

ZENworks 2020 Update 1 自述文件

2020 年 6 月

本自述文件中的信息与 ZENworks 2020 Update 1 版本相关。

- ◆ [ZENworks 2020 Update 1 中的新功能](#)（第 1 页）
- ◆ [计划部署 ZENworks 2020 Update 1](#)（第 1 页）
- ◆ [下载和部署 ZENworks 2020 Update 1](#)（第 3 页）
- ◆ [ZENworks 2020 Update 1 中已解决的问题](#)（第 4 页）
- ◆ [ZENworks 2020 Update 1 中仍然存在的问题](#)（第 4 页）
- ◆ [ZENworks 2020 Update 1 中的已知问题](#)（第 4 页）
- ◆ [其他文档](#)（第 7 页）
- ◆ [法律声明](#)（第 7 页）

ZENworks 2020 Update 1 中的新功能

有关此版本中包括的新功能的信息，请参见 [《ZENworks 2020 Update 1 中的新功能》](#)。

计划部署 ZENworks 2020 Update 1

请遵照以下准则规划如何在您的管理区域中部署 ZENworks 2020 Update 1:

- ◆ 如果您使用的是 ZENworks 2017 上的磁盘加密或更早版本的全盘加密代理，要将这些代理更新到 ZENworks 2020 Update 1，必须先执行一些额外的步骤，然后才可将这些受管设备上的 ZENworks 代理更新到 ZENworks 2020 Update 1。这些步骤包括解密适用的设备、去除然后删除早于 17.1 版本的磁盘加密策略，并在更新 ZENworks 代理后部署新的磁盘加密策略。

有关从 17.0 或更早版本更新全盘加密代理的完整指导，请参见 [《ZENworks 2020 Update 1 - Full Disk Encryption Update Reference》](#)（ZENworks 2020 Update 1 - 全盘加密更新参考手册）。

- ◆ 必须先升级主服务器，然后将从属服务器更新到 ZENworks 2020 Update 1，最后更新受管设备。在将区域中的所有主服务器升级到 ZENworks 2020 Update 1 之前，请不要升级受管设备和从属服务器（也不要再在区域中添加新的 2020 Update 1 代理）。

注释：在升级所有主服务器之前，代理可能会从区域中接收不一致的数据。因此，此部分的过程应在尽量短的时间内进行 - 最好是在升级第一个主服务器之后立即进行。

- ◆ 您可以直接将 2020 Update 1 版本部署到以下设备上：

| 设备类型 | 操作系统 | 最低的 ZENworks 版本 |
|-------|---------------------|-------------------------|
| 主服务器 | Windows 和 Linux | ZENworks 2020 版和其后的版本 |
| 从属服务器 | Windows、Linux 和 Mac | ZENworks 11.3.x 版和其后的版本 |
| 受管设备 | Windows | ZENworks 11.3.x 版和其后的版本 |
| | Linux | ZENworks 11.3.x 版和其后的版本 |
| | Mac | ZENworks 11.3.x 版和其后的版本 |

- ◆ 升级到 ZENworks 2020 Update 1 之后，系统将重引导一次。但是，在以下情况下，需要重引导两次：
 - ◆ 如果您在启用端点安全性的情况下从 11.3.x 更新到 ZENworks 2020 或其后的版本 (2020 Update 1)，则需要再次重引导以装载 ZESNETAccess 驱动程序。
 - ◆ 如果受管设备使用的是 Windows 10，且启用了客户端自我防御，当您从 11.4.x 升级到 ZENworks 2020 或其后的版本 (2020 Update 1) 时，需要在 ZENworks 控制中心禁用客户端自我防御，重引导受管设备，然后运行更新，这需要再次重引导设备。

重要：运行早于 11.3.x 的版本的受管设备必须先升级到 11.3.x。系统会在升级到 11.3.x 之后重引导，然后会在部署 ZENworks 2020 Update 1 系统更新后再次重引导。

- ◆ 在安装系统更新之前，请确保以下位置有足够的可用磁盘空间：

| 位置 | 说明 | 磁盘空间 |
|---|---------------------------------|--------|
| Windows: %zenworks_home%\install\downloads | 用于维护代理包。 | 6.2 GB |
| Linux: opt/novell/zenworks/install/downloads | | |
| Windows: %zenworks_home%\work\content-repo | 用于将 zip 文件导入内容系统。 | 6.2 GB |
| Linux: /var/opt/novell/zenworks/content-repo | | |
| 代理超速缓存 | 用于下载更新 ZENworks 服务器所需的相应系统更新内容。 | 1.5 GB |
| 系统更新文件被复制到的位置。这只适用于用于导入系统更新 zip 文件的 ZENworks 服务器 | 用于储存下载的系统更新 zip 文件。 | 6.2 GB |

下载和部署 ZENworks 2020 Update 1

有关下载和部署 ZENworks 2020 Update 1 的指导，请参见《[ZENworks System Updates Reference](#)》（ZENworks 系统更新参考手册）。

要使用 ZCC 中的检查更新操作查看可用的更新列表，您需要先执行以下章节中详述的步骤重新注册系统更新权利：

重新注册系统更新权利以激活 ZENworks 许可证

- 1 登录 ZENworks 控制中心 (ZCC)。
- 2 导航到配置 > 基础结构管理 > 系统更新设置。
- 3 在“系统更新权利”部分，单击权利状态字段旁边的配置链接。
- 4 指定电子邮件地址和激活代码。
Micro Focus Customer Center 中的系统更新权利或 ZENworks Configuration Management 激活代码下会提供激活代码。
- 5 单击激活。激活许可证后，您可以在系统更新页面中单击操作 > 检查更新来查看可用的系统更新。
有关详细信息，请参见 [TID 7024521](#)。

如果您的管理区域包含版本低于 ZENworks 2020 的主服务器，则只有在所有这些主服务器都已升级到 ZENworks 2020 之后，才能将 ZENworks 2020 Update 1 部署到这些主服务器。有关指导，请参见《[ZENworks 升级指南](#)》。

有关管理任务，请访问 [ZENworks 2020 Update 1](#) 文档网站。

重要：在将区域中的所有连接代理从属服务器更新之前，请勿更新远程管理 (RM) 查看器。要通过连接代理执行远程管理，需要确保 RM 查看器和连接代理的版本相同。

务必在下载和部署 ZENworks 2017 Update 1 更新之前阅读[计划部署 ZENworks 2020 Update 1](#)（第 1 页）。

在区域中的所有主服务器都已升级到 ZENworks 2020 之前，请勿部署 ZENworks 2020 Update 1

要执行此更新，需要对数据库纲要进行更改。在初始增补程序安装期间，服务将只在总主服务器或专用主服务器上运行。这是为了确保其他主服务器不会尝试访问数据库中正在更改的表。

更新总主服务器或专用主服务器后，其余服务器上将继续运行服务；如果更新是指派到所有服务器，则会同时应用该更新。

注释：在更新期间，您不需要在服务器上手动停止或启动服务。服务将会自动停止和启动。

如果您推迟系统更新并注销受管设备，系统会根据部署日程安排在设备上应用系统更新。

有关 ZENworks 2017 Update 1 管理区域中受支持受管设备和从属服务器版本的列表，请参见[受支持的受管设备和从属服务器版本](#)。

ZENworks 2020 Update 1 中已解决的问题

此版本中解决了先前版本中发现的部分问题。有关已解决问题的列表，请参见[支持知识库](#)中的 TID 7024523。

ZENworks 2020 Update 1 中仍然存在的问题

在 ZENworks 2020 Update 1 的先前版本中发现的部分问题仍未得到解决。请查看以下自述文档了解详细信息：

- ◆ [ZENworks 2020 自述文件](#)

ZENworks 2020 Update 1 中的已知问题

本章包含有关使用 ZENworks 2020 Update 1 时可能发生的问题的信息：

- ◆ [ZENworks Patch Management](#)（第 4 页）
- ◆ [ZENworks 代理](#)（第 5 页）
- ◆ [YUM 服务](#)（第 6 页）
- ◆ [ZENworks Full Disk Encryption](#)（第 6 页）
- ◆ [ZENworks Endpoint Security](#)（第 6 页）
- ◆ [Vertica](#)（第 7 页）

ZENworks Patch Management

- ◆ 升级到 ZENworks 2020 Update 1 后，在低于 Update 1 的版本中创建的自定义增补程序的部署分发包细节不会显示在该增补程序的“关系”选项卡中（第 4 页）
- ◆ 如果在刷新时执行增补程序（漏洞检测）扫描，其他分发包的安装可能会出现延迟（第 4 页）
- ◆ 如果等待下载的增补程序在增补程序源中已禁用，在订阅更新期间它们可能会停滞在“已排入队列”状态（第 5 页）

升级到 ZENworks 2020 Update 1 后，在低于 Update 1 的版本中创建的自定义增补程序的部署分发包细节不会显示在该增补程序的“关系”选项卡中

升级到 ZENworks 2020 Update 1 后，在旧版 ZENworks 中创建的自定义增补程序的部署分发包细节不会显示在自定义增补程序的“关系”选项卡中。

解决方法：无

如果在刷新时执行增补程序（漏洞检测）扫描，其他分发包的安装可能会出现延迟

在刷新时执行增补程序扫描（漏洞检测）可能需要一段时间，导致其他分发包的安装延迟。

解决方法：作为最佳实践，建议您不要在刷新时执行增补程序扫描。

如果等待下载的增补程序在增补程序源中已禁用，在订阅更新期间它们可能会停滞在“已排入队列”状态

如果等待下载的增补程序由于被取代已在增补程序源中禁用，在订阅更新期间，这些增补程序可能会停滞在“已排入队列”状态。

解决方法：登录 ZCC，导航到“安全性”>“增补程序下载细节”，然后在“超速缓存状态”窗格中单击“操作”>“取消待处理下载”。

ZENworks 代理

- ◆ [RHEL 8.0 设备上出现 ZENworks 图标显示问题（第 5 页）](#)
- ◆ [在使用通配符证书的区域中，Linux 主服务器的 CSR 为空（第 5 页）](#)
- ◆ [数据库中未更新 JoinProxy 细节（第 5 页）](#)

RHEL 8.0 设备上出现 ZENworks 图标显示问题

ZENworks 图标未显示在 RHEL 8.0 设备的桌面菜单栏上。

解决方法：无。

在使用通配符证书的区域中，Linux 主服务器的 CSR 为空

在使用通配符证书的区域中，Linux 主服务器上的代理不会列出任何 CSR。

解决方法：在代理上，运行 `zac cache-clear` 命令并重启动代理服务。有关 ZAC 命令的详细信息，请参见《[ZENworks 命令行实用程序参考手册](#)》。

数据库中未更新 JoinProxy 细节

远程控制受管设备时，即使通过 JoinProxy 连接了受管设备，JoinProxy 细节也不会显示在 ZCC 中。Zen-join 代理日志文件中会记录“No Primary Server is available to update Joinproxy information into database”讯息，并且在技术人员应用程序中，服务器状态显示为“最近的服务器不可用”。

解决方法：在代理上，运行 `zac cache-clear` 命令并重启动代理服务。有关 ZAC 命令的详细信息，请参见《[ZENworks 命令行实用程序参考手册](#)》。

YUM 服务

- ◆ 在 ZENworks 主服务器上托管 YUM 服务时出现问题（第 6 页）

在 ZENworks 主服务器上托管 YUM 服务时出现问题

托管 YUM 服务时可能会出现以下问题：

- ◆ 如果您在 ZENworks 2017 设备上托管 YUM 服务，该服务在迁移到 ZENworks 2020 后可能会变成不可用状态。迁移后会删除所有现有 YUM 储存库的细节，因而必须重新创建这些储存库。
- ◆ 如果您在独立的 ZENworks 2017 Linux 主服务器上托管 YUM 服务，该服务在主服务器直接升级（无需通过 ZENworks 2017.x 更新）到 ZENworks 2020 后可能会变成不可用状态。虽然 YUM 储存库的细节不会被删除，但用户必须手动重新配置 YUM 服务。

解决方法：如果 YUM 服务在升级后不可用，请联系 Micro Focus 客户关怀部门，获取有关如何正确重新配置该服务的信息。

ZENworks Full Disk Encryption

- ◆ 在操作系统为 Windows 7 的受管设备上，使用 PBA 的单点登录出现问题（第 6 页）
- ◆ 虚拟机 (VM) 上的其他分区不会加密（第 6 页）

在操作系统为 Windows 7 的受管设备上，使用 PBA 的单点登录出现问题

出于安全原因，在某些操作系统为 Windows 7 的受管设备上，使用预引导鉴定 (PBA) 的单点登录可能不会鉴定 Windows 登录。

解决方法：用户可能需要在 使用 PBA 进行鉴定后的一分钟内按 Ctrl+Alt+Del，以使单点登录正常工作。如果已跳过单点登录，用户仍可使用其 Windows 身份凭证登录。

虚拟机 (VM) 上的其他分区不会加密

磁盘加密策略设计为仅加密“固定磁盘”。出于安全原因，如果在向 VM 上的其他分区指派磁盘加密策略时选择“加密所有驱动器”选项，系统可能会将这些设备解释为“可卸储存”驱动器。

解决方法：在磁盘加密策略配置中，使用“加密特定的本地固定卷”选项而不是“加密所有本地固定卷”选项，为具有多个卷的 VM 指派一个驱动器盘符。

ZENworks Endpoint Security

- ◆ 如果重新安装 ZENworks 代理时不重引导系统，可能会阻止安装 zeswifi 驱动程序（第 6 页）

如果重新安装 ZENworks 代理时不重引导系统，可能会阻止安装 zeswifi 驱动程序

每次在受管设备上安装或卸载 ZENworks 代理后，都需要重引导系统。如果在设备上安装 ZENworks 代理后未重引导又再次安装该代理，则重新安装后可能需要重引导两次，以安装 zeswifi 驱动程序。否则，在实施端点安全性 Wi-Fi 策略时可能会遇到问题。

Vertica

- ◆ 在多节点 Vertica 群集环境中进行系统更新期间，当 `verticaDBMigrate` 配置操作无法完成时，`dashlet` 中会显示不一致的数据（第 7 页）

在多节点 Vertica 群集环境中进行系统更新期间，当 `verticaDBMigrate` 配置操作无法完成时，`dashlet` 中会显示不一致的数据

将系统更新到 ZENworks 2020 Update 1 版本期间，启用了 Vertica 的设备服务器会运行 `verticaDBmigrate` 配置操作。运行此操作的目的是将 RDBMS 中的新表迁移到最新版本中新增的 Vertica 数据库。如果 Vertica 群集中存在多个节点，其中的一个节点将运行此配置操作，而其余节点以及非设备服务器将完成系统更新。但是，如果配置操作出于任何原因未在运行该操作的服务器上完成，当您从成功完成系统更新的其他服务器访问 `dashlet` 数据时，可能会发现 `dashlet` 中新表的数据不一致。这些表将从 RDBMS 而不是 Vertica 数据库获取数据。

解决方法：在启用了 Vertica 的所有设备服务器上手动运行 `verticaDBmigrate` 配置操作。有关此配置操作的详细信息，请参见《*Vertica Reference Guide*》（Vertica 参考指南）中的“[Migrating Data to Vertica](#)”（将数据迁移到 Vertica）。

其他文档

本自述文件列出了 ZENworks 2020 Update 1 版本特有的问题。有关所有其他 ZENworks 2020 Update 1 文档，请访问 [ZENworks 2020 文档网站](#)。

法律声明

有关法律声明、商标、免责声明、担保、出口和其他使用限制、美国政府权限、专利政策以及 FIPS 合规性的信息，请参见 <https://www.novell.com/company/legal/>。

版权所有 © 2008 - 2020 Micro Focus Software Inc. 保留所有权利。

