上显示系统资源清册
  - 获得存储详细信息
  - 获得电源监测详细信息
  - 在连接配置文件页上的创建、显示、编辑、删除和测试连接配置文件
  - 计划、更新和删除资源清册计划
  - 在主机上运行资源清册

# 用户和凭据管理

## 预加载帐户

下表介绍了预加载的 OMIVV 帐户：

**表. 4: 预加载帐户**

| 用户帐户 | 说明 |
|---|---|
| OpenManage Integration for VMware vCenter 管理员 | OMIVV Web 应用程序管理的默认用户。 |
| 只读用户。 | OMIVV 提供单个默认本地只读用户帐户。<br>管理员只能使用虚拟机远程控制台登录到 OMIVV。<br>在故障排除期间可以使用此帐户查看关键设备状态和日志。 |
| Linux 操作系统 root | root 操作系统帐户不可访问。技术支持团队使用 root 帐户调试字段问题。 |

## 默认凭据

下表介绍了预加载的 OMIVV 帐户的默认凭据。

**表. 5: 默认凭据**

| 帐户 | 用户 | 密码 |
|---|---|---|
| OpenManage Integration for VMware vCenter 管理员 | 管理员 | 在部署后的首次启动时设置。有关更改 admin 密码的更多信息，请参阅更改 OMIVV 设备密码 页面上的 18。 |
| 只读用户 | 只读 | 在部署后的首次启动时设置。在以只读用户身份登录后，可以使用标准 Linux 密码更改命令重新配置只读用户密码。 |
| Linux 操作系统 root | Root | 操作系统 root 密码是在部署 OMIVV 时设置的。 |

# 管理凭据

如果您是第一次登录 Dell EMC 管理控制台，请以管理员身份登录（默认用户名为 admin）。

**注:** 如果忘记了管理员密码，将无法从 OMIVV 设备恢复。

## 更改 OMIVV 设备密码

**关于此任务**

可以在 vSphere 客户端中使用控制台更改 OMIVV 设备密码。

**步骤**

1. 打开 OMIVV Web 控制台。
2. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置**实用程序中，单击**更改管理员密码**。
   按照屏幕上的说明设置密码。
3. 在**当前密码**文本框中，输入当前管理员密码。
4. 在**新密码**文本框中输入新密码。
5. 在**确认新密码**文本框中输入新密码。
6. 单击**更改管理员密码**。

# 授权

OMIVV 设备支持单个管理用户。

登录 OMIVV 后，管理员只能访问 OMIVV 设备配置功能，如：

- 注册新 vCenter 服务器
- 配置设备
- 使用 RPM 以及备份和还原升级 OMIVV 设备
- 设置网络时间协议服务器
- 配置部署模式
- 生成证书签名请求 (CSR)
- 上传 HTTPS 证书
- 设置全局警报
- 生成和下载故障排除捆绑包

# 网络安全性

通过限制 TCP 和 UDP 端口的入站和出站网络流量，OMIVV 设备使用预配置的防火墙来增强安全性。本部分的表中列出了 OMIVV 使用的入站和出站端口。

## 网络暴露

OpenManage Integration for VMware vCenter 在与远程系统通信时使用入站和出站端口。

## 出站端口

在连接到远程系统时，OMIVV 可以使用出站端口。

下表中列出的端口是 OMIVV 出站端口。

**表. 6: 出站端口**

### 表. 6: 出站端口

| 端口号 | 第 4 层协议 | 服务 |
|---|---|---|
| 7 | TCP、UDP | ECHO |
| 22 | TCP | SSH |
| 25 | TCP | SMTP |
| 53 | UDP、TCP | DNS |
| 67、68 | TCP | DHCP |
| 80 | TCP | HTTP |
| 88 | TCP、UDP | Kerberos |
| 111 | TCP、UDP | ONC RPC |
| 123 | TCP、UDP | NTP |
| 161-163 | TCP、UDP | SNMP |
| 389 | TCP、UDP | LDAP |
| 443 | TCP | HTTPS |
| 448 | TCP | Data Protection Search Admin REST API |
| 464 | TCP、UDP | Kerberos |
| 514 | TCP、UDP | rsh |
| 587 | TCP | SMTP |
| 636 | TCP、UDP | LDAPS |
| 902 | TCP | VMWare ESXi |
| 2049 | TCP、UDP | NFS |
| 2052 | TCP、UDP | mountd、clearvisn |
| 3009 | TCP | Data Domain REST API |
| 5672 | TCP | RabbitMQ over amqp |
| 8443 | TCP | MCSDK 8443 替代 443 |
| 9002 | TCP | Data Protection Advisor REST API |
| 9443 | TCP | Avamar 管理控制台 Web 服务 |

## 入站端口

在连接到 OMIVV 时可供远程系统使用的入站端口。

下表列出的端口是 OMIVV 入站端口。

### 表. 7: 入站端口

| 端口号 | 第 4 层协议 | 服务 |
|---|---|---|
| 22 | TCP | SSH |
| 80 | TCP | HTTP |
| 443 | TCP | HTTPS |
| 5671 | TCP | RabbitMQ over amqp |

# 数据安全

OMIVV 维护的数据存储在设备内的内部数据库中，不能从外部访问。

通过 OMIVV 传输的数据受到安全通信信道的保护。

**注:** 建议 RESTful API 用户根据您的环境限制存储安全检索的凭据和数据。

# 加密

OMIVV 对以下组件使用加密：

- 访问控制
- 验证
- 数字签名

# 管理证书

OMIVV 使用证书进行安全 HTTP 访问 (HTTPS)。

默认情况下，OMIVV 将对 HTTPS 安全事务安装和使用自签名证书。

为增强安全性，建议使用证书颁发机构 (CA) 签名的或自定义的证书。

自签名证书足以在 Web 浏览器和服务器之间建立加密通道。自签名证书不可用于身份验证。

您可以使用以下类型的证书进行 OMIVV 身份验证：

- 自签名证书

  当设备的主机名更改时，OMIVV 会生成自签名证书。
- 由受信证书颁发机构 (CA) 供应商签名的证书。

**注:** 创建证书时，请考虑公司策略。

## 更新已注册 vCenter 服务器的证书

### 关于此任务

OpenManage Integration for VMware vCenter 通过使用 2048 位密钥长度的 RSA 加密标准，使用 OpenSSL API 创建证书签名请求 (CSR)。

如果 vCenter 服务器上的证书更改，请使用以下任务为 OMIVV 导入新证书：

### 步骤

1. 转至 https://<设备 IP 或主机名>。
2. 在左侧窗格中，单击 **VCENTER 注册**。
   已注册的 vCenter 服务器显示在工作窗格中。
3. 要更新 vCenter 服务器 IP 或主机名的证书，请单击**更新**。

## 生成证书签名请求 (CSR)

### 前提条件

默认情况下，OMIVV 具有自签名证书。如果您需要自定义证书颁发机构 (CA) 签名的 OMIVV 证书，则建议先上传新证书再注册 vCenter。

### 关于此任务

生成新 CSR 可阻止通过以前生成的 CSR 创建的证书上传到设备。要生成 CSR，请执行以下操作：

**步骤**

1. 在**设备管理**页面中，单击 **HTTPS 证书**区域中的**生成证书签名请求。**
   此时将显示一条消息，表明如果生成新请求，则使用以前的 CSR 创建的证书无法再上传到设备。要继续请求，请单击**继续。**
2. 如果继续请求，则在**生成证书签名请求**对话框中，输入通用名称、组织名称、地点、省/自治区/直辖市、国家/地区、电子邮件地址和主题备用名称 (SAN) 等相关信息，然后单击 **继续。**

   **注:** OMIVV 不支持 SAN 的多个值。

3. 单击**下载**，然后将所得 CSR 保存到可访问的位置。

## 上传 HTTPS 证书

**前提条件**

确保证书使用 PEM 格式。

**关于此任务**

您可以使用 HTTPS 证书在 OMIVV 设备和主机系统或 vCenter 之间进行安全通信。要设置此类型的安全通信，请将 CSR 证书发送到签署机构，然后使用管理控制台上载生成的 CSR。还有一个自签名的默认证书可用于安全通信；此证书对于每个安装来说都是唯一的。

**步骤**

1. 在**设备管理**页面中，单击 **HTTPS 证书**区域中的**上传证书。**
2. 在**上传证书**对话框中单击**确定。**
3. 要上传证书，请单击**浏览**，然后单击**上传。**
   要检查状态，请转至已注册 vCenter 的 vSphere Client 的**事件控制台。**

**结果**

在上传证书时，OMIVV 管理控制台在最长 3 分钟内无响应。完成“上传 HTTPs 证书”任务后，关闭该浏览器会话，然后在新的浏览器会话中访问管理员门户。

## 还原默认的 HTTPS 证书

**步骤**

1. 在**设备管理**页面中，单击 **HTTPS 证书** 区域中的**还原默认证书。**
2. 在**还原默认证书**对话框中，单击**应用。**

**结果**

在还原证书时，OMIVV 管理控制台在最长 3 分钟内无响应。在还原默认 HTTPs 证书任务完成后，关闭浏览器会话并在新的浏览器会话中访问管理员门户。

# 审计和日志记录

管理员用户可以使用 OMIVV 管理控制台生成包含所有相关日志的故障排除捆绑包。

有关更多信息，请参阅 创建和下载故障排除捆绑包 页面上的 22。

只读帐户通过允许用户在运行时读取设备的各种参数，可帮助排除设备故障。有关检查特定参数的高级故障排除技术支持指南。

**注:** 只有 OMIVV 管理员用户可以在设备上执行写入操作。OMIVV 日志中不提供用户审核。有关从 vCenter 插件执行的 vCenter 操作的详细信息，请参阅 vCenter 审核日志。对于 RESTful API，客户端必须能够处理审核日志记录。

## 创建和下载故障排除捆绑包

**关于此任务**

故障排除捆绑包含有 OMIVV 设备日志记录信息，可用于帮助解决问题或将其发送给技术支持部门。OMIVV 不会记录任何用户敏感数据。

**步骤**

1. 在**支持**页面上，单击**创建并下载故障排除捆绑包。**
   此时将显示**故障排除捆绑包**对话框。
2. 在**故障排除捆绑包**对话框中，单击**创建。**
   根据日志的大小，创建捆绑包可能需要一些时间。
3. 要保存文件，请单击**下载。**
   此时会显示 Dell EMC OMIVV 管理控制台登录页面。
4. 登录 Dell EMC OMIVV 管理控制台。
5. 下载故障处理包。有关更多信息，请参阅 生成和下载故障排除捆绑包 页面上的 22。

## 生成和下载故障排除捆绑包

**前提条件**

要生成故障排除捆绑包，请确保您登录到管理员门户。

**关于此任务**

故障排除捆绑包含有 OMIVV 日志记录信息，可用于帮助解决问题或将其发送给技术支持部门。

**步骤**

1. 在**设备管理**页面中，单击**生成故障排除捆绑包。**
2. 单击**下载故障排除捆绑包。**

# 可服务性

通过支持网站 **https://www.dell.com/support** 可访问许可信息、产品文档、咨询、下载和故障排除信息。此信息可帮助您在联系支持团队之前解决产品问题。

OMIVV 服务人员不需要特殊登录。如果故障排除包不足以解决问题，该人员可以启用 root 用户来收集更多信息。

确保在第一时间安装安全修补程序和其他更新，包括 OMIVV vCenter 操作系统更新。

## 安全修补程序

定期 OMIVV 更新，包括安全更新，以及根据需要发布的纯安全更新。

更新是由补丁累积形成的，并在支持网站上发布，OMIVV 用户同样也是在 vCenter 上收到通知。

# OMIVV 操作系统更新

针对 OMIVV 操作系统的安全修补程序和修复程序会定期发布。

这些修复程序必须通过 RPM 更新包安装在 OMIVV 的现有 OVF 部署上。强烈建议您通过 RPM 更新在 OMIVV 服务器上安装这些安全修补程序和修复程序（如果有）。

# 产品代码完整性

OMIVV 软件安装程序由 Dell 签名。建议您验证 OMIVV 安装程序签名的真实性。

# 5

# 其他配置和管理

**主题：**



## OpenManage Integration for VMware vCenter (OMIVV) 许可

OMIVV 有两种类型的许可证：

- 评估许可证 — 当 OMIVV 设备首次开机时，将自动安装评估许可证。试用版包含一个评估许可证，可由 OMIVV 管理五个主机（服务器）。此 90 天的试用版本是发货时随附的默认许可证。
- 标准许可证 — 您可以购买由 OMIVV 管理的任意数量的主机许可证。此许可证包括产品支持和 OMIVV 设备更新。标准许可证可使用三年或五年。购买的任何附加许可证都会延长现有许可证的期限。标准许可证会覆盖评估许可证。

单个 XML 密钥的许可证期限基于原始订单的销售日期计算。任何已上传新许可证将在任何先前的到期许可的 90 天宽限期结束后反映在计数中。

OMIVV 最多支持 15 个 vCenter 实例。从评估许可证升级到完整标准许可证后，您将收到一封订单确认电子邮件，然后便可从 Dell Digital Locker 下载许可证文件。将许可证 .XML 文件保存到您的本地系统，并使用**管理控制台**上传新的许可证文件。

购买许可证时，可从 Dell Digital Lockerhttps://www.dell.com/support 下载 .XML 文件（许可证密钥）。如果您无法下载许可证密钥，请转至 **https://www.dell.com/support** 处的联系订单支持找到您的产品对应的区域 Dell 支持电话号码，联系 Dell 支持部门。

许可会在 OMIVV 管理控制台中显示以下信息：

- 最大 vCenter 连接许可证数 — 可启用最多 15 个注册的和使用中的 vCenter 连接。
- 最大主机连接许可证数 — 已购买的主机连接数量（对于单个 OMIVV 实例，最多支持 2000 个主机）。
- 使用中 — 使用中的 vCenter 连接或主机连接许可证的数量。对于主机连接，该数量代表已进行过资源清册的主机（或服务器）的数量。
- 可用 — 可供未来使用的 vCenter 连接或主机连接许可证的数量。

在尝试将主机添加到主机凭据配置文件时，如果许可的主机的数量超出许可证数量，将无法添加更多主机。OMIVV 不支持管理超过主机许可证的数量的主机数。

使用 OMIVV RESTful API 获取有关许可证的详细信息。有关更多信息，请参阅 https://www.dell.com/support 上的 *OpenManage Integration for VMWARE API 指南*。

**注:** 任何活动许可证都可以用于 OMIVV 5.x 版本。从以前的 OMIVV 实例备份或从 Digital Locker 再次下载的许可证可以用于 OMIVV 的当前实例。

## 保护真实性和完整性

为确保产品完整性，OMIVV 安装和更新组件已经过签名。

为确保通信完整性，建议使用 CA 签名的证书。

## 管理 OMIVV 中的备份和还原

为防止 OMIVV 发生灾难情况，建议您对 OMIVV 执行备份。需要时，您可通过这些备份还原 OMIVV。有关备份和还原的更多信息，请参阅 **https://www.dell.com/support** 上的 OMIVV 用户指南。