MICRO FOCUS

ZENworks 2020 Update 2

新功能参考手册

2021 年 8 月

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/。

目录

关于本指南

本 《*ZENworks 新功能参考手册*》介绍 ZENworks 2020 Update 2 版本中的新功能。本指南包括以下几章：

适用对象

本指南的适用对象为 ZENworks 管理员。

反馈

我们希望收到您对本手册和本产品中包含的其他文档的意见和建议。请使用联机文档每个页面底部的**评论主题**功能。

其他文档

ZENworks 还有采用 PDF 和 HTML 格式的其他支持文档，可供您了解并实施本产品。有关其他文档，请访问 ZENworks 文档网站。

1 ZENworks 2020 Update 2 中的新功能

以下几节介绍 ZENworks 2020 Update 2 中的新功能和增强功能：

平台支持

此版本支持下列新平台：

- CentOS （作为受管设备）
- macOS 11 (Big Sur) （作为受管设备）
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 （主服务器）
  - SLES 15 SP2 （受管设备 - 包括 SLES for SAP）
  - SLED 15 SP2 （受管设备）
- 新的 RHEL 和 Scientific Linux 平台
  - Scientific Linux 7.7 和 7.8
  - RHEL 7.8 和 8.2

安装和升级

由于 ZENworks 的目标是采用更稳健、更灵活的体系结构，并与 Micro Focus 标准保持一致，因此 ZENworks 2020 Update 2 版本为安装和升级过程引入了一些增强功能。此版本中引入的更改如下：

安装 Docker 和 Docker Compose

在 Linux 主服务器上升级或安装 ZENworks 2020 Update 2 之前，需要在该服务器上安装 Docker 和 Docker Compose。有关 Docker 的详细信息，请参见 https://docs.docker.com/。

将服务器数据迁移到新文件路径

在 Windows、 Appliance 或 Linux 主服务器上升级到 ZENworks 2020 Update 2 后，之前位于 Novell 文件路径中的 ZENworks 服务器数据 （例如 MSI、 RPM、日志和配置文件）将移至新 Micro Focus 文件路径。

例如，在 Linux 服务器上，之前位于 /etc/opt/novell/zenworks 中的配置文件现在位于 /etc/opt/microfocus/zenworks 中。同样，在 Windows 服务器上，之前位于 C:\Program Files (x86)\Novell\ZENworks\conf 中的配置文件现在位于 C:\Program Files (x86)\Micro Focus\ZENworks\conf 中。

与 ZENworks 代理相关的文件和数据仍将保留在旧 Novell 位置。

ZENworks 服务器服务已更名

在 Windows、 Appliance 或 Linux 主服务器上升级到 ZENworks 2020 Update 2 后，某些 ZENworks 服务器服务（例如 ZENServer、ZENLoader 和 ZENJoinProxy 服务）将从 Novell 更名为 Micro Focus。例如，在 Linux 服务器上， novell-zenserver.service 将更名为 microfocus-zenserver.service。

引入了一个新环境变量

对于 Windows 服务器，引入了一个新环境变量 %ZENSERVER_HOME%，该变量同样指向非默认路径的服务器安装位置 (C:\Program Files(x86)\Micro Focus\ZENworks)。

TLS 版本

如果您全新安装了 ZENworks 2020 Update 2，区域中默认会启用 TLS 1.2，当您尝试注册 Microsoft.NET 版本低于 4.7 的设备时，设备注册将会失败，但会在设备上安装代理。

如果您要将现有区域升级到 ZENworks 2020 Update 2，则默认不会启用 TLS 1.2。如果您要在区域中启用 TLS 1.2，则某些功能可能无法按预期工作，并且请确保区域中的所有设备上都安装了 Microsoft.NET 4.7。

如果您已在区域中启用 TLS 1.2，那么要想注册设备，应在设备上安装 Microsoft .NET 4.7。

替换主服务器

有关将第一台主服务器替换为第二台主服务器或将现有主服务器替换为新的主服务器的更多细节，请参见 《*ZENworks Disaster Recovery Reference*》（ZENworks 灾难恢复参考手册）中的 “*Replacing Primary Servers*” （替换主服务器）。

将主服务器迁移到 Appliance

有关将现有主服务器 （Windows 或 Linux）迁移到 Appliance 服务器的过程的更多细节，请参见 《*ZENworks Primary Server and Satellite Reference*》（ZENworks 主服务器和从属服务器参考手册）中的 “*Moving from a Windows or Linux Primary Server to Appliance*” （从 Windows 或 Linux 主服务器迁移到 Appliance）。

ZENworks Configuration Management

Windows 10 设备管理

ZENworks 2020 Update 2 版本中添加了一些新功能，可让您使用 Windows 10 设备上的内置 MDM 代理来管理这些设备的整个生命周期。为了应对超出 Windows 10 设备功能范围之外的使用情形，您还可以在使用 Windows 10 MDM 代理的设备上部署 ZENworks 代理。

有关本节中所列各项功能的详细信息，请参见 《Windows MDM Reference》（Windows MDM 参考手册）。

新功能如下：

配置功能

您现在可以配置 Windows 通知服务 (WNS)，以向通过 Windows 新式管理功能管理的 Windows 设备发送推送通知。

注册功能

引入了下列注册功能。

注册方法：可以使用以下方法将 Windows 10 设备注册到 ZENworks。

- 供应包 (PPKG) 注册
- 加入 Azure Active Directory (Azure AD)
- AutoPilot 注册

部署 ZENworks 代理：现在，您可以在已使用 MDM 注册模式注册的 Windows 10 设备上部署 ZENworks 代理。

配置使用条款：您可以为设备指派使用条款策略，以添加在使用 Azure AD Join 或 Auto Pilot 注册功能注册 Windows 10 设备时，要在代理上显示的使用条款内容。

管理功能

引入了下列管理功能：

部署 Windows 10 MDM 分发包：现在，您可以将以下分发包部署到 Windows 10 MDM 设备：

注释：对这些分发包的支持属于实验性支持，应该仅用于评估目的。

- 使用 “Windows 10 MDM - 安装 MSI” 分发包在 Windows 10 MDM 设备上部署 Microsoft 安装程序 (MSI) 包。
- 使用 Windows 10 MDM CSP 分发包分发配置服务提供程序 (CSP)，以在 Windows 10 MDM 设备上部署通过 CSP 提供的各种配置。

启动快速任务：支持对 Windows 10 MDM 设备执行以下快速任务：

- 删除设备
- 取消注册设备
- 淘汰设备
- 取消淘汰设备
- 丢失设备
- 取消注册设备

其他功能

针对 Windows 10 MDM 功能引入的一些其他功能如下：

- Windows 10 设备支持自动调节。
- CA 重建过程现在会向 Windows 10 MDM 设备颁发证书。
- MS Graph API 设置已更名为 Azure MDM 应用程序，需要进行重新配置才能利用此版本中引入的新增强功能。

开始使用新式管理

“ 移动设备管理入门 ” 页面已更新，现在还包含 Windows 10 MDM 设备的注册和管理功能。有关详细信息，请参见 《Modern Management Reference》（新式管理参考手册）。

ZENworks 映像

在 WinPE 上使用分发包名称恢复映像：在 ZENworks 2020 Update 1 及更低版本上， WinPE 发行套件支持使用 IMG 命令通过提供映像名称来恢复映像，而该命令无法识别是否通过该命令传递了分发包。从 ZENworks 2020 Update 2 开始， WinPE 发行套件上支持 IMG 分发包命令。有关详细信息，请参见 《Preboot Services and Imaging》（预引导服务和映像）指南。

读取 ZENworks 映像信息的新工具：zmginfo 工具可帮助您收集有关映像的信息。当您的内容储存库或共享路径中有多个映像，而您需要收集每个映像的相关信息时，可以使用此工具来节省时间。您可以使用 zmginfo 工具收集映像的基本信息或全面信息。管理员可以使用 zmginfo 创建分发包 xml，这些文件可作为分发包导入，用来将所有 linux 基本映像转换为 winpe 基本映像。

有关详细信息，请参见 《Preboot Services and Imaging》（预引导服务和映像）指南。

ZENworks Remote Management

远程控制具有活动 RDP 会话的设备：现在，您可在具有活动 RDP 会话的设备上像起动常规远程管理会话一样起动远程会话。有关详细信息，请参见 《Remote Management Reference》（远程管理参考手册）指南。

录制远程管理会话 （实验性支持）：可让受管设备上的用户录制远程管理会话。有关详细信息，请参见 《Remote Management Reference》（远程管理参考手册）指南。

移动设备管理

对 Android 分发包启用设备指派：为批准的 Google Play 商店 APP 创建的 Android 分发包先前仅可指派给用户，现在也可指派给设备。有关详细信息，请参见 《Mobile Management Reference》（移动设备管理参考手册）。

供应系统 APP：使用分发包功能，您可以在 Android 设备上启用或禁用系统 APP。系统 APP 是设备上已预安装的内置 APP。有关详细信息，请参见 《Mobile Management Reference》（移动设备管理参考手册）。

开始使用新式管理：“ 移动设备管理入门 ” 页面已翻新，现在还包含 Windows 10 MDM 设备的注册和管理功能。此外，此页面上还包含与注册和管理 Apple 和 Android 设备相关的一些其他功能。有关详细信息，请参见 《Modern Management Reference》（新式管理参考手册）。

修改 Android 设备日志位置 Android 设备上 ZENworks APP 日志的位置已变为 Android/data/com.novell.zapp/files/Documents/zapp.log。要共享这些日志，您需要在 Android 设备上部署 Files APP。

分发包管理

“ 复制关系 ” 工作流程中引入了新的失败时继续选项。如果在将关系从一台设备复制到另一组对象时发生错误，针对其余对象的操作仍将继续。操作结束时将显示错误的细节，并会提供一个选项用于导出操作细节，以供进一步参考及采取相应措施。有关详细信息，请参见 《Software Distribution Reference》（软件分发参考手册）。

杂项

让客户可以使用 puppet-agent 包的最新版本：以前， ZENworks 将 puppet-agent 包作为内部版本的一部分提供，以便用户可以使用 Puppet 策略。但是，由于 puppet-agent 版本会持续更新，因此在 ZENworks 发布后，用户便无法使用 puppet-agent 包的最新版本。从此版本开始，

要使 Puppet 策略在 ZENworks 2020 Update 2 及更高版本的 Linux 受管设备上生效，您需要确保设备上安装了 puppet-agent 包。有关详细信息，请参见 《Configuration Policies Reference》（配置策略参考手册）。

ZENworks 中的安全性增强功能

此版本中引入了安全性增强功能，让您即使在 DMZ 环境中也能安全地注册设备并与其通讯。

- 如果您全新安装了 ZENworks 2020 Update 2，则所有主服务器上默认都会启用该安全性设置。
- 如果您要升级主服务器，则默认将禁用该安全性设置。
- 如果您已将新的主服务器添加到区域中，则在升级到 ZENworks 2020 Update 2 后，默认将启用该安全性设置。

您需要运行以下 zman 命令来启用该设置：

- 引入了 zman ssassc (Security-Set-Agent-Server-Secure-Communication)，可让您启用或禁用针对 ZENworks 代理与 ZENworks 服务器之间通讯的鉴定。

有关此版本中引入的安全性增强功能的详细信息，请参见 《ZENworks Securing Devices Reference》（ZENworks 保护设备安全参考手册）。

设备注册

预先批准设备注册

预先批准的设备是管理员已批准要添加到区域中的设备。此功能特别适合用于在批量注册一组已知设备时必须预先批准一些设备的情况。您还可以使用此功能来允许对已知设备进行调节 （如果需要）。

使用授权密钥

ZENworks 代理可使用授权密钥来授权自己注册到区域以及在安装期间与服务器进行任何通讯。

保障受管设备和 iOA 设备注册的安全

要将更新的 iOA 代理或受管设备注册到区域，您需要在设备注册期间指定授权密钥，或确保设备包含在预先批准的设备列表中。

设备通讯

使用 OSP 进行设备通讯 （包括 ZCC 登录）

对于大部分功能， ZENworks 已改为使用 O-Auth 协议来建立用户身份。因此，产品中引入了名为 OSP 的新服务，用于登录到 ZCC、进行服务间通讯以及设备与服务器之间的通讯。

保护设备、主服务器和从属服务器之间内容传输和收集的安全

引入此项新安全性功能后，将通过 SSL 在受管设备、主服务器和从属服务器之间进行端到端内容收集和传输。这可以通过在 ZCC 中配置相应设置或使用新引入的 zman 命令来实现。

保护设备与主服务器或从属服务器之间的 Web 服务通讯的安全

为了进一步保护 ZENworks 代理与 ZENworks 主服务器和从属服务器之间的 Web 服务通讯的安全，此版本中针对 Web 服务调用引入了安全性增强功能。

Microsoft 数据加密策略驱动器排除项

现在，当在受管设备上实施 Microsoft 数据加密策略时，可按该策略中的驱动器类型将可卸数据驱动器排除在加密范围之外。

反恶意软件

ZENworks 反恶意软件是 ZENworks Endpoint Security Management 的一个新组件，位于 ZENworks 控制中心的 “ 安全性 ” 分组之下。反恶意软件是一种压缩解决方案，可保护受管设备免受所有最新恶意软件的威胁。将反恶意软件代理部署到区域中的设备上后，它会持续从反恶意软件云服务接收恶意软件签名文件更新，以便通过访问时扫描和按需扫描来检测恶意软件感染情况。受感染文件会被隔离，直到已被杀毒。

有关本节中主题的详细信息，请参见以下内容：

- 《ZENworks Endpoint Security Antimalware Reference》（ZENworks Endpoint Security 反恶意软件参考手册）

防范恶意软件 - 入门页面

安全性的入门页面中包含一个额外的选项卡式页面，名为 “ 防范恶意软件 ”。您可以使用此页面作为配置、部署以及自定义 ZENworks 反恶意软件必须提供的所有功能的单一访问点。

反恶意软件更新权利

您需要有反恶意软件更新权利才能将反恶意软件策略部署到设备。在评估模式下激活端点安全性管理时，该权利会自动启用，持续时间为整个评估期。

Windows Endpoint Security 策略

可使用四个新策略来管理反恶意软件的部署、自定义和连续性：

反恶意软件实施策略：这是基本策略，会在受管设备上安装反恶意软件代理。必须部署此策略才能使用任何其他反恶意软件策略。该策略包含所有恶意软件扫描类型的配置，包括访问时扫描、全扫描、快速扫描、外部设备扫描以及上下文按需扫描。策略还提供隔离行为设置，以及用于定义要排除在扫描范围之外的内容的设置。

如果部署策略后最终用户权限和通知的默认设置保持不变，最终用户将有权在其端点上访问代理状态控制台。在该控制台上，用户可启动自己的扫描、查看扫描和代理更新状态，以及接收受策略控制的代理活动的通知。

反恶意软件扫描排除项策略：反恶意软件具有扫描排除项，包括内置排除项，以及您可以添加到任何反恶意软件策略的自定义扫描排除项。如果还为相同设备指派了其他反恶意软件策略，将根据设备指派实施扫描排除项策略，这样可通过更简单的方式在区域中传播扫描排除项。可以针对特定扫描类型启用或禁用排除项。

反恶意软件自定义扫描策略：如果怀疑有特定威胁或者要扫描受管设备上的具体位置，可使用自定义扫描策略更有针对性地扫描这些设备上的本地驱动器。自定义扫描策略有自己的日程安排，而反恶意软件实施策略则不同，它使用为其配置的区域日程安排。

反恶意软件网络扫描策略：网络扫描策略也是一种更有针对性的扫描方法，但明确用于扫描网络驱动器上的文件夹和文件。该策略也有自己的日程安排，并包含用于向网络位置进行鉴定的额外设置。

反恶意软件安全性 Dashlet

安全性仪表板中默认包含四个新 dashlet，用于监视恶意软件威胁、恶意软件扫描及恶意软件签名更新。

设备恶意软件状态：此 dashlet 显示在所选检测时间段内区域中各台设备的恶意软件状态。

设备上次恶意软件扫描：此 dashlet 显示区域中的设备防御恶意软件威胁的状况。它默认显示有关在指定时间段内对设备执行的任何扫描类型的信息。

恶意软件威胁排行榜：此 dashlet 显示区域中的恶意软件威胁排行榜。默认会根据受感染设备数显示恶意软件威胁排行榜。

设备恶意软件签名版本：此 dashlet 显示区域中的设备上安装的恶意软件签名版本和反恶意软件代理版本列表。

设备反恶意软件页面

此页面包含一个新选项卡，选择某个设备后可以访问该选项卡。它提供选定设备的恶意软件威胁的快照状态、扫描日程安排以及隔离文件信息。您也可以在该设备上对文件执行特定的操作、启动扫描，以及更新反恶意软件代理和恶意软件签名版本。

恶意软件威胁细节页面

在设备的“反恶意软件”页面的“恶意软件威胁”部分中，单击某个恶意软件威胁链接可访问此页面。此页面提供有关选定威胁的详细信息以及已受该威胁感染的设备的细节。

反恶意软件快速任务

当在 ZENworks 控制中心的“设备”分组中选择一台或多台安装了反恶意软件代理的设备后，可在选定设备上运行五个新的快速任务。其中包括以下快速任务：

- 启动恶意软件扫描
- 更新恶意软件签名
- 更新反恶意软件代理
- 恢复恶意软件隔离区中的文件
- 删除恶意软件隔离区中的文件

反恶意软件 zac 命令

反恶意软件附带数个此组件特有的新 zac 命令。其中包括用于在设备上启动恶意软件扫描、检查反恶意软件代理的恶意软件状态、安装、更新或去除代理、删除隔离区中的文件的命令，以及其他命令。

反恶意软件区域配置页面

ZENworks 主配置页面中的“安全性”分组中现在包含三个新的区域配置页面。其中每个页面都包含您可以自定义的默认设置。这些页面如下：

反恶意软件代理日程安排：配置恶意软件扫描和恶意软件签名更新的日程安排。您可以在设备文件夹级别和设备级别覆盖此日程安排。

反恶意软件代理通知：配置反恶意软件代理在受管设备上显示的警报和通知。您可以在设备文件夹级别和设备级别覆盖这些设置。

反恶意软件配置：指定将 ZENworks 主服务器作为反恶意软件服务器使用，为此必须进行手动配置以部署反恶意软件组件。还可为反恶意软件代理配置维护日程安排。

按需内容配置页面

ZENworks 主配置页面中的“分发包”、“策略”和“内容”分组中现在包含这个新的区域配置页面。可使用该页面管理区域中内容分发的内容下载速率和内容超速缓存大小，目前包括反恶意软件签名文件和反恶意软件代理更新。

反恶意软件服务状态

现在，您可在 ZCC 的“诊断”页面中访问反恶意软件服务状态。

反恶意软件数据库

ZENworks 2020 Update 2 中新增了反恶意软件数据库。目的是通过“反恶意软件”页面和反恶意软件安全性 dashlet 为反恶意软件的监控功能提供数据。经过配置后，此数据库会与 ZENworks 数据库同步，因此它们的数据库类型必须相同。例如：PostgreSQL、 Microsoft SQL Server 或 Oracle。

可从 ZENworks 控制中心中的“安全性”下的“防范恶意软件 - 入门”页面配置反恶意软件数据库。如果反恶意软件数据库将配置为使用尚不存在的外部数据库，可以通过 CLI 命令使用 setup.exe 文件创建一个外部数据库。