Windows Server 入门

项目 • 2024/06/05

Windows Server 是一个平台，用于构建连接的应用程序、网络和 Web 服务的基础结构，包括从工作组到数据中心。 它将本地环境与 Azure 连接起来，增加了额外的安全层，同时帮助实现应用程序和基础结构的现代化。

此文章集合中包含的详细信息可帮助你理解并充分利用 Windows Server 以及确定你是否已准备好迁移到最新版本。 检查完系统要求、升级选项和其他 Windows Server 相关信息后，即可开始安装最佳版本和满足你需求的安装选项。

> **提示**
>
> 若要下载 Windows Server，请在评估中心参阅 **Windows Server 评估**。

> **备注**
>
> 若想要了解不再受支持的早期版本的相关信息，请参阅 **Windows 旧版文档**。

支持和反馈

有关 Windows Server 的最新信息，请访问 Windows Server 博客，及时了解 Windows Server 工程团队发布的公告、功能、事件和其他信息。 还可以访问 Windows Server 社区，共享最佳做法、获取最新咨询并向专家学习 Windows Server。

了解

浏览 Windows Server 的学习路径，可通过这些路径促进新技能的学习，并借助分步指南加速部署进程。 可以了解如何部署、配置和管理 Windows Server，并了解网络基础结构、文件服务器和存储管理、Hyper-V 和虚拟化以及更多内容。

Windows 预览体验计划

针对 Windows Server 的 Windows 预览体验计划提供了 Windows Server 预览版本，这使你可以提前了解、测试 Windows Server，同时帮助打造未来版本的 Windows Server。 要了解详细信息，可以从针对 Windows Server 的 Windows 预览体验计划开始，并参与 Windows 服务器预览体验成员社区。

后续步骤

首先，通过以下资源了解更多信息。

- Windows Server 2025 中的新增功能概述了 Windows Server 中的最新功能。
- 了解不同的服务渠道，每个渠道的用途，以及对工作负载和支持的意义。
- 比较 Windows Server 2022 中各版本的差异。
- 根据是需要桌面体验还是需要最小核心界面，选择正确的安装选项。
- 了解运行 Windows Server 的硬件要求。
- 遵循关于 Windows Server 部署、配置和管理的学习路径。
- 如果仍需要使用 Windows Server 2012 或 Windows Server 2012 R2 扩展安全更新，有助于确保安全，并发布分级为关键和重要的公告。

Windows Server 2022 中的新增功能

项目 • 2024/07/10 • 适用于: ✅ Windows Server 2022

这篇文将介绍 Windows Server 2022 中的一些新增功能。 Windows Server 2022 建立在 Windows Server 2019 的强大基础之上，在三个关键主题上引入了许多创新：安全性、Azure 混合集成和管理以及应用程序平台。

Azure Edition

可借助 Windows Server 2022 Datacenter: Azure Edition，利用云的优势使 VM 保持最新状态，同时最大限度地减少停机时间。 本部分介绍 Windows Server 2022 Datacenter: Azure Edition 中的一些新功能。 阅读适用于 Windows Server 服务的 Azure Automanage 一文，详细了解适用于 Windows Server 的 Azure Automanage 如何将这些新功能引入 Windows Server Azure Edition。

Windows Server 2022 Datacenter: Azure Edition 建立在 Datacenter Edition 的基础上，可提供仅限 VM 的操作系统，有助于通过基于 QUIC 的 SMB、热补丁和 Azure 扩展网络等高级功能帮助利用云的优势。 本部分介绍其中一些新功能。

比较 Windows Server 2022 中各版本的差异。 还可阅读适用于 Windows Server 服务的 Azure Automanage 一文，详细了解适用于 Windows Server 的 Azure Automanage 如何将这些新功能引入 Windows Server Azure Edition。

2023 年 4 月

热修补

Windows Server 2022 Datacenter：Azure Edition Hotpatching 现在已推出 Azure 中适用于桌面体验的公共预览版，也是 Azure Stack HCI 版本 22H2 上支持的来宾 VM。

2022 年 9 月

本部分列出了 Windows Server Datacenter: Azure Edition 中现已提供的功能和改进，从 2022-09 基于 x64 的系统的 Microsoft 服务器操作系统版本 21H2 的累积更新 (KB5017381) 开始。 安装累积更新后，OS 内部版本号将为 20348.1070 或更高。

数据传输的存储副本压缩

此更新包括对源服务器和目标服务器之间传输的数据的存储副本压缩。 此新功能压缩源系统中的复制数据，通过网络发送，然后解压缩并保存在目标系统中。 在传输相同数据量的情况下，压缩需要更少的网络数据包，从而实现更高的吞吐量和更低的网络利用率。更高的数据吞吐量还可缩短同步时间，这在灾难恢复等场景中十分需要。

新的存储副本 PowerShell 参数可用于现有命令，请查看 Windows PowerShell StorageReplica 参考以了解详细信息。 有关存储副本的详细信息，请参阅存储副本概述。

支持 Azure Stack HCI

使用此版本，可在 Azure Stack HCI 版本 22H2 上运行 Windows Server 2022 Datacenter: Azure Edition 作为受支持的来宾 VM。 如果 Azure Edition 在 Azure Stack HCI 上运行，你将能够在数据中心和边缘位置使用所有现有功能，包括适用于服务器核心的热补丁和基于 QUIC 的 SMB。

开始使用已启用 Arc 的 Azure Stack HCI 上的 Azure 市场或通过 ISO 部署 Windows Server 2022 Datacenter: Azure Edition。 可从此处下载 ISO：

- Windows Server 2022 Datacenter: Azure Edition (EN-US) ISO
- Windows Server 2022 Datacenter: Azure Edition (ZH-CN) ISO

Azure 订阅支持在 Azure Stack HCI 上运行的任何虚拟机实例上使用 Windows Server Datacenter: Azure Edition。 有关详细信息，请参阅产品条款产品条款 。

要详细了解最新的 Azure Stack HCI 功能，请参阅 Azure Stack HCI 版本 22H2 中的新增功能一文。

通过已启用 Arc 的 Azure Stack HCI 上的 Azure 市场部署（预览版）

Windows Server 2022 Datacenter: Azure Edition 映像将在已启用 Arc 的 Azure Stack HCI 的 Azure 市场中提供，用户可通过 Azure 认证映像轻松试用、购买和部署。

要详细了解已启用 Azure Arc 的 Azure Stack HCI 功能的 Azure 市场集成，请参阅 Azure Stack HCI 版本 22H2 中的新增功能一文。

Azure Edition（初始版本）

本部分列出了 2021 年 9 月发布的 Windows Server Datacenter: Azure Edition 中提供的功能和改进。

Azure Automanage - 热补丁

热修补是 Azure Automanage 的一部分，是在新的 Windows Server Azure Edition 虚拟机 (VM) 上安装更新的一种新方式，安装后无需重启。 有关详细信息，请参阅 Azure Automanage 文档。

基于 QUIC 的 SMB

基于 QUIC 的 SMB 更新了 SMB 3.1.1 协议，以在 Windows Server 2022 Datacenter: Azure Edition、Windows 11 及更高版本以及支持 QUIC 协议的第三方客户端中使用 QUIC 协议而不是 TCP 协议。 通过结合使用基于 QUIC 的 SMB 和 TLS 1.3，用户和应用程序可以安全可靠地通过 Azure 中运行的边缘文件服务器访问数据。 在 Windows 上，移动设备用户和远程办公用户不再需要使用 VPN 通过 SMB 来访问其文件服务器。 有关详细信息，请参阅基于 QUIC 的 SMB 文档以及使用 Automanage 计算机最佳做法管理基于 QUIC 的 SMB。

要详细了解 QUIC，请查看 RFC 9000。

适用于 Azure 的扩展网络

使用 Azure 扩展网络，可将本地子网扩展到 Azure，使本地虚拟机在迁移到 Azure 时保留其原始的本地专用 IP 地址。 要了解详细信息，请参阅 Azure 扩展网络。

所有版本

本部分介绍所有版本的 Windows Server 2022 中的一些新功能。 要详细了解不同版本，请查看比较 Windows Server 2022 的 Standard、Datacenter 和 Datacenter: Azure Edition 版本一文。

安全性

Windows Server 2022 中的新增安全功能结合了 Windows Server 中跨多个领域的其他安全功能，以提供针对高级威胁的深度防御和保护。 Windows Server 2022 中的高级多层安全性提供了服务器目前所需的全面保护。

安全核心服务器

OEM 合作伙伴提供的经过认证的安全核心服务器硬件提供更多的安全保护措施，可有效防范复杂攻击。 在处理一些最具数据敏感性的行业的任务关键型数据时，使用经过认证的安全核心服务器硬件可以更加安心。 安全核心服务器使用硬件、固件和驱动程序功能来实现高级 Windows Server 安全功能。 其中许多功能可通过 Windows 安全核心电脑获

取，现在还可通过安全核心服务器硬件和 Windows Server 2022 获取。 有关安全核心服务器的详细信息，请参阅安全核心服务器。

硬件信任根

通过使用 BitLocker 驱动器加密这样的功能，受信任的平台模块 2.0 (TPM 2.0) 安全加密处理器芯片为敏感加密密钥和数据提供安全的基于硬件的存储（包括系统完整性度量）。 TPM 2.0 可以验证服务器是否已使用合法代码启动，以及后续代码执行是否可信任该服务器（也就是"硬件根信任"）。

固件保护

固件以高特权执行，通常对传统的防病毒解决方案不可见，这导致基于固件的攻击数量增加。 安全核心服务器使用动态信任根衡量 (DRTM) 技术来衡量和验证启动过程。 安全核心服务器还可以使用直接内存访问 (DMA) 保护来隔离驱动程序对内存的访问。

UEFI 安全启动

UEFI 安全启动 是一种安全标准，可保护服务器免受恶意 rootkit 攻击。 安全启动可确保服务器仅启动硬件制造商信任的固件和软件。 服务器启动时，固件会检查每个启动组件的签名，包括固件驱动程序和 OS。 如果签名有效，则服务器将会启动，而固件会将控制权转递给 OS。

基于虚拟化的安全性 (VBS)

安全核心服务器支持基于虚拟化的安全性 (VBS) 和基于虚拟机监控程序的代码完整性 (HVCI)。 VBS 使用硬件虚拟化功能创建安全内存区域并将其与正常操作系统隔离，防范加密货币挖矿攻击中使用的一系列漏洞。 VBS 还支持使用 Credential Guard，其中用户凭据和机密存储在操作系统无法直接访问的虚拟容器中。

HVCI 使用 VBS 大大增强了代码完整性策略的实施。 内核模式完整性会防止未签名的内核模式驱动程序或系统文件加载到系统内存中。

内核数据保护 (KDP) 为包含不可执行数据的内核内存提供只读内存保护，其中内存页受虚拟机监控程序保护。 KDP 可保护 Windows Defender System Guard 运行时中的关键结构不被篡改。

安全的连接

传输：Windows Server 2022 上默认启用 HTTPS 和 TLS 1.3

安全连接是当今互连系统的核心。 传输层安全性 (TLS) 1.3 是 Internet 部署最广泛的安全协议的最新版本，它对数据进行加密，以在两个终结点之间提供安全的信道。 Windows Server 2022 上现在默认启用 HTTPS 和 TLS 1.3，旨在保护连接到服务器的客户端的数据。 它不再使用过时的加密算法，提供比旧版本更高的安全性，旨在实现尽可能多的握手加密。 详细了解受支持的 TLS 版本和受支持的密码套件。

尽管协议层中的 TLS 1.3 现已默认启用，但应用程序和服务也需要主动支持它。 Microsoft 安全博客在通过 TLS 1.3 将传输层安全性提升到新水平 一文中进行了更详细的介绍。

安全 DNS：通过基于 HTTPS 的 DNS 实现 DNS 名称解析请求的加密

现在，Windows Server 2022 中的 DNS 客户端支持基于 HTTPS 的 DNS (DoH)，后者使用 HTTPS 协议加密 DNS 查询。 DoH 有助于防止窃听和篡改你的 DNS 数据，尽可能保护流量的私密性。 详细了解如何配置 DNS 客户端以使用 DoH。

服务器消息块 (SMB)：SMB AES-256 加密适用于最有安全意识的用户

Windows Server 现在支持将 AES-256-GCM 和 AES-256-CCM 加密套件用于 SMB 加密。 Windows 连接到也支持这种方法的另一台计算机时，将自动协商更高级的密码方法，也可通过组策略强制执行该方法。 Windows Server 仍支持 AES-128 来实现下层兼容性。 AES-128-GMAC 签名现在还可以加快签名速度。

SMB：针对内部群集通信的东-西 SMB 加密控制

Windows Server 故障转移群集现支持对加密和签名群集共享卷 (CSV) 及存储总线层 (SBL) 的节点内存储通信进行精细控制。 若在使用存储空间直通，现在可决定在群集本身内加密或签名东-西通信，以获得更高的安全性。

SMB 直通和 RDMA 加密

SMB 直通和 RDMA 为存储空间直通、存储副本、Hyper-V、横向扩展文件服务器和 SQL Server 等工作负载提供高带宽、低延迟网络结构。 Windows Server 2022 中的 SMB 直通现在支持加密。 以前，启用 SMB 加密会禁用直接数据放置；这是有意为之的，但严重影响了性能。 现在，数据在放置之前进行加密，使性能下降相对较小，同时通过 AES-128 和 AES-256 保护提高了数据包保密性。

如需详细了解 SMB 加密、签名加速、安全 RDMA 和群集支持，请参阅 SMB 安全增强功能。

Azure 混合功能

可以通过 Windows Server 2022 中的内置混合功能来提高效率和灵活性，从而可以比以往更轻松地将数据中心扩展到 Azure。

已启用 Azure Arc 的 Windows Server

已启用 Azure Arc 的 Windows Server 2022 服务器通过使用 Azure Arc 将本地和多云 Windows Server 引入 Azure。这种管理体验旨在使你能够采用与本地 Azure 虚拟机一致的管理方式。 当混合计算机连接到 Azure 时，它将成为一台联网计算机，被视为 Azure 中的资源。 有关详细信息，请参阅通过 Azure Arc 支持服务器文档。

添加 Windows Server

从 KB5031364 更新开始，现在可通过一个简单的过程添加 Windows Server。

若要添加新的 Windows Server，请转到任务栏右下角的 Azure Arc 图标，并启动 Azure Arc 安装程序来安装和配置 Azure 连接计算机代理。 安装后，可使用 Azure 连接 计算机代理，而你的 Azure 帐户没有额外费用。 在服务器上启用 Azure Arc 后，可以在任务栏图标中看到状态信息。

若要了解详细信息，请参阅通过 Azure Arc 安装程序将 Windows Server 计算机连接到 Azure。

Windows 管理中心

用于管理 Windows Server 2022 的 Windows Admin Center 的改进包括：报告上述安全核心功能的当前状态，在适用情况下允许客户启用这些功能。 有关这些改进以及 Windows Admin Center 更多改进的详细信息，请参阅 Windows Admin Center 文档。

应用程序平台

有多项针对 Windows 容器的平台改进，包括应用程序兼容性和 Kubernetes 的 Windows 容器体验。

下面是部分新功能：

- 将 Windows 容器映像大小减少多达 40%，这使启动时间缩短 30%，从而优化了性能。
- 应用程序现在可以将 Azure Active Directory 与组托管服务帐户 (gMSA) 配合使用，且无需通过域加入的方式加入容器主机。 Windows 容器现在还支持 Microsoft 分布式事务控制 (MSDTC) 和 Microsoft 消息队列 (MSMQ)。

- 现可为进程隔离的 Windows Server 容器分配简单总线。 在需要通过 SPI、I2C、GPIO 和 UART/COM 进行通信的容器中运行的应用程序现在可执行此操作。
- 我们已在 Windows 容器中实现 DirectX API 硬件加速支持，以支持使用本地图形处理单元 (GPU) 硬件进行机器学习 (ML) 推理等方案。 有关详细信息，请参阅博客文章在 Windows 容器中引入 GPU 加速。
- 还有其他几项增强功能，可简化 Kubernetes 的 Windows 容器体验。 这些增强功能包括支持将主机进程容器用于节点配置、IPv6 支持以及使用 Calico 实现一致的网络策略。
- 我们更新了 Windows Admin Center，使用户能轻松容器化 .NET 应用程序。 应用程序位于容器中后，可以将其托管在 Azure 容器注册表上，然后将其部署到其他 Azure 服务，包括 Azure Kubernetes 服务。
- 由于支持 Intel Ice Lake 处理器，Windows Server 2022 可支持业务关键型和大型应用程序，这些应用程序需要高达 48 TB 的内存和在 64 个物理插槽上运行的 2048 个逻辑内核。 使用 Intel Ice Lake 上的 Intel Secured Guard Extension (SGX) 进行机密计算，可以通过使用受保护的内存将应用程序彼此隔离，从而提高应用程序安全性。

若要了解有关新功能的详细信息，请参阅 Windows Server 2022 中 Windows 容器的新增功能。

其他关键功能

远程桌面 IP 虚拟化

从 KB5030216 更新开始，现在可使用远程桌面 IP 虚拟化。

远程桌面 IP 虚拟化通过支持 Winsock 应用程序的按会话和每程序远程桌面 IP 虚拟化来模拟单用户桌面。 若要了解详细信息，请参阅 Windows Server 中的远程桌面 IP 虚拟化。

适用于 Server Core 安装的任务计划程序和 Hyper-V 管理器

我们在此版本的“应用兼容性按需功能”功能包中添加了两个管理工具：任务计划程序 (taskschd.msc)，以及 Hyper-V 管理器 (virtmgmt.msc)。 有关详细信息，请参阅 Server Core 应用兼容性按需功能 (FOD)。

适用于 AMD 处理器的嵌套虚拟化

嵌套虚拟化是一项功能，使你可以在 Hyper-V 虚拟机 (VM) 内运行 Hyper-V。 Windows Server 2022 通过使用 AMD 处理器引入对嵌套虚拟化的支持，为环境提供更多的硬件选择。 有关详细信息，请参阅嵌套虚拟化文档。

Microsoft Edge 浏览器

Windows Server 2022 中随附了 Microsoft Edge，替代了 Internet Explorer。 它建立在 Chromium 开源基础上，并以 Microsoft 的安全性和创新为后盾。 可以通过桌面体验安装选项将其用于 Server。 有关详细信息，请参阅 Microsoft Edge Enterprise 文档。 与 Windows Server 其余部分不同，Microsoft Edge 的支持生命周期遵循新式生命周期。 有关详细信息，请参阅 Microsoft Edge 生命周期文档。

网络性能

UDP 性能改进

由于 RTP 和自定义 (UDP) 流式传输和游戏协议越来越受欢迎，UDP 正成为一种热门的协议，具有越来越多的网络流量。 在 UDP 基础上构建的 QUIC 协议使 UDP 的性能达到与 TCP 一样的水平。 值得注意的是，Windows Server 2022 包括 UDP 分段卸载 (USO)。 USO 将发送 UDP 数据包所需的大部分工作从 CPU 转移到网络适配器的专用硬件。 UDP 接收端合并 (UDP RSC) 使客户对 USO 赞誉不绝，它可合并数据包并减少进行 UDP 处理的 CPU 使用率。 此外，我们还对 UDP 的数据传输和接收路径进行了数百项改进。 Windows Server 2022 和 Windows 11 都具有此项新功能。

TCP 性能改进

Windows Server 2022 使用 TCP HyStart++ 来减少连接启动期间的数据包丢失（尤其是在高速网络中），并使用 RACK 来减少重发超时 (RTO)。 这些功能在传输堆栈中默认启用，并提供更流畅的网络数据流和更好的高速性能。 Windows Server 2022 和 Windows 11 都具有此项新功能。

Hyper-V 虚拟交换机改进

Hyper-V 中的虚拟交换机已通过更新的接收段合并 (RSC) 进行了增强。 RSC 让虚拟机监控程序网络能够合并数据包并作为一个更大的段进行处理。 CPU 周期减少，段将在整个数据路径中保持合并，直到被目标应用程序处理。 RSC 让虚拟 NIC 从外部主机接收的网络流量，以及虚拟 NIC 发送到同一主机上另一个虚拟 NIC 的网络流量的性能都得到了提高。

在 vSwitch 中，RSC 还可以在数据遍历 vSwitch 之前将多个 TCP 段合并为一个更大的段。 此更改还提高了虚拟工作负载的网络性能。 默认情况下，RSC 在外部虚拟交换机上处于启用状态。

System Insights 磁盘异常情况检测

系统见解通过 Windows Admin Center 提供另一项功能：磁盘异常情况监测。

磁盘异常情况检测新功能可以突出显示磁盘的行为何时与往常不同。 尽管不同的情况并不一定是坏事，但在排查系统上的问题时，查看这些异常瞬间可能会有所帮助。 此功能也适用于运行 Windows Server 2019 的服务器。

Windows 更新回滚改进

如果在安装最新驱动程序或质量 Windows 更新后出现启动失败，服务器现在可以通过删除更新立即自动恢复。 如果在最近安装驱动程序质量更新后设备无法正常启动，Windows 现在会自动卸载更新，使设备能够恢复正常运行。

此功能要求服务器结合 Windows 恢复环境分区使用 Server Core 安装选项。

存储

Windows Server 2022 包含以下存储更新。 存储也受到 System Insights 磁盘异常情况检测和 Windows 管理中心更新的影响。

存储迁移服务

使用 Windows Server 2022 中存储迁移服务的增强功能，可以更轻松地将更多源位置的存储迁移到 Windows Server 或迁移到 Azure。 下面是在 Windows Server 2022 上运行存储迁移服务器业务流程协调程序时可用的功能：

- 将本地用户和组迁移到新服务器。
- 从故障转移群集迁移存储、迁移到故障转移群集，以及在独立服务器和故障转移群集之间迁移。
- 从使用 Samba 的 Linux 服务器迁移存储。
- 使用 Azure 文件同步更轻松地将迁移后的共享同步到 Azure。
- 迁移到 Azure 等新网络。
- 将 NetApp CIFS 服务器从 NetApp FAS 阵列迁移到 Windows Server 和群集。

可调整的存储修复速度

“用户可调整的存储修复速度”是存储空间直通的一项新功能，此功能可对数据重新同步过程进行更强的控制。 使用“可调整的存储修复速度”功能，可将资源分配给“修复数据副本”（复原）或“运行活动工作负载”（性能）。 控制修复速度，有助于提高可用性，并可让你更灵活、更有效地为群集提供服务。

更快的修复和重新同步

在节点重启和磁盘故障等事件之后进行的存储修复和重新同步现在速度快两倍。 修复时间差异变小，因此，你可以更好地确定修复所需的时间，这已通过向数据跟踪添加更多粒度来实现。 目前修复只会移动需要移动的数据，从而减少所使用的系统资源和耗费的时间。

在独立服务器上使用存储空间的存储总线缓存

存储总线缓存现在可用于独立服务器。 它可以显著提高读取和写入性能，同时保持存储效率和较低的操作成本。 与存储空间直通的实现类似，此功能将速度较快的介质（例如 NVMe 或 SSD）与速度较慢的介质（例如 HDD）绑定在一起来创建层。 为缓存保留了部分更快的介质层。 若要了解详细信息，请参阅在独立服务器上使用存储空间启用存储总线缓存。

ReFS 文件级快照

Microsoft 的复原文件系统 (ReFS) 现在包括使用快速元数据操作来拍摄文件快照的功能。 快照与 ReFS 块克隆的不同之处在于，克隆是可写的，而快照是只读的。 此功能在具有 VHD/VHDX 文件的虚拟机备份场景中尤其有用。 ReFS 快照的独特之处在于，它们使用固定时间，而不考虑文件大小。 对快照的支持在 ReFSUtil 中提供或作为 API 提供。

SMB 压缩

利用 Windows Server 2022 和 Windows 11 中的 SMB 的增强功能，用户或应用程序可以在通过网络传输文件时对其进行压缩。 用户不再需要手动压缩文件，就能在较慢或较拥塞的网络上更快地传输。 有关详细信息，请参阅 SMB 压缩。

容器

Windows Server 2022 包括对 Windows 容器的以下更改。

Server Core 映像大小减小

我们减小了服务器核心映像的大小。 由于减小了映像大小，因此可以更快地部署容器化应用程序。 在 Windows Server 2022 中，正式发布时的 Server Core 容器映像发布到制造 (RTM) 层在磁盘上的未压缩大小为 2.76 GB。 与正式发布时的 Windows Server 2019 RTM 层（磁盘上未压缩的大小为 3.47 GB）相比，该层的磁盘占用量减少了 33%。 虽然不应期望总映像大小会减少 33%，但 RTM 层大小越小通常意味着总映像大小会更小。

> **备注**
>
> Windows 容器基础映像分为两层：RTM 层和补丁层，其中包含覆盖在 RTM 层上的 OS 库和二进制文件的最新安全修复程序。 补丁层的大小在容器映像支持周期的整个生命周期内都会发生变化，具体取决于二进制文件中的更改数量。 将容器基础映像拉取到新主机上时，需要拉取这两个层。

所有 Windows 容器映像的支持周期更长

Windows Server 2022 映像（包括 Server Core、Nano Server 和 Server 映像）提供 5 年的主流支持和 5 年的扩展支持。 此更长的支持周期将确保你有时间实现、使用、升级或迁移（如果适用于你的组织）。 有关详细信息，请参阅 Windows 容器基础映像生命周期和 Windows Server 2022 生命周期。

虚拟化时区

使用 Windows Server 2022，Windows 容器现在可以独立于主机维护虚拟化时区配置。 主机时区通常使用的所有配置现在都为每个容器进行了虚拟化和实例化。 要配置容器时区，可以使用 tzutil 命令实用工具或 Set-TimeZone Powershell cmdlet。 要了解详细信息，请参阅虚拟化时区。

重叠网络支持的可伸缩性改进

Windows Server 2022 汇总了已在 Windows Server 的四个早期半年频道 (SAC) 版本中进行的多项性能和缩放性方面的改进（但尚未向后移植到 Windows Server 2019）：

- 在相同节点上使用数百个 Kubernetes 服务和 Pod 时的端口耗尽问题现已修复。
- 改进了 Hyper-V 虚拟交换机 (vSwitch) 中的数据包转发性能。
- 提高了 Kubernetes 中容器网络接口 (CNI) 重启的可靠性。
- 改进了主机网络服务 (HNS) 控制平面以及 Windows Server 容器和 Kubernetes 网络使用的数据平面。

要详细了解重叠网络支持的性能和可伸缩性改进，请参阅适用于 Windows 的 Kubernetes 重叠网络。

重叠网络和 l2bridge 网络的直接服务器返回路由

直接服务器返回 (DSR) 是负载均衡系统中的一种非对称网络负载分布，这意味着发出请求和响应流量使用不同的网络路径。 使用不同的网络路径有助于避免额外的跃点并减少延迟，这不仅可以加快客户端与服务之间的响应时间，还可以从负载均衡器中移除额外的负载。 DSR 可以透明地提高应用程序的网络性能，此过程中几乎不需要更改基础结构。

要了解详细信息，请参阅 Kubernetes 中的 Windows 支持简介中的 DSR。

gMSA 改进

你可以将组托管服务帐户 (gMSA) 与 Windows 容器结合使用，以促进 Active Directory (AD) 身份验证。 最初在 Windows Server 2019 中引入时，gMSA 需要将容器主机加入域以从 Active Directory 检索 gMSA 凭据。 在 Windows Server 2022 中，具有未加入域的主机的容器的 gMSA 使用可移植用户标识而不是主机标识来检索 gMSA 凭据。 因此，无需再手动地将 Windows 工作器节点加入域。 经过身份验证后，Kubernetes 会将用户标识保存为机密。 主机未加入域的容器的 gMSA 提供了一种灵活性，可在不将主机节点加入到域的情况下使用 gMSA 创建容器。

要了解有关 gMSA 改进的详细信息，请参阅为 Windows 容器创建 gMSA。

IPv6 支持

Windows 中的 Kubernetes 现在支持 Windows Server 中基于 L2bridge 的网络中的 IPv6 双堆栈。 IPv6 依赖于 Kubernetes 使用的 CNI，并且还需要 Kubernetes 1.20 版本或更高版本来启用端到端的 IPv6 支持。 有关详细信息，请参阅 Kubernetes 中的 Windows 支持简介中的 IPv4/IPv6。

使用 Calico for Windows 为 Windows 工作器节点提供多子网支持

现在，通过主机网络服务 (HNS) 可以使用更严格的子网（例如前缀更长的子网），还可以为每个 Windows 工作器节点使用多个子网。 以前，HNS 将 Kubernetes 容器终结点配置限制为仅使用底层子网的前缀长度。 第一个使用此功能的 CNI 是 Calico for Windows。 有关详细信息，请参阅主机网络服务中的多子网支持。

用于节点管理的 HostProcess 容器

HostProcess 容器是一种新的容器类型，它直接在主机上运行，并扩展了 Windows 容器模型，以支持更广泛的 Kubernetes 群集管理场景。 使用 HostProcess 容器，用户可以打包和分发需要主机访问的管理操作，同时保留容器提供的版本控制和部署方法。 你可以将 Windows 容器用于 Kubernetes 中的各种设备插件、存储和网络管理场景。

HostProcess 容器具有以下优点：

- 群集用户不再需要登录，并单独配置每个 Windows 节点，便可执行管理任务和管理 Windows 服务。
- 用户可以利用容器模型将管理逻辑部署到任意数量的群集中。
- 用户可以在现有的 Windows Server 2019 或或更高版本基础映像之上构建 HostProcess 容器，通过 Windows 容器运行时进行管理，并以主机域中可用的任何用户身份运行。
- 通过 HostProcess 容器，可以在 Kubernetes 中更好地管理 Windows 节点。

有关详细信息，请参阅 Windows HostProcess 容器。

Windows Admin Center 改进

Windows Server 2022 扩展了添加到 Windows Admin Center 的容器扩展，以从 .NET Framework 容器化基于 ASP.NET 的现有 Web 应用程序。 可以使用开发人员提供的静态文件夹或 Visual Studio 解决方案。

Windows Admin Center 包括以下增强功能：

- 容器扩展现在支持 Web 部署文件，使你能够从正在运行的服务器中提取应用及其配置，然后将应用程序容器化。
- 可以在本地验证映像，然后将该映像推送到 Azure 容器注册表。
- Azure 容器注册表和 Azure 容器实例现在具有基本管理功能。 现在可以使用 Windows Admin Center UI 创建和删除注册表、管理映像、启动和停止新容器实例。

Azure Migrate 应用容器化工具

Azure Migrate 应用容器化是一种端到端解决方案，用于将现有 Web 应用程序容器化并将其移动到 Azure Kubernetes 服务。 可以评估现有的 Web 服务器、创建容器映像、将映像推送到 Azure 容器注册表、创建 Kubernetes 部署，最后将其部署到 Azure Kubernetes 服务。

有关 Azure Migrate 应用容器化工具的详细信息，请参阅 ASP.NET 应用容器化和迁移到 Azure Kubernetes 服务和 Java Web 应用容器化和迁移到 Azure Kubernetes 服务。

反馈

Windows Server 2019 中的新增功能

项目 • 2024/08/05 • 适用于: ✅ Windows Server 2019

本文介绍 Windows Server 2019 中的一些新增功能。 Windows Server 2019 在 Windows Server 2016 的坚实基础上构建，围绕以下四个关键主题实现了很多创新：混合云、安全性、应用程序平台、超融合基础设施 (HCI)。

常规

Windows Admin Center

Windows Admin Center 是本地部署的基于浏览器的应用，用于管理服务器、群集、超融合基础设施和 Windows 10 电脑。 它不会在 Windows 之外产生额外费用，并可以在生产中使用。

可将 Windows Admin Center 安装在 Windows Server 2019 和 Windows 10 以及更低版本的 Windows 和 Windows Server 上，并可用它来管理运行 Windows Server 2008 R2 及更高版本的服务器和群集。

有关详细信息，请参阅 Windows Admin Center。

桌面体验

Windows Server 2019 是长期服务频道 (LTSC) 版本，因此包含**桌面体验**。 根据设计，半年频道 (SAC) 版本不包含桌面体验；严格地说，这些版本属于 Server Core 和 Nano Server 容器映像版本。 与使用 Windows Server 2016 一样，可以在安装操作系统时选择 Server Core 安装或带桌面体验的 Server 安装。

系统见解

系统见解是 Windows Server 2019 中提供的一项新功能，以本机方式为 Windows Server 带来了本地预测分析功能。 这些预测功能中的每种功能都受机器学习模型支持，可在本地分析 Windows Server 系统数据（例如性能计数器和事件）。 系统见解可让你了解服务器的运行状况，并帮助减少与被动管理 Windows Server 部署中的问题相关的运营费用。

混合云

Server Core 应用兼容性按需功能

Server Core 应用兼容性按需功能 (FOD) 包含带桌面体验的 Windows Server 的一部分二进制文件和组件，因此显著提高了应用兼容性。 服务器核心通过不添加 Windows Server 桌面体验图形环境本身来尽可能地将其保持精简，从而提高功能和兼容性。

此可选按需功能在单独的 ISO 上提供，可通过 DISM 将其仅添加到 Windows Server 核心安装和映像中。

已将 Windows 部署服务 (WDS) 传输服务器角色添加到服务器核心

传输服务器只包含 WDS 的核心网络部分。 现在可将服务器核心与传输服务器角色配合使用，创建从独立服务器传输数据（包括操作系统映像）的多播命名空间。 如果想要一个 PXE 服务器，以便客户端通过 PXE 启动并下载你自己的自定义安装应用程序，则也可使用它。

远程桌面服务与 Azure AD 的集成

通过集成 Azure AD，可以利用条件访问策略、多重身份验证、使用 Azure AD 的其他 SaaS 应用的集成身份验证等等。 有关详细信息，请参阅将 Azure AD 域服务与 RDS 部署集成。

网络

我们对核心网络堆栈进行了多项改进，例如 TCP 快速打开 (TFO)、接收窗口自动调整、IPv6 等。 有关详细信息，请参阅核心网络堆栈功能改进 文章。

动态 vRSS 和 VMMQ

过去，当网络吞吐量首次达到 10GbE 或更高时，虚拟机队列和虚拟机多队列 (VMMQ) 会为单个 VM 提供更高的吞吐量。 遗憾的是，成功所需的规划、基线、优化和监控的工作比 IT 管理员预期的要大得多。

Windows Server 2019 通过根据需要动态分布和优化网络工作负载的处理来改进这些优化。 Windows Server 2019 可确保峰值效率，并减轻 IT 管理员的配置负担。 若要了解详细信息，请参阅 Azure Stack HCI 的主机网络要求。

安全性

Windows Defender 高级威胁防护 (ATP)

ATP 的深度平台传感器和响应操作可暴露内存和内核级别攻击，并通过抑制恶意文件和终止恶意进程进行响应。

- 有关 Windows Defender ATP 的详细信息，请参阅 Windows Defender ATP 功能概述。
- 若要详细了解如何载入服务器，请参阅将服务器载入 Windows Defender ATP 服务。

Windows Defender ATP 攻击防护是一组新的主机入侵防护功能，可用于平衡安全风险和生产力要求。 Windows Defender 攻击防护旨在锁定设备，使其免受各种不同攻击媒介的威胁，并阻止恶意软件攻击中常用的行为。 组件如下：

- 攻击面减少 (ASR) 是一组控件，企业可以通过它们阻止可疑的恶意文件，防止恶意软件入侵计算机。 例如 Office 文件、脚本、横向移动、勒索软件行为和基于电子邮件的威胁。
- 网络保护可通过 Windows Defender SmartScreen 阻止设备上的出站进程访问不受信任的主机/IP 地址，保护终结点免受基于 Web 的威胁。
- 受控文件夹访问权限 可阻止不受信任的进程访问受保护的文件夹，保护敏感数据免受勒索软件的威胁。
- Exploit Protection 是针对漏洞利用的一组缓解措施（代替 EMET），可以轻松地进行配置以保护系统和应用程序。
- Windows Defender 应用程序控制（也称为代码完整性 (CI) 策略）已在 Windows Server 2016 中发布。 我们已通过包含默认 CI 策略简化了部署。 默认 CI 策略允许所有 Windows 内置文件和 Microsoft 应用程序（如 SQL Server），并阻止可以绕过 CI 的已知可执行文件。

软件定义的网络 (SDN) 的安全性

SDN 的安全性提供多种功能来增强客户运行工作负荷的信心，不管是在本地运行，还是作为服务提供商在云中运行。

这些安全增强功能集成到了 Windows Server 2016 中 引入的全面 SDN 平台中。

有关 SDN 中新增功能的完整列表，请参阅 Windows Server 2019 的 SDN 中的新增功能。

受防护的虚拟机的改进

我们对受防护的虚拟机进行了以下改进。

分支机构改进

现在可以利用新的回退 HGS 和脱机模式功能在计算机上运行受防护的虚拟机，以间歇性方式连接到主机保护者服务。 可以通过回退 HGS 配置第二组用于 Hyper-V 的 URL，试试是否无法访问主 HGS 服务器。

即使你无法访问 HGS，脱机模式也可以让你继续启动受防护的 VM。 只要 VM 已成功启动一次并且主机的安全配置并未更改，就也能通过脱机模式启动 VM。

故障排除改进

我们还通过启用对 VMConnect 增强会话模式和 PowerShell Direct 的支持，简化了受防护 VM 的故障排除。 这些工具适用于到 VM 的网络连接已断开，需要更新其配置才能恢复访问的情况。 若要了解详细信息，请参阅受保护的结构和受防护的 VM。

你不需要配置这些功能，因为当将受防护的 VM 放置在运行 Windows Server 1803 版本或更高版本的 Hyper-V 主机上时，这些功能会自动变为可用状态。

Linux 支持

如果运行混合 OS 环境，那些现在可以通过 Windows Server 2019 在受防护的虚拟机内运行 Ubuntu、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server。

HTTP/2 实现更快、更安全的 Web

- 改进了连接合并，可提供不间断且正确加密的浏览体验。
- 升级了 HTTP/2 的服务器端加密套件协商，以便于自动减轻连接故障以及轻松进行部署。
- 已将默认 TCP 拥塞提供程序更改为 Cubic，为你提供更大的吞吐量！

加密网络

虚拟网络加密对具有**启用加密**标签的子网中的虚拟机之间的虚拟网络流量进行加密。 加密网络还使用虚拟子网上的数据报传输层安全性 (DTLS) 来加密数据包。 DTLS 可以保护你的数据不被访问物理网络的任何人窃听、篡改和伪造。

有关详细信息，请参阅加密网络。

防火墙审核

防火墙审核是 SDN 防火墙的一项新功能，用于记录已启用日志记录的 SDN 防火墙规则和访问控制列表 (ACL) 处理的任何流。

虚拟网络对等

使用虚拟网络对等互连可以无缝连接两个虚拟网络。 建立对等互连后，虚拟网络就会作为一个整体出现在监控中。

出口计量

出站计量为出站数据传输提供使用计量。 网络控制器使用此功能为每个虚拟网络保留 SDN 内使用的所有 IP 范围的允许列表。 这些列表将任何指向未包含在所列 IP 范围内的目的地的数据包视为出站数据传输计费。

存储

下面是我们对 Windows Server 2019 中的存储做出的一些更改。 存储还受重复数据删除更新的影响，特别是对 DataPort API 的更新，以便优化重复数据删除卷的入口或出口。

File Server Resource Manager

现在可以阻止文件服务器资源管理器服务启动时在所有卷上创建变更日志（也称为 USN 日志）。 通过阻止产生此更改，可以节省每个卷的空间，但会禁用实时文件分类。 有关详细信息，请参阅文件服务器资源管理器概述。

SMB

- 默认情况下，Windows Server 不再安装 SMB1 客户端和服务器。 此外，SMB2 及更高版本中作为来宾进行身份验证的功能默认情况下处于关闭状态。 有关详细信息，请查看在 Windows 10 版本 1709 和 Windows Server 版本 1709 及更高版本中默认不会安装 SMBv1。
- 现在，可以在 SMB2+ 中为旧版应用程序禁用 Oplock。 还可以要求客户端在每个连接的基础上进行签名或加密。 有关详细信息，请参阅 SMBShare PowerShell 模块帮助。

存储迁移服务

使用存储迁移服务可以更轻松地将服务器迁移到更高版本的 Windows Server。 此图形工具在服务器上列出数据，然后将数据和配置传输到较新的服务器。 存储迁移服务还可以

将旧服务器的标识移动到新服务器，这样用户就不必重新配置其配置文件和应用。 有关详细信息，请参阅存储迁移服务。

Windows Admin Center 版本 1910 添加了部署 Azure 虚拟机的功能。 此更新将 Azure VM 部署集成到存储迁移服务中。 有关详细信息，请参阅 Azure VM 迁移。

在安装了 KB5001384 的 Windows Server 2019 上或在 Windows Server 2022 上运行存储迁移服务器业务流程协调程序时，还可以访问以下发布到制造后 (RTM) 功能：

- 将本地用户和组迁移到新服务器。
- 从故障转移群集迁移存储、迁移到故障转移群集，以及在独立服务器和故障转移群集之间迁移。
- 从使用 Samba 的 Linux 服务器迁移存储。
- 使用 Azure 文件同步更轻松地将已迁移的共享同步到 Azure 中。
- 迁移到 Azure 等新网络。
- 将 NetApp 通用 Internet 文件系统 (CIFS) 服务器从 NetApp 联合身份验证服务 (FAS) 阵列迁移到 Windows 服务器和群集。

存储空间直通

下面是存储空间直通中的新增功能。 有关如何获取经过验证的存储空间直通系统的详细信息，请参阅 Azure Stack HCI 解决方案概述。

- 用于 ReFS 卷的删除重复和压缩功能。 具有可选压缩功能的可变大小块存储可最大限度地提高节省率；而多线程后处理体系结构可最大程度地降低性能影响。 此功能支持高达 64 TB 的卷，并将对每个文件的前 4 MB 进行重复数据消除。

- 本机支持持久性内存，使你可以像 PowerShell 或 Windows Admin Center中的任何其他驱动器一样管理永久性内存。 此功能支持 Intel Optane DC PM 和 NVDIMM-N 持久性内存模块。

- 边缘处双节点超聚合基础结构的嵌套复原。 借助基于 RAID 5+1 的新软件复原选项，现在可以同时应对两次硬件故障。 双节点存储空间直通群集为应用和虚拟机提供持续可访问的存储，即使一个服务器节点发生故障，另一个服务器结点发生驱动器故障。

- 双服务器群集现在可以使用 U 盘作为见证。 如果在服务器出现故障后进行备份，则 U 盘群集知道哪个服务器有最新数据。 有关详细信息，请参阅我们的存储空间直通公告博客文章和为故障转移群集配置文件共享见证。

- Windows Admin Center支持一个仪表板，可让你直接管理和监视存储空间直通。 可以监视从整体群集级别到单个 SSD 或 HDD 的 IOPS 和 IO 延迟，而无需额外付费。 若要了解详细信息，请参阅什么是 Windows Admin Center？ 。

- 性能历史记录是一项新功能，可轻松了解资源利用率和度量。 若要了解详细信息，请参阅存储空间直通的性能历史记录。
- 使用最多 64 个卷（最多 64 TB）的容量，每个群集可扩展到 4 PB。 还可以将多个群集拼接成一个群集集，以便在单个存储命名空间内实现更大的规模。
- 利用镜像加速奇偶校验，可以构建包含镜像和奇偶校验策略的存储空间直通卷，类似于 RAID-1 和 RAID-5/6 的混合。 镜像加速奇偶校验现在比 Windows Server 2016 快两倍。
- 驱动器延迟异常检测会自动识别 PowerShell 和 Windows Admin Center 中具有“异常延迟”状态的速度缓慢的驱动器。
- 手动分隔卷的分配以提高容错能力。 有关详细信息，请参阅分隔存储空间直通中的卷的分配。

存储副本

下面是存储副本中的新增功能。

- 存储副本现已在 Windows Server 2019 Standard Edition 和 Windows Server 2019 Datacenter Edition 中提供。 但是，使用 Standard Edition，只能复制一个卷，并且该卷的大小只能达到 2 TB。
- 测试故障转移是一项新功能，允许你在目标服务器上临时装载复制存储的快照，以便进行测试或备份。 有关详细信息，请参阅有关存储副本的常见问题。
- 存储副本日志性能改进，例如改进了全闪存储和相互复制的存储空间直通群集的复制吞吐量和延迟。
- Windows Admin Center 支持，包括使用服务器管理器对服务器到服务器、群集到群集和拉伸群集复制进行图形化复制管理。

重复数据删除

Windows Server 2019 现在支持复原文件系统 (ReFS)。 通过 ReFS 使用 ReFS 文件系统的重复数据删除和压缩功能，可在同一卷上存储多达十倍的数据。 可变大小的区块存储附带了一种可选的压缩功能，可以最大程度地节省成本，而多线程后处理体系结构将性能影响降到最低。 ReFS 支持高达 64 TB 的卷，并将对每个文件的前 4 TB 进行重复数据消除。 若要了解详细信息，请参阅如何在 Windows Admin Center 中启用重复数据删除和压缩，以获取快速视频演示。

故障转移群集

我们在 Windows Server 2019 中为故障转移群集添加了以下功能：

- 群集集将多个群集组合成松散耦合的多个故障转移群集，这些群集有三种类型：计算、存储和超聚合。 这种分组增加了单个软件定义的数据中心 (SDDC) 解决方案中的服务器数量，超出了当前群集的限制。 使用群集集，可以在群集集内的群集之间移动联机虚拟机。 有关详细信息，请参阅部署群集集。

- 默认情况下，群集现在是 Azure 感知群集。 Azure 感知群集会自动检测它们何时在 Azure IaaS 虚拟机中运行，然后优化其配置以实现最高级别的可用性。 这些优化包括主动故障转移和记录 Azure 计划内维护事件。 自动优化使部署更加简单，因为不需要将负载均衡器配置为分布式网络名称作为群集名称。

- 跨域群集迁移使故障转移群集能够动态地从一个 Active Directory 域移动到另一个 Active Directory 域，简化了域整合，并允许硬件合作伙伴创建群集并在以后将其加入客户的域。

- USB 见证功能允许你使用连接到网络交换机的 USB 驱动器作为见证，以确定群集仲裁。 此功能包括对任何符合 SMB2 标准的设备的扩展文件共享见证支持。

- 现在默认情况下启用 CSV 缓存，从而大幅提升了虚拟机性能。 MSDTC 现在支持群集共享卷，以允许在存储空间直通上部署 MSDTC 工作负载，例如 SQL Server。 增强型逻辑可利用自我修复检测分区节点，以恢复节点的群集成员身份。 增强型群集网络路由检测和自我修复。

- 现在集成了群集感知更新 (CAU)，并可感知存储空间直通，验证并确保了每个节点上数据重新同步完成。 群集感知更新仅在必要时检查更新以智能重启。 此功能允许重启群集中的所有服务器进行计划内维护。

- 现在，可以在以下方案中使用文件共享见证：

    - 由于远程位置导致 Internet 访问缺失或极差，从而阻止使用云见证。

    - 磁盘见证缺少共享驱动器。 例如，不使用共享磁盘的配置，例如存储空间直通超聚合配置、SQL Server Always On 可用性组 (AG) 或 Exchange 数据库可用性组 (DAG)。

    - 由于群集位于 DMZ 后面，因此缺少域控制器连接。

    - 没有 Active Directory 群集名称对象 (CNO) 的工作组或跨域群集。 Windows Server 现在还阻止将 DFS 命名空间共享用作位置。 将文件共享见证添加到 DFS 共享可能会导致群集不稳定，因此我们从不支持此配置。 我们添加了用来检测共享是否使用 DFS 命名空间以及是否检测到 DFS 命名空间的逻辑，故障转移群集管理器会阻止创建见证服务器，并显示有关不受支持的错误消息。

- 已实现群集强化功能，可增强群集共享卷和存储空间直通通过服务器消息块 (SMB) 进行群集内部通信的安全性。 此功能利用证书提供尽可能安全的平台。 通过这样做，故障转移群集现在可以在不依赖 NTLM 的情况下运行，从而可以建立安全基线。

- 故障转移群集不再使用 NTLM 身份验证。 相反，Windows Server 2019 群集现在仅使用 Kerberos 和基于证书的身份验证。 用户无需进行任何更改或部署任何内容即可利用此安全增强功能。 此更改还允许在禁用 NTLM 的环境中部署故障转移群集。

应用程序平台

Windows 上的 Linux 容器

现在可以使用相同的 Docker 守护程序在同一容器主机上运行基于 Windows 和 Linux 的容器。 你现在可以使用异构容器主机环境，为应用程序开发人员提供灵活性。

针对 Kubernetes 的内置支持

Windows Server 2019 通过推出半年渠道版本不断改进计算、联网和存储功能，以支持 Kubernetes 在 Windows 上运行。 即将推出的 Kubernetes 版本中将提供更多详细信息。

- Windows Server 2019 中的容器网络极大地提高了 Windows 上 Kubernetes 的可用性。 我们已增强平台网络复原能力以及对容器网络插件的支持。

- 在 Kubernetes 上部署的工作负荷能够利用网络安全性来保护使用嵌入式工具的 Linux 和 Windows 服务。

容器改进

- **改进了集成身份**

  我们简化了容器中的集成 Windows 身份验证并提高了其可靠性，解决了早期 Windows Server 版本中的几个限制。

- **提高了应用程序兼容性**

  实现基于 Windows 的应用程序的容器化变得更加简单：提高了现有 **windowsservercore** 映像的应用兼容性。 对于具有更多 API 依赖项的应用程序，现在还增加了第三个基本映像：**windows**。

- **占用空间更小，性能更高**

基本容器映像的下载大小、在磁盘上的大小和启动时间都得到了改善，以加快容器工作流的处理速度。

- **使用 Windows Admin Center（预览版）的管理体验**

  现在，使用 Windows Admin Center 的新扩展，用户可以比以往更轻松地查看计算机上正在运行哪些容器并管理各个容器。 查找 Windows Admin Center 公共源中的“容器”扩展。

计算改进

- **VM 启动排序** VM 启动排序也通过 OS 和应用程序感知得到了改进，提供增强的触发器，在一个 VM 已启动、下一个 VM 未启动时触发。
- 利用**对 VM 的存储类内存支持**，可以在非易失性 DIMM 上创建 NTFS 格式的直接访问卷，并且可以向 Hyper-V VM 公开这些卷。 Hyper-V VM 现在能够利用存储类内存设备的低延迟性能优势。
- **Hyper-V VM 的永久性内存支持** 为了在虚拟机中充分利用持久性内存（也称为存储类内存）的高吞吐量和低延迟，现在可以将它直接投影到虚拟机中。 永久性内存可帮助你大大降低数据库事务延迟或缩短出现故障时低延迟内存中数据库的恢复时间。
- **容器存储 - 永久性数据卷** 应用程序容器现在具有对卷的持久访问权限。 有关详细信息，请参阅群集共享卷 (CSV)、存储空间直通 (S2D)、SMB 全局映射的容器存储支持。
- **虚拟机配置文件格式（更新）** 已为配置版本为 8.2 及更高版本的虚拟机添加了 VM 来宾状态文件（`.vmgs`）。 VM 来宾状态文件包括设备状态信息（以前是 VM 运行时状态文件的一部分）。

加密网络

加密网络 - 虚拟网络加密允许对在标记为**启用加密**的子网内相互通信的虚拟机之间的虚拟网络流量进行加密。 它还利用虚拟子网上的数据报传输层安全性 (DTLS) 来加密数据包。 DTLS 可以防止能够访问物理网络的任何人进行窃听、篡改和伪造。

虚拟工作负荷的网络性能提升

虚拟工作负荷的网络性能提升可最大程度地提升虚拟机的网络吞吐量，无需不断地调整或过度预配主机。 提升后的性能可降低操作和维护成本，同时提高主机的可用密度。 这些新功能包括：

- 动态虚拟机多队列 (d.VMMQ)
- 在 vSwitch 中接收段合并

低额外延迟后台传输

低额外延迟后台传输 (LEDBAT) 是一款针对延迟进行优化的网络拥塞控制提供程序，旨在自动产生为用户和应用程序分配的带宽。 LEDBAT 在网络未使用时使用可用带宽。 此技术用于在整个 IT 环境中部署较大的关键更新，而不会影响面向客户的服务和关联带宽。

Windows 时间服务

Windows 时间服务包括符合 UTC 标准的闰秒级支持、称为精确时间协议的新时间协议和端到端可追溯性。

高性能 SDN 网关

Windows Server 2019 中的高性能 SDN 网关极大地提高了 IPsec 和 GRE 连接的性能，在显著降低 CPU 使用率的同时提供超高性能吞吐量。

用于 SDN 的新部署 UI 和 Windows Admin Center 扩展

现在，借助 Windows Server 2019，可以通过用于充分利用 SDN 的新部署 UI 和 Windows Admin Center 扩展来轻松实现部署和管理。

适用于 Linux 的 Windows 子系统 (WSL)

WSL 使服务器管理员可以使用 Windows Server 上的 Linux 中的现有工具和脚本。 命令行博客 中展示的许多改进现在都是 Windows Server 的一部分，包括后台任务、DriveFS、WSLPath 和更多其他内容。

Active Directory 联合身份验证服务

适用于 Windows Server 2019 的 Active Directory 联合身份验证服务 (AD FS) 包括以下更改。

受保护的登录

AD FS 的受保护登录现在包括以下更新：

- 用户现在可以将第三方身份验证产品作为首要因素，而无需公开密码。 在外部身份验证提供程序可以证明两个因素的情况下，其可以使用多重身份验证 (MFA)。
- 用户现在可以在使用非密码选项作为首要因素后，将密码作为额外因素。 这种内置支持改善了 AD FS 2016 的整体体验，AD FS 2016 需要下载 GitHub 适配器。
- 用户现在可以生成自己的插件风险评估模块，以在预身份验证阶段阻止特定类型的请求。 此功能使使用云智能（如标识保护）来阻止风险用户或交易变得更加容易。 有关详细信息，请参阅使用 AD FS 2019 风险评估模型生成插件。
- 通过添加以下功能，改进 Extranet 智能锁定 (ESL) 快速修复工程 (QFE)：
  - 现在，你可以在受经典 Extranet 锁定功能保护的同时使用审核模式。
  - 用户现在可以对熟悉的位置使用独立的锁定阈值。 使用此功能，可以在公共服务帐户中运行多个应用实例，以便在最小程度上中断密码。

其他安全改进

AD FS 2019 包括以下安全改进：

- 使用 SmartCard 登录的远程 PowerShell 允许用户通过运行 PowerShell 命令通过智能卡远程连接到 AD FS。 用户还可以使用此方法管理所有 PowerShell 函数，包括多节点 cmdlet。
- HTTP 标头自定义允许用户自定义在 AD FS 响应期间创建的 HTTP 标头。 标头自定义包括以下类型的标头：
  - HSTS，它仅允许在 HTTPS 终结点上使用 AD FS 终结点，以便合规浏览器强制执行。
  - X-frame-options，使 AD FS 管理员可允许特定信赖方为 AD FS 交互式登录页面嵌入 iFrame。 只应在 HTTPS 主机上使用此标头。
  - 未来的标头。 还可以配置多个未来的标头。

  有关详细信息，请参阅使用 AD FS 2019 自定义 HTTP 安全响应标头。

身份验证和策略功能

AD FS 2019 包含以下身份验证和策略功能：

- 用户现在可以创建规则来指定部署调用哪个身份验证提供程序进行额外身份验证。 此功能有助于在身份验证提供程序之间转换，并保护对额外身份验证提供程序有特殊要求的特定应用。

- 基于传输层安全性 (TLS) 的设备身份验证的可选限制，以便只有需要 TLS 的应用程序才能使用它们。 客户可以将基于客户端 TLS 的设备身份验证仅限于执行基于设备的条件访问的应用程序。 此功能可防止对不需要基于 TLS 的设备身份验证的应用程序发出不必要的设备身份验证提示。

- AD FS 现在支持根据第二因素凭据的新鲜度重新执行第二因素凭据。 此功能允许用户在第一个事务时只需要 TFA，然后在定期的基础上只需要第二个因素。 只能在可以在请求中提供额外参数的应用程序上使用此功能，因为它不是 AD FS 中的可配置设置。 如果你在 Microsoft Entra ID 联合域信任设置中，将**在 X 天内记住我的 MFA** 设置配置为将 *supportsMFA* 设置为 **True**，则 Microsoft Entra ID 支持此参数。

单一登录改进

AD FS 2019 还包括以下单一登录 (SSO) 改进：

- AD FS 现在使用分页的 UX 流和中心用户界面 (UI)，为用户提供更流畅的登录体验。此更改反映了 Azure AD 中提供的功能。 可能需要更新组织的徽标和背景图像，以适应新的 UI。

- 我们修复了在 Windows 10 设备上使用主刷新令牌 (PRT) 身份验证时导致 MFA 状态不持久的问题。 现在，应该不那么频繁地提示用户输入第二因素凭据。 现在，当设备身份验证在客户端 TLS 和 PRT 身份验证上成功时，体验应保持一致。

对生成新式业务线应用的支持

AD FS 2019 包括以下功能，以支持构建新式业务线 (LOB) 应用：

- AD FS 现在包括 OAuth 设备流配置文件支持，用于使用没有 UI 外围应用的设备登录，以支持丰富的登录体验。 此功能允许用户在不同的设备上完成登录。 Azure Stack 中的 Azure 命令行接口 (CLI) 体验需要此功能，也可以在其他方案中使用它。

- 不再需要 *Resource* 参数使用 AD FS，这符合当前的 OAUth 规范。 客户端现在只需要提供依赖方信任标识符作为 scope 参数，并提供请求的权限。

- 可以使用 AD FS 响应中的跨源资源共享 (CORS) 标头。 这些新标题允许用户生成单页应用程序，其允许客户端 JavaScript 库通过从 AD FS 上的 Open ID Connect (OIDC) 发现文档中查询签名密钥来验证 *id_token* 签名。

- AD FS 包括对 OAuth 中安全身份验证代码流的用于代码交换的证明密钥 (PKCE) 支持。 这一额外的安全层可以防止恶意参与者劫持代码并从不同的客户端重放代码。

- 我们修复了导致 AD FS 仅发送 x5t 声明的次要问题。 AD FS 现在还发送一个儿童声明，表示用于签名验证的密钥 ID 提示。

可支持性改进

管理员现在可以配置 AD FS，允许用户将错误报告和调试日志以 ZIP 文件的形式发送给他们，以便进行故障排除。 管理员还可以配置简单邮件传输协议 (SMTP) 连接，以自动将 ZIP 文件发送到分类电子邮件帐户。 另一个设置允许管理员基于该电子邮件自动为其支持系统创建票证。

部署更新

AD FS 2019 中现已包含以下部署更新：

- AD FS 具有与其 Windows Server 2016 版本类似的功能，可以更容易地将 Windows Server 2016 服务器场升级到 Windows Server 2019 服务器场。 添加到 Windows Server 2016 服务器场的 Windows Server 2019 服务器在你准备升级之前，其行为只会像 Windows Server 2016 服务器一样。 有关详细信息，请参阅升级到 Windows Server 2016 中的 AD FS。

SAML 更新

AD FS 2019 包含以下安全断言标记语言 (SAML) 更新：

- 我们在这些方面修复了聚合联合身份验证支持中的问题，例如 InCommon：
  - 改善了聚合联合元数据文档中许多实体的缩放。 以前，这些实体的缩放不会成功，并返回 ADMIN0017 错误消息。
  - 现在，可以通过运行 `Get-AdfsRelyingPartyTrustsGroup` PowerShell cmdlet，使用 *ScopeGroupID* 参数进行查询。
  - 改进了对重复 *entityID* 值的错误情况的处理。

范围参数中的 Azure AD 样式资源规范

之前，AD FS 要求所需的资源和范围在任何身份验证请求中都位于单独参数中。 例如，以下示例 OAuth 请求包含一个 scope 参数：

```
HTTP

https:&#47;&#47;fs.contoso.com/adfs/oauth2/authorize?
response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:adfs:cl
aimsxray&scope=oauth&redirect_uri=https:&#47;&#47;adfshelp.microsoft.com/
ClaimsXray/TokenResponse&prompt=login
```

借助 Windows Server 2019 上的 AD FS，你现在可以传递嵌入在 scope 参数中的资源值。 此更改与针对 Microsoft Entra ID 的身份验证一致。

现在可以将 scope 参数组织成一个用空格分隔的列表，其中每个实体的结构都作为资源/范围。

> **备注**
>
> 只能在身份验证请求中指定一个资源。 如果你在请求中包含多个资源，则 AD FS 将返回错误，且身份验证将失败。

反馈

此页面是否有帮助? 是 否

Windows Server 2016 中的新增功能

项目 • 2024/08/05 • 适用于: ✅ Windows Server 2016

本文介绍 Windows Server 2016 中的一些新增功能，这些功能在你使用此版本时最可能具有最大影响力。

计算

虚拟化区域包括适用于 IT 专业人员的虚拟化产品和功能，可用于设计、部署和维护 Windows Server。

常规

由于 Win32 Time 和 Hyper-V 时间同步服务的改进，物理和虚拟计算机从更高的时间准确性中受益。 现在，Windows Server 可以托管与即将推出的要求 UTC 准确性为 1 ms 的规则相容的服务。

Hyper-V

Hyper-V 网络虚拟化 (HNV) 是 Microsoft 更新的软件定义的网络 (SDN) 解决方案的基本构建基块，并完全集成到 SDN 堆栈中。 Windows Server 2016 包括针对 Hyper-V 的以下更改：

- Windows Server 2016 现在包括一个可编程的 Hyper-V 交换机。 Microsoft 的网络控制器使用 Open vSwitch Database Management Protocol (OVSDB) 作为 SouthBound 接口 (SBI)，将 HNV 策略向下推送到每个主机上运行的主机代理。 主机代理使用 VTEP 架构 的自定义来存储此策略，并将复杂的流规则编程到 Hyper-V 交换机的高性能流引擎中。 Hyper-V 交换机中的流引擎与 Azure 使用的流引擎相同。 通过网络控制器和网络资源提供商的整个 SDN 堆栈也与 Azure 一致，使其性能与 Azure 公有云相当。 在 Microsoft 的流引擎中，Hyper-V 交换机通过简单的匹配操作机制来处理无状态和有状态流规则，该机制定义了如何在交换机中处理数据包。

- HNV 现在支持虚拟可扩展局域网 (VXLAN) 协议 封装。 HNV 使用 VXLAN 协议，通过 Microsoft 网络控制器以 MAC 分发模式，将租户过度网络 IP 地址映射到物理底层网络 IP 地址。 NVGRE 和 VXLAN 任务卸载支持第三方驱动程序以提高性能。

- Windows Server 2016 包括一个软件负载均衡器 (SLB)，它完全支持虚拟网络流量以及与 HNV 的无缝交互。 高性能流引擎在数据平面 v-Switch 上实现 SLB，由网络控制器对其进行虚拟 IP (VIP) 或动态 IP (DIP) 映射控制。

- HNV 实现正确的 L2 以太网标头，以确保与依赖于行业标准协议的第三方虚拟和物理设备的互操作性。 Microsoft 确保所有传输的数据包在所有字段中都具有符合要求的值，以保证互操作性。 HNV 需要在物理 L2 网络中支持巨型帧 (MTU > 1780)，以解决 NVGRE 和 VXLAN 等封装协议带来的数据包开销。 巨型帧支持确保连接到 HNV 虚拟网络的来宾虚拟机保持 1514 MTU。

- Windows 容器支持增加了性能改进，简化了网络管理，并在 Windows 10 上支持 Windows 容器。 有关详细信息，请参阅我们的 Windows 容器文档和容器：Docker、Windows 和趋势。

- Hyper-V 现在与连接待机兼容。 在使用始终开启/始终连接 (AOAC) 电源模式的计算机上安装 Hyper-V 角色时，现在可以将其配置为使用连接待机电源状态。

- 离散设备分配允许你为虚拟机 (VM) 提供对某些 PCIe 硬件设备的直接和独占访问权限。 此功能绕过 Hyper-V 虚拟化堆栈，从而加快了访问速度。 有关详细信息，请参阅离散设备分配和离散设备分配 - 说明和背景。

- Hyper-V 现在支持第 1 代 VM 中操作系统磁盘的 BitLocker 驱动器加密。 此保护方法取代了仅在第 2 代 VM 中可用的虚拟受信任的平台模块 (TPM)。 若要解密磁盘并启动 VM，Hyper-V 主机必须是授权的受保护结构的一部分，或者具有 VM 的保护者之一的私钥。 密钥存储需要版本 8 VM。 有关详细信息，请参阅在 Windows 或 Windows Server 上的 Hyper-V 中升级虚拟机版本。

- 主机资源保护通过跟踪过高的活动级别来防止 VM 使用过多的系统资源。 当监视检测到 VM 中异常高的活动级别时，它会限制 VM 消耗的资源量。 可以通过在 PowerShell 中运行 Set-VMProcessor cmdlet 来启用此功能。

- 现在，在运行 Linux 或 Windows 操作系统的第 2 代 VM 中，可以在 VM 运行时使用热添加或删除来添加或删除网络适配器，而不会停机。 还可以在 VM 运行时调整分配给 VM 的内存量，即使你没有在运行 Windows Server 2016 及更高版本或 Windows 10 及更高版的第 1 代和第 2 代 VM 上启用动态内存。

- Hyper-V 管理器现在支持以下功能：

  - 备用凭据，允许在连接到另一台 Windows Server 2016 或 Windows 10 远程主机时，在 Hyper-V 管理器中使用一组不同的凭据。 还可以保存这些凭据，以便更轻松地登录。

  - 现在，可以在运行 Windows Server 2012 R2、Windows Server 2012、Windows 8.1 和 Windows 8 的计算机上管理 Hyper-V。

  - Hyper-V 管理器现在使用 WS-MAN 协议与远程 Hyper-V 主机进行通信，该协议允许 CredSSP、Kerberos 和 NTLM 身份验证。 使用 CredSSP 连接到远程 Hyper-V 主机时，可以执行实时迁移，而无需在 Active Directory 中启用约束委派。

WS-MAN 还使启用主机进行远程管理变得更加容易。 WS-MAN 通过端口 80（该端口默认处于打开状态）进行连接。

- 适用于 Windows 来宾的集成服务的更新现在通过 Windows 更新进行分发。 服务提供程序和私有云主机可以为拥有 VM 的租户提供对应用更新的控制。 Windows 租户现在可以通过单个方法使用所有最新更新来升级其 VM。 有关 Linux 租户如何使用集成服务的详细信息，请参阅 Windows Server 和 Windows 上 Hyper-V 支持的 Linux 和 FreeBSD 虚拟机。

  > **ⓘ 重要**
  >
  > 适用于 Windows Server 2016 的 Hyper-V 不再包含 vmguest.iso 映像文件，因为它不再是必需的。

- 在第 2 代 VM 上运行的 Linux 操作系统现在可以在启用“安全启动”选项的情况下启动。 在 Windows Server 2016 主机上支持安全启动的操作系统包括 Ubuntu 14.04 及更高版本、SUSE Linux Enterprise Server 12 及更高版本、Red Hat Enterprise Linux 7.0 及更高版本以及 CentOS 7.0 及更高版本。 首次启动 VM 之前，必须将其配置为在 Hyper-V 管理器、Virtual Machine Manager 中或通过在 PowerShell 中运行 Set-VMFirmware cmdlet 来使用 Microsoft UEFI 证书颁发机构。

- 第 2 代 VM 和 Hyper-V 主机现在可以使用更多的内存和虚拟处理器。 还可以为主机配置比以前版本更多的内存和虚拟处理器。 这些更改支持诸如运行大型内存数据库以进行联机事务处理 (OLTP) 和电子商务数据仓库 (DW) 等方案。 有关详细信息，请参阅用于内存中事务处理的 Windows Server 2016 Hyper-V 大规模 VM 性能。 有关版本兼容性和支持的最大配置的详细信息，请参阅在 Windows 或 Windows Server 上的 Hyper-V 中升级虚拟机版本和计划 Windows Server 中的 Hyper-V 可扩展性。

- 使用嵌套虚拟化功能可将 VM 用作 Hyper-V 主机，并在虚拟化主机中创建 VM。 可以使用此功能生成至少运行 Windows Server 2016 或 Windows 10 且具有支持 Intel VT-x 处理器的开发和测试环境。 有关详细信息，请参阅什么是嵌套虚拟化？ 。

- 现在，可以设置生产检查点，以符合运行生产工作负载的 VM 的支持策略。 这些检查点在来宾设备内部的备份技术上运行，而不是在已保存的状态下运行。 Windows VM 使用卷快照服务 (VSS)，而 Linux VM 刷新文件系统缓冲区来创建与文件系统一致的检查点。 仍然可以通过使用标准检查点来使用基于保存状态的检查点。 有关详细信息，请参阅在 Hyper-V 中的标准检查点或生产检查点之间进行选择。

  > **ⓘ 重要**

新 VM 使用生产检查点作为默认值。

- 现在，可以调整共享虚拟硬盘（`.vhdx` 文件）的大小，以便在不停机的情况下进行来宾群集。 还可以使用来宾群集通过使用 Hyper-V 副本进行灾难恢复来保护共享虚拟硬盘。 只能在通过 Windows Management Instrumentation (WMI) 启用复制的来宾群集中的集合上使用此功能。 有关详细信息，请参阅 Msvm_CollectionReplicationService 类和虚拟硬盘共享概述。

  > **备注**
  >
  > 无法通过 PowerShell cmdlet 或使用 WMI 接口管理集合的复制。

- 备份单个虚拟机时，无论主机是否已群集化，都不建议使用 VM 组或快照集合。 这些选项旨在备份使用共享 vhdx 的客户群集。 相反，建议使用 Hyper-V WMI 提供程序 (V2) 拍摄快照。

- 现在可以创建受防护的 Hyper-V VM，其中包括阻止主机上的 Hyper-V 管理员检查、篡改或从受防护的 VM 状态窃取数据的功能。 数据和状态已加密，因此 Hyper-V 管理员无法查看视频输出和可用磁盘。 还可以将 VM 限制为仅在主机保护者服务器确定为正常且可信的主机上运行。 有关详细信息，请参阅受保护的结构和受防护的 VM 概述。

  > **备注**
  >
  > 受防护的 VM 与 Hyper-V 副本兼容。 若要复制受防护的虚拟机，必须授权要复制的主机运行该受防护的 VM。

- 通过群集虚拟机的启动顺序优先级功能，可以更好地控制哪些群集 VM 首先启动或重新启动。 通过确定启动顺序优先级，可以在启动使用这些服务的 VM 之前启动提供服务的 VM。 可以使用 PowerShell cmdlet 定义集、将 VM 添加到集以及指定依赖项，如 New-ClusterGroupSet、Get-ClusterGroupSet 和 Add-ClusterGroupSetDependency。

- VM 配置文件现在使用 `.vmcx` 文件扩展名格式，而运行时状态数据文件则使用 `.vmrs` 文件扩展名格式。 这些新的文件格式在设计时考虑到了更高效的读写。 如果发生存储故障，更新的格式还可以降低数据损坏的可能性。

  > **重要**

`.vmcx` 文件扩展名表示二进制文件。 适用于 Windows Server 2016 的 Hyper-V 不支持编辑 `.vmcx` 或 `.vmrs` 文件。

- 我们更新了与版本 5 VM 的版本兼容性。 这些 VM 与 Windows Server 2012 R2 和 Windows Server 2016 兼容。 但是，与 Windows Server 2019 兼容的版本 5 VM 只能在 Windows Server 2016 上运行，而不能在 Windows Server 2012 R2 上运行。 如果将 Windows Server 2012 R2 VM 移动或导入到运行更高版本的 Windows Server 的服务器，则必须手动更新 VM 配置以使用更高版本的 Windows Server 的功能。 有关版本兼容性和更新功能的详细信息，请参阅在 Windows 或 Windows Server 上的 Hyper-V 中升级虚拟机版本。

- 现在，可以为第 2 代 VM 使用基于虚拟化的安全功能（例如 Device Guard 和 Credential Guard），以保护操作系统免受恶意软件攻击。 这些功能在运行版本 8 或更高版本的 VM 中可用。 有关详细信息，请参阅在 Windows 或 Windows Server 上的 Hyper-V 中升级虚拟机版本。

- 现在，可以使用 Windows PowerShell Direct 运行 cmdlet，从主机配置 VM，作为 VMConnect 或远程 PowerShell 的替代方案。 不需要满足任何网络或防火墙要求，也不需要特殊的远程管理配置即可开始使用它。 有关详细信息，请参阅使用 PowerShell Direct 管理 Windows 虚拟机。

Nano Server

Nano Server 具有一个已更新的模块，用于构建 Nano Server 映像，包括物理主机和来宾虚拟机功能的更大分离度，以及对不同 Windows Server 版本的支持。 有关详细信息，请参阅安装 Nano Server。

恢复控制台也有改进，其中包括入站和出站防火墙规则分离及 WinRM 配置修复功能。

受防护的虚拟机

Windows Server 2016 提供新的基于 Hyper-V 的受防护的虚拟机，以保护任何第 2 代虚拟机免受已损坏的结构影响。 Windows Server 2016 中引入的功能如下所示：

- 新的“支持加密”模式提供比为普通虚拟机提供的更多、但比“防护”模式少的保护功能，同时仍支持 vTPM、磁盘加密、实时迁移通信加密和其他功能，包括直接构造管理便利（例如虚拟机控制台连接和 Powershell Direct）。

- 完全支持将现有非受防护的第 2 代虚拟机转换为受防护的虚拟机，包括自动磁盘加密。

- Hyper-V 虚拟机管理器现在可以查看授权运行的受防护的虚拟机上的结构，为结构管理员提供了一种打开受防护的虚拟机的密钥保护程序 (KP) 并查看结构是否有权在其上运行的方式。
- 你可以转换运行的主机保护者服务上的证明模式。 现在你可以即时在不太安全但更简单、基于 Active Directory 的证明和基于 TPM 的证明之间进行切换。
- 基于 Windows PowerShell 的端到端诊断工具能够检测到 Hyper-V 主机和主机保护者服务中的错误配置或错误。
- 恢复环境不仅提供在虚拟机可正常运行的构造中安全地排查故障并修复受防护的虚拟机的方法，还提供与受防护的虚拟机本身相同的保护级别。
- 主机保护者服务支持现有的安全 Active Directory – 可以指示主机保护者服务使用现有的 Active Directory 林作为其 Active Directory，而不是创建自己的 Active Directory 实例

有关使用受防护的虚拟机的详细信息和说明，请参阅受保护的结构和受防护的 VM。

身份标识和访问控制

身份标识中的新功能提高了组织保护 Active Directory 环境的能力，并帮助他们迁移到仅限云的部署和混合部署，其中某些应用程序和服务托管在云中，其他的则托管在本地。

Active Directory 证书服务

Windows Server 2016 中的 Active Directory 证书服务 (AD CS) 增加了对 TPM 密钥证明的支持：现可使用智能卡 KSP 进行密钥证明，而未加入域的设备现在可以使用 NDES 注册，以获得可证明 TPM 中密钥的证书。

Privileged Access Management

特权访问管理 (PAM) 有助于缓解 Active Directory 环境的安全问题，这些问题是由凭据盗窃技术（例如哈希传递、鱼叉式网络钓鱼等）引起的。 可以使用 Microsoft Identity Manager (MIM) 配置此新的管理访问解决方案，它引入了以下功能：

- 由 MIM 预配的堡垒 Active Directory 林对现有林具有特殊的 PAM 信任。 堡垒林是一种新型的 Active Directory 环境，由于与现有林隔离，并且仅允许访问特权帐户，因此没有恶意活动。
- MIM 中用于请求管理权限的新流程，包括用于批准请求的新工作流。

- MIM 为响应管理权限请求而在堡垒林中预配的新影子安全主体（或组）。 影子安全组有一个属性，该属性引用现有林中的管理组的 SID。 这样影子组就可以访问现有林中的资源，而无需更改任何访问控制列表 (ACL)。
- 过期链接功能，可为影子组启用有时间限制的成员身份。 可以将用户添加到组中一段时间，使他们能够执行管理任务。 有时间限制的成员身份由传播到 Kerberos 票证生存期的生存时间 (TTL) 值配置。

  > ⓘ **备注**
  >
  > 过期链接适用于所有链接属性。 但是，只有组和用户之间的 *member/memberOF* 链接属性关系预配置了 PAM，以使用过期链接功能。

- 内置的 Kerberos域控制器 (KDC) 增强功能允许 Active Directory 域控制器在用户对管理组具有多个有时间限制的成员身份时，将 Kerberos 票证生存期限制为尽可能低的 TTL 值。 例如，如果你是有时间限制的组 **A** 的成员，那么在登录时，Kerberos 票证授予票证 (TGT) 的有效期等于你在组 **A** 中的剩余时间。如果你同时加入了有时间限制的组 **B**，而该组的 TTL 比组 **A** 低，那么 TGT 的有效期就等于你在组 **B** 中的剩余时间。
- 新的监视功能使你能够识别哪些用户请求了访问权限、管理员授予了他们哪些访问权限以及他们在登录时执行了哪些活动。

若要了解有关 PAM 的详细信息，请参阅针对 Active Directory 域服务的特权访问管理。

Microsoft Entra 联接

Microsoft Entra 联接增强了企业、商业和教育客户的身份体验，并改进了企业和个人设备的功能。

- 新式设置现在可在公司拥有的 Windows 设备上使用。 使用核心 Windows 功能不再需要个人 Microsoft 帐户，它们现在可以通过使用现有的用户工作帐户运行，以确保合规性。 这些服务将在连接到内部 Windows 域的电脑和加入到 Microsoft Entra 的设备上运行。 这些设置包括：
  - 漫游或个性化、辅助功能设置和凭据
  - 备份和还原
  - 使用工作帐户访问 Microsoft Store
  - 动态磁贴和通知

- 在无法连接到 Windows 域的移动设备（例如，手机和平板电脑）上访问组织资源，而无论它们是企业自有的还是自带设备 (BYOD)。
- 对 Office 365 和其他组织应用、网站和资源使用单一登录 (SSO)。
- 在 BYOD 设备上，将本地域或 Azure AD 中的工作帐户添加到个人拥有的设备。 可以使用 SSO 通过应用或 Web 访问工作资源，同时保持与条件帐户控制和设备运行状况证明等新功能的兼容性。
- 移动设备管理 (MDM) 集成允许将设备自动注册到移动设备管理 (MDM) 工具（Microsoft Intune 或第三方）。
- 为组织中的多个用户设置“展台”模式和共享设备。
- 开发人员体验让你可以使用共享的编程堆栈构建同时满足企业和个人上下文需求的应用。
- “映像”选项让你可以在映像和允许用户在首次运行体验期间直接配置公司拥有的设备之间进行选择。

Windows Hello for Business

对于组织和消费者而言，Windows Hello 企业版是一种基于密钥的身份验证方法，它比密码身份验证更有优势。 这种形式的身份验证依赖于可以抵抗破坏、盗窃和网络钓鱼的凭据。

用户使用链接到证书或非对称密钥对的生物识别或 PIN 登录到设备。 标识提供者 (IDP) 通过将用户的公钥映射到 IDLocker 来验证用户的身份，并通过一次性密码 (OTP)、通过电话或不同的通知机制来提供登录信息。

有关详细信息，请参阅 Windows Hello for Business。

弃用文件复制服务 (FRS) 和 Windows Server 2003 功能级别

尽管文件复制服务 (FRS) 和 Windows Server 2003 功能级别已在早期版本的 Windows Server 中弃用，但我们想提醒你：AD DS 不再支持 Windows Server 2003。 应从域中删除任何运行 Windows Server 2003 的域控制器。 还应将域和林功能级别至少提升到 Windows Server 2008。

在 Windows Server 2008 及更高的域功能级别，AD DS 使用分布式文件服务 (DFS) 复制在域控制器之间复制 SYSVOL 文件夹内容。 如果在 Windows Server 2008 或更高的域功能级别创建新的域，DFS 复制会自动复制 SYSVOL 文件夹。 如果在较低的功能级别创建了域，则在复制 SYSVOL 文件夹时，必须从使用 FRS 复制迁移到使用 DFS 复制。 有关更详细的迁移步骤，请参阅安装、升级到或迁移到 Windows Server。

有关更多信息，请参阅以下资源：

- 理解 Active Directory(R) 域服务 (AD DS) 功能级别
- 如何提高 Active Directory 域和林功能级别

Active Directory 联合身份验证服务

Windows Server 2016 中的 Active Directory 联合身份验证服务 (AD FS) 包括使你可以配置 AD FS 以对轻型目录访问协议 (LDAP) 目录中存储的用户进行身份验证的新功能。

Web 应用程序代理

Web 应用程序代理的最新版本专注于为更多应用程序实现发布和预身份验证的新功能以及改进的用户体验。 查看新功能的完整列表，其中包括针对丰富的客户端应用（如 Exchange ActiveSync）的预身份验证以及用于更轻松地发布 SharePoint 应用的通配符域。 有关详细信息，请参阅 Windows Server 2016 中的 Web 应用程序代理。

管理

管理和自动化部分重点介绍适用于想要运行和管理 Windows Server 2016（包括 Windows PowerShell）的 IT 专业人员的工具和参考信息。

Windows PowerShell 5.1 包含重要的新功能（包括支持使用类进行开发、可扩展其用途的新安全功能），提高其可用性，并允许你更轻松、全面地控制和管理基于 Windows 的环境。 有关详细信息，请参阅 WMF 5.1 中的新方案和功能。

Windows Server 2016 的新增功能包括：在 Nano Server 上本地运行 PowerShell.exe（不再仅限于远程），新增“本地用户和组”cmdlet 来替换 GUI，添加了 PowerShell 调试支持，并添加了对 Nano Server 中安全日志记录和脚本以及 JEA 的支持。

下面是一些其他新管理功能：

Windows Management Framework (WMF) 5 中的 PowerShell 期望状态配置 (DSC)

Windows Management Framework 5 包括对 Windows PowerShell 期望状态配置 (DSC)、Windows 远程管理 (WinRM) 和 Windows 管理规范 (WMI) 的更新。

有关测试 Windows Management Framework 5 的 DSC 功能的详细信息，请参阅验证 PowerShell DSC 的功能 中所论述的一系列博客文章。 若要下载，请参阅 Windows Management Framework 5.1。

用于软件发现、安装和清单的 PackageManagement 统一包管理

Windows Server 2016 和 Windows 10 引入了一种新的 PackageManagement 功能（以前称为 OneGet），该功能可以允许 IT 专业人员或开发人员使软件发现、安装、清单 (SDII) 在本地或远程自动进行，无论安装程序技术为何，也不管软件位于何处。

有关详细信息，请参阅 https://github.com/OneGet/oneget/wiki。

有助于数字取证和减少安全漏洞的 PowerShell 增强功能

为了帮助负责调查受损系统的团队（有时称为“蓝队”），我们已添加其他 PowerShell 日志记录和其他数字取证功能，并且已添加有助于在脚本中减少漏洞的功能，例如受限的 PowerShell 和安全 CodeGeneration API。

有关详细信息，请参阅 PowerShell ♥ 蓝队 博客文章。

网络

网络部分论述了适用于 IT 专业人员的网络产品和功能，可用于设计、部署和维护 Windows Server 2016。

软件定义的网络

软件定义的网络 (SDN) 是一个新的软件定义数据中心 (SDDC) 解决方案，其中包括以下功能：

- 网络控制器，可用于自动配置网络基础结构，而无需手动执行网络设备和服务的配置。 网络控制器在其带有 JavaScript 对象表示法 (JSON) 有效负载的北向接口上使用表述性状态传输 (REST)。 网络控制器南向接口使用 Open vSwitch 数据库管理协议 (OVSDB)。

- Hyper-V 的新功能：

  - Hyper-V 虚拟交换机，可用于创建分布式交换和路由，以及与 Microsoft Azure 保持一致和兼容的策略实施层。 若要了解详细信息，请参阅 Hyper-V 虚拟交换机。

  - 远程直接内存访问 (RDMA) 和交换机嵌入式组合 (SET)，用于创建虚拟交换机。 无论你是否已在使用 SET，都可以在绑定到 Hyper-V 虚拟交换机的网络适配器上设置 RDMA。 SET 可以为虚拟交换机提供与 NIC 组合类似的功能。 有关详细信息，请参阅 Azure Stack HCI 的主机网络要求。

    - 虚拟机多队列 (VMMQ) 通过为每个 VM 分配多个硬件队列来提高 VMQ 吞吐量。默认队列将成为 VM 的一组队列，并在队列之间分配流量。
    - 软件定义网络的服务质量 (QoS) 在默认类别带宽内管理通过虚拟交换机的默认流量类别。

- 网络功能虚拟化 (NFV)，可用于将硬件设备执行的网络功能镜像或路由到虚拟设备，例如负载均衡器、防火墙、路由器、交换机等。 还可以使用 System Center Virtual Machine Manager 部署和管理整个 SDN 堆栈。 可以使用 Docker 来管理 Windows Server 容器网络，并将 SDN 策略与虚拟机和容器关联。

- 提供精细访问控制列表 (ACL) 的数据中心防火墙，可用于在 VM 接口级别或子网级别应用防火墙策略。 若要了解详细信息，请参阅什么是数据中心防火墙？。

- RAS 网关，可用于在虚拟网络和物理网络之间路由流量，包括从云数据中心到租户的远程站点的站点到站点 VPN 连接。 边界网关协议 (BGP)，可用于在所有网关方案中部署和提供网络之间的动态路由，包括 Internet 密钥交换版本 2 (IKEv2) 站点到站点虚拟专用网络 (VPN)、第 3 层 (L3) VPN 和通用路由封装 (GRE) 网关。 网关现在还支持网关池和 M+N 冗余。 若要了解详细信息，请参阅什么是用于软件定义的网络的远程访问服务 (RAS) 网关？。

- 软件负载均衡器 (SLB) 和网络地址转换 (NAT) 通过支持直接服务器返回来提高吞吐量。 这允许返回网络流量绕过负载均衡多路复用器，并且可以使用南北和东西第 4 层负载均衡器和 NAT 来实现。 若要了解详细信息，请参阅什么是用于 SDN 的软件负载均衡器 (SLB)？和网络功能虚拟化。

- 在数据平面上运行的灵活封装技术，支持虚拟可扩展 LAN (VxLAN) 和网络虚拟化通用路由封装 (NVGRE)。

有关详细信息，请参阅计划软件定义的网络基础结构。

云缩放基础知识

Windows Server 2016 包含以下云规模基础知识：

- 聚合网络接口卡 (NIC)，允许使用单个网络适配器进行管理、启用了远程直接内存访问 (RDMA) 的存储和租户流量。 聚合 NIC 降低了数据中心中每台服务器的成本，因为它需要更少的网络适配器来管理每台服务器不同类型的流量。

- 数据包直通提供高网络流量吞吐量和低延迟数据包处理基础结构。

- 交换机嵌入式组合 (SET) 是集成到 Hyper-V 虚拟交换机中的 NIC 组合解决方案。SET 允许将多达 8 个物理 NIC 组合成一个 SET 组，从而提高可用性并提供故障转移。 在 Windows Server 2016 中，可以创建仅限于使用服务器消息块 (SMB) 和

RDMA 的 SET 组。 还可以使用 SET 组为 Hyper-V 网络虚拟化分配网络流量。 有关详细信息，请参阅 Azure Stack HCI 的主机网络要求。

TCP 性能改进

默认初始拥塞窗口 (ICW) 已从 4 增加到 10 并已实现 TCP 快速打开 (TFO)。 TFO 减少了建立 TCP 连接所需的时间，并且增加的 ICW 允许在初始突发中传输较大的对象。 此组合可以显著减少在客户端和云之间传输 Internet 对象所需的时间。

当从数据包丢失恢复时，为了改善 TCP 行为，我们实施了 TCP 尾部丢失探测 (TLP) 和最新确认 (RACK)。 TLP 可帮助将转发超时 (RTO) 转换为快速恢复，而 RACK 可减少快速恢复所需的时间，以重新传输丢失的数据包。

动态主机配置协议 (DHCP)

Windows Server 2016 中的动态主机配置协议 (DHCP) 有以下更改：

- 从 Windows 10 版本 2004 开始，当运行 Windows 客户端并使用连接的 Android 设备连接到 Internet 时，连接现在标记为按流量计费。 某些 Windows 设备上显示为 MSFT 5.0 的传统客户端供应商名称现在是 MSFT 5.0 XBOX。
- 从 Windows 10 版本 1803 开始，DHCP 客户端现在可以从系统连接到的 DHCP 服务器读取并应用选项 119（即域搜索选项）。 域搜索选项还为短名称的 DNS 查找提供域名服务 (DNS) 后缀。 有关详细信息，请参阅 RFC 3397。
- DHCP 现在支持选项 82（子选项 5）。 可以使用此选项来允许 DHCP 代理客户端和中继代理请求特定子网的 IP 地址。 如果使用的是配置了 DHCP 选项 82（子选项 5）的 DHCP 中继代理，则中继代理可以从特定 IP 地址范围请求 DHCP 客户端的 IP 地址租约。 有关详细信息，请参阅 DHCP 子网选择选项。
- DNS 记录注册在 DNS 服务器上失败的情况的新日志记录事件。 有关详细信息，请参阅用于 DNS 注册的 DHCP 日志记录事件。
- DHCP 服务器角色不再支持网络访问保护 (NAP)。 DHCP 服务器不强制执行 NAP 策略，DHCP 作用域无法启用 NAP。 同时充当 NAP 客户端的 DHCP 客户端计算机使用 DHCP 请求 (SoH) 发送运行状况声明。 如果 DHCP 服务器运行的是 Windows Server 2016，则这些请求会像没有 SoH 时那样进行处理。 DHCP 服务器向客户端授予正常的 DHCP 租约。 如果运行 Windows Server 2016 的服务器是将身份验证请求转发到支持 NAP 的网络策略服务器 (NPS) 的远程身份验证拨入用户服务 (RADIUS) 代理，则 NPS 会将这些客户端评估为不支持 NAP，从而导致 NAP 处理失败。 有关 NAP 和 NAP 弃用的详细信息，请参阅 Windows Server 2012 R2 中删除或弃用的功能。

GRE 隧道

RAS 网关现在支持高可用性的通用路由封装 (GRE) 隧道，用于实现站点到站点连接和网关的 M+N 冗余。 GRE 是一种轻型隧道协议，可以在 Internet 协议网间上的虚拟点对点链路内封装各种网络层协议。 有关详细信息，请参阅 Windows Server 2016 中的 GRE 隧道。

IP 地址管理 (IPAM)

IPAM 具有以下更新：

- 增强的 IP 地址管理。 IPAM 改进了处理 IPv4 /32 和 IPv6 /128 子网以及在 IP 地址块中查找空闲 IP 地址子网和范围等方案的功能。
- 现在，可以运行 `Find-IpamFreeSubnet` cmdlet 来查找可用于分配的子网。 此函数不分配子网，只报告其可用性。 但是，可以将 cmdlet 输出通过管道传输到 `Add-IpamSubnet` 以创建子网。 有关详细信息，请参阅 Find-IpamFreeSubnet。
- 现在，可以运行 `Find-IpamFreeRange` cmdlet 在 IP 块、前缀长度和请求的子网数量内查找可用的 IP 地址范围。 此 cmdlet 不分配 IP 地址范围，只报告其可用性。 但是，可以将输出通过管道传输到 `AddIpamRange` cmdlet 中以创建范围。 有关详细信息，请参阅 Find-IpamFreeRange。
- 增强的 DNS 服务管理：
  - 非 DNSSEC DNS 服务器的 DNS 资源记录集合。
  - 配置所有类型的非 DNSSEC 资源记录的属性和操作。
  - 对加入域的 Active Directory 集成和文件支持的 DNS 服务器进行 DNS 区域管理。 可以管理所有类型的 DNS 区域，包括主区域、辅助区域和存根区域。
  - 在辅助区域和存根区域上触发任务，无论它们是正向查找区域还是反向查找区域。
  - 基于角色的访问控制，用于记录和区域的受支持 DNS 配置。
  - 条件转发器
- 集成的 DNS、DHCP 和 IP 地址 (DDI) 管理。 现在，可以在 IP 地址清单中查看与 IP 地址关联的所有 DNS 资源记录。 还可以自动保留 IP 地址的指针 (PTR) 记录，并管理 DNS 和 DHCP 操作的 IP 地址生命周期。
- 多个 Active Directory 林支持。 当安装 IPAM 的林与每个远程林之间存在双向信任关系时，可以使用 IPAM 管理多个 Active Directory 林的 DNS 和 DHCP 服务器。 有

关详细信息，请参阅管理多个 Active Directory 林中的资源。

- 通过"清除利用率数据"功能，可以通过删除旧的 IP 利用率数据来减小 IPAM 数据库的大小。 只需指定一个日期，IPAM 就会删除所有早于或等于输入的日期的数据库条目。 有关详情，请参阅清除利用率数据.
- 现在可以使用基于角色访问控制 (RBAC) 在 PowerShell 中定义 IPAM 对象的访问范围。 有关详细信息，请参阅使用 Windows PowerShell 管理基于角色的访问控制和 Windows PowerShell 中的 IP 地址管理 (IPAM) 服务器 cmdlet。

有关详细信息，请参阅管理 IPAM。

安全和保障

安全和保障部分包含适用于 IT 专业人员的安全解决方案和功能，可支持在数据中心和云环境中进行部署。 有关 Windows Server 2016 中常规安全性的信息，请参阅安全和保障。

Just Enough Administration

Windows Server 2016 中的 Just Enough Administration 是一种安全技术，可使能由 Windows PowerShell 管理的任何内容均可进行委派管理。 功能包括对在网络标识下运行、通过 PowerShell Direct 连接、安全地复制文件到 JEA 终结点或从 JEA 终结点安全地复制文件及配置 PowerShell 控制台来在 JEA 上下文中默认启动的支持。 有关详细信息，请参阅 GitHub 上的 JEA。

Credential Guard

凭据保护使用基于虚拟化的安全性来隔离密钥，以便只有特权系统软件可以访问它们。 有关详细信息，请参阅使用 Credential Guard 保护派生的域凭据。

适用于 Windows Server 2016 的 Credential Guard 包括以下针对已登录用户会话的更新：

- Kerberos 和新技术 LAN 管理器 (NTLM) 使用基于虚拟化的安全技术来保护登录用户会话的 Kerberos 和 NTLM 密钥。
- Credential Manager 利用基于虚拟化的安全性来保护已保存的域凭证。 已登录的凭据和已保存的域凭据不会传递给使用远程桌面的远程主机。
- 可以在没有统一可扩展固件接口 (UEFI) 锁的情况下启用 Credential Guard。

Remote Credential Guard

Credential Guard 包括对 RDP 会话的支持，以便用户凭据能够保留在客户端上，且不会在服务器端暴露。 它还提供远程桌面的单一登录体验。 有关详细信息，请参阅使用 Windows Defender Credential Guard 保护派生的域凭据。

适用于 Windows Server 2016 的远程 Credential Guard 包括以下针对已登录用户的更新：

- 远程 Credential Guard 会在客户端设备上保存已登录用户凭据的 Kerberos 和 NTLM 密钥。 远程主机以用户身份评估网络资源的任何身份验证请求都要求客户端设备使用密钥。
- 使用远程桌面时，远程 Credential Guard 可保护提供的用户凭据。

域保护

域保护现在需要一个 Active Directory 域。

PKInit 更新扩展支持

Kerberos 客户端现在会尝试使用 PKInit 更新扩展来进行基于公钥的登录。

KDC 现在支持 PKInit 更新扩展。 但在默认情况下，它们不提供 PKInit 更新扩展。

有关详细信息，请参阅 Kerberos 客户端和 KDC 对 RFC 8070 PKInit 更新扩展的支持。

滚动仅限公钥的用户的 NTLM 机密

从 Windows Server 2016 域功能级 (DFL) 开始，DC 现在支持滚动仅公钥用户的 NTLM 密钥。 此功能在较低的领域功能级别 (DFL) 中不可用。

> ⚠ **警告**
>
> 将 2016 年 11 月 8 日更新前启用的 DC 添加到支持滚动 NTLM 密钥的域中可能会导致 DC 崩溃。

对于新的域，此功能默认为启用。 对于现有域，必须在 Active Directory 管理中心为其进行配置。

从 Active Directory 管理中心，右键单击左窗格中的域，然后选择**属性**。 选中**对于需要使用 Windows Hello for Business 或智能卡进行交互式登录的用户，在登录期间启用滚动**

即将过期的 NTLM 密钥复选框。 之后，选择“确定”以应用此更改。

当用户受限于已加入域的特定设备时，允许网络 NTLM

在 Windows Server 2016 DFL 及更高版本中，当用户被限制使用特定的域连接设备时，DC 现在可以支持允许网络 NTLM。 运行比 Windows Server 2016 更早操作系统的 DFL 无法使用此功能。

要配置此设置，请在身份验证策略中选择**限制用户使用选定设备时，允许 NTLM 网络身份验证**。

有关详细信息，请参阅身份验证策略和身份验证策略接收器。

Device Guard（代码完整性）

Device Guard 通过创建指定哪些代码可以在服务器上运行的策略提供内核模式代码完整性 (KMCI) 和用户模式代码完整性 (UMCI)。 请参阅 Windows Defender Device Guard 简介：基于虚拟化的安全性和代码完整性策略。

Windows Defender

Windows Server 2016 的 Windows Defender 概述。 默认情况下，Windows Server Antimalware 已在 Windows Server 2016 中安装并处于启用状态，但是 Windows Server Antimalware 的用户界面尚未安装。 但是，Windows Server Antimalware 会在没有用户界面的情况下更新反恶意软件定义并保护计算机。 如果需要 Windows Server Antimalware 的用户界面，则可以使用“添加角色和功能向导”在操作系统安装之后安装它。

控制流防护

控制流防护 (CFG) 是一种平台安全功能，旨在防止内存损坏漏洞。 有关详细信息，请参阅 Control Flow Guard（控制流防护）。

存储

Windows Server 2016 中的存储包括软件定义存储以及传统文件服务器的新功能和增强功能。

Storage Spaces Direct

存储空间直通允许通过使用具有本地存储的服务器构建高可用性和可缩放存储。 该功能简化了软件定义的存储系统的部署和管理并且允许使用 SATA SSDs 和 NVMe 磁盘设备等新型磁盘设备，而之前群集存储空间无法使用共享磁盘。

有关详细信息，请参阅存储空间直通。

存储副本

存储副本可在各个服务器或群集之间实现存储不可知的块级同步复制，以便在站点间进行灾难恢复及故障转移群集扩展。 同步复制支持物理站点中的镜像数据和在崩溃时保持一致的卷，以确保文件系统级别的数据损失为零。 异步复制允许超出都市范围、可能存在数据损失的站点扩展。

有关详细信息，请参阅存储副本。

服务存储质量 (QoS)

现在可以使用存储服务质量 (QoS) 来集中监控端到端存储性能，并使用 Windows Server 2016 中的 Hyper-V 和 CSV 群集创建策略。

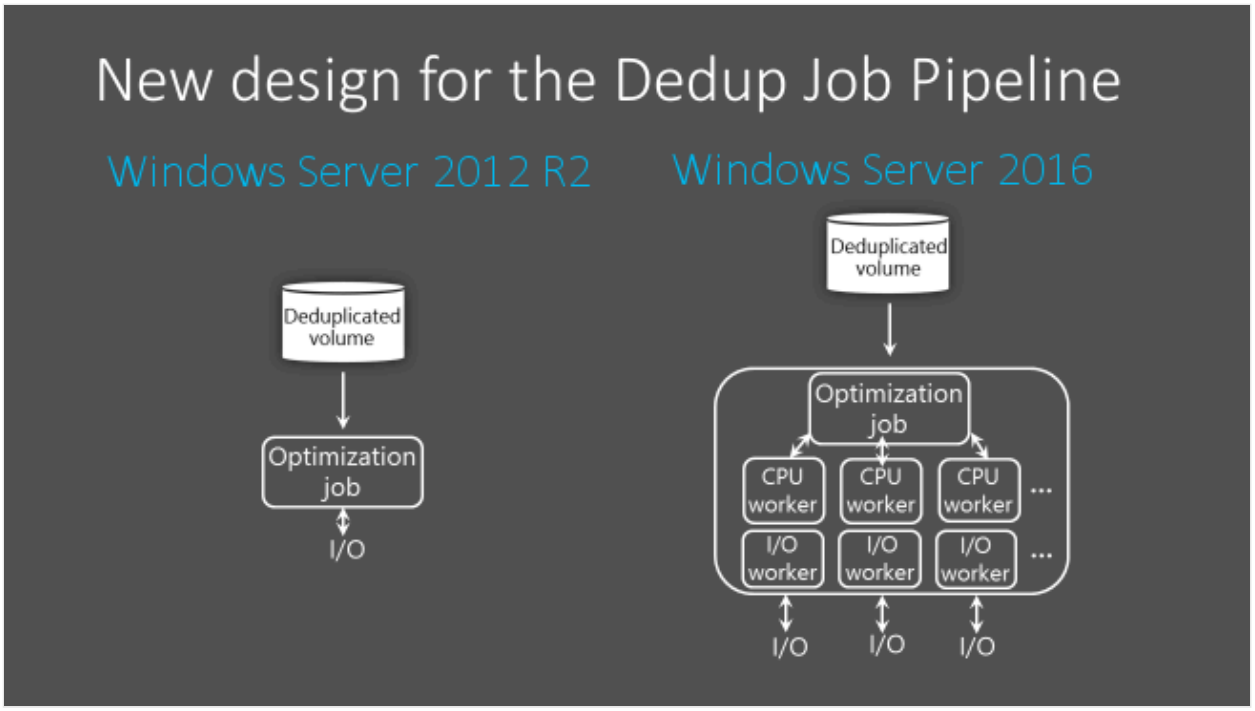
有关详参细信息，请阅服务存储质量。

重复数据删除

Windows Server 2016 包括以下用于重复数据删除的新功能。

支持大型卷

从 Windows Server 2016 开始，重复数据删除作业管道现在可以通过对每个卷使用许多 I/O 队列，并行运行多个线程。 此更改将性能提高到以前只能通过将数据划分为几个较小的卷来实现的水平。 这些优化适用于所有重复数据删除作业，而不仅仅是优化作业。 下图演示了管道在 Windows Server 版本之间的变化。



由于这些性能改进，在 Windows Server 2016 上，重复数据删除在高达 64 TB 的卷上具有高性能。

大文件支持

从 Windows Server 2016 开始，重复数据删除可以使用流映射结构和其他改进来提高优化吞吐量和访问性能。 重复数据删除处理管道还可以在故障转移方案后恢复优化，而不是从头开始。 此更改将文件的性能提高到 1 TB，使管理员能够将重复数据删除节省应用于更大范围的工作负载，例如与备份工作负载相关的大型文件。

支持 Nano Server

Nano Server 是 Windows Server 2016 中新的无外设部署选项，与 Windows Server Core 部署选项相比，需要更小的系统资源占用，启动速度更快，需要更少的更新和重启。 Nano Server 还完全支持重复数据删除。 有关 Nano Server 的详细信息，请参阅容器基础映像。

简化了虚拟化备份应用程序的配置

从 Windows Server 2016 开始，虚拟化备份应用程序的重复数据删除方案已大大简化。 此方案现在是预定义的“使用类型”选项。 不再需要手动优化重复数据删除设置，只需像启用常规用途文件服务器和虚拟桌面基础结构 (VDI) 一样为卷启用重复数据删除即可。

群集 OS 滚动升级支持

运行重复数据删除的 Windows Server 故障转移群集可以混合使用运行 Windows Server 2012 R2 和 Windows Server 2016 版本重复数据删除的节点。 此混合模式群集功能可在群集滚动升级期间对所有重复数据删除卷进行完全数据访问。 现在，可以在运行早期版本 Windows Server 的群集上逐步推出较新版本的重复数据删除，而不会出现任何停机时间。

现在，还可以在 Hyper-V 上使用滚动升级。 通过滚动 Hyper-V 群集升级，现在可以将运行 Windows Server 2019 或 Windows Server 2016 的节点添加到具有运行 Windows Server 2012 R2 的节点的 Hyper-V 群集。 添加运行更高版本的 Windows Server 的节点后，可以在不停机的情况下升级群集的其余部分。 群集在 Windows Server 2012 R2 功能级别运行，直到升级群集中的所有节点并在 PowerShell 中运行 Update-ClusterFunctionalLevel 以更新群集功能级别。 有关滚动升级过程工作原理的更详细说明，请参阅群集操作系统滚动升级。

> **备注**
>
> Windows 10 上的 Hyper-V 不支持故障转移群集。

SMB 针对 SYSVOL 和 NETLOGON 连接的强化改进

在 Windows 10 和 Windows Server 2016 中，默认情况下，与 Active Directory 域服务的客户端连接使用域控制器上的 SYSVOL 和 NETLOGON 共享。 现在，这些连接需要使用 Kerberos 等服务进行 SMB 签名和相互身份验证。 如果 SMB 签名和相互身份验证都不可用，Windows 10 或 Windows Server 2016 计算机不会处理基于域的组策略和脚本。 此更改可保护设备免受中间敌手攻击。

> **备注**
>
> 这些设置的注册表值默认情况下并不出现，但在通过编辑组策略或其他注册表值替代前，强化规则仍然适用。

有关这些安全改进的详细信息，请参阅 MS15-011：组策略中的漏洞 以及 MS15-011 和 MS15-014：强化组策略 。

工作文件夹

工作文件夹服务器在运行 Windows Server 2016 且工作文件夹客户端是 Windows 10 时，Windows Server 2016 功能改进了更改通知。 当文件更改同步到工作文件夹服务器时，服务器现在会立即通知 Windows 10 客户端，然后同步文件更改。

ReFS

ReFS 的下一次迭代为具有不同工作负载的大规模存储部署提供支持，从而为数据提供可靠性、复原能力和可伸缩性。

ReFS 引入了下列改进功能：

- 新的存储层功能，提供更快的性能和更大的存储容量，包括以下内容：
  - 同一虚拟磁盘上的多个复原类型在性能层中使用镜像，在容量层中使用奇偶校验。
  - 提高对偏移工作集的响应能力。
- 引入块克隆以提高 VM 操作的性能，例如 `.vhdx` 检查点合并操作。
- 一种新的 ReFS 扫描工具，可以帮助恢复泄露的存储并对严重损坏事件中的数据进行补救。

故障转移群集

Windows Server 2016 中包括多个服务器的新功能和增强功能，它们使用故障转移群集功能组合到单个容错群集中。

群集操作系统滚动升级

群集操作系统滚动升级允许管理员将群集节点的操作系统从 Windows Server 2012 R2 升级至 Windows Server 2016，且无需中断 Hyper-V 或横向扩展文件服务器工作负载。 使用此功能可以避免服务级别协议 (SLA) 的停机时间损失。

有关详细信息，请参阅群集操作系统滚动升级。

云见证

云见证是 Windows Server 2016 中一种新型的故障转移群集仲裁见证，它将 Microsoft Azure 作为仲裁点。 与其他仲裁见证一样，云见证获取投票，并可以参与仲裁计算。 可以使用“配置群集仲裁向导”将云见证配置为仲裁见证。

有关详细信息，请参阅部署故障转移群集的云见证。

虚拟机复原

Windows Server 2016 包括改进的虚拟机 (VM) 计算复原能力，可帮助减少计算群集中的群集内通讯问题。 这种增强的复原能力包括以下更新：

- 现在，可以配置以下选项来定义 VM 在暂时性故障期间的行为：
  - **复原级别**定义部署应如何处理暂时性故障。
  - **复原期**定义允许所有 VM 独立运行的时间长度。
- 运行状况不佳的节点将被隔离，并且不再被允许加入群集。 此功能可防止运行状况不佳的节点对其他节点和整个群集产生负面影响。

有关计算复原能力功能的详细信息，请参阅 Windows Server 2016 中的虚拟机计算复原能力。

Windows Server 2016 VM 还包括新的存储复原能力功能，用于处理暂时性存储故障。 改进的复原能力有助于在存储中断时保持租户 VM 会话状态。 当 VM 与其底层存储断开连接时，它会暂停并等待存储恢复。 暂停时，VM 会保留存储故障时在其中运行的应用程序的上下文。 当 VM 和存储之间的连接恢复时，VM 将返回到其正在运行的状态。 因此，租户计算机的会话状态在恢复时会保留。

新的存储复原能力功能也适用于来宾群集。

诊断改进

为了帮助诊断故障转移群集的问题，Windows Server 2016 包括以下改进：

- 群群日志文件的几个增强功能（如时区信息和 DiagnosticVerbose 日志）使故障转移群集问题的排除变得更加容易。 有关详细信息，请参阅 Windows Server 2016 故障转移群集故障排除增强功能 - 群集日志。
- 一种新型的活动内存转储会筛选出分配给 VM 的大多数内存页，从而使 memory.dmp 文件更小，更易于保存或复制。 有关详细信息，请参阅 Windows Server 2016 故障转移群集故障排除增强功能 - 活动转储。

站点感知故障转移群集

Windows Server 2016 包括站点感知故障转移群集，可根据其物理位置或站点在拉伸群集中启用组节点。 群集站点感知改进了群集生命周期内的重要操作，例如故障转移行为、位置策略、节点间的信号检测和仲裁行为等。 有关详细信息，请参阅 Windows Server 2016 中的站点感知故障转移群集。

工作组和多域群集

在 Windows Server 2012 R2 及之前版本中，仅可以在已加入相同域的成员节点间创建群集。 Windows Server 2016 打破了这些障碍，并引入了创建故障转移群集的功能，且无需 Active Directory 依赖项。 现在可以使用以下配置创建故障转移群集：

- 单域群集，其所有节点都已加入同一个域。
- 多域群集，其节点是不同域的成员。
- 工作组群集，其节点是未加入域的成员服务器或工作组。

有关详细信息，请参阅 Windows Server 2016 中的工作组和多域群集

虚拟机负载均衡

虚拟机负载均衡是故障转移群集中的一项新功能，可在群集中的节点之间无缝对 VM 进行负载均衡。 此功能根据节点上的 VM 内存和 CPU 利用率标识已超额提交的节点。 然后，实时将 VM 从已超额提交的节点实时迁移到具有可用带宽的节点。 可以调整功能平衡节点的力度，以确保最佳的群集性能和利用率。 默认情况下，负载均衡在 Windows Server 2016 技术预览版中处于启用状态。 但是，启用 SCVMM 动态优化时，会禁用负载均衡。

虚拟机启动顺序

虚拟机启动顺序是故障转移群集中的一项新功能，它为群集中的 VM 和其他组引入了启动顺序业务流程。 现在，可以将 VM 分组到层中，然后在不同层之间创建启动顺序依赖项。 这些依赖项可确保最重要的 VM（例如域控制器或实用工具 VM）首先启动。 低优先级层上的 VM 只有在它们依赖启动的 VM 之后才会启动。

简化的 SMB 多通道和多 NIC 群集网络

故障转移群集网络不再局限于每个子网或网络只有一个网络接口卡 (NIC)。 使用简化的服务器消息块 (SMB) 多通道和多 NIC 群集网络，网络配置是自动的，子网上的每个 NIC 都可用于群集和工作负载流量。 此增强功能使客户可以最大化 Hyper-V、SQL Server 故障转移群集实例和其他 SMB 工作负载的网络吞吐量。

有关详细信息，请参阅简化的 SMB 多通道和多 NIC 群集网络。

应用程序开发

Internet Information Services (IIS) 10.0

Windows Server 2016 中的 IIS 10.0 Web 服务器提供的新增功能包括：

- 在网络堆栈中支持 HTTP/2 协议，并与 IIS 10.0 集成，允许 IIS 10.0 网站针对支持的配置为 HTTP/2 请求自动提供服务。 与 HTTP/1.1 相比，这会有大量的增强功能，例如，更有效地重用连接和减少延迟、提高网页的加载速度。
- 在 Nano Server 中运行和管理 IIS 10.0 的功能。 请参阅 Nano Server 上的 IIS。
- 支持通配符主机头，使管理员能够为域设置 Web 服务器，然后让 Web 服务器为任何子域的请求提供服务。
- 一个用于管理 IIS 的新 PowerShell 模块 (IISAdministration)。

有关详细信息，请参阅 IIS。

分布式事务处理协调器 (MSDTC)

Microsoft Windows 10 和 Windows Server 2016 中添加了三个新功能：

- 资源管理器可以使用资源管理器重新加入的新界面，以在数据库由于错误重启后确定未决事务的结果。 有关详细信息，请参阅 IResourceManagerRejoinable::Rejoin。
- DSN 名称限制从 256 字节扩大到 3072 字节。 有关详细信息，请参阅 IDtcToXaHelperFactory::Create、IDtcToXaHelperSinglePipe::XARMCreate 或 IDtcToXaMapper::RequestNewResourceManager。
- 利用改进的跟踪功能，可以设置注册表项以在跟踪日志文件名中包括映像文件路径，以便能够告知要检查的跟踪日志文件。 有关为 MSDTC 配置跟踪的详细信息，请参阅如何在基于 Windows 的计算机上为 MS DTC 启用诊断跟踪。

DNS 服务器

Windows Server 2016 包含以下域名系统 (DNS) 服务器的更新。

DNS 策略

可以配置 DNS 策略以指定 DNS 服务器如何响应 DNS 查询。 你可以根据客户端 IP 地址、当天时间和其他几个参数配置 DNS 响应。 DNS 策略支持位置感知 DNS、流量管理、负载均衡、拆分式 DNS 和其他方案。 有关详细信息，请参阅 DNS 策略方案指南。

RRL

你可以在 DNS 服务器上启用响应速率限制 (RRL)，避免恶意系统使用 DNS 服务器对 DNS 客户端发起分布式拒绝服务 (DDoS) 攻击。 RRL 可避免 DNS 服务器同时响应过多的请求，当僵尸网络同时发送多个请求以尝试中断服务器操作时，该功能可以保护它。

DANE 支持

你可以使用基于 DNS 的命名实体身份验证 (DANE) 支持（RFC 6394 和 RFC 6698）来指定 DNS 客户端应从哪个证书颁发机构获得 DNS 服务器托管域名的证书。 这可以防止某种形式的中间人攻击，即恶意攻击者破坏 DNS 缓存并将 DNS 名称指向他们自己的 IP 地址。

未知记录支持

你可以使用未知记录功能添加 DNS 服务器未显式支持的记录。 当 DNS 服务器无法识别记录的 RDATA 格式时，该记录就是未知记录。 Windows Server 2016 支持未知记录类型 (RFC 3597)，因此你可以将未知记录以二进制在线格式添加到 Windows DNS 服务器区域。 Windows 缓存解析程序已经可以处理未知的记录类型。 Windows DNS 服务器不会对未知记录执行特定于记录的处理，但可以在收到查询时发送这些记录。

IPv6 根提示

Windows DNS 服务器现在包括 Internet 编号分配机构 (IANA) 发布的 IPv6 根提示。 通过对 IPv6 根提示的支持，你可以进行使用 IPv6 根服务器执行名称解析的 Internet 查询。

Windows PowerShell 支持

Windows Server 2016 中包含可用于用 PowerShell 配置 DNS 的新命令。 有关详细信息，请参阅 Windows Server 2016 DnsServer 模块和 Windows Server 2016 DnsClient 模块。

Nano Server 支持基于文件的 DNS

在 Windows Server 2016 中，DNS 服务器可以部署在 Nano Server 映像上。 如果使用的是基于文件的 DNS，则可以使用此部署选项。 通过在 Nano Server 映像上运行 DNS 服务器，可以在减少占用空间、快速启动和最少修补的情况下运行 DNS 服务器。

> **备注**
>
> Nano Server 不支持 Active Directory 集成 DNS。

DNS 客户端

DNS 客户端服务现在为具有多个网络接口的计算机提供增强支持。

多宿主计算机还可以使用 DNS 客户端服务绑定来改进服务器解析：

- 当使用特定接口上配置的 DNS 服务器来解析 DNS 查询时，DNS 客户端在发送查询信息前先绑定该接口。 此绑定允许 DNS 客户端指定应该进行名称解析的接口，从而优化应用程序和 DNS 客户端之间通过网络接口的通信。
- 如果使用的 DNS 服务器是由名称解析策略表 (NRPT) 中的组策略设置指定的，则 DNS 客户端服务不会绑定到指定的接口。

> **备注**
>
> 对 Windows 10 中 DNS 客户端服务的更改也会呈现在运行 Windows Server 2016 及更高版本的计算机中。

远程桌面服务

远程桌面服务 (RDS) 针对 Windows Server 2016 进行了以下更改。

应用兼容性

RDS 和 Windows Server 2016 与许多 Windows 10 应用程序兼容，可带来与物理桌面几乎完全相同的用户体验。

Azure SQL 数据库

远程桌面 (RD) 连接代理现在可以在共享的 Azure 结构化查询语言 (SQL) 数据库中存储所有部署信息，如连接状态和用户/主机映射。 此功能允许使用高可用性环境，而无需使用 SQL Server AlwaysOn 可用性组。 有关详细信息，请参阅将 Azure SQL DB 用于远程桌面连接代理高可用性环境。

图形改进

Hyper-V 的离散设备分配允许将主机上的图形处理单元 (GPU) 直接映射到虚拟机 (VM) 上。 如果 VM 上的任何应用程序所需的 GPU 超过 VM 所能提供的 GPU，则可以改为使用映射的 GPU。 我们还改进了 RemoteFX vGPU，包括对 OpenGL 4.4、OpenCL 1.1、4K 分辨率和 Windows Server VM 的支持。 有关详细信息，请参阅离散设备分配。

RD 连接代理改进

我们改进了 RD 连接代理在登录风暴（用户登录请求高发期）期间处理连接的方式。 RD 连接代理现在可以处理超过 10,000 个并发登录请求！ 维护方面的改进还允许更轻松地对

部署进行维护，一旦服务器准备好重新上线，就能快速将其添加回环境中。 有关详细信息，请参阅改进的远程桌面连接代理性能。

RDP 10 协议更改

远程桌面协议 (RDP) 10 现在使用 H.264/AVC 444 编解码器，可对视频和文本进行优化。 此版本还包括笔远程处理支持。 这些新功能让远程会话感觉更像是本地会话。 有关详细信息，请参阅 Windows 10 和 Windows Server 2016 中的 RDP 10 AVC/H.264 改进。

个人会话桌面

个人会话桌面是一项新功能，允许在云中托管自己的个人桌面。 管理权限和专用会话主机消除了托管环境的复杂性，用户可以像管理本地桌面一样管理远程桌面。 有关详细信息，请参阅个人会话桌面。

Kerberos 身份验证

Windows Server 2016 包括以下 Kerberos 身份验证更新。

KDC 支持基于公钥信任的客户端身份验证

密钥分发中心 (KDC) 现在支持公钥映射。 如果为帐户预配公钥，则 KDC 将使用该密钥显式地支持 Kerberos PKInit。 由于没有证书验证，因此 Kerberos 支持自签名证书，但不支持身份验证机制保证。

无论如何配置 UseSubjectAltName 设置，已配置为使用密钥信任的帐户都将仅使用密钥信任。

Kerberos 客户端和对 RFC 8070 PKInit Freshness Extension 的 KDC 支持

从 Windows 10 版本 1607 和 Windows Server 2016 开始，Kerberos 客户端可以使用 RFC 8070 PKInit 更新扩展进行基于公钥的登录。 默认情况下，KDC 已禁用 PKInit 更新扩展；因此，若要启用该功能，则必须在域中的所有 DC 上配置对 PKInit 更新扩展 KDC 管理模板策略的 KDC 支持。

当域位于 Windows Server 2016 域功能级别 (DFL)，策略有以下可用设置：

- 已禁用：KDC 永远不会提供 PKInit Freshness Extension，也不会在未检查新鲜度的情况下接受有效的身份验证请求。 用户不会收到新的公钥标识 SID。

- **支持**：Kerberos 根据请求支持 PKInit 更新扩展。 成功使用 PKInit Freshness Extension 进行身份验证的 Kerberos 客户端收到新的公钥标识 SID。
- 必需：成功进行身份验证需要 PKInit Freshness Extension。 不支持 PKInit 更新扩展的 Kerberos 客户端在使用公钥凭据时总是会失败。

已加入域的设备对使用公钥进行身份验证的支持

如果域连接的设备可以将其绑定的公钥注册到 Windows Server 2016 域控制器 (DC)，则设备就可以使用公钥通过 Kerberos PKInit 进行 Windows Server 2016 DC 身份验证。

与 Windows Server 2016 域控制器注册了绑定公钥的域连接的设备现在可以使用用于初始身份验证的 Kerberos 公钥加密 (PKInit) 协议来对 Windows Server 2016 域控制器进行身份验证。 若要了解详细信息，请参阅已加入域的设备公钥身份验证。

密钥分发中心 (KDC) 现在支持使用 Kerberos 密钥信任来进行身份验证。

有关详细信息，请参阅 KDC 对密钥信任帐户映射的支持。

Kerberos 客户端允许在服务主体名称 (SPN) 中使用 IPv4 和 IPv6 地址主机名

从 Windows 10 版本 1507 和 Windows Server 2016 开始，可以将 Kerberos 客户端配置为支持 SPN 中的 IPv4 和 IPv6 主机名。 有关详细信息，请参阅为 IP 地址配置 Kerberos。

若要在 SPN 中配置对 IP 地址主机名的支持，请创建一个 TryIPSPN 条目。 默认情况下，注册表中不存在此条目。 应将此条目放置在以下路径上：

```text
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters
```

创建条目后，将其 DWORD 值更改为 1。 如果未配置此值，Kerberos 将不会尝试使用 IP 地址主机名。

只有在 Active Directory 中注册了 SPN，Kerberos 身份验证才能成功。

KDC 对密钥信任帐户映射的支持

域控制器现在支持密钥信任帐户映射，并回退到 SAN 行为中的现有 AltSecID 和用户主体名称 (UPN)。 可以将 UseSubjectAltName 变量配置为以下设置：

- 将变量设置为 0 表示需要显式映射。 用户必须使用密钥信任或设置 ExplicitAltSecID 变量。
- 将变量设置为 1（默认值）允许进行隐式映射。
  - 如果在 Windows Server 2016 或更高版本中为帐户配置密钥信任，则 KDC 将使用密钥信任进行映射。
  - 如果 SAN 中没有 UPN，KDC 将尝试使用 AltSecID 进行映射。
  - 如果 SAN 中有 UPN，KDC 将尝试使用 UPN 进行映射。

Active Directory 联合身份验证服务 (AD FS)

适用于 Windows Server 2016 的 AD FS 包含以下更新。

使用 Microsoft Entra 多重身份验证登录

AD FS 2016 基于 Windows Server 2012 R2 中 AD FS 的多重身份验证 (MFA) 功能生成。 现在，可以允许只需要 Microsoft Entra 多重身份验证身份验证码而不是用户名或密码的登录。

- 将 Microsoft Entra 多重身份验证配置为主要身份验证方法时，AD FS 会从 Azure Authenticator 应用中提示用户输入用户名和一次性密码 (OTP) 代码。
- 将 Microsoft Entra 多重身份验证配置为辅助或额外身份验证方法时，用户需要提供主要身份验证凭据。 用户可以使用 Windows 集成身份验证登录，可以请求用户名和密码、智能卡或用户或设备证书。 接下来，用户会看到一个提示，要求输入他们的辅助凭据，例如文本、语音或基于 OTP 的 Microsoft Entra 多重身份验证登录。
- 新的内置 Microsoft Entra 多重身份验证适配器为使用 AD FS 的 Microsoft Entra 多重身份验证提供了更简单的设置和配置。
- 组织可以使用 Microsoft Entra 多重身份验证，而不需要本地 Microsoft Entra 多重身份验证服务器。
- 可以为 intranet、extranet 配置 Microsoft Entra 多重身份验证，或将其作为任何访问控制策略的一部分进行配置。

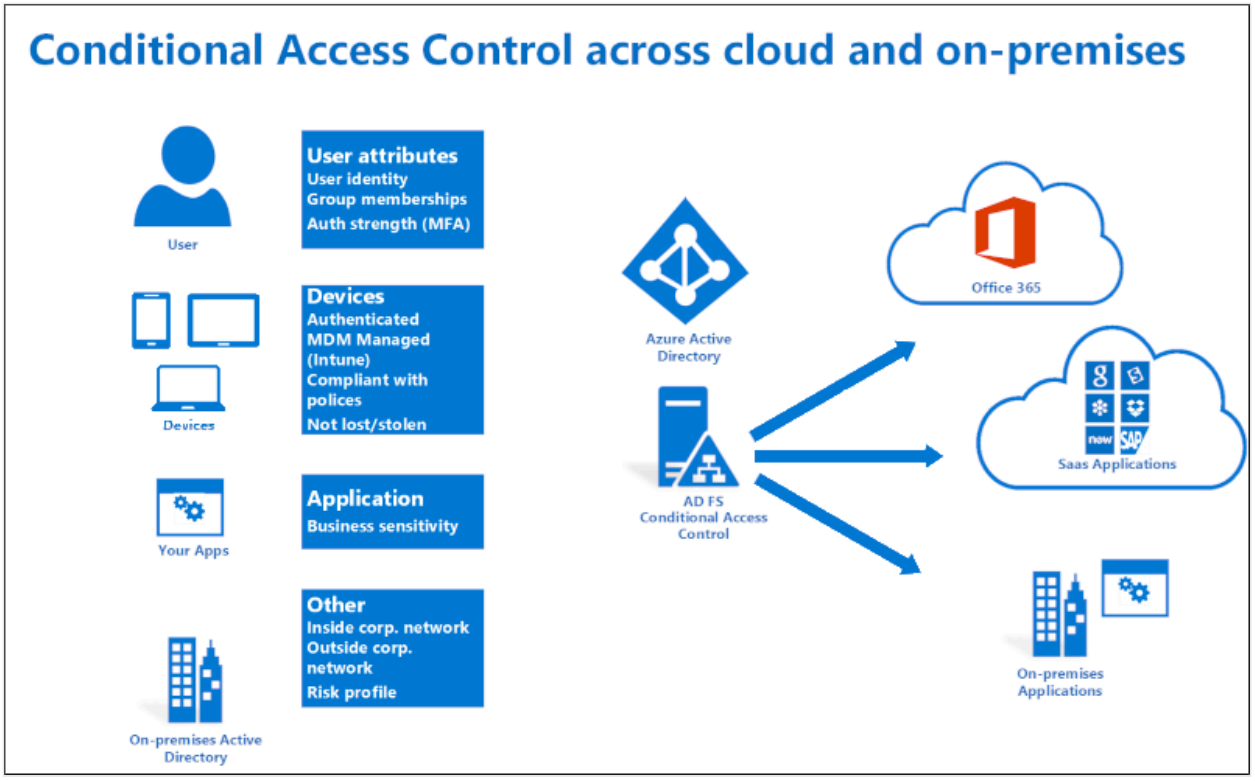
有关使用 AD FS 进行 Azure AD 多重身份验证的详细信息，请参阅配置 AD FS 2016 和 Microsoft Entra 多重身份验证。

从兼容设备进行无密码访问

AD FS 2016 基于以前的设备注册功能生成，可基于设备符合性状态在设备上启用登录和访问控制。 用户可以使用设备凭据登录，每当设备属性发生变化时，AD FS 都会重新评估符合性，这样你就可以始终确保策略得到实施。 此功能支持以下策略：

- 仅允许从托管和/或符合的设备进行访问。
- 仅允许从托管和/或符合的设备进行 Extranet 访问。
- 对于未托管或不符合的计算机，需要多重身份验证。

AD FS 在混合方案中提供条件访问策略的本地组件。 向 Azure AD 注册设备以对云资源进行条件访问时，还可以将设备标识用于 AD FS 策略。



有关在云中使用基于设备的条件访问的详细信息，请参阅 Azure Active Directory 条件访问。

有关将基于设备的条件访问与 AD FS 配合使用的详细信息，请参阅基于设备的条件访问与 AD FS 规划和 AD FS 中的访问控制策略。

通过 Windows Hello 企业版登录

Windows 10 设备引入了 Windows Hello 和 Windows Hello 企业版，将用户密码替换为受用户手势（例如，输入 PIN、指纹等生物识别手势或面部识别）保护的强设备绑定用户凭据。 使用 Windows Hello，用户可以从 Intranet 或 Extranet 登录到 AD FS 应用程序，而无需密码。

有关在组织中使用 Windows Hello 企业版的详细信息，请参阅在组织中启用 Windows Hello 企业版。

新式身份验证

AD FS 2016 支持最新的新式协议，可为 Windows 10 以及最新的 iOS 和 Android 设备和应用提供更好的用户体验。

有关详细信息，请参阅适用于开发人员的 AD FS 方案。

无需了解声明规则语言即可配置访问控制策略

以前，AD FS 管理员必须使用 AD FS 声明规则语言配置策略，这使得配置和维护策略变得困难。 借助访问控制策略，管理员可以使用内置模板来应用常见的策略。 例如，可以使用模板应用以下策略：

- 仅允许 Intranet 访问。
- 允许所有人，并要求来自 Extranet 的人员进行 MFA。
- 允许所有人，并要求来自特定组的人员进行 MFA。

模板易于自定义。 可以应用额外的例外或策略规则，并且可以将这些更改应用于一个或多个应用程序，以实现一致的策略执行。

有关详细信息，请参阅 AD FS 中的访问控制策略。

启用使用非 AD LDAP 目录进行登录

许多组织将 Active Directory 和第三方目录结合在一起。 AD FS 支持对存储在符合轻型目录访问协议 (LDAP) v3 的目录中的用户进行身份验证，这意味着现在可以在以下方案下使用 AD FS：

- 符合 LDAP v3 的第三方目录中的用户。
- 未配置 Active Directory 双向信任的 Active Directory 林中的用户。
- Active Directory 轻型目录服务 (AD LDS) 中的用户。

有关详细信息，请参阅 Configure AD FS to authenticate users stored in LDAP directories。

自定义 AD FS 应用程序的登录体验

以前，Windows Server 2012 R2 中的 AD FS 为所有信赖方应用程序提供一种通用的登录体验，并能够为每个应用程序自定义基于文本的内容的子集。 通过 Windows Server 2016，你不仅可为每个应用程序自定义消息，还可以自定义图像、徽标和 Web 主题。 此外，你还可以创建新的自定义 Web 主题，并为每个依赖方应用这些主题。

有关详细信息，请参阅 AD FS 用户登录自定义。

简化的审核，以便更轻松地进行行政管理

在以前版本的 AD FS 中，单个请求可能会生成许多审核事件。 有关登录或令牌颁发活动的相关信息往往缺失或分散在多个审核事件中，从而使问题难以诊断。 因此，默认情况下关闭了审核事件。 但是，在 AD FS 2016 中，审核流程更加精简，相关信息更容易找到。 有关详细信息，请参阅 Windows Server 2016 中 AD FS 的审核增强功能。

改进了与 SAML 2.0 的互操作性，以参与联合身份验证

AD FS 2016 包含更多 SAML 协议支持，包括支持基于包含多个实体的元数据导入信任。 此更改使你可以将 AD FS 配置为参与联合身份验证，例如 InCommon 联合身份验证和其他符合 eGov 2.0 标准的实现。

有关详细信息，请参阅 SAML 2.0 的改进互操作性。

Microsoft 365 联合身份验证用户的简化密码管理

可以将 AD FS 配置为向其保护的任何依赖方信任或应用程序发送密码过期声明。 在不同的应用程序中，这些声明的出现方式各不相同。 例如，使用 Office 365 作为你的信赖方时，会将更新实施到 Exchange 和 Outlook，以通知联合身份验证用户其密码即将过期。

有关详细信息，请参阅配置 AD FS 以发送密码过期声明。

从 Windows Server 2012 R2 中的 AD FS 迁移到 Windows Server 2016 中的 AD FS 更简单

以前，迁移到新版 AD FS 需要将配置设置从 Windows Server 场导出到新的并行服务器场。 Windows Server 2016 上的 AD FS 通过取消对并行服务器场的要求，使这一过程变得更加容易。 将 Windows Server 2016 服务器添加到 Windows Server 2012 R2 服务器场时，新服务器的行为就像 Windows Server 2012 R2 服务器一样。 准备好升级并删除旧服务器后，可以将操作级别更改为 Windows Server 2016。 有关详细信息，请参阅升级到 Windows Server 2016 中的 AD FS。

反馈

此页面是否有帮助? 是 否

Windows Server 服务频道

项目 • 2023/10/07

从 2023 年 9 月开始，Windows Server 有两个主要可用发布渠道：长期服务渠道和年度渠道。 长期服务渠道 (LTSC) 提供一个长期选项，侧重于提供传统的质量和安全更新生命周期，而年度渠道 (AC) 提供更频繁的发布。 AC 更频繁的发布使你能够更快地利用创新，重点关注容器和微服务。

长期服务频道 (LTSC)

使用长期服务渠道，通常每 2-3 年发布一次新的 Windows Server 主要版本。 用户有权享受五年的主流支持和五年的延长支持。 此渠道为系统提供了较长的维护选项和一致性，并且可以与带有桌面体验安装选项的服务器核心或服务器一起安装。

年度渠道 (AC)

用于容器的 Windows Server 年度渠道是用于托管 Windows Server 容器的操作系统。 通过年度渠道，需要快速创新的客户能够更快地使用新的操作系统功能，特别是基于容器和微服务的功能。 若要详细了解适用于容器的 Windows Server 年度渠道，请参阅我们的 TechCommunity 公告。

此渠道发布的每个版本自初始版本开始可享受 24 个月的支持服务。 此渠道只能与服务器核心安装选项一起安装。 可使用软件保障和 Visual Studio 订阅等会员计划为批量授权的客户提供年度渠道。

年度渠道发行版不是更新，而是年度渠道中的下一个 Windows Server 发行版。 若要迁移到年度渠道版本，必须执行干净安装。

年度渠道中的 Windows Server 发布通常每 12 个月进行一次。 每个发布的 24 个月支持生命周期为 18 个月的主流支持，加 6 个月的延长支持。 若要了解有关生命周期的详细信息，请参阅 Windows Server 2022 生命周期。 每个发布都基于发布周期进行命名; 例如，**版本 23H2** 是 2023 年下半年的一个发布。

主要区别

下表总结了不同频道之间的主要差异：

说明	长期服务频道	年度渠道
建议方案	通用文件服务器、Microsoft 和非 Microsoft 工作负载、传统应用、基础架构角色、软件定义数据中心和超融合基础	容器化应用程序、容器主机会受益于更快速的创新

说明	长期服务频道	年度渠道
最新发布	通常为 2-3 年	通常为 12 个月
支持	5 年的主流支持和 5 年的延长支持	18 个月的主流支持，加 6 个月的延长支持
激活	所有 Windows Server 激活密钥	Windows Server Datacenter 激活密钥
许可	所有许可计划	仅限软件保障客户
获取媒体	所有分发渠道	仅限批量许可服务中心 (VLSC) 和 Visual Studio 订阅
安装选项	Server Core 和带桌面体验的 Server	仅限容器主机的服务器核心

设备兼容性

运行年度渠道发布的最低硬件要求将与运行最新 Windows Server 长期服务渠道发布的要求相同。 大多数硬件驱动器仍可在这些发布中正常工作。

维护

在 Microsoft 生命周期页中列出的日期之前，长期服务渠道和年度渠道两种发布都将由安全更新和非安全更新进行支持。 区别在于支持发布的时间长度，如本文的年度渠道 (AC) 部分所述。

维护工具

可以使用多种工具维护 Windows Server。 每个选项都有优点和缺点，从功能和控制到简洁性和低管理要求都涵盖在内。 以下是可用于管理维护更新的维护工具示例：

- **Windows 更新（独立）** ：此选项仅适用于已连接到 Internet 并已启用 Windows 更新的服务器。
- **Windows Server Update Services (WSUS)** 可在大范围内控制 Windows Server 和 Windows 客户端更新，并且内置在 Windows Server 操作系统中。 可以延迟更新，添加审批层，并选择在准备就绪时将其部署到特定计算机或计算机组。
- **Microsoft Endpoint Configuration Manager** 可最大程度地控制维护。 可以延迟更新、批准更新，并且可以使用多种选项指向部署以及管理带宽使用情况和部署次数。

可以继续将相同的流程用于年度渠道发布：例如，如果已使用 Configuration Manager 管理更新，则可以继续使用。 同样，如果正在使用 WSUS，也可以继续使用。

在何处获取年度渠道

可以从以下位置获取年度渠道发布：

- 批量许可服务中心 (VLSC)：拥有软件保障的批量许可客户可以通过转到批量许可服务中心并选择“**登录**”来获取此版本。 最后，选择“**下载**”和“**密钥**”，搜索“年度渠道”，然后下载媒体。

- Visual Studio 订阅：Visual Studio 订阅者可以从 Visual Studio 订阅者下载页下载年度渠道发布。 如果还不是订阅者，请转到 Visual Studio 订阅进行注册，然后访问 Visual Studio 订阅者下载页。 通过 Visual Studio 订阅获得的版本仅用于开发和测试。

激活年度渠道发布

需要使用从 VLSC 获取的激活密钥激活安装。 如果使用 KMS，则年度渠道发布在发布前使用上一个 LTSC 发布的同一 CSVLK。 例如，随 Windows Server 2022 发布或之后发布的年度渠道将使用 Windows Server 2022 CSVLK。 有关详细信息，请参阅 KMS 客户端安装密钥。

如何判断服务器运行的是 LTSC 还是 AC 版本

长期服务渠道发布可以与年度渠道新版本同时发布。 若要确定服务器是否正在运行年度渠道版本，必须查看操作系统版本。 产品名称不反映服务渠道。 若要确定服务器运行的是 LTSC 还是 AC 发布，可以运行 Get-ComputerInfo PowerShell 命令。 以下示例为运行 Windows Server 2022 Datacenter Edition (LTSC) 的计算机。

若要确定操作系统版本，请运行以下命令：

PowerShell

```
Get-ComputerInfo  | fl WindowsProductName,OSDisplayVersion
```

下面是运行 Windows Server LTSC 的计算机的示例输出。

输出

```
WindowsProductName : Windows Server 2022 Datacenter
```

```
OSDisplayVersion    : 21H2
```

下面是运行适用于容器的 Windows Server 年度渠道的计算机的示例输出。

输出

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 23H2
```

提示

`OSDisplayVersion` 仅适用于 Windows Server 2022 及更高版本 年度渠道发布不适用于 Windows Server 2019 及更早版本。 如果运行的是 Windows Server 2019 或更早版本，则会运行 LTSC 版本。

下表列出了 Windows Server LTSC 和 AC 发布及其相应的操作系统版本。

频道	操作系统显示版本
LTSC	21H2
年度渠道	23H2

该指南旨在帮助识别并区分 LTSC 和 SAC，且仅用于生命周期和常规清单目的， 而不用于应用程序兼容性或用于表示特定的 API 图面。 应用开发人员应使用其它指南，以在系统生命周期内添加组件、API 和功能之前或之时确保它们的兼容性。 若要详细了解如何以编程方式确定版本，请参阅 操作系统版本。

什么是适用于 Windows Server 的 Azure Edition?

项目 • 2024/11/02 • 适用于: ✅ Windows Server 2025, ✅ Windows Server 2022

Windows Server Datacenter：Azure Edition 是以创新和虚拟化为重点的 Windows Server 版本，并优化为在 Azure 上运行。 Azure Edition 提供长期服务渠道 (LTSC) 和年度产品更新，并在前 3 年提供两个主要产品更新。 Azure Edition 还为 Windows Server 用户提供了比 Windows Server 标准和数据中心版更快的新功能。

年度 Azure Edition 更新是使用 Windows 更新交付的，而不是完整的 OS 升级。 作为本年度更新节奏的一部分，Azure Edition Insider 预览体验计划提供了访问最终正式发布的早期内部版本的机会。 要开始使用 Azure Edition 预览体验计划预览版，请访问 Azure Edition 预览版 Azure 市场套餐。 有关每个预览版的详细信息在发布到 Microsoft 技术社区的 Windows Server 预览体验成员空间的版本公告中共享。

主要差异

下表对主要差异进行了汇总：

展开表

说明	Windows Server 标准版，数据中心版	Windows Server 数据中心：Azure Edition
最新发布	通常为 2-3 年	通常为 2-3 年
产品更新	新版本	每年，前 3 年提供两个主要更新
支持	5 年的主流支持和 5 年的延长支持	5 年的主流支持和 5 年的延长支持
服务频道	长期服务频道	长期服务频道
谁可以使用?	所有频道的所有客户	仅限软件保障、Windows Server 订阅和云客户
安装选项	服务器核心、具有桌面体验的服务器、Nano Server 容器映像	服务器核心和带桌面体验的服务器。 不支持 Windows Server 容器。
操作系统环境 (OSE)	物理还是虚拟	仅限虚拟
关联的虚拟化权利	适用于数据中心的标准、无限制数据中心虚拟 OSE 的 2 个虚拟 OSE	无

功能因映像而异，要了解更多详细信息，请参阅 Windows Server Datacenter 入门：Azure Edition。

> **提示**
>
> 有关详细信息，请参阅 **Microsoft 软件许可条款**。 许可条款根据商业许可计划、零售、原始设备制造商 (OEM) 等分销渠道而异。

关键功能

热补丁

从 Windows Server 2022 Datacenter：Azure 版本开始，热补丁支持你在不重新启动的情况下在 VM 上应用安全更新。 与 Azure、Azure 来宾修补服务以及适用于 Window Server 的 Automanage 一起使用时，可自动执行热修补的载入、配置和业务流程。 要了解详细信息，请参阅适用于新虚拟机的热修补。

支持的平台

运行在 Azure 和 Azure Stack HCI 上的 VM 的以下操作系统支持热修补：

- Windows Server 2022 数据中心：Azure Edition 核心
- Windows Server 2022 数据中心：具有桌面体验的 Azure Edition

> **备注**
>
> Windows Server 容器基础映像不支持热修补。

基于 QUIC 的 SMB

从 Windows Server 2022 数据中心：Azure Edition 开始，基于 QUIC 的 SMB 为电信公司、移动设备用户和分支机构提供“SMB VPN”。 基于 QUIC 的 SMB 通过不受信任的网络（如 Internet）提供与边缘文件服务器的安全可靠连接。 QUIC 是 HTTP/3 中使用的 IETF 标准化协议，旨在通过 TLS 1.3 提供最大数据保护，并且需要无法禁用的加密。 SMB 在 QUIC 隧道中的行为正常，这意味着用户体验不会更改。 SMB 功能（如多通道、签名、压缩、持续可用性和目录租用）可正常工作。

基于 QUIC 的 SMB 还与适用于 Windows Server 的 Azure Automanage 计算机最佳做法集成，以帮助简化基于 QUIC 的 SMB 管理。 QUIC 使用证书来提供其加密，而组织经常

难以维护复杂的公钥基础结构。 Azure Automanage 计算机最佳做法可确保证书不会在没有警告的情况下过期，且基于 QUIC 的 SMB 会保持启用状态，以实现最大服务连续性。

要了解详细信息，请参阅基于 QUIC 的 SMB 和使用 Automanage 计算机最佳做法进行基于 QUIC 的 SMB 管理。

数据传输的存储副本压缩

从适用于 Windows Server 2022 数据中心：Azure Edition 的更新 1 开始，可以在源服务器和目标服务器之间压缩存储副本数据。 在传输相同数据量的情况下，压缩需要更少的网络数据包，从而实现更高的吞吐量和更低的网络利用率。 更高的数据吞吐量还可缩短同步时间，这在灾难恢复等场景中十分需要。

要了解有关存储副本功能的详细信息，请参阅存储副本功能

适用于 Azure 的扩展网络

从 Windows Server 2022 数据中心：Azure Edition 开始，使用 Azure 扩展网络，可将本地子网扩展到 Azure 中，从而支持本地虚拟机在迁移到 Azure 时保留其原始的本地专用 IP 地址。 要了解详细信息，请参阅
Azure 扩展网络。

Windows Server 数据中心：Azure Edition 入门

要开始使用 Azure Edition，请使用首选方法创建 Azure 或 Azure Stack HCI VM，然后选择要使用的 *Windows Server 数据中心：Azure Edition* 映像。

> **ⓘ 重要**
>
> 某些功能具有在 VM 创建过程中要执行的特定配置步骤，处于预览状态的某些功能则具有特定的选择加入和门户查看要求。 请参阅各个功能主题，以详细了解如何将该功能与 VM 配合使用。

> **⊗ 注意**
>
> 一旦安装了 Windows Server Datacenter: Azure Edition，就无法将操作系统切换回非 Azure Edition 操作系统。 如果出现这种情况，则需要重新安装以前的操作系统。

要详细了解如何使用 Azure 或 Azure Stack HCI 创建虚拟机，请参阅在 Azure 门户中创建 Windows 虚拟机和在 Azure Stack HCI 中部署 Windows Server Azure Edition VM。

后续步骤

- 比较 Windows Server 2022 的标准、数据中心和数据中心：Azure Edition 版本
- 适用于新虚拟机的热修补
- 为从 ISO 生成的 Azure Edition 虚拟机启用热补丁
- 基于 QUIC 的 SMB
- 使用 Azure 扩展网络将本地子网扩展到 Azure 中

反馈

此页面是否有帮助? 是 否

Windows Server 版本的比较

项目 • 2024/11/02 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

使用本文来比较 Standard、Datacenter 和 Datacenter：Azure Edition 版本的 Windows Server，了解哪种是最合适的版本。

> **提示**
>
> 如果要查找有关 Windows Server 中的锁定和限制的信息，请参阅 **Windows Server 中的锁定和限制比较**。

可用角色和功能

展开表

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
.NET Framework 3.5 功能		✓	✓	✓
.NET Framework 4.8 功能		✓	✓	✓
激活		✓	✓	✓
	自动虚拟机激活	! 2	✓	✓
	密钥管理服务 (KMS)	✓	✓	✗ 2
Active Directory 证书服务		✓	✓	✓
	证书注册策略 Web 服务	✓	✓	✓
	证书注册 Web 服务	✓	✓	✓
	证书颁发机构	✓	✓	✓

功能	子功能	标准版	Datacenter 版	Datacenter: Azure 版本
	证书颁发机构 Web 注册	✓	✓	✓
	网络设备注册服务	✓	✓	✓
	联机响应程序	✓	✓	✓
Active Directory 域服务		✓	✓	✓
Active Directory 联合身份验证服务		✓	✓	✓
Active Directory 轻型目录服务		✓	✓	✓
Active Directory 权限管理服务		✓	✓	✓
后台智能传送服务 (BITS)		✓	✓	✓
BitLocker 驱动器加密		✓	✓	✓
BitLocker 网络解锁		✓ 2	✓ 2	✓ 2
BranchCache		✓	✓	✓
NFS 客户端		✓	✓	✓
数据中心桥接		✓	✓	✓
设备运行状况证明		✓	✓	✓
DHCP 服务器		✓	✓	✓
直接播放		✓ 2	✓ 2	✓ 2
DLNA 解码器和 Web 媒体流		✓ 2	✓ 2	✓ 2
DNS 服务器		✓	✓	✓

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
增强存储		✓	✓	✓
故障转移群集		✓	✓	✓
传真服务器		✓	✓	✓
文件和存储服务		✓	✓	✓
	网络文件的 BranchCache	✓	✓	✓
	重复数据删除	✓	✓	✓
	DFS 命名空间	✓	✓	✓
	DFS 复制	✓	✓	✓
	文件服务器	✓	✓	✓
	文件服务器资源管理器	✓	✓	✓
	文件服务器 VSS 代理服务	✓	✓	✓
	iSCSI 目标服务器	✓	✓	✓
	iSCSI 目标存储提供程序(VDS 和 VSS 硬件提供程序)	✓	✓	✓
	NFS 服务器	✓	✓	✓
	SMB 1.0/CIFS 文件共享支持	✓	✓	✓
	SMB 带宽限制	✓	✓	✓
	基于 QUIC 的 SMB	✗	✗	✓
	工作文件夹	✓	✓	✓
	存储迁移服务	✓	✓	✓
	存储迁移服务代	✓	✓	✓

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
	理			
	存储空间	✓	✓	✓
	存储空间直通	✗	✓	✓
	存储副本	✓	✓	✓
组策略管理		✓	✓	✓
主机保护者 Hyper-V 支持		✗	✓	✓
主机保护者服务		✓	✓	✓
热修补		✗	✗	✓
I/O 服务质量		✓	✓	✓
IIS 可承载 Web 核心		✓	✓	✓
IP 地址管理 (IPAM) 服务器		✓	✓	✓
管理 OData IIS 扩展		✓	✓	✓
媒体基础		✓	✓	✓
消息队列		✓	✓	✓
	消息队列 DCOM 代理	✓	✓	✓
	消息队列服务	✓	✓	✓
Microsoft Defender 防病毒		✓	✓	✓
多路径 I/O		✓	✓	✓
多点连接器		✓	✓	✓
网络 ATC		✓	✓	✓
网络控制器		✗	✓	✓

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
网络负载均衡		✓	✓	✓
Network Policy and Access Services		✓ 2	✓ 2	✓ 2
网络虚拟化		✓	✓	✓
打印和文档服务		✓	✓	
	Internet 打印	✓ 2	✓ 2	✓ 2
	行式打印机后台程序 (LPD) 服务	✓ 2	✓ 2	✓ 2
	打印服务器	✓ 2	✓ 2	✓ 2
优质 Windows 音频视频体验		✓	✓	✓
RAS 连接管理器管理工具包 (CMAK)		✓	✓	✓
远程访问		✓	✓	✓
	DirectAccess 和 VPN (RAS)	✓	✓	✓
	路由	✓	✓	✓
	Web 应用程序代理	✓	✓	✓
远程协助		✓ 2	✓ 2	✓ 2
远程桌面服务		✓ 2	✓ 2	✓ 2
远程差分压缩		✓	✓	✓
Remote Server Administration Tools		✓	✓	✓
HTTP 代理上的 RPC		✓	✓	✓

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
安装和启动事件收集		✓	✓	✓
简单 TCP/IP 服务		✓ 2	✓ 2	✓ 2
SNMP 服务		✓	✓	✓
软件负载平衡器		✓	✓	✓
系统数据存档工具		✓	✓	✓
系统见解		✓	✓	✓
Telnet 客户端		✓	✓	✓
TFTP 客户端		✓ 2	✓ 2	✓ 2
虚拟化		✓	✓	✓
	容器	✓	✓	ⓧ
	Hyper-V	✓	✓	✓
	用于结构管理的 VM 防护工具	✓	✓	✓
批量激活服务		✓	✓	✓
Web 服务器 (IIS)		✓	✓	✓
	FTP 服务器	✓	✓	✓
	Web 服务器	✓	✓	✓
WebDAV 重定向程序		✓	✓	✓
Windows 生物识别框架		✓ 2	✓ 2	✓ 2
Windows 部署服务		✓	✓	✓
Windows Identity Foundation 3.5		✓ 2	✓ 2	✓ 2

功能	子功能	标准版	Datacenter 版	Datacenter：Azure 版本
Windows 内部数据库		✓	✓	✓
Windows PowerShell		✓	✓	✓
	Windows PowerShell 2.0 Engine	✓	✓	✓
	Windows PowerShell 5.1	✓	✓	✓
	Windows PowerShell Desired State Configuration 服务	✓	✓	✓
	Windows PowerShell Web 访问	✓	✓	✓
Windows Process Activation Service		✓	✓	✓
Windows Search 服务		✓ 2	✓ 2	✓ 2
Windows Server 备份		✓	✓	✓
Windows Server 迁移工具		✓	✓	✓
Windows Server Update Services		✓	✓	✓
基于 Windows 标准的存储管理		✓	✓	✓
适用于 Linux 的 Windows 子系统		✓	✓	✓
Windows TIFF IFilter		✓ 2	✓ 2	✓ 2

功能	子功能	标准版	Datacenter 版	Datacenter: Azure 版本
WinRM IIS 扩展		✓	✓	✓
WINS 服务器		✓	✓	✓
无线 LAN 服务		✓	✓	✓
WoW64 支持		✓	✓	✓
XPS 查看器		✓ 2	✓ 2	✓ 2

1. 以来宾身份，条件是托管在使用 Datacenter 版本激活的虚拟化主机上
2. 由 Azure 激活，不能配置为 KMS 主机
3. 已安装为具有桌面体验的服务器

反馈

此页面是否有帮助? 是 否

Windows Server 版本的比较

项目 • 2024/11/02 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

使用本文来比较 Standard、Datacenter 和 Datacenter：Azure Edition 版本的 Windows Server，了解哪种是最合适的版本。

> **提示**
>
> 如果要查找有关 Windows Server 中的锁定和限制的信息，请参阅 **Windows Server 中的锁定和限制比较**。

可用角色和功能

展开表

功能	子功能	标准版	Datacenter 版
.NET Framework 3.5 功能		✓	✓
.NET Framework 4.7 功能		✓	✓
激活		✓	✓
	自动虚拟机激活	! 2	✓
	密钥管理服务 (KMS)	✓	✓
Active Directory 证书服务		✓	✓
	证书注册策略 Web 服务	✓	✓
	证书注册 Web 服务	✓	✓
	证书颁发机构	✓	✓
	证书颁发机构 Web 注册	✓	✓

功能	子功能	标准版	Datacenter 版
	网络设备注册服务	✓	✓
	联机响应程序	✓	✓
Active Directory 域服务		✓	✓
Active Directory 联合身份验证服务		✓	✓
Active Directory 轻型目录服务		✓	✓
Active Directory 权限管理服务		✓	✓
后台智能传送服务 (BITS)		✓	✓
BitLocker 驱动器加密		✓	✓
BitLocker 网络解锁		✓ 2	✓ 2
BranchCache		✓	✓
NFS 客户端		✓	✓
数据中心桥接		✓	✓
设备运行状况证明		✓	✓
DHCP 服务器		✓	✓
直接播放		✓ 2	✓ 2
DLNA 解码器和 Web 媒体流		✓ 2	✓ 2
DNS 服务器		✓	✓
增强存储		✓	✓
故障转移群集		✓	✓
传真服务器		✓	✓
文件和存储服务		✓	✓

功能	子功能	标准版	Datacenter 版
	网络文件的 BranchCache	✓	✓
	重复数据删除	✓	✓
	DFS 命名空间	✓	✓
	DFS 复制	✓	✓
	文件服务器	✓	✓
	文件服务器资源管理器	✓	✓
	文件服务器 VSS 代理服务	✓	✓
	iSCSI 目标服务器	✓	✓
	iSCSI 目标存储提供程序(VDS 和 VSS 硬件提供程序)	✓	✓
	NFS 服务器	✓	✓
	SMB 1.0/CIFS 文件共享支持	✓	✓
	SMB 带宽限制	✓	✓
	工作文件夹	✓	✓
	存储迁移服务	✓	✓
	存储迁移服务代理	✓	✓
	存储空间	✓	✓
	存储空间直通	✗	✓
	存储副本	✓	✓
组策略管理		✓	✓
主机保护者 Hyper-V 支持		✗	✓
主机保护者服务		✓	✓

功能	子功能	标准版	Datacenter 版
I/O 服务质量		✓	✓
IIS 可承载 Web 核心		✓	✓
IP 地址管理 (IPAM) 服务器		✓	✓
Internet 存储名称服务器 (iSNS)		✓	✓
管理 OData IIS 扩展		✓	✓
媒体基础		✓	✓
消息队列		✓	✓
	消息队列 DCOM 代理	✓	✓
	消息队列服务	✓	✓
Microsoft Defender 防病毒		✓	✓
多路径 I/O		✓	✓
多点连接器		✓	✓
网络 ATC		✓	✓
网络控制器		ⓧ	✓
网络负载均衡		✓	✓
Network Policy and Access Services		✓ 2	✓ 2
网络虚拟化		✓	✓
打印和文档服务		✓	✓
	Internet 打印	✓ 2	✓ 2
	行式打印机后台程序 (LPD) 服务	✓ 2	✓ 2
	打印服务器	✓ 2	✓ 2
优质 Windows 音频视		✓	✓

功能	子功能	标准版	Datacenter 版
频体验			
RAS 连接管理器管理工具包 (CMAK)		✓	✓
远程访问		✓	✓
	DirectAccess 和 VPN (RAS)	✓	✓
	路由	✓	✓
	Web 应用程序代理	✓	✓
远程协助		✓ 2	✓ 2
远程桌面服务		✓ 2	✓ 2
远程差分压缩		✓	✓
Remote Server Administration Tools		✓	✓
HTTP 代理上的 RPC		✓	✓
安装和启动事件收集		✓	✓
简单 TCP/IP 服务		✓ 2	✓ 2
SNMP 服务		✓	✓
软件负载平衡器		✓	✓
系统数据存档工具		✓	✓
系统见解		✓	✓
Telnet 客户端		✓	✓
TFTP 客户端		✓ 2	✓ 2
虚拟化		✓	✓
	容器	✓	✓
	Hyper-V	✓	✓
	用于结构管理的 VM 防护工具	✓	✓

功能	子功能	标准版	Datacenter 版
批量激活服务		✓	✓
Web 服务器 (IIS)		✓	✓
	FTP 服务器	✓	✓
	Web 服务器	✓	✓
WebDAV 重定向程序		✓	✓
Windows 生物识别框架		✓ 2	✓ 2
Windows 部署服务		✓	✓
Windows Identity Foundation 3.5		✓ 2	✓ 2
Windows 内部数据库		✓	✓
Windows PowerShell		✓	✓
	Windows PowerShell 2.0 Engine	✓	✓
	Windows PowerShell 5.1	✓	✓
	Windows PowerShell Desired State Configuration 服务	✓	✓
	Windows PowerShell Web 访问	✓	✓
Windows Process Activation Service		✓	✓
Windows Search 服务		✓ 2	✓ 2
Windows Server 备份		✓	✓
Windows Server 迁移工具		✓	✓
Windows Server Update Services		✓	✓

功能	子功能	标准版	Datacenter 版
基于 Windows 标准的存储管理		✓	✓
适用于 Linux 的 Windows 子系统		✓	✓
Windows TIFF IFilter		✓ 2	✓ 2
WinRM IIS 扩展		✓	✓
WINS 服务器		✓	✓
无线 LAN 服务		✓	✓
WoW64 支持		✓	✓
XPS 查看器		✓ 2	✓ 2

1. 以来宾身份，条件是托管在使用 Datacenter 版本激活的虚拟化主机上

2. 已安装为具有桌面体验的服务器

反馈

此页面是否有帮助? 是 否

Windows Server 版本的比较

项目 • 2024/11/02 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

使用本文来比较 Standard、Datacenter 和 Datacenter：Azure Edition 版本的 Windows Server，了解哪种是最合适的版本。

> **提示**
>
> 如果要查找有关 Windows Server 中的锁定和限制的信息，请参阅 **Windows Server 中的锁定和限制比较**。

可用角色和功能

展开表

功能	子功能	标准版	Datacenter 版
.NET Framework 3.5 功能		✓	✓
.NET Framework 4.6 功能		✓	✓
激活		✓	✓
	自动虚拟机激活	! 2	✓
	密钥管理服务 (KMS)	✓	✓
Active Directory 证书服务		✓	✓
	证书注册策略 Web 服务	✓	✓
	证书注册 Web 服务	✓	✓
	证书颁发机构	✓	✓
	证书颁发机构 Web 注册	✓	✓

功能	子功能	标准版	Datacenter 版
	网络设备注册服务	✓	✓
	联机响应程序	✓	✓
Active Directory 域服务		✓	✓
Active Directory 联合身份验证服务		✓	✓
Active Directory 轻型目录服务		✓	✓
Active Directory 权限管理服务		✓	✓
后台智能传送服务 (BITS)		✓	✓
BitLocker 驱动器加密		✓	✓
BitLocker 网络解锁		✓ 2	✓ 2
BranchCache		✓	✓
NFS 客户端		✓	✓
数据中心桥接		✓	✓
设备运行状况证明		✓	✓
DHCP 服务器		✓	✓
直接播放		✓ 2	✓ 2
DLNA 解码器和 Web 媒体流		✓ 2	✓ 2
DNS 服务器		✓	✓
增强存储		✓	✓
故障转移群集		✓	✓
传真服务器		✓	✓
文件和存储服务		✓	✓

功能	子功能	标准版	Datacenter 版
	网络文件的 BranchCache	✓	✓
	重复数据删除	✓	✓
	DFS 命名空间	✓	✓
	DFS 复制	✓	✓
	文件服务器	✓	✓
	文件服务器资源管理器	✓	✓
	文件服务器 VSS 代理服务	✓	✓
	iSCSI 目标服务器	✓	✓
	iSCSI 目标存储提供程序(VDS 和 VSS 硬件提供程序)	✓	✓
	NFS 服务器	✓	✓
	SMB 1.0/CIFS 文件共享支持	✓	✓
	SMB 带宽限制	✓	✓
	工作文件夹	✓	✓
	存储空间	✓	✓
	存储空间直通	✗	✓
	存储副本	✗	✓
组策略管理		✓	✓
主机保护者 Hyper-V 支持		✗	✓
主机保护者服务		✓	✓
I/O 服务质量		✓	✓
IIS 可承载 Web 核心		✓	✓

功能	子功能	标准版	Datacenter 版
IP 地址管理 (IPAM) 服务器		✓	✓
Internet 存储名称服务器 (iSNS)		✓	✓
管理 OData IIS 扩展		✓	✓
媒体基础		✓	✓
消息队列		✓	✓
	消息队列 DCOM 代理	✓	✓
	消息队列服务	✓	✓
Microsoft Defender 防病毒		✓	✓
多路径 I/O		✓	✓
多点连接器		✓	✓
MultiPoint Services		✓	✓
网络 ATC		✓	✓
网络控制器		ⓧ	✓
网络负载均衡		✓	✓
Network Policy and Access Services		✓ 2	✓ 2
打印和文档服务		✓	✓
	Internet 打印	✓ 2	✓ 2
	行式打印机后台程序 (LPD) 服务	✓ 2	✓ 2
	打印服务器	✓ 2	✓ 2
	分布式扫描服务器	✓ 2	✓ 2
优质 Windows 音频视频体验		✓	✓

功能	子功能	标准版	Datacenter 版
RAS 连接管理器管理工具包 (CMAK)		✓	✓
远程访问		✓	✓
	DirectAccess 和 VPN (RAS)	✓	✓
	路由	✓	✓
	Web 应用程序代理	✓	✓
远程协助		✓ 2	✓ 2
远程桌面服务		✓ 2	✓ 2
远程差分压缩		✓	✓
Remote Server Administration Tools		✓	✓
HTTP 代理上的 RPC		✓	✓
安装和启动事件收集		✓	✓
简单 TCP/IP 服务		✓ 2	✓ 2
SNMP 服务		✓	✓
软件负载平衡器		✓	✓
Telnet 客户端		✓	✓
TFTP 客户端		✓ 2	✓ 2
虚拟化		✓	✓
	容器	✓	✓
	Hyper-V	✓	✓
	用于结构管理的 VM 防护工具	✓	✓
批量激活服务		✓	✓
Web 服务器 (IIS)		✓	✓

功能	子功能	标准版	Datacenter 版
	FTP 服务器	✓	✓
	Web 服务器	✓	✓
WebDAV 重定向程序		✓	✓
Windows 生物识别框架		✓ 2	✓ 2
Windows 部署服务		✓	✓
Windows Identity Foundation 3.5		✓ 2	✓ 2
Windows 内部数据库		✓	✓
Windows PowerShell		✓	✓
	Windows PowerShell 2.0 Engine	✓	✓
	Windows PowerShell 5.1	✓	✓
	Windows PowerShell Desired State Configuration 服务	✓	✓
	Windows PowerShell Web 访问	✓	✓
Windows Process Activation Service		✓	✓
Windows Server Essentials 体验		✓	✓
Windows Search 服务		✓ 2	✓ 2
Windows Server 备份		✓	✓
Windows Server 迁移工具		✓	✓
Windows Server Update Services		✓	✓
基于 Windows 标准的存储管理		✓	✓

功能	子功能	标准版	Datacenter 版
Windows TIFF IFilter		✓ 2	✓ 2
WinRM IIS 扩展		✓	✓
WINS 服务器		✓	✓
无线 LAN 服务		✓	✓
WoW64 支持		✓	✓
XPS 查看器		✓ 2	✓ 2

1. 以来宾身份，条件是托管在使用 Datacenter 版本激活的虚拟化主机上

2. 已安装为具有桌面体验的服务器

反馈

此页面是否有帮助? 是 否

Windows Server 的硬件要求

项目 • 2024/10/23

若要正确安装 Windows Server，则计算机必须满足本文所述的最低硬件要求。 如果计算机不符合这些要求，则可能无法正确安装本产品。 实际要求会因系统配置和所安装的应用程序及功能而异。

除非另有指定，否则这些最低硬件要求适用于针对 Windows Server Standard 版和 Windows Server Datacenter 版的所有安装选项（Server Core 以及附带桌面体验的 Server）。

> **ⓘ 重要**
>
> 因为可能的部署方案多种多样，所以确定推荐的硬件要求有些不切实际，只是大体适用而已。 请针对要部署的每个服务器角色查阅相关文档，以便获得特定服务器角色的资源需求的更多详细信息。 要获得最佳结果，请安排测试部署来确定特定部署方案的相应硬件要求。

组件

CPU

处理器性能不仅取决于处理器的时钟频率，还取决于处理器内核数以及处理器缓存大小。 处理器要求如下。

最低要求：

- 1.4 GHz 64 位处理器
- 与 x64 指令集兼容
- 支持 NX 和 DEP
- 支持 CMPXCHG16b、LAHF/SAHF 和 PrefetchW 指令
- 支持二级地址转换（EPT 或 NPT）
- 支持 SSE4.2（流式处理 SIMD 扩展 4.2）指令集
- 支持 POPCNT 指令

可利用 Coreinfo（Windows Sysinternals 所含工具）来验证 CPU 的功能。

其他要求

根据具体场景，还需考虑其他硬件要求：

- DVD 驱动器（如果要从 DVD 媒体安装操作系统）

仅某些功能需要以下项目：

- 基于 UEFI 2.3.1c 的系统和支持安全启动的固件
- 受信任的平台模块 (TPM)
- 支持超级 VGA (1024 x 768) 或更高分辨率的图形设备和监视器
- 键盘和 Microsoft 鼠标（或其他兼容的指点设备）
- Internet 访问（可能需要付费）

> **备注**
>
> 需要 TPM 芯片才能使用某些功能，例如 **BitLocker 驱动器加密。** 如果计算机具有 TPM，则它须满足以下要求：
>
> - 基于硬件的 TPM 必须实现的 TPM 规范的版本 2.0。
> - 实现 2.0 版的 TPM 必须具有符合以下条件之一的 EK 证书：由硬件供应商预配到 TPM 或在首次启动期间能够由设备进行检索。
> - 实现 2.0 版的 TPM 必须随附有 SHA 256 PCR 库并且对 SHA 256 实现 PCR 0 到 23。 可以将 TPM 与单个可切换 PCR 库一起寄送，后者可用于 SHA-1 和 SHA-256 度量。

反馈

从 Windows Server 2022 开始已移除或不再开发的功能

项目 • 2024/04/29

Windows Server 的每一次发布都增加了新的特性和功能；我们偶尔也会删除特性和功能，通常是因为我们增加了更好的选项。 以下是有关 Windows Server 2022 中已删除的功能的详细信息。

> **提示**
>
> - 可以通过加入 Windows 预览体验计划企业版 来提前使用 Windows Server 版本 - 这是测试功能变动的好方法。

本列表可能会更改，可能未全部包括每个受影响的特性或功能。

半年频道

我们秉承以客户为中心的原则，会逐渐将长期服务频道 (LTSC) 作为主要发布频道。 当前的半年频道 (SAC) 版本将持续到其主流支持结束日期，Windows Server 20H2 版为 2022 年 5 月 10 日，Windows Server 2004 版为 2021 年 12 月 14 日

需要注意的是，之前在半年频道中发布的容器和微服务创新现在将继续随 Azure Kubernetes 服务 (AKS)、Azure Stack HCI 上的 AKS 以及与 Kubernetes 社区合作进行的其他平台改进一起发布。 通过长期服务频道，Windows Server 的主要新版本将每 2-3 年发布一次，容器主机和容器映像有望保持这一节奏。

已在此版本中移除的功能

我们即将从 Windows Server 2022 安装的产品映像中移除以下功能。 除非你使用了替代方法，否则依赖于这些功能的应用程序或代码都将无法工作。

展开表

功能	说明
Internet 存储名称服务 (iSNS) 服务器服务	考虑在 Windows Server 版本 1709 中移除 iSNS 服务器服务后，现在已将其从 Windows Server 2022 中移除。 你仍可以连接到 iSNS 服务器或单独添加 iSCSI 目标。

不再开发的功能

我们不再积极开发这些功能，并有可能在未来更新中将其删除。 部分功能已被替换为其他特性或功能，另外一些现在从其他提供源提供。

展开表

功能	说明
TLS 1.0 和 1.1	在过去的几年里，由于各种安全问题，Internet 标准和监管机构弃用或禁止了 TLS 版本 1.0 和 1.1。 在 Windows Server 的未来版本中，默认情况下将禁用 TLS 1.0 和 1.1。 有关详细信息，请参阅 TLS 版本 1.0 和 1.1 禁用资源。
Windows Internet 名称服务 (WINS)	WINS 是旧计算机名称注册和解析服务。 应将 WINS 替换为域名系统 (DNS)。 有关详细信息，请参阅 Windows Internet 名称服务 (WINS)。
受保护的结构和受防护的虚拟机 (VM)	Windows Server 和 Azure Stack HCI 与 Azure 保持一致，以利用对 Azure 机密计算和 Azure 安全中心的持续增强。 通过这种一致性，可以将更多云安全产品/服务扩展到客户数据中心（本地）。 Microsoft 将继续为这些功能提供支持，但不再有进一步的开发。 在 Windows 的客户端版本上，远程服务器管理工具 (RSAT)：将删除受防护的 VM 工具功能。
通过运行 `sconfig.cmd` 从命令提示符 (CMD) 窗口启动 SConfig	从 Windows Server 2022 开始，SConfig 会在你登录运行服务器核心安装选项的服务器时默认启动。 此外，PowerShell 现在是服务器核心上的默认 shell。 如果退出 SConfig，将转到常规的交互式 PowerShell 窗口。 同样，可以选择退出 SConfig autolaunch。 这种情况下，你将在登录时看到一个 PowerShell 窗口。 在任一情况下，通过运行 `SConfig` 即可从 PowerShell 启动 SConfig。 如果需要，也可以从 PowerShell 启动旧版命令提示符 (CMD)。 但为了简化不同的转换选项，我们将从操作系统的下一个版本中删除 `sconfig.cmd`。 如果需要从 CMD 窗口启动 SConfig，则首先必须启动 PowerShell。
Windows 部署服务 (WDS) boot.wim 映像部署	WDS 的操作系统部署功能将逐渐弃用。 依赖于 Windows Server 2022 安装媒体中的 boot.wim 的工作流将显示一条非阻止性弃用通知，但工作流不会受到其他影响。 Windows 11 工作流以及依赖于安装媒体中的 boot.wim 的未来版 Windows Server 的工作流将被阻止。 Microsoft Endpoint Configuration Manager 或 Microsoft Deployment Toolkit (MDT) 等可替代 WDS，能够为部署 Windows 映像带来更好、更灵活、功能更丰富的体验。 我们建议改用上述任一解决方案。 WDS PXE 启动不受影响。 你仍可以使用 WDS 来对设备进行 PXE 启动，以自定义启动映像。 此外，你仍可以从网络共享运行安装程序。 使用自定义 boot.wim 映像的工作流（例如 Configuration Manager 或 MDT）也不会受到此更改的影响。

功能	说明
LSARPC 接口	用于通过网络访问 EFS 加密文件的命名管道 \PIPE\lsarpc 将被禁用，并最终从将来的 Windows 版本中删除。 仍可使用命名管道 \PIPE\efsrpc 访问加密文件。
LBFO 上的 Hyper-V vSwitch	在将来的版本中，Hyper-v vSwitch 将不再有绑定到 LBFO 团队的能力。 而是必须通过交换机嵌入式组合 (SET) 进行绑定。 此更改仅适用于 Hyper-V vSwitch；其他非 Hyper-V 场景仍完全支持 LBFO。
基于 XDDM 的远程显示驱动程序	从此版本开始，远程桌面服务将为单个会话远程桌面使用基于 Windows 显示驱动程序模型 (WDDM) 的间接显示驱动程序 (IDD)。 在将来的版本中，会删除对基于 Windows 2000 显示驱动程序模型 (XDDM) 的远程显示驱动程序的支持。 使用基于 XDDM 的远程显示驱动程序的独立软件供应商应该计划迁移到 WDDM 驱动程序模型。 有关实现远程显示间接显示驱动程序的详细信息，请参阅 IddCx 版本 1.4 及更高版本的更新。
UCS 日志收集工具	UCS 日志收集工具尽管并不是专门在 Windows Server 上使用，但它即将由 Windows 10 中的反馈中心取代。

从 Windows Server 2019 开始移除或不再开发的功能

项目 • 2023/08/30

Windows Server 的每一次发布都增加了新的特性和功能；我们偶尔也会删除特性和功能，通常是因为我们增加了更好的选项。 以下是有关 Windows Server 2019 中已删除的功能的详细信息。

> **提示**
>
> - 可以通过加入 **Windows 预览体验计划** 来提前使用 Windows Server 版本 - 这是测试功能变动的好方法。

本列表可能会更改，可能未全部包括每个受影响的特性或功能。

已在此版本中移除的功能

我们即将从 Windows Server 2019 安装的产品映像中删除以下功能。 除非你使用了替代方法，否则依赖于这些功能的应用程序或代码都将无法工作。

功能	说明
业务扫描，也称为“分布式扫描管理 (DSM)”	我们即将删除此安全扫描和扫描程序管理功能 - 没有任何设备支持此功能。
打印组件 - 现在为 Server Core 安装提供可选的组件	在以前 Windows Server 版本中，打印组件默认已在 Server Core 安装选项中禁用。 我们已在 Windows Server 2016 中更改此设置，默认会启用打印组件。 在 Windows Server 2019 中，Server Core 安装再一次默认禁用这些打印组件。 如果需要启用打印组件，可以通过运行 `Install-WindowsFeature Print-Server` cmdlet 来执行此操作。
Server Core 安装中的远程桌面连接代理和远程桌面虚拟化主机	大多数远程桌面服务部署通过远程桌面会话主机 (RDSH) 归置这些角色，这需要具有桌面体验的服务器。 为了和 RDSH 保持一致，我们也会将这些角色更改为也需要具有桌面体验的服务器。 不再提供可在 Server Core 安装中使用的这些 RDS 角色。 如果你需要作为远程桌面基础结构的一部分部署这些角色，可以在 Windows Server 桌面体验上进行安装。 这些角色还包含在 Windows Server 2019 的桌面体验安装选项中。
RemoteFX 3D 显示适配器 (vGPU)	我们正在开发用于虚拟化环境的新图形加速选项。 还可以使用离散设备分配 (DDA) 作为备选。

功能	说明
Nano Server 安装选项	Nano Server 不可用作可安装的主机操作系统。 相反，Nano Server 可用作容器操作系统。 若要详细了解作为容器的 Nano Server，请参阅 Windows 容器基础映像。
服务器消息块 (SMB) 版本 1	从此版本开始，默认不再安装服务器消息块 (SMB) 版本 1。 有关详细信息，请参阅在 Windows 10 版本 1709、Windows Server 版本 1709 及更高版本中默认不会安装 SMBv1
文件复制服务	Windows Server 2003 R2 中引入的文件复制服务已替换为 DFS 复制。 需要将将 FRS 用于 sysvol 文件夹的任何域控制器迁移到 DFS 复制。
Hyper-V 网络虚拟化 (HNV)	网络虚拟化现在包含在 Windows Server 中，作为软件定义网络 (SDN) 解决方案的一部分。 SDN 解决方案还包括网络控制器、软件负载均衡、用户定义的路由和访问控制列表。

不再开发的功能

我们不再积极开发这些功能，并有可能在未来更新中将其删除。 部分功能已被替换为其他特性或功能，另外一些现在从其他提供源提供。

功能	说明
Hyper-V 中的密钥存储驱动器	我们不再开发 Hyper-V 中的密钥存储驱动器功能。 如果你使用的是第 1 代虚拟机 (VM)，请查看第 1 代 VM 虚拟化安全性来了解今后的选项。 如果你正在创建新的 VM，请结合 TPM 设备使用第 2 代虚拟机，以实现更安全的解决方案。
受信任的平台模块 (TPM) 管理控制台	以前在 TPM 管理控制台中提供的信息现在会在 Windows Defender 安全中心的**设备安全性**页中提供。
主机防护服务 Active Directory 证明模式	我们不再开发主机保护者服务 Active Directory 证明模式 - 而是添加了一种新的证明模式主机密钥证明。 与基于 Active Directory 的证明相比，主机密钥证明更简单，且兼容性相当。 与 Active Directory 证明相比，此新模式为安装体验提供等效的功能、更简单的管理和更少的基础结构依赖关系。 主机密钥证明的硬件要求不比 Active Directory 证明更高，因此，所有现有系统可与新模式保持兼容。 如需详细了解证明选项，请参阅部署受保护的主机。
OneSync 服务	OneSync 服务可以同步邮件、日历和人员应用的数据。 我们已在 Outlook 应用中添加了一个同步引擎用于提供相同的同步。
远程差异压缩 API 支持	借助远程差异压缩 API 支持，可以使用压缩技术来实现与远程源同步数据，最大程度地减少通过网络发送的数据量。
WFP 轻型筛选交换机扩展	WFP 轻型筛选交换机扩展可让开发人员构建 Hyper-V 虚拟交换机的简单网络数据包筛选扩展。 可以通过创建完整的筛选扩展来实现相同的功能。 因此，我们将来会删除此扩展。

功能	说明
IIS 6 管理兼容性	我们正在考虑替换的特定功能如下： • IIS 6 元数据库兼容性（Web 元数据库） • IIS 6 管理控制台（Web 旧管理控制台） • IIS 6 脚本工具（Web 旧脚本） • IIS 6 WMI 兼容性 (Web-WMI) IIS 6 元数据库兼容性充当基于 IIS 6 的元数据库脚本和基于文件的由 IIS 7 或更新版本使用的配置之间的模拟层。 应使用 Microsoft.Web.Administration 命名空间等工具，开始将管理脚本直接迁移到基于 IIS 文件的目标配置。 你还应该从 IIS 6.0 或更早版本中启动迁移，并移到最新版本的 IIS，此最新版本始终可在最新版本的 Windows Server 中获得。
IIS 摘要式身份验证	已计划替换此身份验证方法。 你应该开始使用其他身份验证方法，如客户端证书映射（请参阅配置一对一客户端证书映射）或 Windows 身份验证（请参阅应用程序设置）。
Internet 存储名称服务 (iSNS)	服务器消息块 (SMB) 特性提供与其他特性基本相同的功能。 有关此特性的背景信息，请参阅服务器消息块概述。
适用于 IIS 的 RSA/AES 加密	我们正在考虑替换此加密方法，因为现已推出优异的加密 API：下一代 (CNG) 方法。 若要了解有关 CNG 加密的详细信息，请参阅关于 CNG。
Windows PowerShell 2.0	此早期版本的 Windows PowerShell 已被一些较新的版本所取代。 为了获得最佳功能和性能，请迁移到 Windows PowerShell 5.0 或更高版本。 请参阅 PowerShell 文档以获取大量信息。
IPv4/6 转换技术（6to4、ISATAP 和直接隧道）	自 Windows 10 版本 1607（周年更新）起，6to4 已默认禁用，自 Windows 10 版本 1703（创建者更新）起，ISATAP 已默认禁用，直接隧道一直被默认禁用。 改用本机 IPv6 支持。
MultiPoint Services	我们不再作为 Windows Server 的一部分开发 MultiPoint 服务角色。 MultiPoint Connector 服务通过按需功能为 Windows Server 和 Windows 10 提供。 可以使用远程桌面服务（尤其是远程桌面服务会话主机）提供 RDP 连接。
脱机符号程序包（调试符号 MSI）	我们不再以可下载的 MSI 形式提供符号程序包。 Microsoft 符号服务器正在转变为一个基于 Azure 的符号存储区。 如果需要 Windows 符号，请连接到 Microsoft 符号服务器在本地缓存符号，或在有 Internet 连接的计算机上通过 SymChk.exe 使用清单文件。
组策略中的软件限制策略	可以使用 AppLocker 或 Windows Defender 应用程序控制，而不是通过组策略使用软件限制策略。 可以使用 AppLocker 和 Windows Defender 应用程序控制来管理用户可以访问哪些应用以及哪些代码可在内核中运行。
使用 SAS 结构的共享配置的存储空间	改为部署存储空间直通。 存储空间直通支持使用 HLK 认证的 SAS 机箱，但是在非共享配置中，如存储空间直通的硬件要求中所述。

功能	说明
Windows Server Essentials 体验	我们不再为 Windows Server Standard 或 Windows Server Datacenter SKU 开发 Essentials 体验角色。 如果需要面向中小型企业的易于使用的服务器解决方案，请查看我们的新 Microsoft 365 商业版 解决方案，或使用 Windows Server 2016 Essentials。

Windows Server 2016 中已删除或弃用的功能

项目 • 2023/08/30

Windows Server 的每一次发布都增加了新的特性和功能；我们偶尔也会删除特性和功能，通常是因为我们增加了更好的选项。 以下是有关 Windows Server 2016 中已删除的功能的详细信息。

> **提示**
>
> - 可以通过加入 **Windows 预览体验计划企业版** 来提前使用 Windows Server 版本 - 这是测试功能变动的好方法。

本列表可能会更改，可能未全部包括每个受影响的特性或功能。

已在此版本中移除的功能

我们即将从 Windows Server 2016 安装的产品映像中移除以下功能。 除非你使用了替代方法，否则依赖于这些功能的应用程序或代码都将无法工作。

> **备注**
>
> 如果你要从低于 Windows Server 2012 R2 或 Windows Server 2012 的服务器版本迁移到 Windows Server 2016，则还应查看 **Windows Server 2012 R2 中删除或弃用的功能**和 **Windows Server 2012 中删除或弃用的功能**。

功能	说明
Microsoft 管理控制台的“共享和存储管理”管理单元	如果想要管理的计算机正在运行的操作系统早于 Windows Server 2016，则使用远程桌面与其连接，并使用“共享和存储管理”管理单元的本地版本。 在运行 Windows 8.1 或更早版本的计算机上，使用 RSAT 中的“共享和存储管理”管理单元查看想要管理的计算机。 在客户端计算机上使用 Hyper-V 运行正在运行具有 RSAT 中的“共享和存储管理”管理单元的 Windows 7、Windows 8 或 Windows 8.1 的虚拟机。
Journal.dll	文件 `Journal.dll` 已从 Windows Server 2016 中删除。 没有替换。
安全配置向导	安全配置向导已删除。 现在默认对功能提供保护。 如果需要控制特定的安全设置，可以使用组策略或 Microsoft Security Compliance Manager。

功能	说明
SQM	管理参与客户体验改进计划的选择加入组件已被删除。

Windows 更新	wuauclt.exe /detectnow 命令已删除，并且不再受支持。 若要触发更新扫描，请运行以下 PowerShell 命令：
	
	`$AutoUpdates = New-Object -ComObject "Microsoft.Update.AutoUpdate"`
	`$AutoUpdates.DetectNow()`

不再开发的功能

我们不再积极开发这些功能，并有可能在未来更新中将其删除。 部分功能已被替换为其他特性或功能，另外一些现在从其他提供源提供。

功能	说明
配置工具	`scregedit.exe` 已弃用。 如果有依赖于 scregedit.exe 的脚本，请调整这些脚本以使用 reg.exe 或 PowerShell 方法。
Sconfig.exe	请改用 Sconfig.cmd。
NetCfg 自定义 API	NetCfg 自定义 API 的 PrintProvider、NetClient 和 ISDN 安装已弃用。
远程管理	WinRM.vbs 已弃用。 使用 PowerShell 的 WinRM 提供程序中的功能代替。
SMB 2+ over NetBT	SMB 2+ over NetBT 已弃用。 相反，实现 SMB over TCP 或 RDMA。

Windows Server 版本信息

项目 • 2024/01/29

从 2023 年 9 月开始，Windows Server 有两个主要可用发布渠道：长期服务渠道 (LTSC) 和年度渠道 (AC)。 长期服务频道提供长期选项，强调稳定性；而年度频道发布更频繁。 Windows Server 半年频道 (SAC) 已于 2022 年 8 月 9 日停用。

使用长期服务渠道，通常每 2-3 年发布一次新的 Windows Server 主要版本。 AC 更频繁的发布使客户能够更快地利用创新，重点是容器和微服务。 有关详细比较，请参阅 Windows Server 服务渠道。

Azure Stack HCI、Windows 容器和Azure Stack HCI 上的 AKS 继续关注虚拟化、容器和微服务创新。

Windows Server 主要版本（按服务选项）

（所有日期均以 ISO 8601 格式列出：YYYY-MM-DD）

展开表

Windows Server 版本	服务选项	版本	可用性日期	最新版本	主要支持结束日期	外延支持结束日期
Windows Server 2022	长期服务频道 (LTSC)	Datacenter、Standard	2021-08-18	20348.2227	2026-10-13	2031-10-14
Windows Server 2019（版本 1809）	长期服务频道 (LTSC)	Datacenter、Standard	2018-11-13	17763.5329	服务终止	2029-01-09
Windows Server 2016（版本 1607）	Long-Term Servicing Branch (LTSB)	Datacenter、Essentials、Standard	2016-08-02	14393.6614	服务终止	2027-01-12

> **备注**
>
> Windows Server 受**固定生命周期策略**管理。 请参阅 Windows **生命周期常见问题解答**和**服务渠道的比较**，详细了解服务要求和其他重要信息。 要详细了解 Windows Server 的生命周期策略，请参阅 Windows Server **版本**。

Windows Server 版本历史记录

下表显示了为 Windows Server 2022 发布的所有每月安全和非安全预览版更新的历史记录。 要查看发行说明并详细了解 Windows Server 2022 更新的内容，请查看 Windows Server 2022 更新历史记录 。

有关 Windows Server 2016 和 Windows Server 2019 版本信息，请参阅 Windows 10 - 版本信息。 这些版本的发行说明可在 Windows Server 2016 更新历史记录 和 Server 2019 更新历史记录 中找到。

Windows Server 2022 （OS 内部版本 20348）

展开表

服务选项	可用性日期	操作系统内部版本	知识库文章
LTSC	2024-01-09	20348.2227	KB5034129
LTSC	2023-12-12	20348.2159	KB5033118
LTSC	2023-11-14	20348.2113	KB5032198
LTSC	2023-10-10	20348.2031	KB5031364
LTSC	2023-09-12	20348.1970	KB5030216
LTSC	2023-08-08	20348.1906	KB5029250
LTSC	2023-07-11	20348.1850	KB5028171
LTSC	2023-06-13	20348.1787	KB5027225
LTSC	2023-05-09	20348.1726	KB5026370
LTSC	2023-04-11	20348.1668	KB5025230
LTSC	2023-03-14	20348.1607	KB5023705
LTSC	2023-02-14	20348.1547	KB5022842
LTSC	2023-01-10	20348.1487	KB5022291
LTSC	2022-12-20	20348.1368	KB5022553
LTSC	2022-12-13	20348.1366	KB5021249
LTSC	2022-11-22	20348.1311	KB5020032
LTSC	2022-11-17	20348.1251	KB5021656

LTSC	2022-11-08	20348.1249	KB5019081
LTSC	2022-10-25	20348.1194	KB5018485
LTSC	2022-10-17	20348.1131	KB5020436
LTSC	2022-10-11	20348.1129	KB5018421
LTSC	2022-09-20	20348.1070	KB5017381
LTSC	2022-09-13	20348.1006	KB5017316
LTSC	2022-08-16	20348.946	KB5016693
LTSC	2022-08-09	20348.887	KB5016627
LTSC	2022-07-19	20348.859	KB5015879
LTSC	2022-07-12	20348.825	KB5015827
LTSC	2022-06-23	20348.803	KB5014665
LTSC	2022-06-14	20348.768	KB5014678
LTSC	2022-05-24	20348.740	KB5014021
LTSC	2022-05-19	20348.709	KB5015013
LTSC	2022-05-10	20348.707	KB5013944
LTSC	2022 年 4 月 25 日	20348.681	KB5012637
LTSC	2022-04-12	20348.643	KB5012604
LTSC	2022-03-22	20348.617	KB5011558
LTSC	2022-03-08	20348.587	KB5011497
LTSC	2022-02-15	20348.558	KB5010421
LTSC	2022-02-08	20348.524	KB5010354
LTSC	2022-01-25	20348.502	KB5009608
LTSC	2022-01-17	20348.473	KB5010796
LTSC	2022-01-11	20348.469	KB5009555
LTSC	2022-01-05	20348.407	KB5010197
LTSC	2021-12-14	20348.405	KB5008223
LTSC	2021-11-22	20348.380	KB5007254

LTSC	2021-11-09	20348.350	KB5007205
LTSC	2021-10-26	20348.320	KB5006745
LTSC	2021-10-12	20348.288	KB5006699
LTSC	2021-09-27	20348.261	KB5005619
LTSC	2021-09-14	20348.230	KB5005575
LTSC	2021-08-26	20348.202	KB5005104

▼ Windows Server 2019（OS 内部版本 17763）

展开表

服务选项	可用性日期	操作系统内部版本	知识库文章
LTSC	2024-01-09	17763.5329	KB5034127
LTSC	2023-12-12	17763.5206	KB5033371
LTSC	2023-11-14	17763.5122	KB5032196
LTSC	2023-10-10	17763.4974	KB5031361
LTSC	2023-09-12	17763.4851	KB5030214
LTSC	2023-08-08	17763.4737	KB5029247
LTSC	2023-07-11	17763.4645	KB5028168
LTSC	2023-06-13	17763.4499	KB5027222
LTSC	2023-05-09	17763.4377	KB5026362
LTSC	2023-04-11	17763.4252	KB5025229
LTSC	2023-03-14	17763.4131	KB5023702
LTSC	2023-02-14	17763.4010	KB5022840
LTSC	2023-01-10	17763.3887	KB5022286
LTSC	2022-12-20	17763.3772	KB5022554
LTSC	2022-12-13	17763.3770	KB5021237
LTSC	2022-11-17	17763.3653	KB5021655
LTSC	2022-11-08	17763.3650	KB5019966

LTSC	2022-10-17	17763.3534	KB5020438
LTSC	2022-10-11	17763.3532	KB5018419
LTSC	2022-09-20	17763.3469	KB5017379
LTSC	2022-09-13	17763.3406	KB5017315
LTSC	2022-08-23	17763.3346	KB5016690
LTSC	2022-08-09	17763.3287	KB5016623
LTSC	2022-07-21	17763.3232	KB5015880
LTSC	2022-07-12	17763.3165	KB5015811
LTSC	2022-06-23	17763.3113	KB5014669
LTSC	2022-06-14	17763.3046	KB5014692
LTSC	2022-05-24	17763.2989	KB5014022
LTSC	2022-05-19	17763.2931	KB5015018
LTSC	2022-05-10	17763.2928	KB5013941
LTSC	2022-04-21	17763.2867	KB5012636
LTSC	2022-04-12	17763.2803	KB5012647
LTSC	2022-03-22	17763.2746	KB5011551
LTSC	2022-03-08	17763.2686	KB5011503
LTSC	2022-02-15	17763.2628	KB5010427
LTSC	2022-02-08	17763.2565	KB5010351
LTSC	2022-01-25	17763.2510	KB5009616
LTSC	2022-01-18	17763.2458	KB5010791
LTSC	2022-01-11	17763.2452	KB5009557
LTSC	2022-01-04	17763.2369	KB5010196
LTSC	2021-12-14	17763.2366	KB5008218
LTSC	2021-11-22	17763.2330	KB5007266
LTSC	2021-11-14	17763.2305	KB5008602
LTSC	2021-11-09	17763.2300	KB5007206

LTSC	2021-10-19	17763.2268	KB5006744
LTSC	2021-10-12	17763.2237	KB5006672
LTSC	2021-09-21	17763.2213	KB5005625
LTSC	2021-09-14	17763.2183	KB5005568
LTSC	2021-08-26	17763.2145	KB5005102
LTSC	2021-08-10	17763.2114	KB5005030
LTSC	2021-07-27	17763.2091	KB5005394
LTSC	2021-07-20	17763.2090	KB5004308
LTSC	2021-07-13	17763.2061	KB5004244
LTSC	2021-07-06	17763.2029	KB5004947
LTSC	2021-06-15	17763.2028	KB5003703
LTSC	2021-06-08	17763.1999	KB5003646
LTSC	2021-05-20	17763.1971	KB5003217
LTSC	2021-05-11	17763.1935	KB5003171
LTSC	2021-04-22	17763.1911	KB5001384
LTSC	2021-04-13	17763.1879	KB5001342
LTSC	2021-03-25	17763.1852	KB5000854
LTSC	2021-03-18	17763.1823	KB5001638
LTSC	2021-03-15	17763.1821	KB5001568
LTSC	2021 年 3 月 9 日	17763.1817	KB5000822
LTSC	2021-02-16	17763.1790	KB4601383
LTSC	2021-02-09	17763.1757	KB4601345
LTSC	2021-01-21	17763.1728	KB4598296
LTSC	2021-01-12	17763.1697	KB4598230
LTSC	2020-12-08	17763.1637	KB4592440
LTSC	2020 年 11 月 19 日	17763.1613	KB4586839
LTSC	2020 年 11 月 17 日	17763.1579	KB4594442

LTSC	2020 年 11 月 10 日	17763.1577	KB4586793
LTSC	2020-10-20	17763.1554	KB4580390
LTSC	2020-10-13	17763.1518	KB4577668
LTSC	2020-09-16	17763.1490	KB4577069
LTSC	2020-09-08	17763.1457	KB4570333
LTSC	2020-08-20	17763.1432	KB4571748
LTSC	2020 年 8 月 11 日	17763.1397	KB4565349
LTSC	2020-07-21	17763.1369	KB4559003
LTSC	2020-07-14	17763.1339	KB4558998
LTSC	2020-06-16	17763.1294	KB4567513
LTSC	2020-06-09	17763.1282	KB4561608
LTSC	2020-05-12	17763.1217	KB4551853
LTSC	2020-04-21	17763.1192	KB4550969
LTSC	2020-04-14	17763.1158	KB4549949
LTSC	2020-03-30	17763.1132	KB4554354
LTSC	2020-03-17	17763.1131	KB4541331
LTSC	2020-03-10	17763.1098	KB4538461
LTSC	2020-02-25	17763.1075	KB4537818
LTSC	2020-02-11	17763.1039	KB4532691
LTSC	2020-01-23	17763.1012	KB4534321
LTSC	2020-01-14	17763.973	KB4534273
LTSC	2019-12-10	17763.914	KB4530715
LTSC	2019-11-12	17763.864	KB4523205
LTSC	2019-10-15	17763.832	KB4520062
LTSC	2019-10-08	17763.805	KB4519338
LTSC	2019-10-03	17763.775	KB4524148
LTSC	2019-09-24	17763.774	KB4516077

LTSC	2019-09-23	17763.740	KB4522015
LTSC	2019-09-10	17763.737	KB4512578
LTSC	2019-08-17	17763.720	KB4512534
LTSC	2019-08-13	17763.678	KB4511553
LTSC	2019-07-22	17763.652	KB4505658
LTSC	2019-07-09	17763.615	KB4507469
LTSC	2019-06-26	17763.593	KB4509479
LTSC	2019-06-18	17763.592	KB4501371
LTSC	2019-06-11	17763.557	KB4503327
LTSC	2019-05-21	17763.529	KB4497934
LTSC	2019-05-19	17763.504	KB4505056
LTSC	2019-05-14	17763.503	KB4494441
LTSC	2019-05-03	17763.475	KB4495667
LTSC	2019-05-01	17763.439	KB4501835
LTSC	2019-04-09	17763.437	KB4493509
LTSC	2019-04-02	17763.404	KB4490481
LTSC	2019-03-12	17763.379	KB4489899
LTSC	2019-03-01	17763.348	KB4482887
LTSC	2019-02-12	17763.316	KB4487044
LTSC	2019-01-22	17763.292	KB4476976
LTSC	2019-01-08	17763.253	KB4480116
LTSC	2018-12-19	17763.195	KB4483235
LTSC	2018-12-11	17763.194	KB4471332
LTSC	2018-12-05	17763.168	KB4469342
LTSC	2018-11-13	17763.134	KB4467708
LTSC	2018-11-13	17763.107	KB4464455
LTSC	2018-10-09	17763.55	KB4464330

LTSC	2018-10-02	17763.1

▼ Windows Server 2016（OS 内部版本 14393）

展开表

服务选项	可用性日期	操作系统内部版本	知识库文章
LTSB	2024-01-09	14393.6614	KB5034119
LTSB	2023-12-12	14393.6529	KB5033373
LTSB	2023-11-14	14393.6452	KB5032197
LTSB	2023-10-10	14393.6351	KB5031362
LTSB	2023-09-12	14393.6252	KB5030213
LTSB	2023-08-08	14393.6167	KB5029242
LTSB	2023-07-11	14393.6085	KB5028169
LTSB	2023-06-23	14393.5996	KB5028623
LTSB	2023-06-13	14393.5989	KB5027219
LTSB	2023-05-09	14393.5921	KB5026363
LTSB	2023-04-11	14393.5850	KB5025228
LTSB	2023-03-14	14393.5786	KB5023697
LTSB	2023-02-14	14393.5717	KB5022838
LTSB	2023-01-10	14393.5648	KB5022289
LTSB	2022-12-13	14393.5582	KB5021235
LTSB	2022-11-17	14393.5502	KB5021654
LTSB	2022-11-08	14393.5501	KB5019964
LTSB	2022-10-18	14393.5429	KB5020439
LTSB	2022-10-11	14393.5427	KB5018411
LTSB	2022-09-13	14393.5356	KB5017305
LTSB	2022-08-09	14393.5291	KB5016622
LTSB	2022-07-12	14393.5246	KB5015808

LTSB	2022-06-14	14393.5192	KB5014702
LTSB	2022-05-19	14393.5127	KB5015019
LTSB	2022-05-10	14393.5125	KB5013952
LTSB	2022-04-12	14393.5066	KB5012596
LTSB	2022-03-08	14393.5006	KB5011495
LTSB	2022-02-08	14393.4946	KB5010359
LTSB	2022-01-17	14393.4889	KB5010790
LTSB	2022-01-11	14393.4886	KB5009546
LTSB	2022-01-05	14393.4827	KB5010195
LTSB	2021-12-14	14393.4825	KB5008207
LTSB	2021-11-14	14393.4771	KB5008601
LTSB	2021-11-09	14393.4770	KB5007192
LTSB	2021-10-12	14393.4704	KB5006669
LTSB	2021-09-14	14393.4651	KB5005573
LTSB	2021-08-10	14393.4583	KB5005043
LTSB	2021 年 7 月 29 日	14393.4532	KB5005393
LTSB	2021-07-13	14393.4530	KB5004238
LTSB	2021-07-07	14393.4470	KB5004948
LTSB	2021-06-08	14393.4467	KB5003638
LTSB	2021-05-11	14393.4402	KB5003197
LTSB	2021-04-13	14393.4350	KB5001347
LTSB	2021-03-18	14393.4288	KB5001633
LTSB	2021 年 3 月 9 日	14393.4283	KB5000803
LTSB	2021-02-09	14393.4225	KB4601318
LTSB	2021-01-12	14393.4169	KB4598243
LTSB	2020-12-08	14393.4104	KB4593226
LTSB	2020 年 11 月 19 日	14393.4048	KB4594441

LTSB	2020 年 11 月 10 日	14393.4046	KB4586830
LTSB	2020-10-13	14393.3986	KB4580346
LTSB	2020-09-08	14393.3930	KB4577015
LTSB	2020 年 8 月 11 日	14393.3866	KB4571694
LTSB	2020-07-14	14393.3808	KB4565511
LTSB	2020-06-18	14393.3755	KB4567517
LTSB	2020-06-09	14393.3750	KB4561616
LTSB	2020-05-12	14393.3686	KB4556813
LTSB	2020-04-21	14393.3659	KB4550947
LTSB	2020-04-14	14393.3630	KB4550929
LTSB	2020-03-17	14393.3595	KB4541329
LTSB	2020-03-10	14393.3564	KB4540670
LTSB	2020-02-25	14393.3542	KB4537806
LTSB	2020-02-11	14393.3504	KB4537764
LTSB	2020-01-23	14393.3474	KB4534307
LTSB	2020-01-14	14393.3443	KB4534271
LTSB	2019-12-10	14393.3384	KB4530689
LTSB	2019-11-12	14393.3326	KB4525236
LTSB	2019-10-15	14393.3300	KB4519979
LTSB	2019-10-08	14393.3274	KB4519998
LTSB	2019-10-03	14393.3243	KB4524152
LTSB	2019-09-24	14393.3242	KB4516061
LTSB	2019-09-23	14393.3206	KB4522010
LTSB	2019-09-10	14393.3204	KB4516044
LTSB	2019-08-17	14393.3181	KB4512495
LTSB	2019-08-13	14393.3144	KB4512517
LTSB	2019-07-16	14393.3115	KB4507459

LTSB	2019-07-09	14393.3085	KB4507460
LTSB	2019-06-27	14393.3056	KB4509475
LTSB	2019-06-18	14393.3053	KB4503294
LTSB	2019-06-11	14393.3025	KB4503267
LTSB	2019-05-23	14393.2999	KB4499177
LTSB	2019-05-19	14393.2972	KB4505052
LTSB	2019-05-14	14393.2969	KB4494440
LTSB	2019-04-25	14393.2941	KB4493473
LTSB	2019-04-25	14393.2908	KB4499418
LTSB	2019-04-09	14393.2906	KB4493470
LTSB	2019-03-19	14393.2879	KB4489889
LTSB	2019-03-12	14393.2848	KB4489882
LTSB	2019-02-19	14393.2828	KB4487006
LTSB	2019-02-12	14393.2791	KB4487026
LTSB	2019-01-17	14393.2759	KB4480977
LTSB	2019-01-08	14393.2724	KB4480961
LTSB	2018-12-19	14393.2670	KB4483229
LTSB	2018-12-11	14393.2665	KB4471321
LTSB	2018-12-03	14393.2641	KB4478877
LTSB	2018-11-27	14393.2639	KB4467684
LTSB	2018-11-13	14393.2608	KB4467691
LTSB	2018-10-18	14393.2580	KB4462928
LTSB	2018-10-09	14393.2551	KB4462917
LTSB	2018-09-20	14393.2515	KB4457127
LTSB	2018-09-11	14393.2485	KB4457131
LTSB	2018-08-30	14393.2457	KB4343884
LTSB	2018-08-14	14393.2430	KB4343887

LTSB	2018-07-30	14393.2396	KB4346877
LTSB	2018-07-24	14393.2395	KB4338822
LTSB	2018-07-16	14393.2368	KB4345418
LTSB	2018-07-10	14393.2363	KB4338814
LTSB	2018-06-21	14393.2339	KB4284833
LTSB	2018-06-12	14393.2312	KB4284880
LTSB	2018-05-17	14393.2273	KB4103720
LTSB	2018-05-08	14393.2248	KB4103723
LTSB	2018-04-17	14393.2214	KB4093120
LTSB	2018-04-10	14393.2189	KB4093119
LTSB	2018 年 3 月 29 日	14393.2156	KB4096309
LTSB	2018-03-22	14393.2155	KB4088889
LTSB	2018-03-13	14393.2125	KB4088787
LTSB	2018-02-22	14393.2097	KB4077525
LTSB	2018-02-13	14393.2068	KB4074590
LTSB	2018-01-17	14393.2035	KB4057142
LTSB	2018-01-03	14393.2007	KB4056890
LTSB	2017-12-12	14393.1944	KB4053579
LTSB	2017-11-27	14393.1914	KB4051033
LTSB	2017-11-14	14393.1884	KB4048953
LTSB	2017-11-02	14393.1797	KB4052231
LTSB	2017-10-17	14393.1794	KB4041688
LTSB	2017-10-10	14393.1770	KB4041691
LTSB	2017-09-28	14393.1737	KB4038801
LTSB	2017-09-12	14393.1715	KB4038782
LTSB	2017-08-28	14393.1670	KB4039396
LTSB	2017-08-16	14393.1613	KB4034661

LTSB	2017-08-08	14393.1593	KB4034658
LTSB	2017-08-07	14393.1537	KB4038220
LTSB	2017-07-18	14393.1532	KB4025334
LTSB	2017-07-11	14393.1480	KB4025339
LTSB	2017-06-27	14393.1378	KB4022723
LTSB	2017-06-13	14393.1358	KB4022715
LTSB	2017-05-09	14393.1198	KB4019472
LTSB	2017-04-11	14393.1066	KB4015217
LTSB	2017-03-20	14393.969	KB4015438
LTSB	2017-03-14	14393.953	KB4013429
LTSB	2017-01-10	14393.693	KB3213986
LTSB	2016-12-13	14393.576	KB3206632
LTSB	2016-12-09	14393.479	KB3201845
LTSB	2016-11-08	14393.447	KB3200970
LTSB	2016-10-27	14393.351	KB3197954
LTSB	2016-10-11	14393.321	KB3194798
LTSB	2016-09-29	14393.222	KB3194496
LTSB	2016-09-20	14393.187	KB3193494
LTSB	2016-09-13	14393.187	KB3189866
LTSB	2016-08-31	14393.105	KB3176938
LTSB	2016-08-23	14393.82	KB3176934
LTSB	2016-08-09	14393.51	KB3176495
LTSB	2016-08-02	14393.10	KB3176929

Windows Server 的扩展安全更新概述

项目 • 2023/08/22

对于需要在支持结束时运行某些旧的 Microsoft 产品的客户，扩展安全更新 (ESU) 计划是最后一种方法。 Windows Server 长期服务渠道 (LTSC) 提供至少 10 年的支持：5 年的主要支持，以及 5 年的外延支持，其中包括常规安全更新。

但是，一旦产品支持结束，这也意味着安全更新和公告结束。 这种情况可能会导致安全问题或符合性问题，并使业务应用程序面临风险。 Microsoft 建议升级到 Windows Server 的当前版本以获得最高级的安全性、性能和创新。

> **提示**
>
> 可以通过 **Microsoft 生命周期**找到有关支持日期的信息。

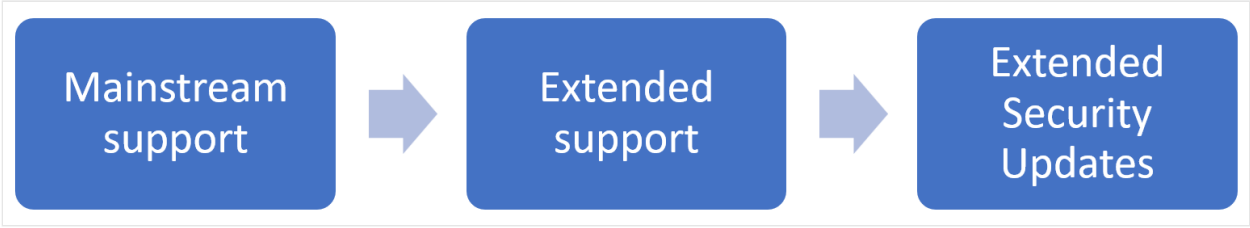
以下版本的 Windows Server 已结束或即将结束扩展支持：

- Windows Server 2008 和 Windows Server 2008 R2 的扩展支持已于 2020 年 1 月 14 日结束。
- Windows Server 2012 和 Windows Server 2012 R2 的扩展支持将于 2023 年 10 月 10 日结束。

什么是扩展安全更新?

Windows Server 的扩展安全更新包括评级为“*严重*”和“*重要*”的安全更新和公告，从扩展支持日期结束算起的最长期限取决于版本。 对于 Azure 中托管的服务器免费提供更新，对于未托管在 Azure 中的服务器，可购买更新。 扩展安全更新不包括新功能、客户请求的非安全修补程序或设计更改请求。 有关详细信息，请参阅生命周期常见问题解答 - 扩展安全更新。

通过扩展安全更新，Windows Server 的这些版本的不同阶段如下所示：



如果尚未升级服务器，则可在过渡期内执行以下操作来保护应用程序和数据：

- 将受影响的现有 Windows Server 工作负载按原样迁移到 Azure 虚拟机 (VM)。 Azure 迁移会在定义的时间段内自动提供扩展安全更新。 扩展安全更新不会在

Azure VM 的成本之上增加额外费用，也无需进行任何其他配置。

- 在准备升级到较新的 Windows Server 版本之前，请为服务器购买扩展安全更新订阅并保持受保护状态。 拥有扩展安全更新订阅时，Microsoft 会为定义的时间段提供更新。 购买订阅后，必须获取产品密钥并将其安装在每个适用的服务器上。 有关详细信息，请参阅如何获取扩展安全更新。

获取扩展安全更新的时间取决于所使用的 Windows Server 版本及其托管位置。 下表列出了每个版本的 Windows Server 的扩展安全更新持续时间。

产品版本	已托管	ESU 持续时间	ESU 结束日期
Windows Server 2008 Windows Server 2008 R2	Azure*	四年	2024 年 1 月 9 日
Windows Server 2008 Windows Server 2008 R2	不在 Azure 中	三年	2023 年 1 月 10 日
Windows Server 2012 Windows Server 2012 R2	Azure*	三年	2026 年 10 月 13 日
Windows Server 2012 Windows Server 2012 R2	不在 Azure 中	三年	2026 年 10 月 13 日

* 包括将 Azure 服务和功能扩展到你所选环境的 Azure Stack 产品组合。

> ⚠ **警告**
>
> 扩展安全更新期限结束后，我们将停止提供更新。 建议尽快将 Windows Server 版本更新到较新的版本。

迁移到 Azure

可以将运行已结束或即将结束扩展支持的 Windows Server 版本的本地服务器迁移到 Azure，在 Azure 中，你可以继续将其作为虚拟机运行。 迁移到 Azure 时，不仅符合安全更新要求，而且还会向工作添加云创新。 迁移到 Azure 的好处包括：

- Azure 中的安全更新。
- 获取一段时间的 Windows Server 关键和重要安全更新，且不会产生任何额外费用。
- 免费 Azure 升级。
- 准备就绪后即可采用更多云服务。
- 通过将 SQL Server 迁移到 Azure VM，可以获取额外三年的 Windows Server 关键安全更新，且不会产生任何额外费用。 还可以将 SQL Server 现代化为 Azure SQL 托

管实例。
- 得益于 Azure 混合权益，可以利用现有的 Windows Server 许可证和 SQL Server 许可证，从而实现 Azure 特有的云成本节省。

若要开始迁移，请了解如何上传通用 VHD 并将其用于在 Azure 中创建新的 VM，或使用 Azure 中的共享映像库。

还可以阅读适用于 Windows Server 的迁移指南，获取有关以下事务的帮助：

- 分析现有 IT 资源。
- 评估部署的当前状态。
- 了解最适合你的方案：是将某些服务和应用程序移动到云中，还是将其保留在本地并升级到最新版本的 Windows Server。

本地升级

如果需要将服务器保留在本地而不是迁移到 Azure 和云，有两种选择：

- 使用受支持的 Windows Server 版本生成新服务器，并迁移应用程序和数据。
- 就地升级到受支持的 Windows Server 版本。

就地升级通常可以将 Windows Server 升级至少一个版本，有时甚至可以升级两个版本。 例如，Windows Server 2012 R2 可以就地升级到 Windows Server 2019。 但是，如果你正在运行 Windows server 2008 或 Windows server 2008 R2，则没有到 Windows Server 2016 或更高版本的直接升级路径。 必须先升级到 Windows Server 2012 R2，然后再升级到 Windows Server 2016 或 Windows Server 2019。

升级时，还可以随时迁移到 Azure。 有关本地升级选项的更多信息，请参阅受支持的 Windows Server 升级路径。

将 SQL Server 与 Windows Servers 并行升级

如果你运行的是已结束或即将结束扩展支持的 SQL Server 版本，你也可以从 SQL Server 的扩展安全更新中获益。 有关详细信息，请参阅 SQL Server 和 Windows Server 的扩展安全更新。

后续步骤

- 了解如何获取 Windows Server 的扩展安全更新 (ESU)。

Windows Server 升级概述

项目 • 2024/11/02 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

升级到更高版本 Windows Server 的过程可能会有很大的不同，具体视你从哪个操作系统入手和选择的路径而定。 我们使用以下术语来区分不同的操作，其中任何一个都可能涉及到新的 Windows Server 部署。

- **升级。** 也称为“就地升级”。 从操作系统的较旧版本移动到较新版本，同时仍在相同的物理硬件上。 本部分将介绍这种方法。

  > **ⓘ 重要**
  >
  > 公有或私有云公司也可能支持就地升级；但是，必须咨询云提供商以了解详细信息。 此外，无法在任何配置为“从 VHD 启动”的 Windows Server 上执行就地升级。 不支持从 Windows Storage Server 版本就地升级。 可以改为执行迁移或安装。

- **安装。** 也称为“全新安装”。 从操作系统的较旧版本移动到较新版本，同时删除较旧的操作系统。
- **迁移。** 通过迁移到另一组硬件或虚拟机，从旧版操作系统迁移到新版操作系统。
- **群集操作系统滚动升级。** 升级群集节点的操作系统，且无需停止 Hyper-V 或横向扩展文件服务器工作负载。 利用此功能可以避免出现可能影响服务级别协议的故障时间。 有关详细信息，请参阅群集 OS 滚动升级
- **许可证转换。** 使用简单的命令和相应的许可证密钥，通过一个步骤将发行版的特定版本转换成同一发行版的另一个版本。 我们称之为“许可证转换”。 例如，如果服务器运行标准版，可以将其转换为数据中心。

应升级到 Windows Server 的哪个版本?

建议升级到 Windows Server 的最新版本。 通过运行最新版本的 Windows Server，可使用最新功能（包括最新的安全功能）并提供最佳性能。

> **提示**

- 从 Windows Server 2025 开始，可以从 Windows Server 2012 R2 及更高版本的 Windows Server 升级。
- 使用 Windows Server 2022 及更早版本，一次最多可以升级到两个版本的较新版本 Windows Server。 例如，Windows Server 2016 可以升级到 Windows Server 2019 或 Windows Server 2022。 如果使用**群集操作系统滚动升级功能**，则一次只能有一个版本。

在此表中，你可以根据当前版本查看支持的升级路径。

展开表

从 升级/升级到	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025
Windows Server 2012	是	是	-	-	-
Windows Server 2012 R2	-	是	是	-	是
Windows Server 2016	-	-	是	是	是
Windows Server Standard 2012 R2	-	-	-	是	是
Windows Server 2022	-	-	-	-	是
Windows Server 2025	-	-	-	-	是

还可以从操作系统的评估版本升级到零售版本，从旧的零售版本升级到较新版本，或者在某些情况下，从操作系统的批量许可版本升级到普通零售版本。 有关就地升级以外的升级选项的详细信息，请参阅 Windows Server 的升级和转换选项。

ⓘ 重要

对 Windows Server 2008 和 Windows Server 2008 R2 的支持已结束。 建议尽快将 Windows Server 版本更新到较新的版本。 最后，详细了解**扩展安全更新 (ESU)**。

后续步骤

现在，你已准备好升级 Windows Server，下面是一些可帮助你入门的文章：

- 安装、升级到或迁移到 Windows Server
- 升级和迁移 Windows Server 中的角色和功能
- 适用于 Windows Server 的升级和转换选项
- 执行 Windows Server 的就地升级

反馈

此页面是否有帮助？ 是 否

功能更新、干净安装或迁移到 Windows Server

项目 • 2024/10/31 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

是时候移动到较新版本的 Windows Server 了吗？ 根据现在正在运行的内容，你有若干选择来实现这一点。 例如，你可以将就地操作系统（OS）升级（功能更新）升级到较新版本的 Windows Server、全新安装较新版本的 Windows Server，甚至将现有系统迁移到 Windows Server。

> **ⓘ 重要**
>
> - 强烈建议在执行就地 OS 功能升级、全新安装或系统迁移到更高版本的 Windows Server 之前，始终备份系统和其他重要文件。
> - 对 Windows Server 2012 和 Windows Server 2012 R2 的扩展支持已于 2023 年 10 月 10 日结束。 可以使用扩展安全更新 (ESU)，其中一种选择是将本地服务器迁移到 Azure，以便在虚拟机上继续运行它们。 若要了解详细信息，请参阅**扩展安全更新概述**。

你可以在 Windows Server 评估版免费下载并试用最新版本的 Windows Server。

就地 OS 升级 （功能更新）

就地 OS 升级（功能更新）执行 Windows Server 安装的功能更新。 你可以升级到更高版本的 Windows Server，同时保留原始设置、服务器角色、功能和数据。 就地功能更新使你可以跨多个版本跳跃。 此方法是移动到更高版本的 Windows Server 的最快方法。 有关 OS 升级路径的详细信息，请参阅应升级到哪个版本的 Windows Server? 请记住，某些角色和功能不支持就地功能升级。 就地功能升级最适合不需要特定原始设备制造商（OEM）硬件驱动程序才能成功升级的虚拟机（VM）。

可以通过以下两种方式之一执行就地升级：从媒体或使用“设置”对话框中的Windows 更新。 使用媒体升级安装涉及下载和准备媒体，例如 ISO、USB 或 DVD 磁盘。 使用“设置”对话框中的Windows 更新进行升级时，可以直接从桌面中的Windows 更新或使用 SConfig for Server Core 进行安装。 有关如何执行就地升级的分步说明，请参阅 执行 Windows Server 就地升级。

群集操作系统滚动升级（功能更新）

群集操作系统滚动升级（功能更新）使管理员能够在不停止 Hyper-V 或横向扩展文件服务器工作负荷的情况下升级群集节点的操作系统。 例如，如果群集中的节点运行的是早期版本的 Windows Server，则管理员可以使用功能更新在它们上安装更高版本，而无需关闭群集，否则会影响服务级别协议（SLA）。 群集感知更新（CAU）是一项功能，可自动执行群集服务器上的软件更新过程，同时保持可用性。 有关更新群集的详细信息，请参阅 群集感知更新概述 和 群集操作系统滚动升级。

如果在 Azure Stack 超融合基础结构（HCI）解决方案上运行 VM，建议使用生命周期管理器（LCM）执行功能更新。 有关详细信息，请参阅 关于 Azure Stack HCI 升级 的详细信息。

清理操作系统安装

Windows Server 的全新 OS 安装是在全新服务器上安装 Windows Server 或覆盖现有 OS 时。 此方法是安装 Windows Server 的最简单方法。 但是，在完成安装之前，必须备份数据并计划如何在安装完成后重新安装现有应用程序。 还应确保你的系统满足 Windows Server 的硬件要求。

迁移

迁移是指将角色或功能从运行 Windows Server 的源计算机移动到也运行 Windows Server 的目标计算机。 此过程是逐步的，一次移动一个角色或功能，而无需升级功能。 可以将系统组件迁移到运行与源计算机或更高版本相同的 Windows Server 版本的计算机。

许可证转换

许可证转换将特定版本的 Windows Server 的特定版系转换为同一版本的另一个版系。 只需运行一个命令并输入要转换为的版系的相应许可证密钥。 例如，如果服务器正在运行 Windows Server 2022 Standard 版系，可以将其转换为 Windows Server 2022 Datacenter 版系。 但是，将版系从 Standard 转换为 Datacenter 时，无法反转此过程来恢复为 Standard 版系。 在某些版本的 Windows Server 中，还可以使用相同命令和相应的许可证密钥在原始设备制造商（OEM）、批量许可和零售版本之间自由转换。

相关内容

- 群集 OS 滚动升级

反馈

此页面是否有帮助? 是 否

“服务器核心”与“带桌面体验的服务器”安装选项

项目 • 2023/08/30

使用安装向导安装 Windows Server 时，可以在“服务器核心”或“带桌面体验的服务器”安装选项之间进行选择。 使用“服务器核心”不会安装标准图形用户界面（桌面体验）；可以使用 PowerShell、服务器配置工具 (SConfig) 或远程方法通过命令行管理服务器。 “带桌面体验的服务器”会安装标准图形用户界面和所有工具，包括客户端体验功能。

建议选择“服务器核心”安装选项，除非你有特殊需求要用到“带桌面体验的服务器”安装选项中包含的附加用户界面元素和图形管理工具。

安装向导列出了下面的安装选项。 在此列表中，不带“桌面体验”的版本是“服务器核心”安装选项：

- Windows Server Standard
- 带桌面体验的 Windows Server Standard
- Windows Server Datacenter
- 带桌面体验的 Windows Server Datacenter

> **备注**
>
> 与某些之前版本的 Windows Server 不同，安装后无法在服务器核心和具有桌面体验的服务器之间转换。 如果稍后安装决定使用其他选项，则需要执行**全新安装**。

差异

“服务器核心”与“带桌面体验的服务器”之间存在一些主要差异：

组件	服务器核心	服务器（提供桌面体验）
用户界面	最小的命令行驱动（PowerShell、SConfig、cmd）	标准 Windows 图形用户界面
磁盘空间	较小的要求	较大的要求
在本地安装、配置和卸载服务器角色	PowerShell	服务器管理器或 PowerShell
角色和功能	某些角色和功能不可用。 有关详细信息，请参阅 Windows Server 中不存在的	所有角色和功能都可用，包括用于应用程序兼容性的角色和功能。

组件	服务器核心	服务器（提供桌面体验）
	角色、角色服务和功能 - 服务器核心。 可以通过应用兼容性按需功能 (FOD) 安装“带桌面体验的服务器”中用于应用程序兼容性的一些功能。	
远程管理	是的，可以使用 GUI 工具（例如 Windows Admin Center、远程服务器管理工具 (RSAT) 或服务器管理器）或通过 PowerShell 进行远程管理。	是的，可以使用 GUI 工具（例如 Windows Admin Center、远程服务器管理工具 (RSAT) 或服务器管理器）或通过 PowerShell 进行远程管理。
潜在攻击面	大大减少受攻击面	未减少
Microsoft 管理控制台	未安装 - 可以使用 应用兼容性按需功能 (FOD) 进行安装。	已安装

> **备注**
>
> 对于 RSAT，必须使用 Windows 10 或更高版本随附的版本。

升级和迁移 Windows Server 中的角色和功能

项目 • 2023/08/30

你可以通过迁移到新服务器来将角色和功能更新为较新版本的 Windows Server，或者，许多情况下还支持就地升级，可在当前版本的基础上安装新版本的 Windows Server。 本文包含一些链接，这些链接指向迁移指南以及包含迁移和就地升级信息的表，可帮助你确定使用哪种方法。

你可以通过使用 Windows Server 迁移工具（一种内置于 Windows Server 的功能，用于迁移角色和功能）迁移多个角色和功能，而可以使用存储迁移服务来迁移文件服务器和存储。

这些迁移指南支持将指定的角色和功能从一台服务器迁移到另一台服务器（非就地升级）。 除非指南中另行说明，否则支持在物理与虚拟计算机之间以及在 Windows Server 的完全安装选项（Windows Server 提供桌面体验或服务器核心）之间进行迁移。

> **ⓘ 重要**
>
> 在开始迁移角色和功能之前，验证源和目标服务器是否都在运行适用于其操作系统的最新更新。
>
> 每当迁移到或升级到任何版本的 Windows Server 时，都应查看并了解**支持生命周期策略**以及该版本的时间范围，并且作出相应的计划。 你可以**搜索生命周期信息**，以便了解你感兴趣的特定 Windows server 版本。

Windows Server 迁移工具

通过使用 Windows Server 迁移工具，可将服务器角色、功能、操作系统设置以及其他数据和共享迁移到服务器，包括较新版本的 Windows 服务器。 它是 Windows Server 的一项功能，因此可使用“添加角色和功能”向导或 PowerShell 轻松进行安装。 详细了解如何安装、使用和删除 Windows Server 迁移工具。

> **ⓘ 备注**
>
> 使用 Windows Server 迁移工具的跨子网迁移适用于 Windows Server 2012 和更高版本。 以前版本的 Windows Server 迁移工具仅支持在同一子网中进行迁移。

迁移指南

你可以在下面找到特定 Windows 角色和功能的迁移指南的链接。

Active Directory

- 适用于 Windows Server 2012 R2 的 Active Directory 证书服务迁移指南
- 适用于 Windows Server 2008 R2 的 Active Directory 证书服务迁移指南
- 将 Active Directory 联合身份验证服务角色服务迁移到 Windows Server 2012 R2
- 将 Active Directory 联合身份验证服务角色服务迁移到 Windows Server 2012
- Active Directory Rights Management Services 迁移和升级指南
- 将域控制器升级到 Windows Server 2012 R2 和 Windows Server 2012
- 适用于 Windows Server 2008 R2 的 Active Directory 域服务和域名系统 (DNS) 服务器迁移指南

BranchCache

- BranchCache 迁移指南

DHCP

- 将 DHCP 服务器迁移到 Windows Server 2012 R2
- 适用于 Windows Server 2008 R2 的动态主机配置协议 (DHCP) 服务器迁移指南

故障转移群集

- 将群集角色迁移到 Windows Server 2012 R2
- 将群集服务和应用程序迁移到 Windows Server 2012

文件和存储服务

- 存储迁移服务
- 将文件和存储服务迁移到 Windows Server 2012 R2

Hyper-V

- 将 Hyper-V 从 Windows Server 2012 迁移到 Windows Server 2012 R2
- 将 Hyper-V 从 Windows Server 2008 R2 迁移到 Windows Server 2012

网络策略服务器

- 将网络策略服务器迁移到 Windows Server 2012
- 将健康注册机构迁移到 Windows Server 2012

打印和文档服务

- 将打印和文档服务迁移到 Windows Server 2012

远程访问

- 将远程访问迁移到 Windows Server 2012

远程桌面服务

- 迁移远程桌面服务
- 将远程桌面服务迁移到 Windows Server 2012 R2
- 迁移 MultiPoint Services

路由和远程访问

- RRAS 迁移指南

Web 服务器 (IIS)

- Web 服务器 (IIS)

Windows Server Update Services

- 将 Windows Server Update Services 迁移到 Windows Server 2012 R2

其他 Windows 迁移指南

- 本地用户和组迁移指南
- IP 配置迁移指南

升级和迁移矩阵

服务器角色	是否可就地升级?	是否支持迁移?	是否无需停机就可完成迁移?
Active Directory 证	是	是	否

服务器角色	是否可就地升级?	是否支持迁移?	是否无需停机就可完成迁移?
书服务			
Active Directory 域服务	是	是	是
Active Directory 联合身份验证服务	否	是	否（需要将新节点添加到场中）
Active Directory 轻型目录服务	是	是	是
Active Directory 权限管理服务	是	是	否
DHCP 服务器	是	是	是
DNS 服务器	是	是	否
故障转移群集	可以，使用群集操作系统滚动升级流程（Windows Server 2012 R2 或更高版本），或由群集为进行升级删除服务器，并随后将服务器添加到其他群集。	是	可以，适用于使用 Hyper-V VM 的故障转移群集或运行横向扩展文件服务器角色的故障转移群集。 请参阅群集操作系统滚动升级（Windows Server 2012 R2 及更高版本）。
文件和存储服务	是	因子功能而异	否
Hyper-V	可以，使用群集操作系统滚动升级流程（Windows Server 2012 R2 及更高版本）	是	可以，适用于使用 Hyper-V VM 的故障转移群集或运行横向扩展文件服务器角色的故障转移群集。 请参阅群集操作系统滚动升级（Windows Server 2012 R2 及更高版本）。
打印和传真服务	否	可以（使用 Printbrm.exe）	否
远程桌面服务	可以，适用于所有子角色，但不支持混合模式场	是	否
Web 服务器 (IIS)	是	是	否

服务器角色	是否可就地升级?	是否支持迁移?	是否无需停机就可完成迁移?
Windows Server Essentials 体验	是	是	否
Windows Server Update Services	是	是	否
工作文件夹	是	是	可以，使用群集操作系统滚动升级流程（Windows Server 2012 R2 及更高版本）。

适用于 Windows Server 的升级和转换选项

项目 • 2024/10/31 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

可以执行就地升级（功能更新）或将 Windows Server 安装转换为较新版本、不同版本或在许可许可的许可选项（例如评估、零售和批量许可）之间进行切换。 本文介绍可帮助你进行规划的选项。

执行升级（功能更新）或转换 Windows Server 安装的过程可能会有很大差异，具体取决于已安装的版本、许可方式以及采用的路径。 我们使用不同的术语来区分操作，其中任何操作都可能涉及 Windows Server 的部署：就地升级、干净安装、群集操作系统（OS）滚动更新、迁移和许可证转换。 可以在安装、更新或迁移到 Windows Server 中了解有关这些条款的详细信息。

升级许可版本的 Windows Server

以下一般准则适用于已获得 **Windows Server** 许可的就地升级（功能更新）路径，即不进行评估：

- 不支持从 32 位到 64 位体系结构的升级。 自 Windows Server 2008 R2 以来的所有 Windows Server 版本都仅有 64 位。
- 不支持从一种语言到另一种语言的升级。
- 如果服务器是一个 Active Directory 域控制器，则无法将其转换为零售版本。 有关重要信息，请参阅将域控制器升级到 Windows Server。
- 不支持从 Windows Server 的预发布版本（预览版）进行升级。 执行 Windows Server 的干净安装。
- 不支持从“Server Core”安装切换到“带桌面体验的 Server”安装的升级，反之亦然。
- 不支持从以前的 Windows Server 安装到 Windows Server 的评估副本升级。 评估版本应安装为干净安装。
- 从以前的版本升级到新版本时，默认情况下保留现有的操作系统版本。 例如，默认从 Standard（旧版本）升级到 Standard（新版本），从 Datacenter（旧版本）升级到 Datacenter（新版本），或从 Datacenter: Azure Editio（旧版本）升级到 Datacenter: Azure Edition（新版本）。
- 或者，升级时可以更改为某些其他版别。 你可以从 Standard 更改为 Datacenter 或 Datacenter: Azure Edition，也可以从 Datacenter 更改为 Datacenter: Azure Edition。 升级时，无法从 Datacenter 更改为 Standard 版或从 Datacenter: Azure Edition 更改为 Standard 或 Datacenter 版。

> ⓘ **备注**
>
> 如果服务器使用 NIC 组合，请在升级之前禁用 NIC 组合，然后在升级完成后重新启用它。 请参阅 **NIC 组合概述** 了解详细信息。

将评估版本转换为零售版本

可以将 Windows Server 的评估版本和版别转换为零售版本和版别。 例如，如果已安装 Standard（桌面体验）版的评估版本，则可以将其转换为 Standard（桌面体验）版或 Datacenter（桌面体验）版的零售版本。

但是，无法将所有 Windows Server 评估版本和版别转换为所有零售版本和版别。 例如，如果已安装评估 Datacenter 版，则只能将其转换为零售 Datacenter 版，无法转换为零售 Standard 版。

在 2016 年之后的 Windows Server 版本中，如果已安装桌面体验评估版本，则无法将它们转换为 Core 零售版本。 如果安装 Standard Core 评估版本，则只能将其转换为零售 Datacenter Core，无法转换为零售 Standard Core。

请务必按照以下过程中的指示运行 `DISM /online /Get-TargetEditions` 命令，以确定可以转换为的零售版本。 如果所需的零售版本未列为目标版本，则需要重新安装所需的零售版本。

> ⓘ **备注**
>
> 要验证服务器是否正在运行评估版本，可以在提升的命令提示符中运行以下命令之一：
>
> - 运行 `DISM /online /Get-CurrentEdition` 并确保当前板别名称包括 `Eval`。
> - 运行 `slmgr.vbs /dlv` 并确保输出包括 `EVAL`。

如果尚未激活 Windows，桌面右下角会显示评估期的剩余时间。

Windows Server Standard 或 Datacenter

如果你的服务器运行的是 Windows Server Standard 或 Datacenter 版的评估版本，则可以将其转换为可用的零售版本。 在提升的命令提示符或 PowerShell 会话中运行以下命令。

1. 通过运行以下命令确定当前版别名称。 输出是版别名称的缩写形式。 例如，Windows Server Datacenter（桌面体验）评估版为 `ServerDatacenterEval`。

   Windows 命令提示符

   ```
   DISM /online /Get-CurrentEdition
   ```

2. 通过运行以下命令验证当前安装可以转换为哪些版别。 在输出中，记下要转换为的版本名称。

   Windows 命令提示符

   ```
   DISM /online /Get-TargetEditions
   ```

3. 运行以下命令以保存适用于 Windows Server 的 Microsoft 软件许可条款，然后你可以查看这些条款。 将 `<target edition>` 占位符替换为上一步中记录的版别名称。

   Windows 命令提示符

   ```
   DISM /online /Set-Edition:<target edition> /GetEula:C:\license.rtf
   ```

4. 在以下命令中输入新的版别名称和相应的零售产品密钥。 设置版本过程要求你接受之前保存的 Windows Server Microsoft软件许可条款。

   Windows 命令提示符

   ```
   DISM /online /Set-Edition:<target edition> /ProductKey:<product key>
   /AcceptEula
   ```

   例如：

   Windows 命令提示符

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:ABCDE-12345-
   ABCDE-12345-ABCDE /AcceptEula
   ```

提示

有关 Dism.exe 的详细信息，请参阅 **DISM 命令行选项**。

重要

无法将 Active Directory 域控制器从评估转换为零售版本。 在这种情况下，请在运行零售版的服务器上安装额外的域控制器，迁移持有的任何 FSMO 角色，并从运行评估版的域控制器中删除 Active Directory 域服务 (AD DS)。 有关详细信息，请参阅**将域控制器升级到 Windows Server**。

Windows Server Essentials

如果服务器运行的是 Windows Server Essentials，则可以在提升的命令提示符中，在以下命令中输入零售、批量许可或 OEM 密钥来将其转换为完整零售版本：

Windows 命令提示符

```
slmgr.vbs /ipk <license key>
```

将 Windows Server Standard 版转换为 Datacenter 版

安装 Windows Server 后，随时都可以将 Windows Server Standard 版转换为 Datacenter 版。 还可以从安装介质运行 `setup.exe` 来升级或修复安装，这有时称为就地修复。 如果运行 `setup.exe` 以在任何版本的 Windows Server 上执行升级或就地修复，结果会是你一开始使用的那个版本。

可以按如下所示将 Windows Server 的 Standard 版转换为 Datacenter 版：

1. 通过运行以下命令，确定 Windows Server Standard 是当前版别名称。 输出是版别名称的缩写形式，例如 Windows Server Standard（桌面体验）版是 `ServerStandard`。

   Windows 命令提示符

   ```
   DISM /online /Get-CurrentEdition
   ```

2. 通过运行以下命令，验证 Windows Server Datacenter 是要转换为的有效选项：

   Windows 命令提示符

   ```
   DISM /online /Get-TargetEditions
   ```

3. 在以下命令中输入 `ServerDatacenter` 和你的零售产品密钥：

   ```
   ```

Windows 命令提示符

```
DISM /online /Set-Edition:ServerDatacenter /ProductKey:<product key>
/AcceptEula
```

在零售、批量许可和 OEM 许可证之间转换

安装 Windows Server 后，可以随时在零售许可证、批量许可许可证或 OEM 许可证之间自由转换。 在执行这种转换期间，版本（Standard 或 Datacenter）保持不变。 如果你一开始是评估版本，则先将其转换为零售版本，然后通过提升的命令提示符运行以下命令来在版本之间进行转换。 提供你的批量许可、零售或 OEM 产品密钥。

Windows 命令提示符

```
slmgr.vbs /ipk <product key>
```

另请参阅

有关升级 Windows Server 的详细信息，请参阅以下文章：

- Windows Server 升级概述
- “Server Core”与“带桌面体验的 Server”安装选项
- 执行 Windows Server 的就地升级
- Azure 中运行 Windows Server 的 VM 的就地升级

反馈

此页面是否有帮助? 是 否

Windows Server 中的虚拟机自动激活

项目 • 2024/10/02

虚拟机自动激活 (AVMA) 充当一个购买证明机制，帮助确保用户根据产品使用权和 Microsoft 软件许可条款使用 Windows 产品。

通过 AVMA 可以在正确激活的 Windows Server Hyper-V 主机上激活 Windows Server 虚拟机 (VM)，即使在断开连接的环境中也是如此。 AVMA 可将 VM 激活绑定到许可的虚拟化主机，并在其启动时激活 VM。 在使用 AVMA 时，你可以获取有关使用情况的实时报告，以及有关虚拟机许可证状态的历史数据。 虚拟化主机上会提供报告和跟踪数据。

实际的应用程序

在虚拟化主机上，AVMA 具有若干优势。

服务器数据中心管理员可以使用 AVMA 来执行以下任务：

- 激活远程位置的 VM。
- 使用或不使用 Internet 连接激活 VM。
- 从虚拟化主机跟踪 VM 使用情况和许可证，而无需对虚拟化系统的任何访问权限。

服务提供商许可协议 (SPLA) 合作伙伴和其他托管提供商无需与租户共享产品密钥或访问租户的 VM 来激活它。 使用 AVMA 时，VM 激活对于租户是透明的。 托管提供商可以使用服务器日志来验证许可证遵从性以及跟踪客户端使用历史记录。

系统要求

要支持虚拟化服务器主机运行来宾 VM，必须将其激活。 为此，请通过批量许可服务中心 或 OEM 提供商获取密钥。

> **备注**
>
> 在故障转移群集中，必须激活群集中的每台虚拟化服务器主机，以便保持来宾 VM 处于激活状态（无论 VM 运行在哪台服务器上）。

AVMA 要求使用安装了 Hyper-V 服务器主机角色的 Windows Server Datacenter 版本。 主机的 Windows Server 版本确定了可在来宾 VM 中激活的版本。 下表列出了每个主机版本能够激活的来宾 VM 版本。 主机版本可以访问其符合条件的来宾 VM 版本的所有版本（数据中心、标准版或 Essentials）。

展开表

服务器主机版本	Windows Server 2025 来宾 VM	Windows Server 2022 来宾 VM	Windows Server 2019 来宾 VM	Windows Server 2016 来宾 VM	Windows Server 2012 R2 来宾 VM
Windows Server 2025	X	X	X	X	X
Windows Server 2022		X	X	X	X
Windows Server 2019			X	X	X
Windows Server 2016				X	X
Windows Server 2012 R2					X

> **备注**
>
> AVMA 不能与其他服务器虚拟化技术一同使用。

如何实施 AVMA

要使用 AVMA 激活 VM，可以使用与要激活的 Windows Server 版本相对应的通用 AVMA 密钥（请参阅 AVMA 密钥中的详细信息）。 要创建 VM 并使用 AVMA 密钥将其激活，请执行以下步骤：

1. 在将要托管 VM 的服务器上，安装并配置 Microsoft Hyper-V Server 角色。 确保已成功激活服务器。 有关详细信息，请参阅 安装 Hyper-V 服务器。
2. 创建一个虚拟机并在其上安装支持的 Windows Server 操作系统。

   > **重要**
   >
   > 必须在 VM 设置中启用**数据交换集成服务**（也称为键值对交换），AVMA 才能工作。 默认情况下，会为新的 VM 启用此功能。

3. 在 VM 上安装 Windows Server 后，在 VM 上安装 AVMA 密钥。 在 PowerShell 或提升的命令提示符下，运行以下命令：

PowerShell

```
slmgr /ipk <AVMA_key>
```

只要虚拟化主机本身已激活，VM 就会自动激活。

> **提示**
>
> 也可以在任何**无人参与安装文件**中添加 AVMA 密钥。

AVMA 密钥

Windows Server 2025

展开表

版本	密钥
数据中心	YQB4H-NKHHJ-Q6K4R-4VMY6-VCH67
数据中心： Azure Edition	6NMQ9-T38WF-6MFGM-QYGYM-88J4F
Standard	WWVGQ-PNHV9-B89P4-8GGM9-9HPQ4

报告和跟踪

虚拟化主机和 VM 之间的键值对 (KVP) 交换为来宾操作系统提供实时跟踪数据，其中包括激活信息。 此激活信息存储在 VM 的 Windows 注册表中。 有关 AVMA 请求的历史数据记录在虚拟化主机上的事件查看器中。

有关 KVP 的详细信息，请参阅数据交换：使用键值对在 Hyper-V 上的主机和来宾之间共享信息。

> **备注**
>
> KVP 数据未受保护。 可以修改它，对其所做的更改不受监视。

> **重要**

如果将 AVMA 密钥更换为其他产品密钥（零售、OEM 或批量许可密钥），则应删除 KVP 数据。

由于 AVMA 激活过程是透明的，因此不会显示任何错误消息。 但 AVMA 请求也会记录在应用程序日志中事件查看器的虚拟化主机上，其事件 ID 为12310，并事件 ID 12309 记录在 VM 上。 VM 上会捕获以下事件：

展开表

通知	说明
AVMA 成功	VM 已激活。
无效主机	虚拟化主机无响应。 如果服务器未运行受支持的 Windows 版本，则可能会发生此事件。
无效数据	此事件通常是由于数据损坏、加密或数据不匹配所导致的虚拟化主机与 VM 之间的通信失败。
拒绝激活	由于 AVMA ID 不匹配，因此虚拟化主机无法激活来宾操作系统。

反馈

此页面是否有帮助? 是 否

密钥管理服务 (KMS) 激活规划

项目 • 2024/10/02

以下概括介绍使用密钥管理服务 (KMS) 激活时需要关注的初步规划注意事项。

KMS 使用客户端-服务器模型来激活客户端，并用于批量激活。 KMS 客户端连接到一台 KMS 服务器（称为 KMS 主机）进行激活。 KMS 主机必须位于本地网络。

KMS 主机不必是专用服务器，KMS 可与其他服务共用一台主机。 可以在运行受支持的 Windows Server 或 Windows 客户端操作系统的任何物理或虚拟系统上运行 KMS 主机。 在 Windows Server 操作系统上运行的 KMS 主机可以激活同时运行服务器和客户端操作系统的计算机。 但是，在 Windows 客户端操作系统上运行的 KMS 主机只能激活同样运行客户端操作系统的计算机。

如需使用 KMS，KMS 主机需要一个密钥向 Microsoft 激活（或验证）该 KMS 主机。 此密钥有时称为 KMS 主机密钥，但它的正式名称为 Microsoft 客户特定批量许可密钥 (CSVLK)。 可以在以下协议的批量许可服务中心 的“产品密钥”部分获取此密钥：开放式、开放式价值、精选、企业和服务提供者许可证。 也可以通过联系本地 Microsoft 激活中心 获得帮助。

操作要求

KMS 能够激活物理和虚拟计算机，但是要使用 KMS 激活，网络中计算机的数量必须达到最低要求（称为激活阈值）。 KMS 客户端只有在达到此阈值之后才会激活。 为确保达到激活阈值，KMS 主机会计算网络中请求激活的计算机的数量。

KMS 主机计算最近的连接数。 当客户端或服务器联系 KMS 主机时，主机将计算机 ID 添加到其计数，然后在其响应中返回当前的计数值。 计数足够高时将激活客户端或服务器。 计数为 25 或更高时将激活客户端。 计数为 5 或更高时，将激活服务器和批量版 Microsoft Office 产品。 KMS 只对过去 30 天内的唯一连接计数，且仅存储 50 个最新联系人。

KMS 激活的有效期为 180 天，这一时期称为激活有效期间隔。 要保持激活状态，KMS 客户端至少要每 180 天连接一次 KMS 主机，以续订他们的激活。 默认情况下，KMS 客户端计算机会每隔7 天尝试一次激活续订。 客户端的激活已续订之后，激活有效期将重新开始计算。

一台 KMS 主机能够支持无限数量的 KMS 客户端。 如果客户端数量超过 50 个，我们建议至少准备两台 KMS 主机，以防某一台 KMS 主机不可用。 大多数组织单位运行两台 KMS 主机可以满足整个基础结构的需求。

第一个 KMS 主机激活之后，第一个主机上使用的 CSVLK 最多可用来激活网络上的另外 5 台 KMS 主机（总共 6 台）。 KMS 主机激活之后，管理员最多可使用同一密钥将同一台主机重新激活 9 次。

如果组织需要 6 个以上的 KMS 主机，可以为组织的 CSVLK 请求额外的激活。 例如，如果一个批量许可协议下有 10 个物理位置，并且希望每个位置都有一个本地 KMS 主机。 如需请求此例外，请联系当地的 Microsoft 激活中心。

默认情况下，运行 Windows Server 和 Windows 客户端批量许可版本的计算机是无需额外配置的 KMS 客户端。

如果要将计算机从 KMS 主机、MAK 或零售版 Windows 转换为 KMS 客户端，请安装适用的 KMS 客户端安装密钥。 有关详细信息，请参阅 KMS 客户端安装密钥。

网络要求

KMS 激活要求 TCP/IP 连接。 KMS 主机可客户端默认配置使用域名系统 (DNS)。 KMS 主机使用 DNS 动态更新来自动发布 KMS 客户端查找并连接主机所需的信息。 您可以接收这些默认设置；如果有特殊的网络和安全配置要求，则可手动配置 KMS 主机和客户端。

默认情况下，KMS 主机配置为在端口 1688 上使用 TCP。

激活版本

下表总结了包括 Windows Server 和 Windows 客户端设备在内的网络的 KMS 主机和客户端版本。

> **重要**
>
> 可能需要对 KMS 服务器进行 Windows 更新以便支持对较新的客户端进行激活。 如果收到激活错误，请检查你是否具有在此表下面列出的相应更新。

Windows Server 2025

展开表

CSVLK 组	CSVLK 可以托管在	Windows 版本由此 KMS 主机激活
适用于 Windows Server 2025 的批量许可证	• Windows Server 2025	• Windows Server 2025（所有版本）

CSVLK 组	CSVLK 可以 托管在	Windows 版本 由此 KMS 主机激活
	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Windows Server 2022（所有版本） • Windows Server 半年频道 • Windows Server 2019（所有版本） • Windows Server 2016（所有版本） • Windows Server 2012 R2（所有版本） • Windows Server 2012（所有版本） • Windows Server 2008 R2（所有版本） • Windows Server 2008（所有版本） • Windows 11 企业版/企业版 N • Windows 11 专业版/专业版 N • 用于工作站的 Windows 11 专业版/用于工作站的专业版 N • Windows 11 教育版/教育版 N • Windows 10 企业版 LTSC/LTSC N/LTSB • Windows 10 企业版/企业版 N • Windows 10 专业版/专业版 N • 用于工作站的 Windows 10 专业版/用于工作站的专业版 N • Windows 10 教育版/教育版 N • Windows 8.1 企业版 • Windows 8.1 专业版 • Windows 7 企业版 • Windows 7 专业版

KMS 主机需要的更新

你可能需要安装以下更新中的一个或多个，具体取决于 KMS 主机运行的操作系统以及你想要激活的操作系统。 如果想要激活比正在运行的 KMS 主机更高的 Windows 版本，则这是需要的。

备注

以下列出的更新是最低要求。 如果更新的累积更新或月度汇总作为选项列出，请为操作系统安装最新可用版本，以获得额外安全性和其他修补程序。

展开表

KMS 主机 OS 版本	要激活的 KMS 客户端 OS 版本	所需的更新
Windows Server 2022	- Windows Server 2025	2024 年 2 月 13 日 - KB5034765 或更高版本的累积更新
Windows Server 2019	- Windows Server 2025 - Windows Server 2022	2024 年 2 月 13 日 - KB5034768 或更高版本的累积更新 2021 年 6 月 8 日 - KB5003646 或更新版本的累积更新
Windows Server 2016	- Windows Server 2022 - Windows Server 2019	2021 年 6 月 8 日 - KB5003638 或更新版本的累积更新
Windows Server 2016	- Windows Server 2019	2018 年 12 月 3 日 - KB4478877 或更新版本的累积更新
Windows Server 2012 R2	- Windows Server 2019 - Windows Server 2016 - Windows 10	2018 年 11 月 27 日 - KB4467695（每月汇总预览版） 或更高版本的每月汇总
Windows Server 2012 R2	- Windows Server 2016 - Windows 10	适用于 Windows 8.1 和 Windows Server 2012 R2 的 2016 年 7 月更新汇总 或更新的每月汇总
Windows Server 2012	- Windows Server 2016 - Windows Server 2012 R2 - Windows 10	适用于 Windows Server 2012 的 2016 年 7 月更新汇总 或更新的每月汇总
Windows Server 2008 R2	- Windows Server 2012 R2 - Windows Server 2012 - Windows 10	使 Windows 7 和 Windows Server 2008 R2 KMS 主机能够激活 Windows 10 的更新
Windows 8.1	- Windows 10	适用于 Windows 8.1 和 Windows Server 2012 R2 的 2016 年 7 月更新汇总 或更新的每月汇总

KMS 主机 OS 版本	要激活的 KMS 客户端 OS 版本	所需的更新
Windows 7	- Windows 10	使 Windows 7 和 Windows Server 2008 R2 KMS 主机能够激活 Windows 10 的更新

反馈

此页面是否有帮助? 是 否

Server Core 应用兼容性按需功能

项目 • 2023/03/21

Server Core 应用兼容性按需功能 (FOD) 是一个可选功能包，从 Windows Server 2019 开始，可随时将其添加到 Windows Server 安装的服务器核心安装中。

有关其他按需功能的详细信息，请参阅按需功能。

为何要安装应用兼容性 FOD?

Server Core 的应用兼容性按需功能 (FOD) 包含带桌面体验的 Server 安装选项的一部分二进制文件和包，因此显著提高了应用兼容性。 此可选包在单独的 ISO 中提供，或者通过 Windows 更新提供，但只能添加到服务器核心安装和映像。

应用兼容性 FOD 提供的两项主要价值为：

- 提高 Server Core 对已上市或已部署的服务器应用程序的兼容性。
- 帮助提供 OS 组件，并提高重要故障排除和调试方案中使用的软件工具的应用兼容性。

作为 Server Core 应用兼容性 FOD 一部分提供的操作系统组件包括：

- Microsoft 管理控制台 (mmc.exe)
- 事件查看器 (Eventvwr.msc)
- 性能监视器 (PerfMon.exe)
- 资源监视器 (Resmon.exe)
- 设备管理器 (Devmgmt.msc)
- 文件资源管理器 (Explorer.exe)
- Windows PowerShell (Powershell_ISE.exe)
- 磁盘管理 (Diskmgmt.msc)
- 故障转移群集管理器 (CluAdmin.msc)

> **备注**
>
> 故障转移群集管理器要求首先添加故障转移群集 Windows Server 功能，此操作可以通过从提升的 PowerShell 会话运行以下命令来完成：

PowerShell

```
Install-WindowsFeature -Name Failover-Clustering -
IncludeManagementTools
```

从 Windows Server 2022 开始，也提供以下组件（使用相同版本的应用兼容性 FOD 时）：

- Hyper-V 管理器 (virtmgmt.msc)
- 任务计划程序 (taskschd.msc)

安装 App Compatibility Feature on Demand

> ⓘ **重要**
>
> - 只能在 Server Core 上安装应用兼容性 FOD。 请勿尝试将 Server Core App Compatibility FOD 添加到具有桌面体验安装选项的服务器。
> - 对于运行 Windows Server 2022 的服务器，请确保在安装应用兼容性 FOD 之前已经安装了**适用于基于 x64 的系统 (KB5009608) 的 Microsoft 服务器操作系统版本 21H2 的累积更新预览版 (2022-01)** 或更高版本的累积更新。 可以通过检查操作系统内部版本号是否为 20348.502 或更高版本来验证这一点。 在此之前，如果尝试使用远程桌面协议 (RDP) 连接到服务器，则可能会看到黑屏且连接已断开。

连接到 Internet

1. 如果服务器可以连接到 Windows 更新，请从权限提升的 PowerShell 会话运行以下命令，然后在该命令完成运行后重启 Windows Server：

PowerShell

```
Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0
```

从 Internet 断开连接

1. 如果服务器无法连接到 Windows 更新，请下载 Windows Server 语言和可选功能 ISO 映像文件，并将 ISO 复制到本地网络上的共享文件夹：

- 如果你有批量许可证，则可以从获取操作系统 ISO 映像文件的同一门户中下载 Windows Server 语言和可选功能 ISO 映像文件：批量许可服务中心。
- Windows Server 语言和可选功能 ISO 映像文件还会在 Microsoft 评估中心或 Visual Studio 门户中为订阅者提供。

> **备注**
>
> 语言和可选功能 ISO 映像文件是 Windows Server 2022 的新增功能。 早期版本的 Windows Server 使用按需功能 (FOD) ISO。

2. 在已连接到本地网络、要将 App Compatibility FOD 添加到的服务器核心计算机上使用管理员帐户登录。

装载 FOD ISO

1. 使用 PowerShell 中的 `New-PSDrive`、命令提示符中的 `net use` 或某种其他方法连接到 FOD ISO 的位置。 例如，在提升的 PowerShell 会话中运行以下命令：

```PowerShell
$credential = Get-Credential

New-PSDrive -Name FODShare -PSProvider FileSystem -Root
"\\server\share" -Credential $credential
```

2. 将 FOD ISO 复制到所选的本地文件夹（复制操作可能需要一些时间）。 用你的文件夹位置和 ISO 文件名编辑下面的变量，并运行以下命令，例如：

```PowerShell
$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"

New-Item -ItemType Directory -Path $isoFolder
Copy-Item -Path "FODShare:\$fodIsoFilename" -Destination $isoFolder -
Verbose
```

3. 使用以下命令装载 FOD ISO：

```PowerShell
$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
```

4. 运行以下命令以获取 FOD ISO 已装载到的驱动器号：

```
PowerShell

$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
```

5. 运行以下命令（具体取决于操作系统版本）：

   对于 Windows Server 2022：

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source
${fodDriveLetter}:\LanguagesAndOptionalFeatures\ -LimitAccess
```

   对于以前版本的 Windows Server：

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source ${fodDriveLetter}:\ -
LimitAccess
```

6. 进度条显示任务完成后，重启操作系统。

选择性地将 Internet Explorer 11 添加到服务器核心

> **备注**
>
> 需要使用 Server Core 应用兼容性 FOD 来添加 Internet Explorer 11，但不需要使用 Internet Explorer 11 来添加 Server Core 应用兼容性 FOD。

> **备注**
>
> 从 Windows Server 2022 开始，尽管可以将 Internet Explorer 11 添加到 Windows Server 的服务器核心安装中，但应改用 **Microsoft Edge**。 Microsoft Edge 内置了 **Internet Explorer 模式**（“IE 模式”），因此你可以直接从 Microsoft Edge 访问基于旧版 Internet Explorer 的网站和应用程序。 有关 Internet Explorer 生命周期策略的信息，请参阅**此处**。

1. 在已添加应用兼容性 FOD 并已在本地复制 FOD 可选包 ISO 的 Server Core 计算机上以管理员身份登录。

2. 使用以下命令装载 FOD ISO。 此步骤假定你已将 FOD ISO 复制到本地。 如果没有，请完成装载 FOD ISO 中的步骤 1 和步骤 2。 命令将从这两个步骤开始执行。 用你的文件夹位置和 ISO 文件名编辑变量，并运行以下命令，例如：

   PowerShell

   ```
   $isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
   $fodIsoFilename = "FOD_ISO_filename.iso"

   $fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
   ```

3. 运行以下命令以获取 FOD ISO 已装载到的驱动器号：

   PowerShell

   ```
   $fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
   ```

4. 运行以下命令（根据你的操作系统版本），使用 `$packagePath` 变量作为 Internet Explorer .cab 文件的路径：

   对于 Windows Server 2022：

   PowerShell

   ```
   $packagePath =
   "${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
   InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

   Add-WindowsPackage -Online -PackagePath $packagePath
   ```

   对于以前版本的 Windows Server：

   PowerShell

   ```
   $packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-
   Optional-Package~31bf3856ad364e35~amd64~~.cab"

   Add-WindowsPackage -Online -PackagePath $packagePath
   ```

5. 进度条显示任务完成后，重启操作系统。

发行说明和建议

> **ⓘ 重要**
>
> - 使用 FoD 安装的包在就地升级到较新的 Windows Server 版本后不会保留。 升级后，必须重新安装它们。
> - 或者，可以将 FoD 包添加到升级介质。 将包添加到升级介质可确保在升级完成后存在任何 FoD 包的新版本。 有关详细信息，请参阅**将功能和可选包添加到脱机 WIM Server Core 映像**部分。

- 安装应用兼容性 FOD 并重新启动服务器后，命令控制台窗口框架颜色将更改为不同的蓝色调。
- 如果同时选择安装 Internet Explorer 11 可选包，不支持双击打开本地保存的 .htm 文件。 但是，可以右键单击并选择“使用 Internet Explorer 打开”，或者可以直接在 Internet Explorer 中选择“文件”>“打开”来打开此类文件。
- 为了进一步使用应用兼容性 FOD 增强 Server Core 的应用兼容性，IIS 管理控制台现已作为一个可选组件添加到 Server Core。 但是，若要使用 IIS 管理控制台，需要先添加应用兼容性 FOD。 IIS 管理控制台依赖于 Microsoft 管理控制台 (mmc.exe)，而后者只能在添加了应用兼容性 FOD 的 Server Core 中使用。 使用 PowerShell cmdlet Install-WindowsFeature 添加 IIS 管理控制台：

  ```
  PowerShell

  Install-WindowsFeature -Name Web-Mgmt-Console
  ```

- 作为一项常规指导，在 Server Core（包含或不包含这些可选包）上安装应用程序时，有时需要使用无提示安装选项和指令。

添加到脱机 WIM Server Core 映像

1. 将语言和可选功能 ISO 以及 Windows Server ISO 映像文件下载到 Windows 计算机上的本地文件夹。 可以在 Windows 台式电脑上完成这些步骤，无需使用 Server Core 安装选项运行 Windows Server。

   - 如果你有批量许可证，则可以从获取操作系统 ISO 映像文件的同一门户中下载 Windows Server 语言和可选功能 ISO 映像文件：批量许可服务中心。
   - Windows Server 语言和可选功能 ISO 映像文件还会在 Microsoft 评估中心或 Visual Studio 门户中为订阅者提供。

   > **ⓘ 备注**

> 语言和可选功能 ISO 映像文件是 Windows Server 2022 的新增功能。 早期版本的 Windows Server 使用按需功能 (FOD) ISO。

2. 通过在权限提升的 PowerShell 会话中运行以下命令，装载语言和可选功能 ISO 和 Windows Server ISO。 用你的文件夹位置和 ISO 文件名编辑变量，并运行以下命令，例如：

```PowerShell
$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"
$wsIsoFilename = "Windows_Server_ISO_filename.iso"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
$wsIso = Mount-DiskImage -ImagePath "$isoFolder\$wsIsoFilename"
```

3. 运行以下命令，获取 FOD ISO 和 Windows Server ISO 已装载到的驱动器号：

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
$wsDriveLetter = ($wsIso | Get-Volume).DriveLetter
```

4. 将 Windows Server ISO 文件的内容复制到本地文件夹，例如 C:\SetupFiles\WindowsServer\Files。 复制操作可能需要一些时间：

```PowerShell
$wsFiles = "C:\SetupFiles\WindowsServer\Files"
New-Item -ItemType Directory -Path $wsFiles

Copy-Item -Path ${wsDriveLetter}:\* -Destination $wsFiles -Recurse
```

5. 使用以下命令获取 install.wim 文件中要修改的映像名称。 将 install.wim 文件的路径添加到 `$installWimPath` 变量（位于 Windows Server ISO 文件的 sources 文件夹内）。 请注意输出中此 install.wim 文件中提供的映像的名称。

```PowerShell
$installWimPath =
"C:\SetupFiles\WindowsServer\Files\sources\install.wim"

Get-WindowsImage -ImagePath $installWimPath
```

6. 使用以下命令（请将示例变量值替换为自己的值，并重复使用前一命令中的 `$installWimPath` 变量），在新文件夹中装载 install.wim 文件。

   - `$wimImageName` - 输入要从上一个命令的输出装载的映像的名称。 此处的示例使用 Windows Server 2022 Datacenter。
   - `$wimMountFolder` - 指定访问 install.wim 文件的内容时要使用的空文件夹。

```
PowerShell

$wimImageName = "Windows Server 2022 Datacenter"
$wimMountFolder = "C:\SetupFiles\WindowsServer\WIM"

New-Item -ItemType Directory -Path $wimMountFolder
Set-ItemProperty -Path $installWimPath -Name IsReadOnly -Value $false
Mount-WindowsImage -ImagePath $installWimPath -Name $wimImageName -Path
$wimMountFolder
```

7. 根据版本使用以下命令（请将示例变量值替换为自己的值）将所需的功能和包添加到装载的 install.wim 映像。

   - `$capabilityName` - 指定要安装的功能（在本例中为“AppCompatibility”功能）的名称。
   - `$packagePath` - 指定要安装的包的路径（在本例中为 Internet Explorer cab 文件）。

   对于 Windows Server 2022：

```
PowerShell

$capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
$packagePath =
"${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
Source "${fodDriveLetter}:\LanguagesAndOptionalFeatures" -LimitAccess
Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
```

   对于以前版本的 Windows Server：

```
PowerShell

$capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
$packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-
Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
```

```
Source "${fodDriveLetter}:\" -LimitAccess
Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
```

8. 使用以下命令（其中使用了前面命令中的 `$wimMountFolder` 变量）卸除映像并将更改提交到 install.wim 文件：

```
PowerShell

Dismount-WindowsImage -Path $wimMountFolder -Save
```

现在，可以在为 Windows Server 安装文件创建的文件夹中运行 setup.exe 来升级服务器（在本示例中，该文件夹为 C:\SetupFiles\WindowsServer\Files）。 现在，此文件夹包含 Windows Server 安装文件及其他功能与可选包。

Windows Server 2022 和 Microsoft 服务器应用程序兼容性

项目 • 2023/07/13

该表罗列支持 Window Server 2022 上安装和功能的 Microsoft 服务器应用程序。 此信息用于快速参考，不用于替代有关单个产品的规格、要求、公告或每个服务器应用程序的常规通信的说明。 请参考每种产品的正式文档以充分了解兼容性和选项。

提示

如果你是要了解有关 Windows Server 与非 Microsoft 应用程序兼容性的详细信息的软件供应商合作伙伴，请访问**商业应用认证门户**。

产品	在服务器核心上受支持	在具有桌面体验的服务器上受支持	Released（已释放）	产品 Web 链接
Azure DevOps Server 2020.1	是*	是	是	Azure DevOps Server 2020.1 发行说明
Configuration Manager（版本 2107）	是的，作为托管客户端和分发点。不是，作为站点服务器。	是的，作为站点服务器/站点系统和托管客户端。	是	对 Windows Server 2022 的支持
Exchange Server 2019 CU12 及更高版本	是	是	是	Exchange Server 可支持性矩阵
Host Integration Server 2020	是	是	是	HIS 2020 - 新增功能、发行说明、系统要求和安装
Microsoft 365 应用	否	是	是	Windows 和 Office 配置支持矩阵
Office Online Server	否	是	是	规划 Office Online Server
Project Server 2019	否	是	是	Project Server 2019 的软件要求- Project Server

产品	在服务器核心上受支持	在具有桌面体验的服务器上受支持	Released（已释放）	产品 Web 链接
Project Server 订阅版	是	是	是	Project Server 订阅版的软件要求
SharePoint Server 2019	否	是	是	SharePoint Server 2019 的硬件和软件要求
SharePoint Server 订阅版	是	是	是	SharePoint Server 订阅版的系统要求
SQL Server 2017	是*	是	是	安装 SQL Server 2017 的硬件和软件要求
SQL Server 2019	是*	是	是	安装 SQL Server 2019 的硬件和软件要求
System Center Data Protection Manager 2019	是的，作为备份工作负载。 不是，作为 DPM 服务器。	是的，作为备份工作负载。 不是，作为 DPM 服务器。	是	针对 System Center Data Protection Manager 准备环境
System Center Data Protection Manager 2022	是*	是	是	针对 System Center Data Protection Manager 准备环境
System Center Operations Manager 2019	是的，作为代理。 不是，作为管理服务器**	是的，作为代理。 不是，作为管理服务器**。	是	System Center Operations Manager 的系统要求
System Center Operations Manager 2022	是*	是	是	System Center Operations Manager 的系统要求
System Center Virtual Machine Manager 2022	是*	是	是	System Center Virtual Machine Manager 系统要求

* 可能存在限制或可能需要服务器核心应用兼容性按需功能 (FOD)。 有关详细信息，请参阅特定产品或按需功能文档。

** 请参阅产品 Web 链接

Windows Server 2019 和 Microsoft 服务器应用程序兼容性

项目 • 2023/08/30

该表罗列支持 Window Server 2019 上安装和功能的 Microsoft 服务器应用程序。 此信息用于快速参考，不用于替代有关单个产品的规格、要求、公告或每个服务器应用程序的常规通信的说明。 请参考每种产品的正式文档以充分了解兼容性和选项。

> **提示**
>
> 如果你是要了解有关 Windows Server 与非 Microsoft 应用程序兼容性的详细信息的软件供应商合作伙伴，请访问**商业应用认证门户**。

产品	在服务器核心上受支持	在具有桌面体验的服务器上受支持	Released（已释放）	产品 Web 链接
Azure DevOps Server 2019	是*	是	是	Azure DevOps Server 2019
Azure DevOps Server 2020	是*	是	是	Azure DevOps Server 2020
Configuration Manager（版本 1806）	“是”表示作为托管客户端，“否”表示作为站点服务器	“是”表示作为托管客户端，“否”表示作为站点服务器	是	Configuration Manager Current Branch 1806 版中的新增功能
Exchange Server 2019	是	是	是	Exchange Server 系统要求
Host Integration Server 2016，CU3	是	是	是	Host Integration Server 系统要求
Office Online Server	否	是	是	规划 Office Online Server
Project Server 2016	否	是	是	Project Server 2016 的软件要求
Project Server 2019	否	是	是	Project Server 2019 的软件要求
Project Server 订阅版	是	是	是	Project Server 订阅版的软件要求

产品	在服务器核心上受支持	在具有桌面体验的服务器上受支持	Released（已释放）	产品 Web 链接
SharePoint Server 2016	否	是	是	SharePoint Server 2016 的硬件和软件要求
SharePoint Server 2019	否	是	是	SharePoint Server 2019 的硬件和软件要求
SharePoint Server 订阅版	是	是	是	SharePoint Server 订阅版的系统要求
Skype for Business 2019	否	是	是	为 Skype for Business Server 安装系统必备
SQL Server 2014	是*	是	是	安装 SQL Server 2014 的硬件和软件要求
SQL Server 2016	是*	是	是	安装 SQL Server 2016 的硬件和软件要求
SQL Server 2017	是*	是	是	安装 SQL Server 2017 的硬件和软件要求
SQL Server 2019	是*	是	是	安装 SQL Server 2019 的硬件和软件要求
System Center Data Protection Manager 2019	否	是	是	针对 System Center Data Protection Manager 准备环境
System Center Operations Manager 2019	是*	是	是	System Center Operations Manager 的系统要求
System Center Virtual Machine Manager 2019	是*	是	是	System Center Virtual Machine Manager 系统要求

*可能存在限制或可能需要服务器核心应用兼容性按需功能 (FOD)。 请参阅特定产品或 FOD 文档。

Windows Server 2016 和 Microsoft 服务器应用程序兼容性

项目 • 2023/08/30

该表罗列支持 Window Server 2016 上安装和功能的 Microsoft 服务器应用程序。 此信息用于快速参考，不用于替代有关单个产品的规格、要求、公告或每个服务器应用程序的常规通信的说明。 请参考每种产品的正式文档以充分了解兼容性和选项。

> **提示**
>
> 如果你是要了解有关 Windows Server 与非 Microsoft 应用程序兼容性的详细信息的软件供应商合作伙伴，请访问**商业应用认证门户**。

产品	Released（已释放）	产品 Web 链接
BizTalk Server 2016	是	Microsoft BizTalk Server
Configuration Manager（版本 1606）	是	Configuration Manager 1606 版中的新增功能
Exchange Server 2016	是	Exchange 2016 的更新
Host Integration Server 2016	是	HIS 2016 中的新增功能
Office Online Server	是	规划 Office Online Server
Project Server 2016	是	Project Server 2016 的软件要求
Project Server 2019	是	Project Server 2019 的软件要求
SharePoint Server 2016	是	SharePoint Server 2016 的硬件和软件要求
SharePoint Server 2019	是	SharePoint Server 2019 的硬件和软件要求
Skype for Business Server 2015	是	如何在 Windows Server 2016 上安装 Skype for Business Server 2015
SQL Server 2012	是	安装 SQL Server 2012 的硬件和软件要求
SQL Server 2014	是	安装 SQL Server 2014 的硬件和软件要求
SQL Server 2016	是	SQL Server 2016
System Center Virtual Machine Manager 2016	是	System Center 中的新增功能

产品	Released（已释放）	产品 Web 链接
System Center Operations Manager 2016	是	System Center 中的新增功能
System Center Data Protection Manager 2016	是	System Center 中的新增功能
Visual Studio Team Foundation Server 2017	是	Team Foundation Server 2017

Windows Server 的 Azure 混合权益

项目 • 2024/08/01

Azure 混合权益使商业客户能够使用其合格的本地许可证，从而以较低的成本在 Azure 上获取 Windows 虚拟机 (VM)。 本文重点介绍使用合格的 Windows Server 许可证在 Azure、Azure Stack HCI 和 Azure Kubernetes 服务 (AKS) 混合部署中节省 Windows Server VM 成本的好处。

有关其他 Azure 混合权益（例如 Microsoft SQL Server），请参阅 Azure 混合权益。

如何才能获得 Azure 混合权益?

要有资格获得适用于 Windows Server 的 Azure 混合权益，你需要有效软件保障或合格订阅许可证的合适计划提供的 Windows Server 本地核心许可证。 软件保障和合格的订阅许可证仅作为某些商业许可协议的一部分提供。 要详细了解商业许可，请参阅 Microsoft 许可资源。 要详细了解 Windows Server 核心许可证，请参阅 Windows Server 产品许可。

> **重要**
>
> - 使用 Azure 混合权益的工作负荷只能在软件保障或订阅许可证期限内运行。 当软件保障或订阅许可证期限即将到期时，必须续订与软件保障或订阅许可证的协议、禁用混合权益功能或取消预配那些使用 Azure 混合权益的工作负荷。
> - 计划的 Microsoft 产品条款优先于本条款。 有关详细信息，请参阅 **Microsoft Azure 产品条款** 并选择计划以显示条款。

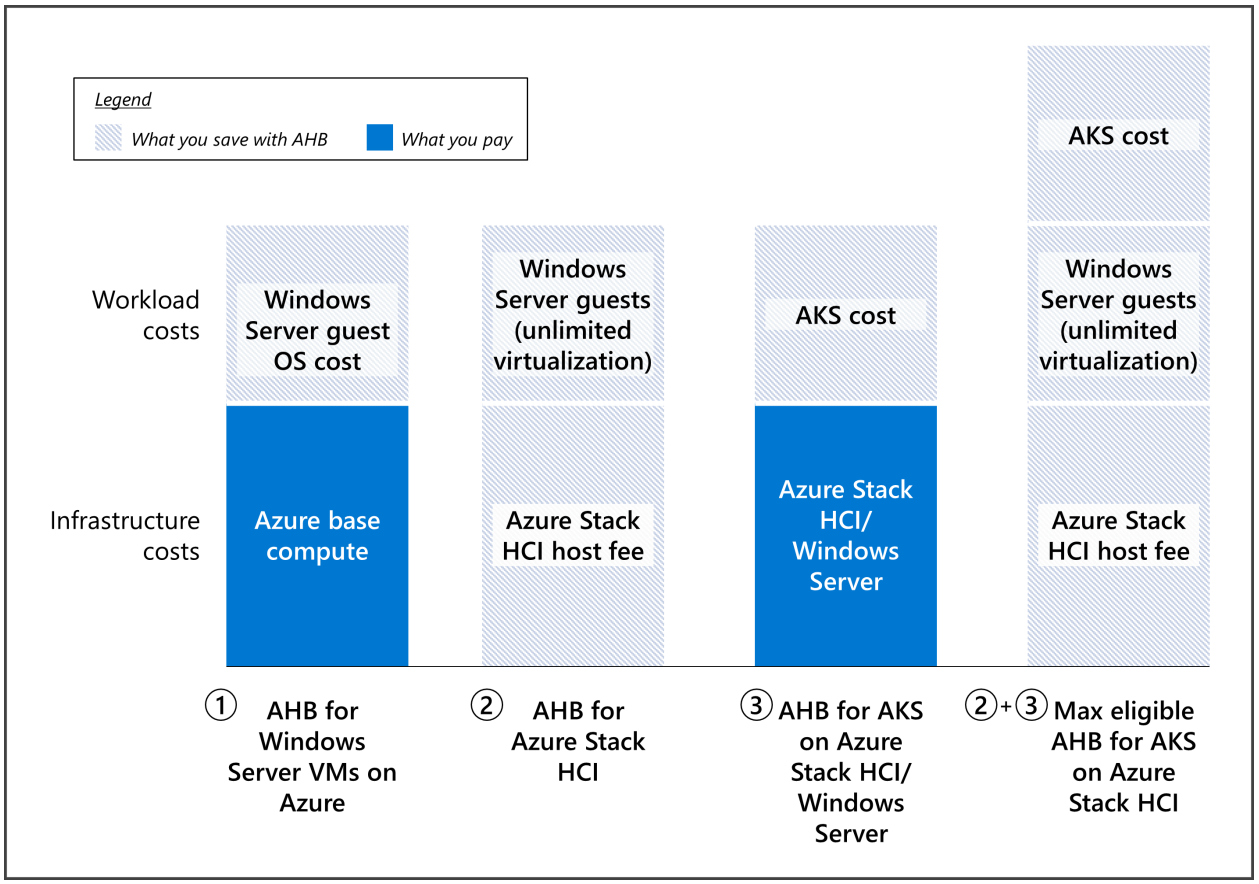
Azure 混合权益包含哪些内容?

如果 Windows Server 的客户通过有效软件保障或合格订阅许可证的适用计划获得许可，则可以使用 Azure 混合权益进一步降低云以及数据中心和边缘位置的成本。

Azure 混合权益可节省以下成本：

- Azure 上的 Windows Server VM：Azure 混合权益涵盖 Windows Server 的许可证，因此你只需支付 VM 的基本计算费用。 基本计算费用等于 VM 的 Linux 费用。
- **Azure Stack HCI**：Azure 混合权益免除 Azure Stack HCI 主机费和 Windows Server 订阅费。 也就是说，免费提供无限的虚拟化权利。 你仍需支付与 Azure Stack HCI 相关的其他成本（例如客户管理的硬件、Azure 服务和工作负荷）。

- **AKS**：在 Windows Server 和 Azure Stack HCI 上运行 AKS 无需额外费用。 你仍需为基本的主机基础结构和 Windows 容器的所有许可证付费，除非你还有资格获得适用于 Azure Stack HCI 的 Azure 混合权益。 拥有适用于 Azure Stack HCI 的 Azure 混合权益后，Azure Stack HCI 主机费和 Windows Server 订阅费可免除。



Azure 混合权益定价

要计算可节省的成本，可使用以下资源：

- **Azure 上的 Windows VM**：Windows 虚拟机定价。 使用 Azure 混合权益节省计算器估算节省的成本，或比较有 Azure 混合权益和没有 Azure 混合权益这两种情况下的 Windows VM 定价。
- **Azure Stack HCI**：Azure Stack HCI 定价。
- **Azure Kubernetes 服务 (AKS)**：Azure Stack HCI 上的 AKS 定价。

获取 Azure 混合权益

选择方案的选项卡。

Azure

按照本部分中的指南获取和维护适用于 Azure 中 Windows VM 的 Azure 混合权益。

许可先决条件

要享有适用于 Azure 中 Windows VM 的 Azure 混合权益，必须满足以下许可先决条件。

许可证类型

- 包含有效软件保障或订阅的 Windows Server Standard。
- 包含有效软件保障或订阅的 Windows Server Datacenter。

许可证数量

每个 VM 至少需要 8 个核心许可证（Datacenter 或 Standard 版本）。 例如，如果运行 4 核实例，则仍然需要 8 个核心许可证。 还可以通过分配与实例核心大小相等的许可证来运行大于 8 个核心的实例。 例如，12 核实例需要 12 个核心许可证。 对于拥有处理器许可证的客户，每个处理器许可证相当于 16 个核心许可证。

使用权利

- **Windows Server Standard 版本：**许可证必须在本地或 Azure 中使用，但不能同时使用。 唯一的例外是一次性的操作，最长 180 天，允许你将相同的工作负荷迁移到 Azure。
- **Windows Server Datacenter 版本：**对于 VM 许可，许可证可无限期在本地和 Azure 中使用。 对于专用主机许可，许可证允许从许可证分配给 Azure 之日起在本地和 Azure 中同时使用 180 天。

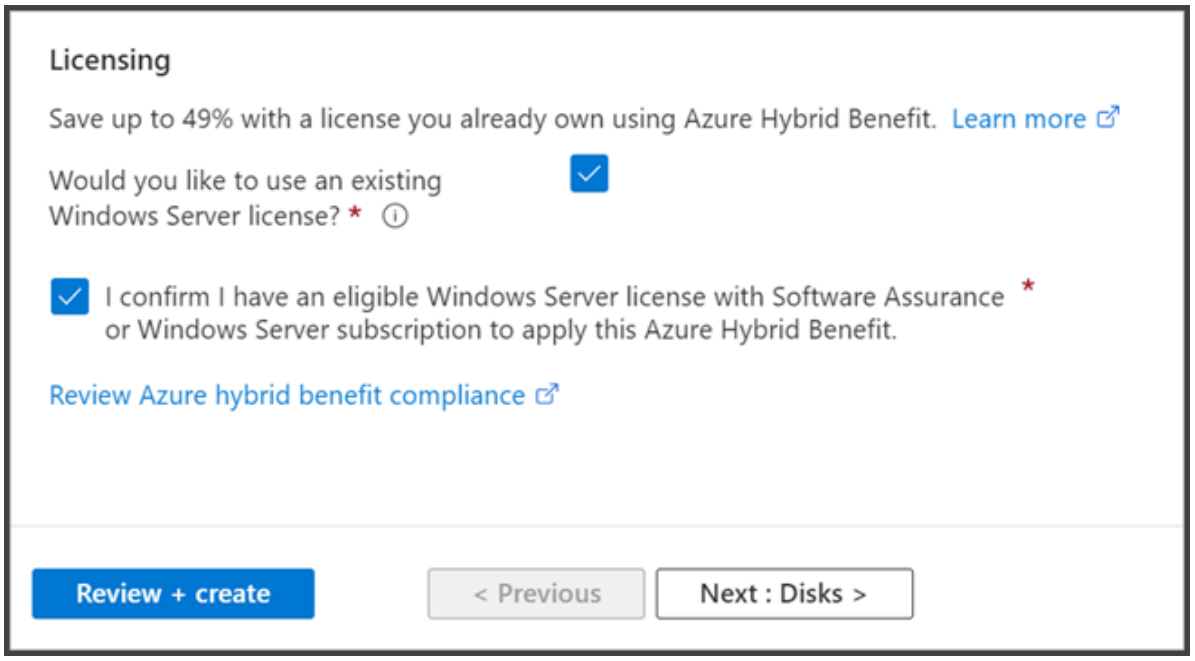
无限制虚拟化

无限制虚拟化权利是指在主机上使用任意数量的 Windows Server VM 的权利。

- **Windows Server Datacenter 版本：**如果为该 Azure 服务器上可用的所有物理核心分配包含有效 SA 或订阅的 Windows Server Datacenter 许可证，则可在 Azure 专用主机上使用任意数量的 Windows Server VM。
- **Windows Server Standard 版本：**无限制虚拟化权利不可用。

如何应用适用于 Azure 中 Windows VM 的 Azure 混合权益

要了解如何使用 Azure 混合权益在 Azure 中部署 Windows Server VM，请按照探索适用于 Windows VM 的 Azure 混合权益中的步骤操作。 为 Windows Server VM 激活 Azure 混合权益的一种方法是在创建 VM 期间选中“许可”下的框，如以下屏幕截图中所示。



如何保持符合性

如果将 Azure 混合权益应用于 Windows Server VM，请在激活此权益之前验证符合条件的许可证数和软件保障（或订阅）覆盖期。 按照上述指南确保使用此权益部署正确数量的 Windows Server VM。

如果已使用 Azure 混合权益运行 Windows Server VM，请清点正在运行的设备数量，并根据你的软件保障或订阅许可证检查此数字。 可联系 Microsoft 许可专家来验证你的软件保障许可情况。

要查看和统计 Azure 订阅中使用 Azure 混合权益部署的所有 VM，请按照探索适用于 Windows VM 的 Azure 混合权益中的步骤列出所有 VM 和虚拟机规模集。

还可查看 Microsoft Azure 账单，确定正运行多少个使用适用于 Windows Server 的 Azure 混合权益的 VM。 有关使用该权益的实例数的信息显示在“其他信息”下方：

JSON


```
"
{"ImageType":"WindowsServerBYOL","ServiceType":"Standard_A1","VMName":""
```

```
,"UsageType":"ComputeHR"}"
```

计费不是实时进行的。 从使用 Azure 混合权益激活 Windows Server VM 到该 VM 显示在帐单上，预计会有几个小时的延迟。

要全面了解许可情况，请清点每个 Azure 订阅。 确认是否已获得使用 Azure 混合权益运行的 Windows Server VM 的完全许可。 无需执行任何进一步操作。

定期进行清点，以确保你使用的任何许可证权益是你有权获得的。 定期清点有助于降低成本，同时确保你始终拥有足够的许可证来覆盖你使用 Azure 混合权益部署的 Windows Server VM。

如果没有足够的合格 Windows Server 许可证用于已部署的 VM，你有三种选择：

- 通过商业许可协议购买软件保障或订阅涵盖的额外 Windows Server 许可证。
- 禁用某些 VM 的 Azure 混合权益，并按常规 Azure 每小时费率购买它们。
- 解除分配某些 VM。

> ⓘ **备注**
>
> Microsoft 保留随时审核客户以验证 Azure 混合权益使用资格的权利。

常见问题解答：Azure 混合权益

哪些区域提供 Azure 混合权益?

Azure 混合权益在所有 Azure 区域和主权云中提供。

如果我的软件保障或订阅到期，我的权益会发生什么变化?

要使用这些权益，软件保障或合格订阅必须有效。 如果选择在软件保障或订阅过期时不续订软件保障或订阅，则需要从 Azure 门户中的资源中删除权益。

什么是软件保障?

软件保障是一项全面的批量许可计划。 软件保障只能通过批量许可提供，并在购买或续订批量许可协议时购买。 它随附在一些协议中，是与其他协议一起提供的可选购买项。 软件保障权益包括新产品版本权限、支持、许可证移动权以及一套独特的技术和服务，以最大限度地利用 IT 投资。

有关批量许可的信息，请参阅 Microsoft 许可。 要详细了解软件保障权益以及每个权益如何帮助满足业务需求，请参阅软件保障权益。

什么是订阅许可证?

订阅许可证是仅在订阅期限内运行软件的许可证。 订阅许可证不包括运行软件的永久权限。

客户如何获得软件保障?

可通过批量许可购买软件保障。 软件保障权益在批量许可服务中心 (VLSC) 中激活。 如果你的组织拥有 Microsoft 产品和服务协议 (MPSA)，则可通过业务中心轻松管理软件保障权益。

另请参阅

- Azure 混合权益产品页
- 探索 Windows VM 的 Azure 混合权益
- Azure Stack HCI 的 Azure 混合权益

反馈

此页面是否有帮助? 是 否

虚拟机的热补丁

项目 • 2024/11/02 • 适用于: ✅ Windows Server 2025, ✅ Windows Server 2022

热修补是在 Windows Server 上安装 OS 安全更新的一种方法，无需重启计算机。 热修补修补正在运行的进程的内存中代码，而无需重启进程。 热修补还提供以下优势：

- 二进制文件减少意味着更新的安装速度更快，消耗的磁盘和 CPU 资源更少。
- 工作负荷影响较低，不需要重启计算机。
- 更好的保护，因为 Hotpatch 更新包的范围限定为 Windows 安全更新，安装速度更快，无需重启计算机。
- 减少暴露于安全风险和更换窗口的时间，并使用 Azure 更新管理器简化补丁编排。

支持的平台

Azure 和 Azure Stack HCI 虚拟机

下表列出了支持 Azure 上 Windows Server 2022 和 Windows Server 2025 热修补的发布者、OS 产品/服务和 SKU 的确切组合。 使用这些组合在 Azure Stack HCI 上创建的虚拟机（VM）也支持热修补。

> **备注**
>
> 不支持 Windows Server 容器基础映像、自定义映像或任何其他发布者、套餐和 SKU 组合。

展开表

发布者	OS 产品/服务	SKU
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core-smalldisk
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch-smalldisk
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-smalldisk

发布者	OS 产品/服务	SKU
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-Core-smalldisk

有关可用映像的详细信息，请参阅 Azure 市场 上的 Windows Server。

连接 Azure Arc 的计算机（预览版）

> **重要**
>
> 已启用 Azure Arc 的 Hotpatch 目前以预览版提供。 有关 beta 版本、预览版或尚未正式发布的版本的 Azure 功能所适用的法律条款，请参阅 **Microsoft Azure 预览版的补充使用条款**。

如果在 Azure Arc 门户中启用该功能，则连接 Azure Arc 的 Windows Server 2025 计算机可以接收 Hotpatche。 若要开始使用已启用 Azure Arc 的 Hotpatch，请使用以下版本之一将 Azure Arc 连接到计算机：

- Windows Server 2025 Datacenter Edition
- Windows Server 2025 标准版

热补丁的工作方式

Hotpatch 首先使用 Windows Server 的当前累积更新建立基线。 每三个月，基线会定期使用最新的累积更新进行刷新。 然后，在累积更新之后的两个月内收到 Hotpatch 版本。 例如，如果 1 月是累积更新，则 2 月和 3 月会有热修补版本。 有关 Hotpatch 发行计划的详细信息，请参阅 适用于 Windows Server 2022 的 Azure Automanage 中的 Hotpatch 发行说明。

有两种类型的基线：计划内基线和计划外基线。

- **计划的基线** 按常规节奏发布，在两者之间发布 Hotpatch 版本。 计划基线包括当月可比较的最新累积更新中的所有更新，并要求重启计算机。
  - 例如，计划的一年发布期可能包括日历年中的四个计划基线版本和 8 个 Hotpatch 版本。
- **计划外的重要更新（如零日修复）期间会发布计划外基线**，当该特定更新无法作为热修补发布时。 当计划外基线发布时，热修补版本将替换为该月的计划外基线。 计

划外基线还包括当月可比较的最新累积更新中的所有更新，因此需要重新启动计算机。
    - 由于这些事件是计划外事件，因此开发人员无法提前预测计划外基线。

热修补更新不需要重启计算机。 由于 Hotpatche 修补正在运行的进程的内存中代码，而无需重启它们，因此应用程序不会受到影响。 这种缺少重启不会影响修补程序本身的性能或功能影响。

支持的更新

热修补涵盖Windows 安全更新，并与在常规非热修补 Windows 更新通道中颁发的安全更新内容保持奇偶校验。

在受支持的 Windows Server 版本上启用 Hotpatch 时，需要考虑一些重要事项。 仍需重启计算机以安装热修补程序中未包含的更新。 安装新基线后，还需要定期重启。 重启可使 VM 与最新累积更新中包含的非安全修补程序保持同步。

以下修补程序当前不包括在 Hotpatch 程序中，并要求你在 Hotpatch 发布月份期间更新计算机：

- 适用于 Windows 的非安全更新
- .NET 更新
- 非 Windows 更新，例如驱动程序、固件更新等。

补丁编排过程

热修补是Windows 更新和典型管理过程的扩展。 但是，Hotpatch 用于修补程序管理的工具类型因所使用的平台而异。

Azure

- 使用受支持的 Windows Server 映像 在 Azure 中创建的 VM 默认已启用自动 VM 来宾修补 。
- 热修补会自动下载并应用分类为“严重”或“安全性”的修补程序。
- 热修补在 VM 时区的非高峰时段应用修补程序。
- Azure 会为你管理修补程序，并根据 可用性优先原则应用修补程序。
- Azure 通过平台运行状况信号监视 VM 运行状况，以检测修补故障。

> **备注**
>
> 无法使用热补丁在 Azure Edition 映像上创建具有统一编排的 VM 规模集 (VMSS)。 若要详细了解规模集统一编排支持哪些功能，请参阅**灵活、统一和可用性集的比较**。

Azure Stack HCI

Azure Stack HCI 可以使用以下工具协调 VM 的热修补更新：

- 组策略配置Windows 更新客户端设置。
- SCONFIG 为 Server Core 配置Windows 更新客户端设置。
- 第三方修补程序管理解决方案。

已连接 Azure Arc 的计算机

连接到 Azure Arc 的计算机可以使用以下工具使用热修补更新：

- Azure 更新管理器
- 组策略配置Windows 更新客户端设置。
- SCONFIG 为 Server Core 配置Windows 更新客户端设置。
- 第三方修补程序管理解决方案。

有关热修补使用的工具的详细信息，请查看我们的 Azure 更新管理器 文档。

了解 Azure 中 VM 的补丁状态

若要查看 VM 的修补程序状态，请在Azure 门户中打开 VM 的“概述”页。 在此处，在“操作”**下**，选择“**更新**”。 建议的更新**下**应会显示修补程序状态和最近安装的修补程序。

在 “**建议的更新** ”页中，可以看到 VM 的热修补状态，以及 VM 是否有可用的修补程序。 正如我们在 Hotpatch 的工作原理中所述，自动 VM 来宾修补会自动在 VM 上安装所有关键和安全修补程序。

这两个类别之外的修补程序不会自动安装，而是作为可用修补程序列表显示在 “**更新符合性** ”选项卡中。 还可以查看 “**更新历史记录** ”选项卡，查看过去 30 天内 VM 上更新部署的修补程序安装详细信息。

自动 VM 来宾修补定期运行可用修补程序的评估，可在“ **更新** ”选项卡中查看这些修补程序。可以通过选择“ **立即** 评估”按钮手动启动评估。 还可以通过选择“立即**安装更新**”按钮按需安装修补程序。 通过此选项，可以选择是在特定修补程序分类下安装所有更新，还是通过提供知识库文章列表来包括或排除各个更新。 但是，请记住，手动安装的修补程序不遵循可用性优先原则，并且可能需要重启 VM。

还可以通过在 PowerShell 中运行 Get-HotFix cmdlet 或通过在桌面体验中查看“设置”**菜单来查看**已安装的修补程序。

对热修补的回滚支持

热修补更新不支持自动回滚。 如果在更新期间或之后遇到问题，则必须卸载最新更新并安装最后一个功能基线更新。 此过程要求重启 VM。

后续步骤

- 自动虚拟机来宾修补
- 为从 ISO 生成的 Azure Edition 虚拟机启用热补丁
- Azure 更新管理
- 如何预览适用于 WIndows Server 2025 的 Azure Arc 连接的热修补

反馈

此页面是否有帮助? 是 否

什么是安全核心服务器?

项目 • 2024/11/02 •

适用于: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

安全核心是提供内置硬件、固件、驱动程序和操作系统安全功能的功能集合。 安全核心系统提供的保护在操作系统启动之前开始，并在运行时继续。 安全核心服务器旨在为关键数据和应用程序提供安全平台。

安全核心服务器建立在三项关键的安全要素之上：

- 创建硬件支持的信任根。
- 防范固件级别攻击。
- 防止 OS 执行未经验证的代码。

是什么造就了安全核心服务器

通过 Microsoft 与电脑制造合作伙伴之间的深入协作，安全核心计划始于 Windows 电脑，提供了有史以来最高级的 Windows 安全性。 Microsoft 进一步扩大了与服务器制造合作伙伴的合作关系，帮助确保 Windows Server 提供安全的操作系统环境。

Windows Server 与硬件紧密集成，提供更高级别的安全性：

- 建议的基线：所有系统的建议最低基准，以使用 TPM 2.0 为硬件信任根和安全启动提供基本的系统完整性。 Windows Server 硬件认证需要 TPM2.0 和安全启动。 若要了解详细信息，请参阅 Microsoft 提高下一个主要 Windows Server 版本的安全标准
- 安全核心服务器：建议用于需要更高级别的保证的系统和行业。 安全核心服务器建立在先前的功能之上，并使用高级处理器功能提供保护，以防范固件攻击。

下表显示了如何使用每个安全概念和功能来创建安全核心服务器。

展开表

概念	功能	要求	建议的基线	安全核心服务器
创建硬件支持的信任根				
	安全启动	默认情况下，在统一可扩展固件接口 (UEFI) BIOS 中启用安全启动。		
	可信平台模块 (TPM) 2.0	满足针对受信任的计算组 (TCG) 规范的最新 Microsoft 要求。		
	已针对 Windows Server 认证	表示服务器系统满足 Microsoft 对于安全性、可靠性和可管理性的最高技术标准。		
	启动 DMA 保护	在具有输入/输出内存管理单元 (IOMMU) 的设备上支持。 例如 Intel VT-D 或 AMD-Vi。		
防范固件级别攻击				
	System Guard 安全启动	在具有与动态可信度量根 (DRTM) 兼容的 Intel 和 AMD 硬件的操作系统中启用。		
防止 OS 执行未经验证的代码				
	基于虚拟化的安全 (VBS)	需要 Windows 虚拟机监控程序，该虚拟机监控程序仅在具有虚拟化扩展（包括 Intel VT-X 和 AMD-v）的 64 位处理器上受支持。		
	虚拟机监控程序增强的代码完整性 (HVCI)	与虚拟机监控程序代码完整性 (HVCI) 兼容的驱动程序以及 VBS 要求。		

创建硬件支持的信任根

UEFI 安全启动是一种安全标准，它通过验证系统启动组件来保护服务器免受恶意 Rootkit 的侵害。 安全启动验证受信任的作者是否已对 UEFI 固件驱动程序和应用程序进行数字签名。 服务器启动时，固件会检查每个启动组件的签名，包括固件驱动程序和 OS。 如果签名有效，则服务器将会启动，而固件会将控制权转递给 OS。

若要详细了解启动过程，请参阅保护 Windows 启动过程。

TPM 2.0 为敏感密钥和数据提供硬件支持的安全存储。 在启动过程中加载的每个组件都会被衡量，并且启动结果会存储在 TPM 中。 通过验证硬件信任根，它提升了 BitLocker 等功能所提供的保护，BitLocker 使用 TPM 2.0，有助于创建基于证明的工作流。 这些基于证明的工作流可以合并到零信任安全策略中。

详细了解受信任的平台模块以及 Windows 如何使用 TPM。

除了安全启动和 TPM 2.0，Windows Server 安全核心还在具有输入/输出内存管理单元 (IOMMU) 的兼容处理器上使用启动 DMA 保护。 例如 Intel VT-D 或 AMD-Vi。 使用启动 DMA 保护，系统在启动期间和操作系统运行时期间可以免受直接内存访问 (DMA) 攻击。

防范固件级别攻击

鉴于固件在操作系统下运行，终结点保护和检测解决方案通常对固件的可见性有限。 固件具有比操作系统和虚拟机监控程序内核更高的访问和特权级别，使其成为攻击者的诱人目标。 针对固件的攻击会破坏操作系统实施的其他安全措施，使得识别系统或用户何时遭到入侵变得更加困难。

从 Windows Server 2022 开始，System Guard 安全启动使用 AMD 和 Intel 的硬件功能保护启动过程免受固件攻击。 借助对动态可信度量根 (DRTM) 技术的处理器支持，安全核心服务器将固件置于硬件支持的沙盒中，有助于限制高特权固件代码中漏洞的影响。 System Guard 使用内置于兼容处理器中的 DRTM 功能来启动操作系统，确保系统使用经过验证的代码启动到受信任的状态。

防止 OS 执行未经验证的代码

安全核心服务器使用基于虚拟化的安全性 (VBS) 和虚拟机监控程序保护的代码完整性 (HVCI) 来创建安全的内存区域，并将其与普通操作系统隔离开来。 VBS 使用 Windows 虚拟机监控程序创建虚拟安全模式 (VSM)，以便在操作系统中提供安全边界，可用于其他安全解决方案。

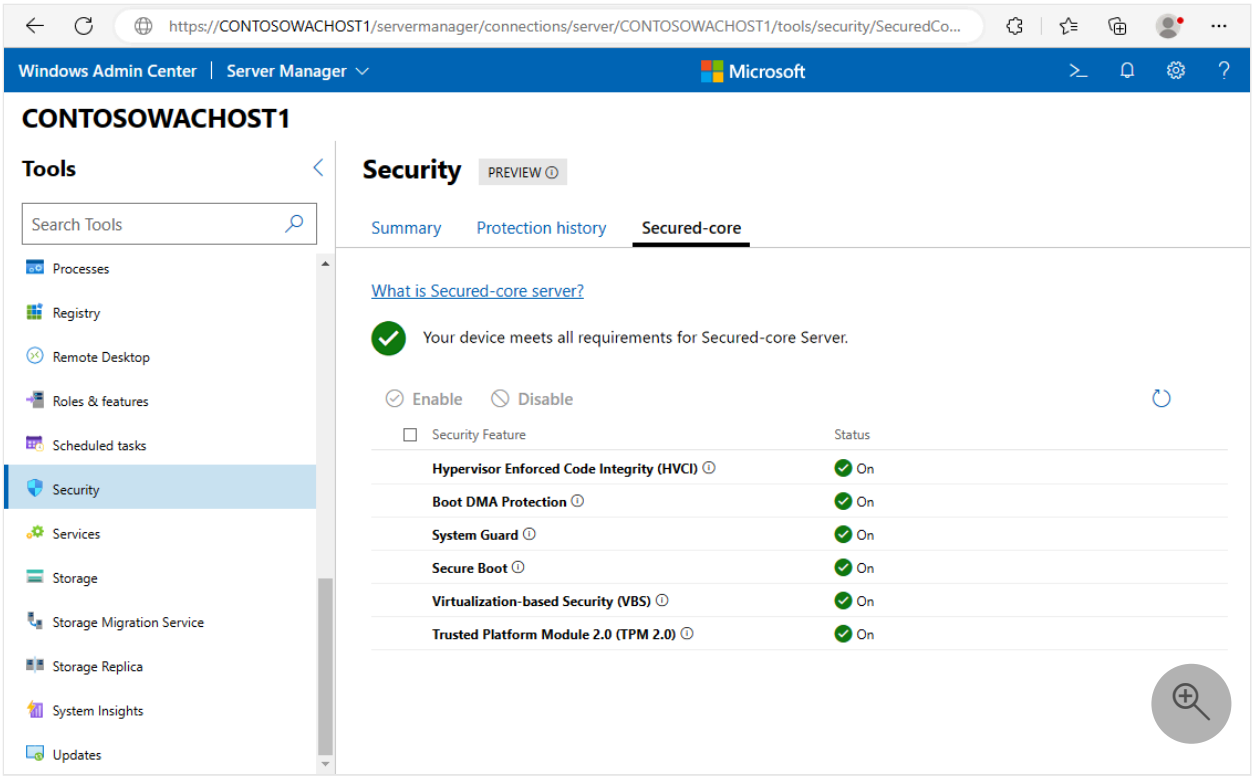
HVCI 通常称为内存完整性保护，是一种安全解决方案，有助于确保仅允许在内核中执行已签名的和受信任的代码。 仅使用已签名的和受信任的代码可防止尝试修改内核模式代码的攻击。 例如，修改驱动程序的攻击，或尝试将恶意代码注入内核的 WannaCry 等攻击。

若要详细了解 VBS 和硬件要求，请参阅基于虚拟化的安全性。

简化管理

可以使用 Windows PowerShell 或 Windows Admin Center 中的安全扩展来查看和配置安全核心系统的 OS 安全功能。 借助 Azure Stack HCI 集成系统，制造合作伙伴进一步简化

了客户的配置体验，使得可立即获取 Microsoft 的最佳服务器安全性。



了解有关 Windows Admin Center 的详细信息。

预防性防御

通过启用安全核心功能，可以主动防御和阻断攻击者可能用来攻击系统的许多路径。 安全核心服务器在技术堆栈的底层启用高级安全功能，在许多安全工具意识到攻击之前保护系统中特权最高的区域。 它还无需执行额外的任务或由 IT 和 SecOps 团队进行监视。

开始你的安全核心之旅

可以在 Windows Server Catalog 中找到已针对安全核心服务器认证的硬件，并在 Azure Stack HCI 目录 中找到已针对 Azure Stack HCI 服务器认证的硬件。 这些经过认证的服务器完全配备了内置于硬件、固件和操作系统中的行业领先的安全缓解措施，可帮助阻止一些最先进的攻击途径。

后续步骤

现在，你已了解什么是安全核心服务器，下面是一些入门资源。 了解如何操作：

- 配置安全核心服务器。
- Microsoft 安全博客中的“Microsoft 通过安全核心向服务器和 Edge 提供高级硬件安全性 ”。

- Microsoft 安全博客中的“新安全核心服务器现可从 Microsoft 生态系统中获取，帮助保护你的基础架构”。
- Windows 硬件兼容性计划规范和策略中的“跨所有 Windows 平台生成与 Windows 兼容的设备、系统和筛选器驱动程序”。

反馈

此页面是否有帮助？ 是 否

如何创建密钥管理服务 (KMS) 激活主机

项目 • 2023/09/03

KMS 使用客户端-服务器模型来激活 Windows 客户端，并用于在本地网络上批量激活。 KMS 客户端连接到一台 KMS 服务器（称为 KMS 主机）进行激活。 KMS 主机可以激活的 KMS 客户端取决于用于激活 KMS 主机的主机密钥。 本文将指导你完成创建 KMS 主机所需的步骤。 如需详细了解 KMS 和初始规划注意事项，请参阅密钥管理服务 (KMS) 激活规划。

先决条件

一台 KMS 主机能够支持无限数量的 KMS 客户端。 如果客户端数量超过 50 个，我们建议至少准备两台 KMS 主机，以防某一台 KMS 主机不可用。 大多数组织单位运行两台 KMS 主机可以满足整个基础结构的需求。

KMS 主机不必是专用服务器，KMS 可与其他服务共用一台主机。 可以在运行受支持的 Windows Server 或 Windows 客户端操作系统的任何物理或虚拟系统上运行 KMS 主机。

用于 KMS 主机的 Windows 版本决定了可为 KMS 客户端激活的 Windows 版本。 请参阅激活版本表，以帮助你确定适合你的环境的版本。

默认情况下，KMS 主机在 DNS 中自动发布 SRV 资源记录。 这使 KMS 客户端能够自动发现 KMS 主机并进行激活，而无需在 KMS 客户端上配置。 可以禁用自动发布，并且可以手动创建记录，如果 DNS 服务不支持动态更新，则这也是自动激活所必需的。

将需要以下项：

- 运行 Windows Server 或 Windows 的计算机。 在 Windows Server 操作系统上运行的 KMS 主机可以激活同时运行服务器和客户端操作系统的计算机，但在 Windows 客户端操作系统上运行的 KMS 主机只能激活也运行客户端操作系统的计算机。
- 你使用的用户帐户必须是 KMS 主机上的管理员组成员。
- 组织的 KMS 主机密钥。 可以从批量许可服务中心 的“产品密钥”部分获取此密钥。

安装和配置 KMS 主机

1. 从提升的 PowerShell 会话中，运行以下命令以安装批量激活服务角色：

```
PowerShell
```

```
Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
```

2. 配置 Windows 防火墙以允许密钥管理服务接收网络流量。 可以针对任何网络配置文件（默认）或域、专用和公共网络配置文件的任意组合允许此设置。 默认情况下，KMS 主机配置为在端口 1688 上使用 TCP。 在下面的示例中，防火墙规则配置为仅允许域和专用网络配置文件的网络流量：

PowerShell

```
Set-NetFirewallRule -Name SPPSVC-In-TCP -Profile Domain,Private -
Enabled True
```

3. 通过运行以下内容启动批量激活工具向导：

PowerShell

```
vmw.exe
```

4. 在“简介”屏幕上，选择“下一步”。 选择“密钥管理服务 (KMS)”作为激活类型，然后输入 以配置要配置的本地服务器或服务器的主机名。

5. 选择“安装 KMS 主机密钥”，输入组织的产品密钥，然后选择“提交” 。

6. 安装产品密钥后，需要激活产品。 单击“下一步” 。

7. 从下拉菜单中选择要激活的产品，然后选择是在线激活还是电话激活。 在本示例中，选择“在线激活”，然后选择“提交”。

8. 激活成功后，将显示 KMS 主机配置。 如果这是你需要的配置，可以选择“关闭”退出向导。 DNS 记录将创建，可以开始激活 KMS 客户端。 如果需要手动创建 DNS 记录，请参阅以下部分。 如果要更改配置设置，请选择“下一步”。

9. 可选：根据要求更改配置值，然后选择“提交” 。

> **备注**
>
> 现在可以开始**激活 KMS 客户端**，但是网络具有的计算机数量不能低于下限（称为激活阈值）。 KMS 主机会对最近连接进行计数，因此当客户端或服务器联系 KMS 主机时，主机将计算机 ID 添加到其计数，然后在其响应中返回当前的计数值。 计数足够高时将激活客户端或服务器。 计数为 25 或更高时将激活 Windows 客户端。 计数为 5 或更大时，将激活 Windows 服务器和批量版 Microsoft Office 产品。 KMS 只对过去 30 天内的唯一连接计数，且仅存储 50 个最新联系人。

手动创建 DNS 记录

如果 DNS 服务不支持动态更新，则必须手动创建资源记录才能发布 KMS 主机。 使用以下信息（更改默认端口号，如果你已在 KMS 主机配置中更改此项）通过 DNS 服务为 KMS 手动创建 DNS 资源记录：

属性	值
类型	SRV
服务/名称	_vlmcs
协议	_tcp
优先度	0
重量	0
端口号	1688
主机名	*KMS 主机的 FQDN*

如果 DNS 服务不支持动态更新，还应禁用所有 KMS 主机上的发布，以防止事件日志收集失败的 DNS 发布事件。

> **提示**
>
> 只要维护所有记录以防止冲突，手动创建的资源记录可以与 KMS 主机在其他域中自动发布的资源记录共存。

禁止发布 DNS 记录

若要禁止 KMS 主机发布 DNS 记录：

1. 通过运行以下内容启动批量激活工具向导：

   ```
   PowerShell
   vmw.exe
   ```

2. 在“简介”屏幕上，选择“下一步”。 选择“密钥管理服务 (KMS)”作为激活类型，然后输入 以配置要配置的本地服务器或服务器的主机名。

3. 选择“跳到配置”，然后选择“下一步” 。

4. 取消选中用于发布 DNS 记录的框，然后选择“提交”。

密钥管理服务 (KMS) 客户端激活和产品密钥

项目 • 2024/10/01

若要使用 KMS，需要有一个在本地网络上可用的 KMS 主机。 使用 KMS 主机激活的计算机需要具有特定的产品密钥。 此密钥有时称为 KMS 客户端密钥，但其正式名称为 Microsoft 通用批量许可证密钥 (GVLK)。 默认情况下，运行 Windows Server 和 Windows 客户端批量许可版本的计算机是无需额外配置的 KMS 客户端，因为相关 GVLK 已经存在。

但是，在某些情况下，需要将 GVLK 添加到要针对 KMS 主机激活的计算机，例如：

- 转换计算机使其不使用多次激活密钥 (MAK)
- 将 Windows 的零售许可证转换为 KMS 客户端
- 如果计算机以前是 KMS 主机

> **ⓘ 重要**
>
> 若要使用此处列出的密钥（它们是 GVLK），你必须首先在本地网络中拥有可用的 KMS 主机。 如果还没有 KMS 主机，请参阅如何**创建 KMS 主机**以了解详细信息。
>
> 如果希望在没有可用的 KMS 主机的情况下在批量激活方案之外激活 Windows（例如，尝试激活 Windows 客户端的零售版本），则**这些密钥将不起作用。** 需要使用另一种激活 Windows 的方法，如使用 MAK 或购买零售许可证。 获取帮助以**查找 Windows 产品密钥**并了解 **Windows 的正版版本**。

安装产品密钥

如果要将计算机从 KMS 主机、MAK 或零售版本 Windows 转换为 KMS 客户端，可以从本文中的列表安装适用的产品密钥 (GVLK)。 若要安装客户端产品密钥，请在客户端上打开一个管理命令提示符，并运行以下命令，然后按 `Enter`：

Windows 命令提示符

```
slmgr /ipk <product key>
```

例如，若要安装 Windows Server 2022 Datacenter 版的产品密钥，请运行以下命令，然后按 `Enter`：

Windows 命令提示符

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

通用批量许可证密钥

在下表中，可找到 Windows 每个版本的 GVLK。 LTSC 是长期服务渠道，而 LTSB 是 Long-Term Servicing Branch 。

Windows Server LTSC

Windows Server 2025

展开表

操作系统版本	KMS 客户端产品密钥
Windows Server 2025 标准	TVRH6-WHNXV-R9WG3-9XRFY-MY832
Windows Server 2025 数据中心	D764K-2NDRG-47T6Q-P8T8W-YP6DF
Windows Server 2025 Datacenter：Azure Edition	XGN3F-F394H-FD2MY-PP6FD-8MCRC

Windows Server 半年频道

Windows Server，版本 20H2、2004、1909、1903 和 1809

展开表

操作系统版本	KMS 客户端产品密钥
Windows Server Standard	N2KJX-J94YW-TQVFB-DG9YT-724CC
Windows Server Datacenter	6NMRW-2C8FM-D24W7-TQWMY-CWH2D

重要

Windows Server 版本 20H2 已于 2022 年 8 月 9 日终止服务，不再接收安全更新。 这包括停用 Windows Server 半年频道 (SAC)，不再提供未来版本。

使用 Windows Server SAC 的客户应迁移到 Azure Stack HCI。 或者，客户可使用 Windows Server 的长期服务渠道。

Windows 11 和 Windows 10（半年频道）

有关受支持的版本和服务终止日期的信息，请参阅 Windows 生命周期情况说明书。

展开表

操作系统版本	KMS 客户端产品密钥
Windows 11 专业版 Windows 10 专业版	W269N-WFGWX-YVC9B-4J6C9-T83GX
Windows 11 专业版 N Windows 10 专业版 N	MH37W-N47XK-V7XM9-C7227-GCQG9
Windows 11 专业工作站版 Windows 10 专业工作站版	NRG8B-VKK3Q-CXVCJ-9G2XF-6Q84J
Windows 11 专业工作站版 N Windows 10 专业工作站版 N	9FNHH-K3HBT-3W4TD-6383H-6XYWF
Windows 11 专业教育版 Windows 10 专业教育版	6TP4R-GNPTD-KYYHQ-7B7DP-J447Y
Windows 11 专业教育版 N Windows 10 专业教育版 N	YVWGF-BXNMC-HTQYQ-CPQ99-66QFC
Windows 11 教育版 Windows 10 教育版	NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
Windows 11 教育版 N Windows 10 教育版 N	2WH4N-8QGBV-H22JP-CT43Q-MDWWJ
Windows 11 企业版 Windows 10 企业版	NPPR9-FWDCX-D2C8J-H872K-2YT43
Windows 11 企业版 N Windows 10 企业版 N	DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4
Windows 11 企业版 G Windows 10 企业版 G	YYVX9-NTFWV-6MDM3-9PT4T-4M68B
Windows 11 企业版 G N Windows 10 企业版 G N	44RPN-FTY23-9VTTB-MP9BX-T84FV

Windows 企业版 LTSC 和 LTSB

Windows 11 LTSC 2024

Windows 10 LTSC 2021、2019

展开表

操作系统版本	KMS 客户端产品密钥
Windows 11 企业版 LTSC 2024 Windows 10 企业版 LTSC 2021 Windows 10 企业版 LTSC 2019	M7XTQ-FN8P6-TTKYV-9D4CC-J462D
Windows 11 企业版 N LTSC 2024 Windows 10 企业版 N LTSC 2021 Windows 10 企业版 N LTSC 2019	92NFX-8DJQP-P6BBQ-THF9C-7CG2H

早期版本的 Windows Server

Windows Server 版本 1803

展开表

操作系统版本	KMS 客户端产品密钥
Windows Server Standard	PTXN8-JFHJM-4WC78-MPCBR-9W4KR
Windows Server Datacenter	2HXDN-KRXHB-GPYC7-YCKFJ-7FVDG

早期版本的 Windows 客户端

Windows 8.1

展开表

操作系统版本	KMS 客户端产品密钥
Windows 8.1 专业版	GCRJD-8NW9H-F2CDX-CCM8D-9D6T9
Windows 8.1 专业版 N	HMCNV-VVBFX-7HMBH-CTY9B-B4FXY
Windows 8.1 企业版	MHF9N-XY6XB-WVXMC-BTDCT-MKKG7

操作系统版本	KMS 客户端产品密钥
Windows 8.1 企业版 N	TT4HM-HN7YT-62K67-RGRQJ-JFFXW

反馈

此页面是否有帮助? 是 否

如何获取 Windows Server 的扩展安全更新 (ESU)

项目 • 2023/10/04

Windows Server 的扩展安全更新 (ESU) 包含评级为“严重”和“重要”的安全更新和公告。 使用 ESU 之前，应阅读 Windows Server 的扩展安全更新概述，以了解什么是 ESU、它们的可用时长以及你可使用的选项。

如何获取 ESU 取决于服务器的托管位置。 可以通过以下选项访问 ESU。

- Azure 虚拟机 - 适用的 Azure 中托管的虚拟机 (VM) 自动启用 ESU，这些更新是免费提供的，无需部署 MAK 密钥或执行任何其他操作。 有关详细信息，请参阅 Azure 上的扩展安全更新。
- 已启用 Azure Arc 的服务器 - 如果服务器位于本地或托管环境中，则可以通过 Azure 门户为 Windows Server 2012 和 2012 R2 或 SQL Server 2012 计算机注册扩展安全更新，通过 Azure Arc 进行连接，并通过 Azure 订阅按月计费。 有关详细信息，请参阅 Azure Arc 启用的扩展安全更新。 [1]
- 非 Azure 物理计算机和虚拟机 - 如果无法使用 Azure Arc 进行连接，请使用非 Azure VM 上的扩展安全更新，方法是使用多次激活密钥 (MAK) 并将其应用于相关服务器。 此 MAK 密钥使 Windows 更新服务器知道你可以继续接收安全更新。 有关详细信息，请参阅从 Microsoft 365 管理中心访问多次激活密钥。 [1]

[1] 使用已启用 Azure Arc 的服务器和非 Azure 计算机时，必须购买 ESU。 若要购买 ESU，必须通过批量许可计划（如企业协议 (EA)、企业协议订阅 (EAS)、教育解决方案合约 (EES) 或服务器和云合约 (SCE)）获得软件保障。

> **备注**
>
> 为本地 VM 或物理服务器购买 ESU 后，多次激活密钥可能需要 3-5 个工作日才可用。 组织可能需要时间来规划和部署新密钥。 在购买 ESU 之前，应记住这些时间线。

Azure 上的扩展安全更新

适用的 Azure 中托管的虚拟机 (VM) 自动启用 ESU，这些更新是免费提供的。 无需配置任何内容，且将 ESU 用于 Azure VM 没有额外费用。 如果将 Azure VM 配置为接收 ESU，则这些更新会自动传送到 Azure VM。

> **备注**
>
> 扩展安全更新在其他 Azure 产品（例如 Azure 专用主机、Azure VMware 解决方案、Azure Nutanix 解决方案和 Azure Stack（Hub、Edge 和 HCI））中也是免费的，并且可能需要其他配置。 请联系 **Microsoft 支持** 获取更多帮助。
>
> Azure 经典 VM (Microsoft.ClassicCompute) 要求额外配置以接收扩展安全更新，原因是它们无权访问 **Azure 实例元数据服务**，而该服务决定了 ESU 的资格。

Azure Arc 启用的扩展安全更新

如果已启用 Azure Arc 的服务器通过 Azure Arc 连接并注册了 ESU，则 ESU 会自动传送到已启用 Azure Arc 的服务器。这也适用于连接到 Azure Arc 的非 Azure 服务器。

可以使用 Azure Policy 或 Azure 门户大规模注册 ESU，无需预付费用，将通过 Azure 订阅按月计费。 也无需激活产品密钥。

已启用 Azure Arc 的服务器还可以使用其他 Azure 服务，例如：

- Azure 更新管理器。
- Microsoft Defender for Cloud。
- Azure Policy（计算机配置）。
- Azure Monitor（VM 见解）。

从 2023 年 9 月起，可以通过 Azure Arc 激活 Windows Server 2012 和 2012 R2 EUS。现在可以将 Windows Server 2012 和 2012 R2 服务器连接到 Azure Arc，将混合计算机连接到已启用 Azure Arc 的服务器。

若要准备在已启用 Arc 的服务器上激活 Windows Server 2012 和 2012 R2 ESU，请执行以下步骤：

1. 登录 Azure 门户 。
2. 在搜索栏中，输入“服务器 - Azure Arc”并选择匹配的服务条目。
3. 将现有的 Windows Server 2012 或 2012 R2 计算机添加到 Azure Arc。若要了解如何开始使用已启用 Azure Arc 的服务器，请参阅将混合计算机与已启用 Azure Arc 的服务器连接。

若要详细了解如何通过 Azure Arc 提供 ESU，请参阅准备为 Windows Server 2012 提供扩展安全更新和 Windows 2012 和 2012 R2 提供扩展安全更新。

从 Microsoft 365 管理中心访问多次激活密钥

无法连接到 Azure Arc 以应用 ESU 的客户可以通过 Microsoft 365 管理中心使用多次激活密钥（MAK）：

1. 登录到 Microsoft 365 管理中心。
2. 选择“你的产品”>“批量许可”>“查看协定”
3. 选择用于购买 ESU 的协议编号旁的三点图标（“更多操作”图标），然后选择“查看产品密钥”。 此页将显示协议提供的所有产品密钥。
4. 获得 MAK 后，在符合条件的服务器上安装新密钥。 若要详细了解如何安装和激活 MAK，请参阅技术社区博客文章为符合条件的 Windows 设备获取扩展安全更新。

下载和安装扩展安全更新

提供、下载和应用 Windows Server 的 ESU 与其他 Windows 更新没有什么不同。 通过 ESU 提供的更新只是安全更新。

必须先安装最新的服务堆栈更新 (SSU) 和许可准备包，然后才能下载和安装 ESU。 若要详细了解安装最新 SSU 和许可准备包所需的步骤，请参阅 KB5031043：在扩展支持于 2023 年 10 月 10 日结束之后继续接收安全更新的过程。

可以使用现有的任何工具和过程来安装更新。 唯一的区别在于，必须使用上一节中生成的密钥来注册系统，才能下载和安装更新。

对于 Azure 中托管的 VM，为服务器启用 ESU 的过程会自动完成。 更新将进行下载和安装，而无需进行其他配置。

为 Windows Server 2012 提供扩展安全更新

项目 • 2024/11/05

本文分步介绍如何将扩展安全更新 (ESU) 提供给已启用 Arc 的服务器中加入的 Windows Server 2012 计算机。 可单独或大规模地向这些计算机提供 ESU。

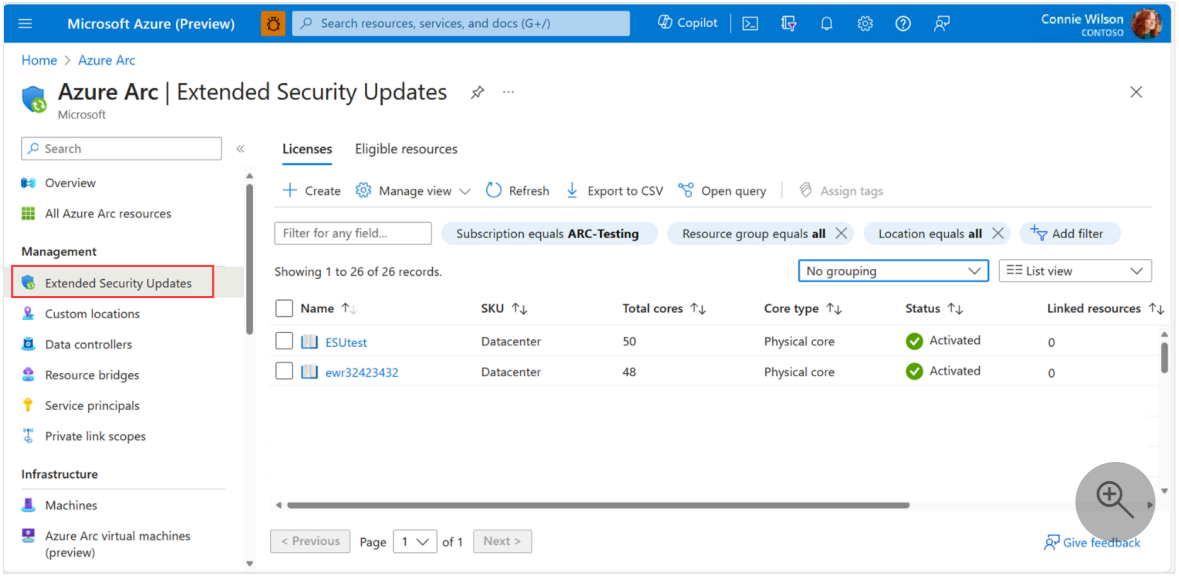
开始之前

计划和准备将计算机加入已启用 Azure Arc 的服务器。 若要了解详细信息，请参阅准备为 Windows Server 2012 提供扩展安全更新。

要创建 ESU 并将其分配至已启用 Arc 的服务器，还需要具有 Azure RBAC 中的参与者角色。

管理 ESU 许可证

1. 在浏览器中，登录到 Azure 门户 。
2. 在“Azure Arc”页上，在左窗格中选择“扩展安全更新”。



在此处，可以查看和创建 ESU 许可证，并查看对 ESU 来说符合条件的资源。

> **备注**
>
> 从“服务器”页查看所有已启用 Arc 的服务器时，横幅指定有多少台 Windows 2012 计算机有资格使用 ESU。 然后，可选择“查看扩展安全更新中的服务器”，来查看符合 ESU 条件的资源列表以及已启用 ESU 的计算机。

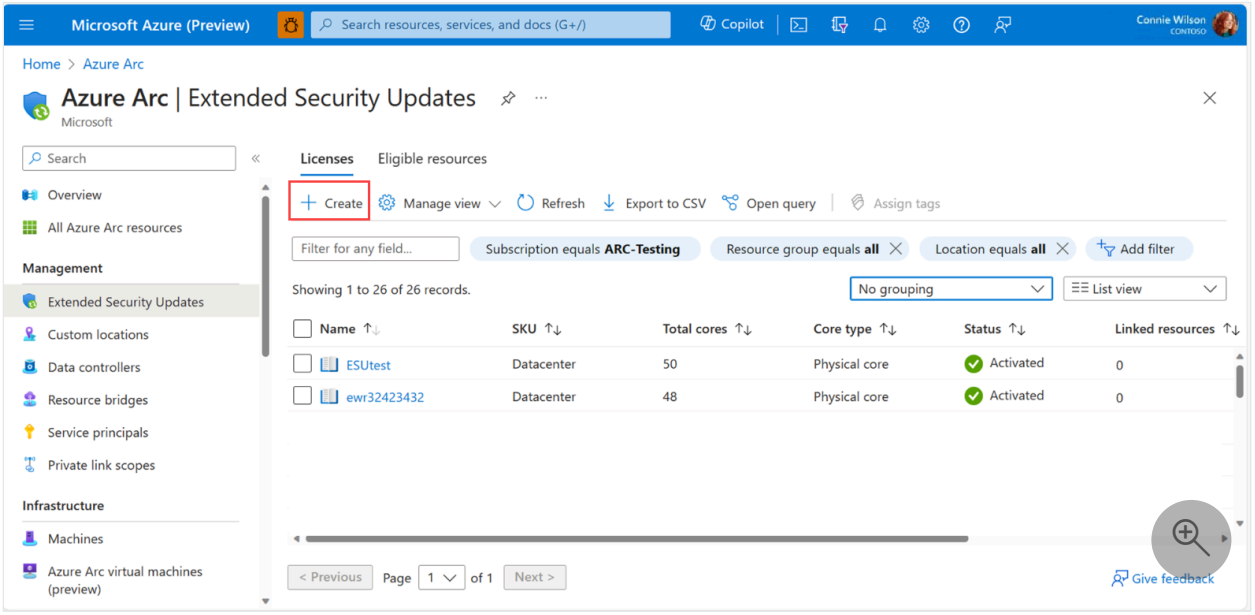
创建 Azure Arc WS2012 许可证

第一步是从 Azure Arc 预配 Windows Server 2012 和 2012 R2 扩展安全更新许可证。将这些许可证链接到下一部分中选择的一个或多个已启用 Arc 的服务器。

预配 ESU 许可证后，需要指定 SKU（标准或数据中心）、核心类型（物理或 vCore），以及用于预配 ESU 许可证的 16 核和 2 核包的数量。 还可在停用状态下预配扩展安全更新许可证，以便它不会启动计费或在创建时正常运行。 此外，预配后可修改与许可证关联的核心。

> **备注**
>
> 要预配 ESU 许可证，你需要证明其 SA 或 SPLA 覆盖范围。

“许可证”了选项卡显示可用的 Azure Arc WS2012 许可证。 你可在此选择一个现有许可证并应用，或创建一个新的许可证。

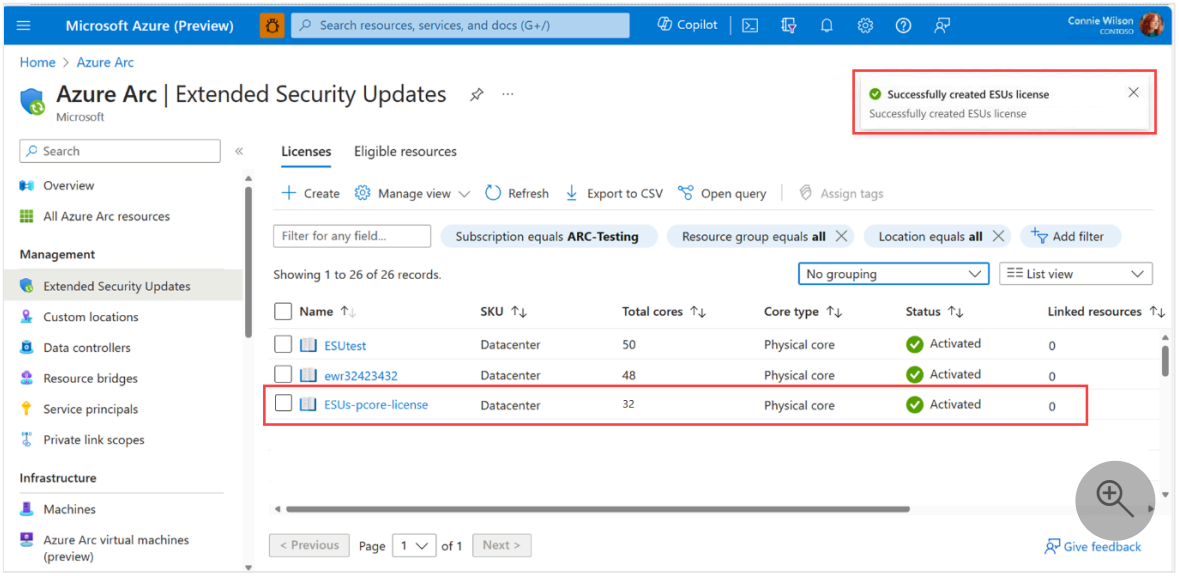


1. 若要创建新的 WS2012 许可证，请选择“创建”，然后在页面上提供配置许可证所需的信息。

若要详细了解如何完成此步骤，请参阅 Windows Server 2012 扩展安全更新的许可证预配指南。

2. 查看提供的信息，然后选择“创建”。

   创建的许可证显示在列表中，你可以按照下一部分中的步骤将其链接到一个或多个已启用 Arc 的服务器。

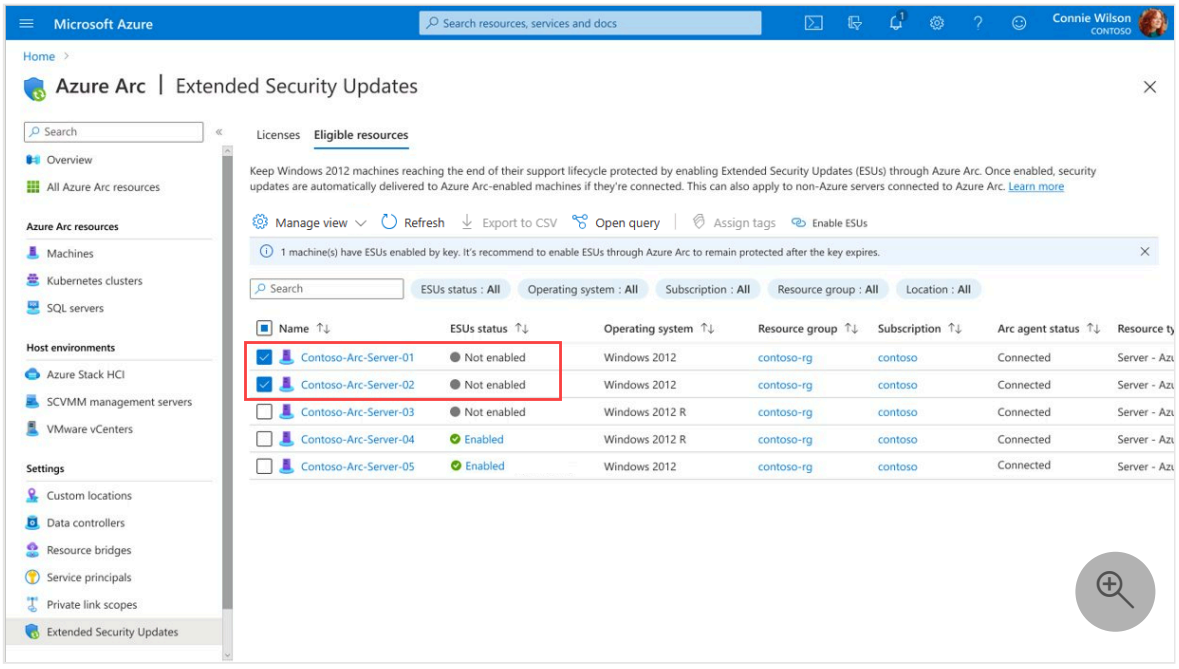


将 ESU 许可证链接到已启用 Arc 的服务器

可以选择一个或多个已启用 Arc 的服务器以链接到扩展安全更新许可证。 将服务器链接到已激活的 ESU 许可证后，服务器有资格接收 Windows Server 2012 和 2012 R2 ESU。

> **备注**
>
> 你可以灵活地配置所选择的修补解决方案来接收这些更新 - 无论它是**更新管理器**、Windows Server Update Services、Microsoft 更新、Microsoft Endpoint Configuration Manager，还是第三方补丁管理解决方案。

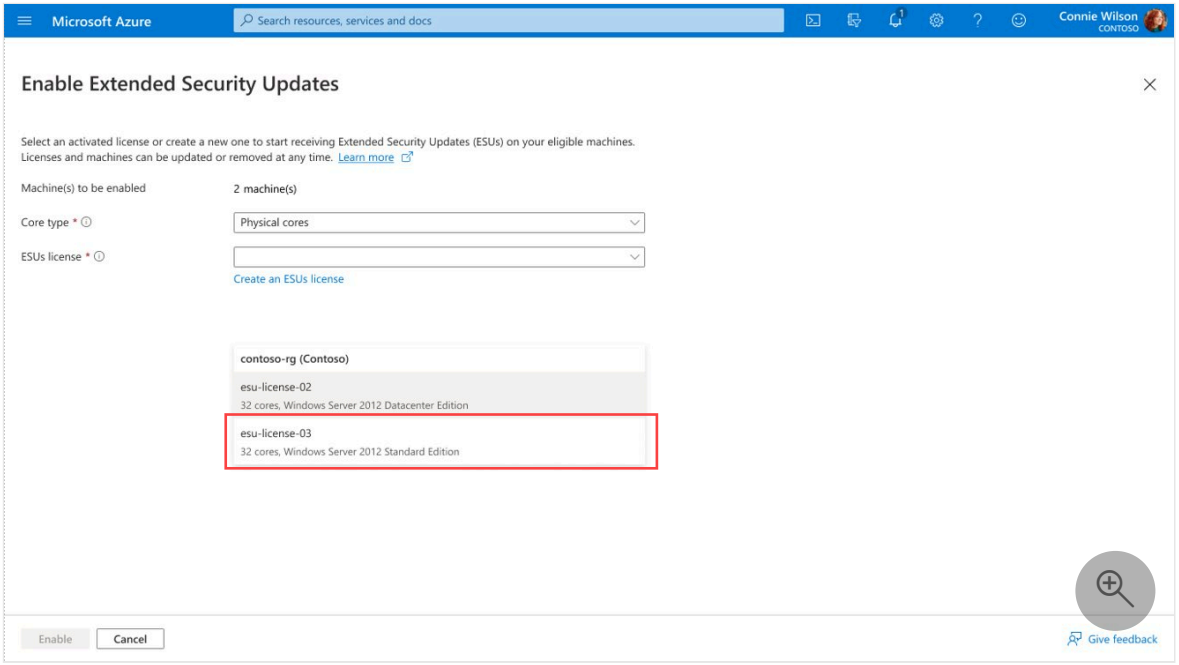
1. 选择“符合条件的资源”选项卡，查看运行 Windows Server 2012 和 2012 R2 的所有已启用 Arc 的服务器的列表。



"ESU 状态"列指示计算机是否已启用 ESU。

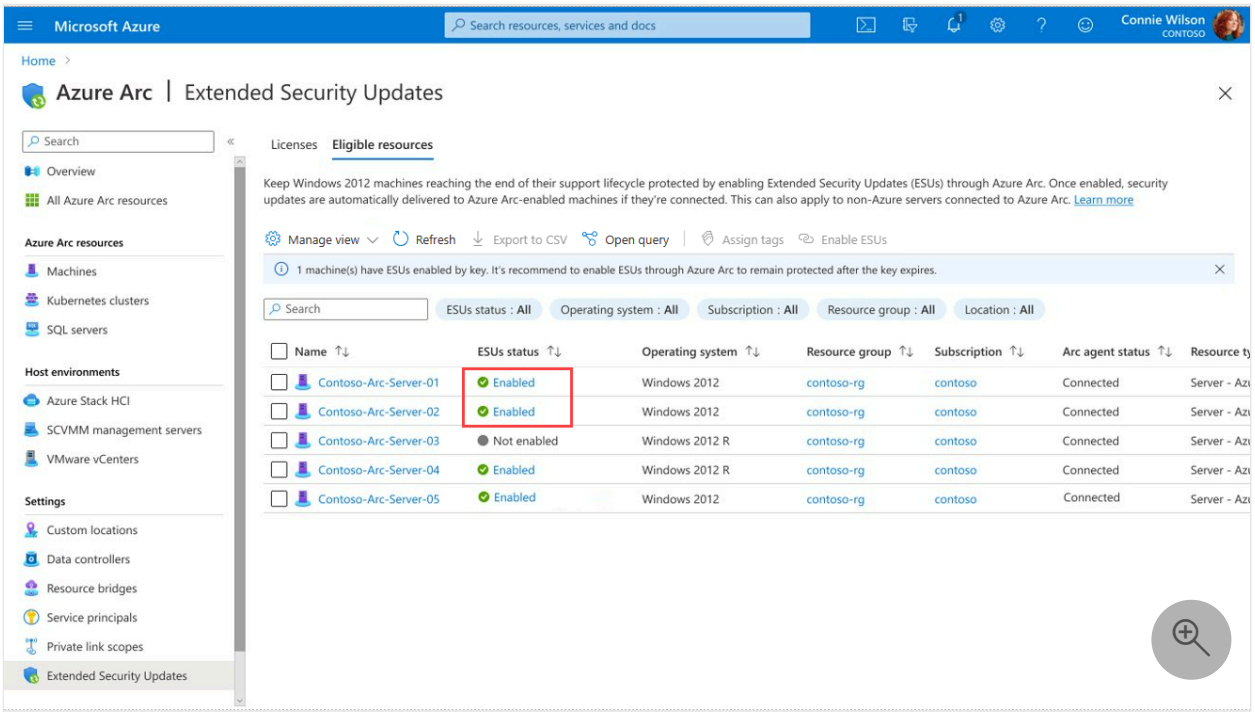
2. 若要为一台或多台计算机启用 ESU，请在列表中选择它们，然后选择"启用 ESU"。

3. 在"启用扩展安全更新"页上，会显示选择启用 ESU 的计算机数以及可应用的 WS2012 许可证。 选择要链接到所选计算机的许可证，然后选择"启用"。



> **备注**
>
> 还可选择"创建 ESU 许可证"，从此页面创建许可证。

所选计算机的状态将更改为"已启用"。



如果在启用过程中发生了任何问题，请参阅 Windows Server 2012 扩展安全更新的交付故障排除来寻求帮助。

大规模 Azure Policy

若要大规模将服务器链接到 Azure Arc 扩展安全更新许可证并锁定许可证修改或创建，请考虑使用以下内置 Azure 策略：

- 启用扩展安全更新 (ESU) 许可证，以在 Windows 2012 计算机的支持生命周期结束后使其保持受保护状态（预览版）
- 拒绝扩展安全更新 (ESU) 许可证创建或修改（预览版）

可以将 Azure 策略指定给目标订阅或资源组，以在审核和管理场景中使用。

其他方案

在一些情况下，你可能有资格接收扩展安全更新补丁，无需额外付费。 Azure Arc 支持的两种场景是：(1) 开发/测试 (Visual Studio) 和（2） 灾难恢复（仅限软件保障或订阅的授权权益 DR 实例）。 这两种场景都要求客户已在使用 Azure Arc 为可计费生产计算机启用的 Windows Server 2012/R2 ESU。

> ⚠ **警告**
>
> 请勿仅为开发/测试或灾难恢复工作负载创建 Windows Server 2012/R2 ESU 许可证。 你不能专门为不计费的工作负载预配 ESU 许可证。 此外，使用 ESU 许可证预

配的所有核心都将完整计费，许可证上的开发/测试核心只要根据下文的条件打标签就不会计费。

为了符合这些场景的要求，你必须已拥有以下项：

- **可计费的 ESU 许可证。** 必须已预配并激活了 WS2012 Arc ESU 许可证，该许可证旨在链接到生产环境中运行的常规已启用 Azure Arc 的服务器（即，通常计费的 ESU 场景）。 应该仅对计费核心预配此许可证，而不要对符合免费扩展安全更新条件的核心预配（例如开发/测试核心）。
- **已启用 Arc 的服务器。** 已将 Windows Server 2012 和 Windows Server 2012 R2 计算机加入已启用 Azure Arc 的服务器，以便进行 Visual Studio 订阅的开发/测试或者进行灾难恢复。

若要免费注册符合 ESU 条件的已启用 Azure Arc 的服务器，请执行以下步骤来进行标记和链接：

1. 使用与相应异常对应的下列名称-值对之一标记 WS2012 Arc ESU 许可证（为生产环境创建，核心仅用于生产环境服务器）和已启用 Azure Arc 的非生产服务器：

   a. 名称：“ESU 用途”；值：“WS2012 VISUAL STUDIO 开发测试”

   b. 名称：“ESU 用途”；值：“WS2012 灾难恢复”

   如果对多个异常场景使用 ESU 许可证，请使用以下标记来标记许可证 - 名称：“ESU 用途”；值：“WS2012 多用途”

2. 将已标记的许可证（为生产环境创建，核心仅用于生产环境服务器）链接到已标记的已启用 Azure Arc 的非生产 Windows Server 2012 和 Windows Server 2012 R2 计算机。 请勿为这些服务器授予核心许可证，也勿仅为这些服务器创建新的 ESU 许可证。

这种链接不会触发合规性冲突或强制阻止，从而让你能够将许可证的应用扩展到其预配的核心之外。 许可证预计仅包括生产服务器和计费服务器的核心。 任何附加的核心都会产生费用，因而会导致超额计费。

> **ⓘ 重要**
>
> 将这些标签添加到许可证不会免收许可证费用或减少待收费的许可证核心数。 这些标签使你可以将 Azure 计算机关联到已配置有应付核心的现有许可证上，而无需创建新的许可证或向免费计算机添加其他核心。

示例：

- 有 8 个 Windows Server 2012 R2 标准实例，每个实例都有 8 个物理核心。 其中六台 Windows Server 2012 R2 标准计算机用于生产，2 台 Windows Server 2012 R2 标准计算机有资格使用免费 ESU，因为操作系统是通过 Visual Studio 开发测试订阅获得许可的。
  - 你应当首先为属于标准版且具有 48 个物理核心的 Windows Server 2012/R2 预配并激活常规 ESU 许可证，以覆盖 6 台生产计算机。 应将此常规生产 ESU 许可证链接到 6 个生产服务器。
  - 接下来，你应重新使用此现有许可证，不要再添加任何核心或预配单独的许可证，并将此许可证关联到 2 台非生产 Windows Server 2012 R2 标准计算机上。 应使用名称：“ESU Usage”和数值：“WS2012 VISUAL STUDIO DEV TEST”来标记许可证和 2 台非生产 Windows Server 2012 R2 标准计算机。
  - 这样将获得 48 核心的 ESU 许可证，而你将为这 48 个核心付费。 只要正确标记 ESU 许可证和开发测试服务器资源，你就不用添加到许可证上的其余 16 个开发测试服务器核心付费。

> **备注**
>
> 一开始需要一个常规生产许可证，而且仅将对生产核心进行计费。

从 Windows Server 2012/2012 R2 升级

将 Windows Server 2012/2012R 计算机升级到 Windows Server 2016 或更高版本时，无需从计算机中删除 Connected Machine 代理。 在升级完成后几分钟内，Azure 中的计算机会显示新的操作系统。 升级的计算机不再需要 ESU，并且不再有资格使用它们。 与与计算机关联的 ESU 许可证都不会自动取消与计算机的关联。 有关手动执行此操作的说明，请参阅取消关联许可证。

评估 WS2012 ESU 补丁状态

要检测已启用 Azure Arc 的服务器是否已使用最新的 Windows Server 2012/R2 扩展安全更新进行修补，请使用 Azure Policy 应在 Windows Server 2012 Arc 计算机-Microsoft Azure 上安装扩展安全更新。 此 Azure Policy 由机器配置提供支持，能够识别服务器是否已收到最新的 ESU 补丁。 这可从 Azure 门户中内置的来宾分配和 Azure Policy 合规性视图中看到。

反馈

此页面是否有帮助? 是 否

提供产品反馈 | 在 Microsoft Q&A 获取帮助

为从 ISO 生成的 Azure Edition 虚拟机启用热补丁

项目 • 2023/11/30

借助 Windows Server 2022 Datacenter: Azure Edition 的热补丁，可在无需进行安装后重启的情况下安装安全更新。 可以将热补丁与桌面体验和 Server Core 结合使用。 本文将介绍如何在使用 ISO 安装或升级操作系统后配置热补丁。

> **备注**
>
> 如果使用的是 Azure 市场，请不要遵循本文中的步骤。 请转而使用 Azure 市场中以下可用于热修补的映像：
>
> - Windows Server 2022 Datacenter：Azure Edition Hotpatch - Gen2
> - Windows Server 2022 Datacenter：Azure Edition Core - Gen2

在 Azure Stack HCI 上为 ISO 部署的计算机使用热补丁时，与将热补丁用作 Azure VM 的 Azure Automanage 的一部分相比，热修补体验存在一些重要差异。

这些差异包括：

- 无法通过 Azure 更新管理器使用热补丁配置。
- 无法禁用热补丁。
- 自动修补业务流程不可用。
- 必须手动执行业务流程（例如，通过 SConfig 使用 Windows 更新）。

先决条件

若要启用热补丁，必须在开始之前满足以下先决条件：

- 托管在受支持平台上的 Windows Server 2022 Datacenter: Azure Edition，例如已启用 Azure 权益的 Azure 或 Azure Stack HCI。
  - Azure Stack HCI 必须为 21H2 版或更高版本。
- 查看“新虚拟机的热补丁”一文的热补丁的工作原理部分。
- 允许 HTTPS (TCP/443) 流量流向以下终结点的出站网络访问或出站端口规则：
  - `go.microsoft.com`
  - `software-static.download.prss.microsoft.com`

准备计算机

在为 VM 启用热补丁之前，必须使用以下步骤准备计算机：

1. 登录到计算机。 如果正在使用 Server Core，则在 SConfig 菜单中，输入选项 15，然后按 Enter 打开 PowerShell 会话。 如果使用的是桌面体验，请通过远程桌面进入 VM 并启动 PowerShell。

2. 通过运行以下 PowerShell 命令来配置正确的注册表设置，启用基于虚拟化的安全性：

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "EnableVirtualizationBasedSecurity"
       Value = "0x1"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

3. 重新启动计算机。

4. 通过运行以下 PowerShell 命令在注册表中配置热补丁表大小：

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
   Manager\Memory Management"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "HotPatchTableSize"
       Value = "0x1000"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

5. 通过运行以下 PowerShell 命令在注册表中为热补丁配置 Windows 更新终结点：

   PowerShell

   ```
   $registryPath = "HKLM:\SOFTWARE\Microsoft\Windows
   NT\CurrentVersion\Update\TargetingInfo\DynamicInstalled\Hotpatch.amd64"
   $nameParameters = $parameters = @{
       Path = $registryPath
       Name = "Name"
       Value = "Hotpatch Enrollment Package"
       Force = $True
   ```

```
}
$versionParameters = $parameters = @{
    Path = $registryPath
    Name = "Version"
    Value = "10.0.20348.1129"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @nameParameters
New-ItemProperty @versionParameters
```

准备好计算机后，现在即可安装热补丁服务包。

安装热补丁服务包

> **备注**
>
> Microsoft 更新目录中当前未发布热补丁先决条件知识库。

若要能够接收热补丁更新，需要下载并安装热补丁服务包。 在 PowerShell 会话中，完成以下步骤：

1. 从 Microsoft 更新目录下载 (KB5003508) Microsoft 更新独立程序包，并使用以下 PowerShell 命令将其复制到计算机：

   PowerShell

   ```
   $parameters = @{
       Uri = "https://go.microsoft.com/fwlink/?linkid=2211714"
       OutFile = ".\KB5003508.msu"
   }
   Invoke-WebRequest @parameters
   ```

2. 若要安装独立程序包，请运行以下命令：

   PowerShell

   ```
   wusa.exe .\KB5003508.msu
   ```

3. 按提示操作。 完成后，选择“完成”。

4. 若要验证安装，请运行以下命令：

   PowerShell

```
Get-HotFix | Where-Object {$_.HotFixID -eq "KB5003508"}
```

> **备注**
>
> 使用 Server Core 时，默认情况下更新设置为手动安装。 你可以使用 SConfig 实用工具更改此设置。

后续步骤

现在，你已针对热补丁对计算机进行了设置，下面是一些可帮助你更新计算机的文章：

- 修补 Server Core 安装。
- 详细了解 Windows Server Update Services (WSUS)。

执行 Windows Server 的功能更新

项目 • 2024/04/15

通过功能更新（也称为就地升级），可从较低版本的操作系统升级到较高版本的操作系统，同时使设置、服务器角色和数据保持不变。 本文介绍如何使用功能升级迁移到更高版本的 Windows Server。

> ⓘ **重要**
>
> - 本文仅介绍非 Azure 服务器和虚拟机 (VM) 的 Windows Server 功能升级过程。 若要对 Azure 虚拟机 (VM) 中运行的 Windows Server 执行功能升级，请参阅 **Azure 中运行 Windows Server 的 VM 的就地升级**。
> - 对于想升级的 Microsoft Entra Connect 用户，请参阅 **Microsoft Entra Connect：从旧版升级到最新版本**。

先决条件

在开始升级之前，请满足以下先决条件：

- 确定要更新到的 Windows Server 版本。
- 请确保拥有有效的产品密钥和激活方法。 密钥和方法可能取决于从中接收 Windows Server 媒体的分发渠道，例如商业许可计划、零售，或原始设备制造商 (OEM)。
- 需要为要升级到的 Windows Server 版本准备安装介质。 可以从 OEM、零售、Visual Studio 订阅和批量许可服务中心 (VLSC) 渠道获取 Windows Server 目标版本的安装介质。
- 有一个计算机之外的位置可用于存储文件，例如 USB 闪存驱动器或网络位置。
- 查看升级和迁移 Windows Server 中的角色和功能。
- 查看 Microsoft 服务器应用程序兼容性。
- 查看任何第三方应用程序供应商支持要求。
- 确保计算机达到以下要求：
  - 满足或超过 Windows Server 的硬件要求。
  - 未在 Azure 中运行。
- 执行计算机的完整备份。 这包括操作系统、应用、数据和服务器上运行的任何虚拟机 (VM)。 可以使用 Windows Server 备份或第三方备份解决方案。

> ⓘ **备注**

- 如果要对安装了 Configuration Manager 的 Windows Server 2012 或 Windows Server 2012 R2 服务器执行功能更新，还需要按照**升级支持 Configuration Manager 的本地基础结构**中的升级前和升级后说明进行操作。

收集诊断信息

建议从设备收集一些信息，以便在功能更新失败时进行诊断和故障排除。 还建议将该信息存储在即使在无法访问设备时也可以访问的位置。

若要收集信息：

1. 打开提升的 PowerShell 提示符，记下当前目录，并运行以下命令。

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsBuildLabEx,WindowsEditionID | Out-File -FilePath .\computerinfo.txt
   systeminfo.exe | Out-File -FilePath systeminfo.txt
   ipconfig /all | Out-File -FilePath ipconfig.txt
   ```

   > **提示**
   >
   > `Get-ComputerInfo` 需要 PowerShell 5.1 或更高版本。 如果 Windows Server 版本不包含 Powershell，可以在注册表中找到此信息。 打开“注册表编辑器”，转到 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion** 项，然后复制并粘贴 Windows Server **BuildLabEx** 和 **EditionID** 值。

2. 使用**文件资源管理器**导航到记下的目录，并将文件**复制**到计算机外的 USB 闪存驱动器或网络位置。

收集与 Windows Server 相关的所有信息后，建议备份服务器操作系统、应用和 VM。 而且，还必须关闭、快速迁移或实时迁移当前正在服务器上运行的所有 VM。 在功能更新期间，不能有任何 VM 在运行。

执行功能更新

现在，你已完成先决条件并且收集了诊断信息，接下来即可执行功能更新。 在本部分中，你将使用 Windows Server 安装程序选择功能更新的设置。 Windows Server 安装程序将使用这些设置更新 Windows Server 版本，在此期间，计算机将重启数次。

若要执行功能更新，请执行以下操作：

1. 使用**文件资源管理器**导航到 Windows Server 安装程序媒体。 然后打开 **setup.exe**。 例如，如果使用删除媒体，则文件路径可能为 *D:\setup.exe*。

   > **ⓘ 重要**
   >
   > 根据安全设置，用户帐户控制可能会提示你允许安装程序对设备进行更改。 如果你愿意继续，请选择“是”。

2. 默认情况下，安装程序会自动下载更新以便进行安装。 如果你同意使用默认设置，请选择“下一步”继续。

   如果不希望安装程序自动下载更新，选择“更改安装程序下载更新的方式”，选择适合你环境的选项，然后选择“下一步”。

3. 如果出现提示，请输入产品密钥，然后选择“下一步”。

4. 选择要安装的 Windows Server 版本，然后选择“下一步”。

5. 查看适用的通知和许可条款。 如果同意条款，请选择“接受”。

6. 选择**保留个人文件和应用**以选择执行功能更新，然后选择**下一步**。

7. 安装程序完成对设备的分析后，将显示“准备安装”屏幕。 若要继续功能更新，请选择**安装**。

将开始功能更新，你应会看到一个进度栏。 功能更新完成后，服务器将重启。

检查功能更新是否成功

完成对 Windows Server 的功能更新后，必须确保功能更新成功。

若要确保功能更新成功，请执行以下操作：

1. 打开提升的 PowerShell 提示符，运行以下命令，验证版本是否与安装过程中选择的媒体和值匹配。

   ```
   PowerShell
   ```

   ```
   Get-ComputerInfo -Property WindowsProductName
   ```

2. 请确保所有应用程序都处于运行状态，并且客户端成功连接到这些应用程序。

如果计算机在功能更新后未按预期工作，请联系 Microsoft 支持部门 寻求技术帮助。

后续步骤

以下文章可帮助你准备和使用新的 Windows Server 版本：

- 安装或卸载角色、角色服务或功能
- Windows Server 管理概述
- 开始使用 Windows Admin Center
- 密钥管理服务 (KMS) 激活规划
- 使用基于 Active Directory 的激活进行激活

如果想要了解有关部署、安装后配置和激活选项的详细信息，请查看 Windows Server 部署、配置和管理学习路径。

配置安全核心服务器

项目 • 2024/01/09

安全核心是提供内置硬件、固件、驱动程序和操作系统安全功能的功能集合。 本文介绍如何使用 Windows Admin Center、Windows Server 桌面体验和组策略配置安全核心服务器。

安全核心服务器旨在为关键数据和应用程序提供安全平台。 有关详细信息，请参阅什么是安全核心服务器?

先决条件

在配置安全核心服务器之前，必须在 BIOS 中安装和启用以下安全组件：

- 安全启动。
- 受信任的平台模块 (TPM) 2.0。
- 系统固件必须满足预启动 DMA 保护要求，并在 ACPI 表中设置适当的标志，以选择加入并启用内核 DMA 保护。 若要详细了解内核 DMA 保护，请参阅适用于 OEM 的内核 DMA 保护（内存访问保护）。
- 在 BIOS 中启用了以下支持的处理器：
  - 虚拟化扩展。
  - 输入/输出内存管理单元 (IOMMU)。
  - 用于测量的动态信任根 (DRTM)。
  - 基于 AMD 的系统也需要透明安全内存加密。

> **ⓘ 重要**
>
> 在 BIOS 中启用每个安全功能可能会因硬件供应商而异。 务必检查硬件制造商的安全核心服务器启用指南。

可以在 Windows Server Catalog 中找到已针对安全核心服务器认证的硬件，并在 Azure Stack HCI 目录 中找到已针对 Azure Stack HCI 服务器认证的硬件。

启用安全功能

若要配置安全核心服务器，需要启用特定的 Windows Server 安全功能，选择相关方法并按照步骤操作。

GUI

下面介绍如何使用用户界面启用安全核心服务器。

1. 从 Windows 桌面中，打开“开始”菜单，选择“Windows 管理工具”，打开“计算机管理”。
2. 在“计算机管理”中，选择“设备管理器”，根据需要解决任何设备错误。
   a. 对于基于 AMD 的系统，在继续操作之前，请确认 DRTM 启动驱动程序设备存在
3. 从 Windows 桌面中，打开“开始”菜单，选择“Windows 安全”。
4. 选择“设备安全”>“核心隔离详细信息”，然后启用“内存完整性”和“固件保护”。你需要首先启用固件保护并重启服务器，否则可能无法启用内存完整性功能。
5. 出现提示时，重启服务器。

服务器重启后，服务器即启用了安全核心服务器。

验证安全核心服务器配置

配置安全核心服务器后，选择相关方法以验证配置。

GUI

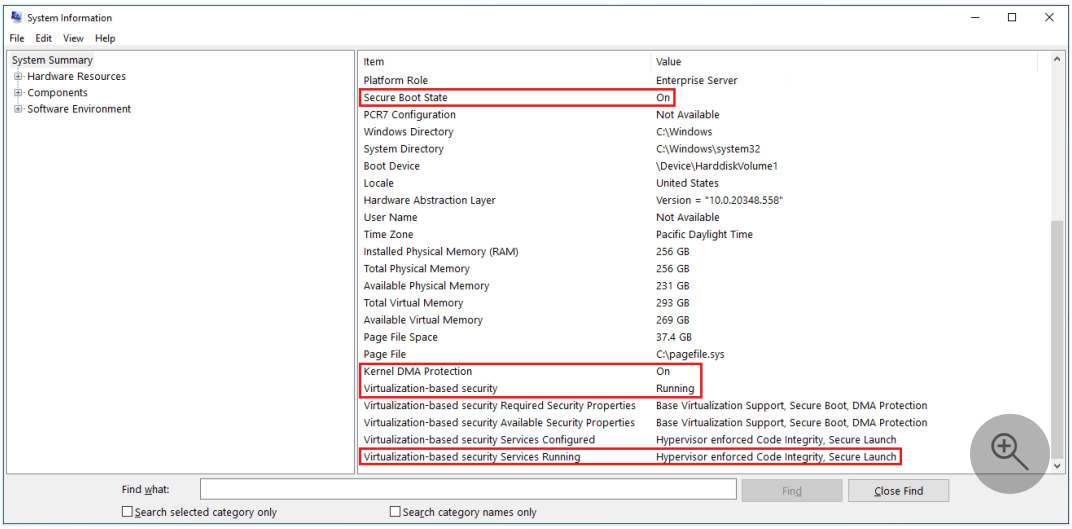
下面介绍如何使用用户界面验证安全核心服务器已配置。

1. 从 Windows 桌面中，打开“开始”菜单，键入 `msinfo32.exe` 以打开系统信息。从“系统摘要”页中，确认：

   a. “安全启动状态”和“内核 DMA 保护”处于“打开”状态。

   b. “基于虚拟化的安全性”处于“正在运行”状态。

   c. 正在运行的“基于虚拟化的安全服务”显示“虚拟机监控程序强制实施的代码完整性”和“安全启动”。



后续步骤

配置安全核心服务器后，下面提供了一些资源以了解有关以下内容的详细信息：

- 基于虚拟化的安全 (VBS)
- 内存完整性和 VBS 启用
- System Guard 安全启动

排查 Windows 批量激活问题

项目 • 2023/08/30

产品激活是在特定计算机上安装软件后验证该软件的过程。 激活确认产品为正版（而不是欺骗性副本），并且产品密钥或序列号有效，并未泄露或吊销。 激活还将建立产品密钥与安装之间的链接或关系。

批量激活是激活批量许可产品的过程。 要成为批量许可客户，组织必须与 Microsoft 签订批量许可协议。 Microsoft 提供定制的批量许可计划，可根据组织大小和购买偏好进行调整。 有关详细信息，请参阅 Microsoft Volume Licensing Service Center（Microsoft 批量许可服务中心）。

Windows Server 2016 激活指南重点介绍密钥管理服务 (KMS) 激活技术。 本部分解决常见问题，并提供针对 KMS 和多个其他批量激活技术的故障排除指南。

批量激活的最佳做法

以下文章提供有关 Microsoft 批量激活技术的技术信息和最佳做法。

密钥管理服务 (KMS)

- 规划批量激活
- Understanding KMS（了解 KMS）
- Deploying KMS Activation（部署 KMS 激活）
- Configuring KMS Hosts（配置 KMS 主机）
- Configuring DNS（配置 DNS）
- 使用密钥管理服务进行激活

基于 Active Directory 的激活 (ADBA)

- Deploy Active-Directory-based Activation（部署基于 Active Directory 的激活）
- 使用基于 Active Directory 的激活进行激活
- 基于 Active Directory 的激活概述

多次激活密钥 (MAK) 激活

- Using MAK Activation（使用 MAK 激活）
- Understanding MAK Activation（了解 MAK 激活）
- Activating MAK Clients（激活 MAK 客户端）

订阅激活

- Windows 10 订阅激活
- 部署 Windows 10 企业版许可证
- CSP 中的 Windows 10 企业版 E3

用于排查激活问题的资源

以下文章提供用于排查批量激活问题的工具的相关指南和信息：

- 密钥管理服务 (KMS) 故障排除指南
- 用于获取批量激活信息的 Slmgr.vbs 选项
- 示例：排查无法激活 ADBA 客户端的问题

以下文章提供用于解决更多特定激活问题的指南：

- 解决常见的激活错误代码
- KMS 激活：已知问题
- MAK 激活：已知问题
- 用于排查 DNS 相关激活问题的指南
- 如何重新生成 Tokens.dat 文件

密钥管理服务 (KMS) 故障排除指南

项目 • 2023/09/22

企业客户将密钥管理服务 (KMS) 设置为部署流程的一部分，因为通过该服务，他们可以使用简单、直接的过程在其环境中激活 Windows。 通常，一旦设置了 KMS 主机，KMS 客户端就会自动连接到主机并自行激活。 然而，有时该流程不会按预期运行。 本文将引导你了解如何解决可能遇到的任何问题。

有关事件日志条目和 `slmgr.vbs` 脚本的详细信息，请参阅批量激活技术参考。

从何处开始对 KMS 进行故障排除

首先，我们来快速回顾一下 KMS 激活的工作原理。 KMS 是一种客户端-服务器模型，与动态主机配置协议 (DHCP) 有一些相似之处。 但是，KMS 会启用产品激活，而不是向客户端针对其请求发出 IP 地址。 KMS 也是一种续订模型，客户端可尝试定期重新激活。 具有两个角色：KMS 主机和 KMS 客户端 。

- KMS 主机在环境中运行激活服务并启用激活。 若要配置 KMS 主机，必须从批量许可服务中心 (VLSC) 安装 KMS 密钥，然后激活服务。
- KMS 客户端是部署于环境中的 Windows 操作系统，需要激活。 KMS 客户端可以运行任何使用批量激活的 Windows 版本。 KMS 客户端附带预装的密钥，称为*通用批量许可密钥* (GVLK) 或 *KMS 客户端安装密钥*。 GVLK 的存在使系统成为了 KMS 客户端。 KMS 客户端使用 DNS SRV 记录 (`_vlmcs._tcp`) 来识别 KMS 主机。 接下来，客户端会自动尝试发现此服务并将其用于激活客户端自身。 在 30 天开箱宽限期内，客户端尝试每两小时激活一次。 KMS 客户端激活后，将尝试每七天续订一次激活。

从故障排除的角度来看，可能必须同时查看主机和客户端才能找出问题发生的原因。

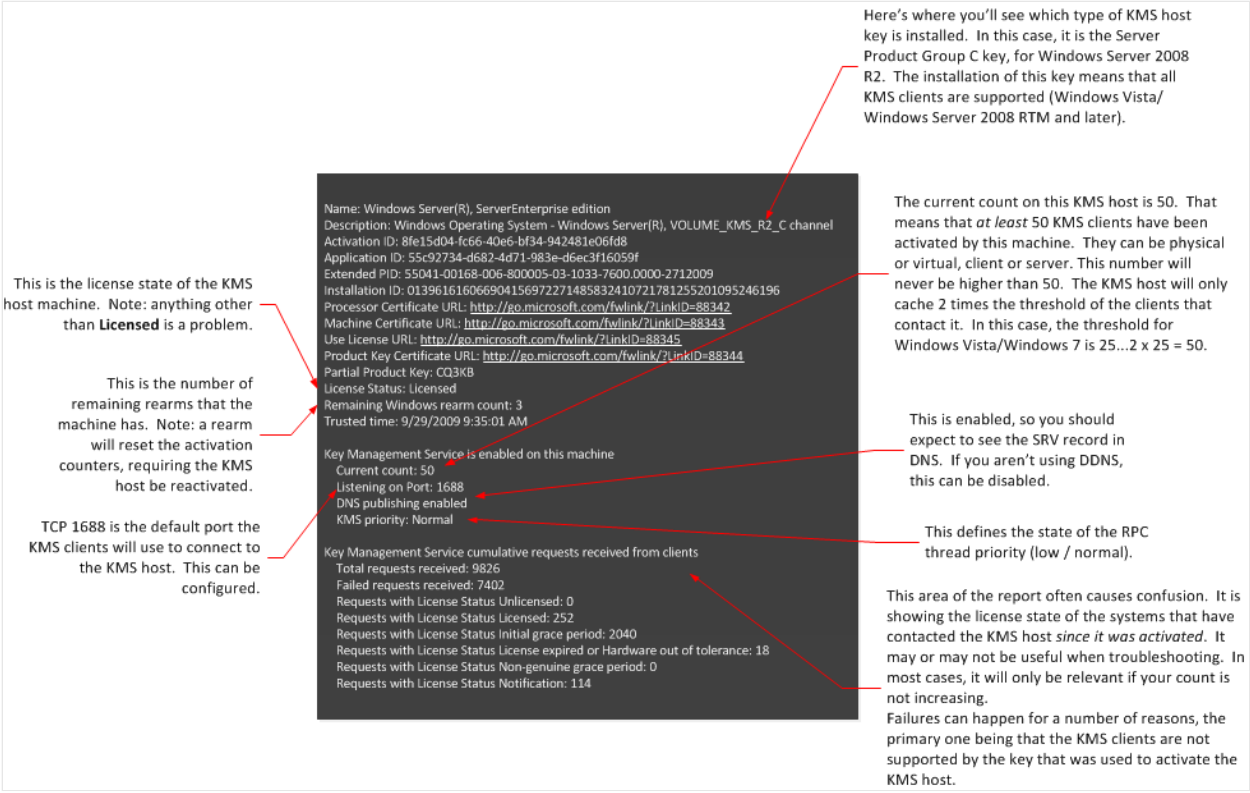
KMS 主机故障排除

在故障排除期间检查 KMS 主机时，应该查看两个方面：

- 在命令行提示符下使用 `slmgr.vbs` 命令检查主机软件许可证服务的状态。
- 检查事件查看器中是否有与许可或激活相关的事件。

使用 slmgr.vbs 命令检查软件许可服务

若要查看软件许可服务的详细输出，请打开提升的命令提示符窗口并输入 `slmgr.vbs /dlv`。 以下屏幕截图显示了在 Microsoft 内的一台 KMS 主机上运行此命令的结果。



以下是故障排除时应注意输出中的一些变量：

- *版本信息*位于 `slmgr.vbs /dlv` 输出的顶部。 版本信息对于确定服务是否是最新的非常有用。 务必确保所有内容都是最新的，因为 KMS 服务支持不同的 KMS 主机密钥。 可以使用此数据来评估当前使用的版本是否支持你尝试安装的 KMS 主机密钥。 有关更新的详细信息，请参阅更新可用于 Windows Vista 和 Windows Server 2008，以扩展对 Windows 7 和 Windows Server 2008 R2 的 KMS 激活支持。

- *名称*指示在 KMS 主机系统上运行的 Windows 版本。 可以使用此信息来排查涉及添加或更改 KMS 主机密钥的问题。 例如，可以使用此信息来验证操作系统版本是否支持你尝试使用的密钥。

- *说明*显示当前安装的密钥。 使用此字段可验证首次激活服务的密钥是否为已部署的 KMS 客户端的正确密钥。

- *许可证状态*显示 KMS 主机系统的状态。 该值应为“已获许可”。 任何其他值都意味着应该重新激活主机。

- *当前计数*显示 **0** 到 **50** 之间的计数。 计数在操作系统之间是累积的，指示在 30 天内尝试激活的有效系统的数目。

  如果计数为 0，则服务最近已激活，或者任何有效的客户端都未连接到 KMS 主机。

  无论环境中存在多少个有效系统，计数都不会增加到 **50** 以上。 该计数设置为仅缓存 KMS 客户端返回的最大许可策略的两倍。 最大策略由 Windows 客户端操作系统设置，这需要来自 KMS 主机的 **25** 或更大计数才能自行激活。 因此，KMS 主机上可以拥有的最大计数是 2 x 25 或 50。 在仅包含 Windows Server KMS 客户端的环

境中，KMS 主机上的最大计数为 **10**。 此限制是因为 Windows Server 版本的阈值为 **5**（2 x 5，或 10）。

当环境中具有已激活的 KMS 主机和足够的客户端，但计数不会增加到 1 以上时，会出现与计数相关的常见问题。 发生此问题时，意味着部署的客户端映像配置不正确，因此系统没有唯一的客户端计算机 ID (CMID)。 有关详细信息，请参阅 KMS 客户端和在将基于 Windows Vista 或 Windows 7 的新客户端计算机添加到网络时，KMS 当前计数不增加。 我们的一名支持上报工程师通过 KMS Host Client Count not Increasing Due to Duplicate CMID（由于CMID 重复导致 KMS 主机客户端计数没有增加）也发布了有关此问题的博客文章。

计数可能不会增加的另一个原因是，环境中的 KMS 主机过多，而计数在所有这些主机中分布。

- 侦听端口。 与 KMS 的通信使用匿名 RPC。 默认情况下，客户端使用 1688 TCP 端口来连接到 KMS 主机。 请确保此端口在 KMS 客户端与 KMS 主机之间打开。 可更改或配置 KMS 主机上的端口。 在通信过程中，KMS 主机会向 KMS 客户端发送端口标识。 如果更改 KMS 客户端上的端口，则在客户端与主机联系时会覆盖端口标识。

我们经常被问及有关 `slmgr.vbs /dlv` 输出"*累计请求数*"部分的问题。 通常，此数据对于故障排除没有用。 KMS 主机会持续记录每个尝试激活或重新激活的 KMS 客户端的状态。 失败的请求表示 KMS 主机不支持某些 KMS 客户端。 例如，如果 Windows 7 KMS 客户端尝试针对使用 Windows Vista KMS 密钥激活的 KMS 主机进行激活，则激活会失败。

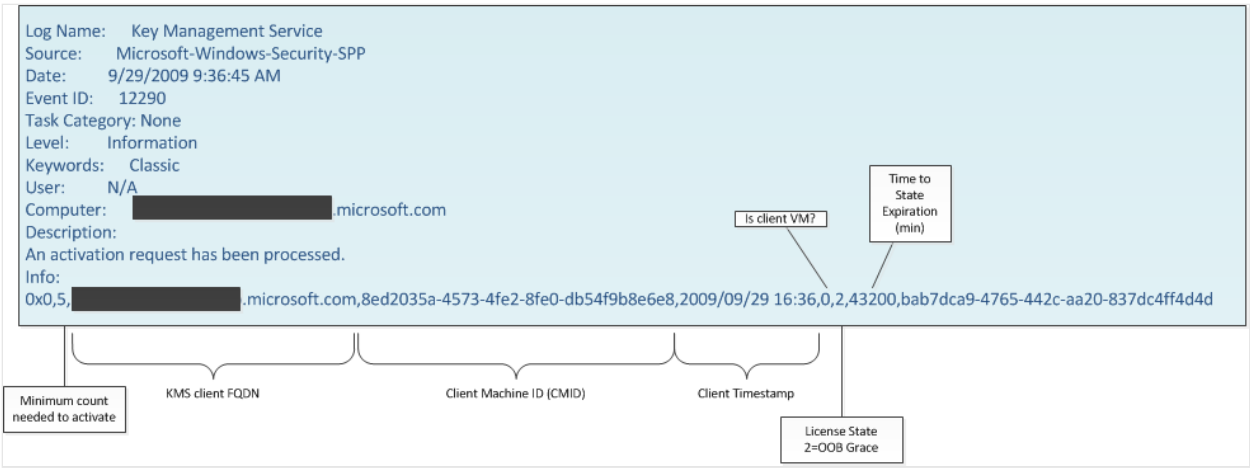
"*具有许可证状态的请求*"行说明过去和现在所有可能的许可证状态。 从故障排除的角度来看，仅当计数不按预期增加时，此数据才适用。 在这种情况下，应看到失败的请求数增加。 若要解决此问题，应检查用于首次激活 KMS 主机系统的产品密钥。 另请注意，仅当重新安装 KMS 主机系统时，累积请求值才会重置。

有用的 KMS 主机事件

你应该熟悉以下部分中描述的事件 ID，以便更有效地排查与主机相关的问题。

事件 ID 12290

当 KMS 客户端在尝试激活时联系主机时，KMS 主机会创建一个标记为*事件 ID 12290* 的日志。 事件 ID 12290 包含可用于确定联系主机的客户端类型以及发生故障的原因的信息。 事件 ID 12290 项的以下段来自 KMS 主机的密钥管理服务事件日志。



事件详细信息包括下列信息：

- *激活所需的最小计数*，报告来自 KMS 主机的计数必须为 **5** 才能激活客户端。 这意味着该操作系统是 Windows Server 操作系统，尽管此变量本身并未指示客户端正在使用哪个版本。 如果客户端未激活，请确保主机的计数允许客户端激活。
- *客户端计算机 ID (CMID)*，这是每个系统上的唯一值。 如果该值不是唯一的，那是因为未正确配置映像以使用 sysprep 进行分发。 若要了解有关通用化计算机的更多信息，请参阅 Sysprep（通用化）Windows 安装。 遇到此问题时，即使环境中有足够的客户端，KMS 主机计数也不会增加。 有关详细信息，请参阅在将基于 Windows Vista 或 Windows 7 的新客户端计算机添加到网络时，KMS 当前计数不增加。
- *许可证状态和状态过期时间*，这是客户端的当前许可证状态。 此变量可以帮助你判断客户端是首次尝试激活还是尝试重新激活。 时间条目还可以指示如果没有其他变化，客户端可以保持该状态多长时间。

如果要对客户端进行故障排除，并且在 KMS 主机上找不到相应的事件 ID 12290，则表示客户端未连接到 KMS 主机。 缺少事件 ID 12290 条目的原因可能包括：

- 网络中断。
- 主机未解析或未在 DNS 中注册。
- 防火墙阻止 TCP 1688。
  - 该端口也可能在环境中的其他位置被阻止，包括 KMS 主机系统本身。 KMS 主机默认具有针对 KMS 的防火墙例外，但此例外不会自动启用。 必须手动启用此例外。
- 事件日志已满。

KMS 客户端记录两个对应事件：事件 ID 12288 和事件 ID 12289。 有关这些事件的信息，请参阅 KMS 客户端部分。

事件 ID 12293

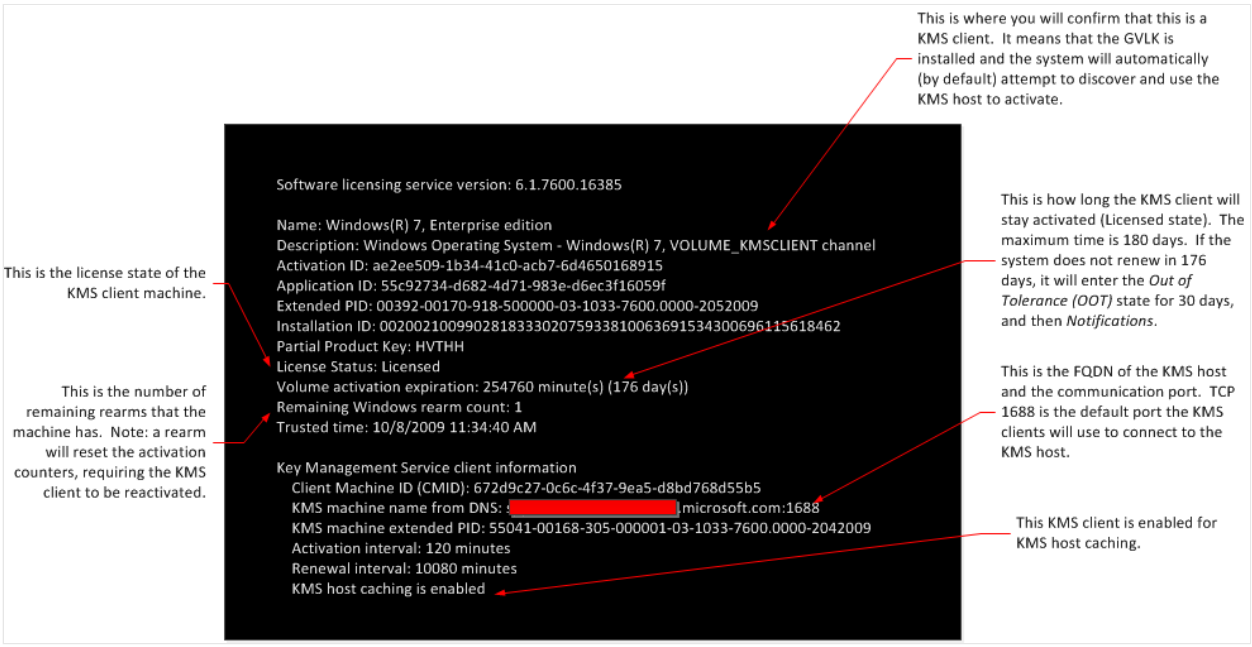
在 KMS 主机上查找的另一个相关事件是*事件 ID 12293*。 此事件表示主机未在 DNS 中发布所需的记录。 这种情况可能会导致失败，应该确保在设置主机之后和部署客户端之前不存在该事件。 有关 DNS 问题的详细信息，请参阅 KMS 和 DNS 问题的常见排查过程。

KMS 客户端

还可以使用 `slmgr.vbs` 命令和事件查看器对 KMS 客户端上的激活进行故障排除。

Slmgr.vbs 和软件许可服务

若要查看软件许可服务的详细输出，请打开提升的命令提示符窗口，并在命令提示符处输入 `slmgr.vbs /dlv`。 以下屏幕截图显示 Microsoft 内其中一台 KMS 主机上此命令的结果。



以下是故障排除时应注意输出中的一些变量：

- *名称*，指示 KMS 客户端系统使用的 Windows 版本。 可以使用此变量来验证尝试激活的 Windows 版本是否与 KMS 兼容。
- *说明*，显示安装了哪个密钥。 例如，`VOLUME_KMSCLIENT` 表示系统已安装 KMS 客户端安装密钥或 GVLK，这是批量许可证媒体的默认配置。 具有 GVLK 的系统会自动尝试使用 KMS 主机激活。 如果此处显示其他值（如 MAK），则必须重新安装 GVLK，才能将此系统配置为 KMS 客户端。 可以按照 KMS 客户端安装密钥中的说明运行 `slmgr.vbs /ipk <GVLK>` 来手动安装密钥，或者按照批量激活管理工具 (VAMT) 技术参考中的说明使用 VAMT。
- *部分产品密钥*，可用于确定 KMS 客户端安装密钥是否与 KMS 客户端使用的操作系统匹配。 默认情况下，正确的密钥存在于使用批量许可服务中心 (VLSC) 门户中的媒体生成的系统上。 在某些情况下，客户可以使用多次激活密钥 (MAK) 激活，直到

环境中具有足够多的系统来支持 KMS 激活为止。 必须在这些系统上安装 KMS 客户端安装密钥，才能将系统从 MAK 转换为 KMS。 使用 VAMT 安装此密钥，并确保使用正确的密钥。

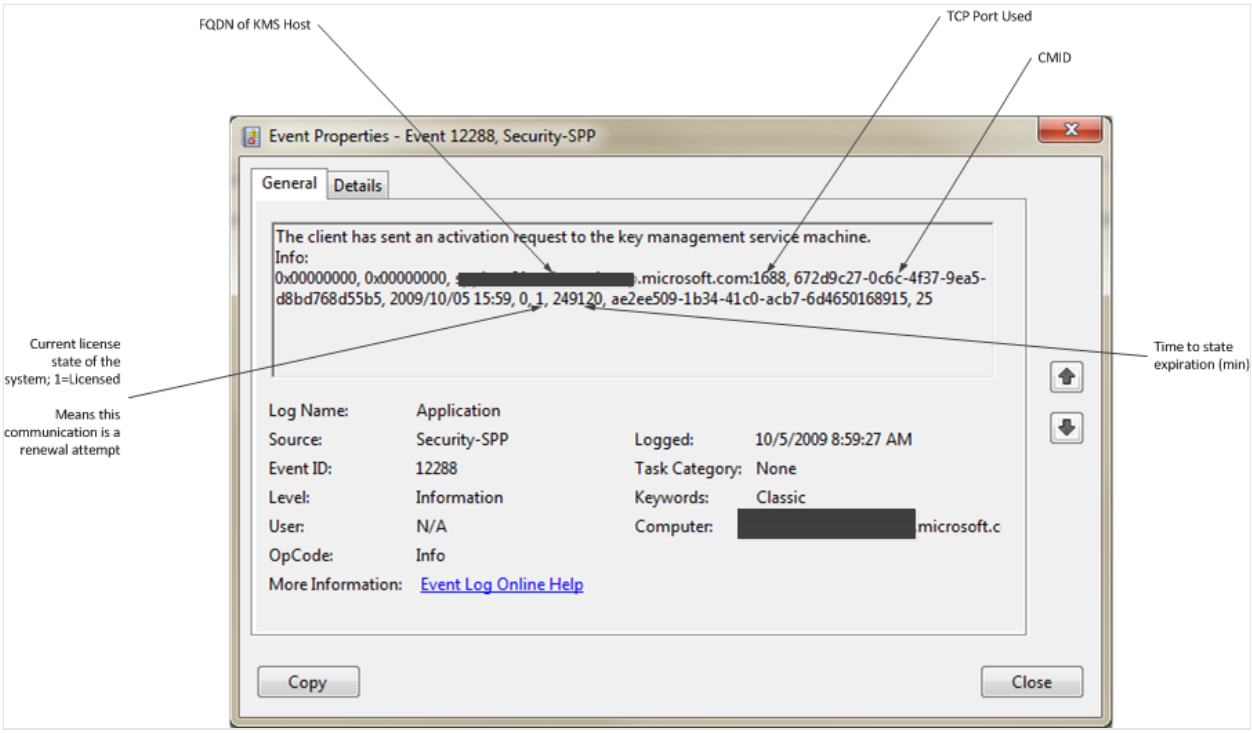
- *许可证状态*显示 KMS 客户端系统的状态。 对于 KMS 激活的系统，此值应为“**已获许可**”。 任何其他值都可能表示存在问题。 例如，如果 KMS 主机正常运行，但 KMS 客户端仍然未激活或停留在**宽限**状态，则意味着某些原因阻止客户端访问主机系统。 这种阻止可能是防火墙问题、网络中断等。
- *客户端计算机 ID (CMID)*，在每个 KMS 客户端中应该是唯一的。 如使用 slmgr.vbs 命令检查软件许可服务中所述，与计数相关的一个常见问题是，无论你在环境中激活多少个 KMS 主机或客户端，计数都不会增加到超过 1。 有关详细信息，请参阅在将基于 Windows Vista 或 Windows 7 的新客户端计算机添加到网络时，KMS 当前计数不增加。
- *DNS 中的 KMS 计算机名称*，显示客户端成功用于激活的 KMS 主机的 FQDN 以及用于通信的 TCP 端口。
- *KMS 主机缓存*，显示是否启用缓存。 通常，缓存默认处于启用状态。 启用缓存后，KMS 客户端将缓存用于激活的 KMS 主机名称，并在重新激活时直接与此主机通信，而不需要查询 DNS。 如果客户端无法与缓存的 KMS 主机联系，则会查询 DNS 来发现新的 KMS 主机。

KMS 客户端事件

以下部分介绍了你应该熟悉的客户端事件，以帮助你更有效地解决潜在问题。

事件 ID 12288 和事件 ID 12289

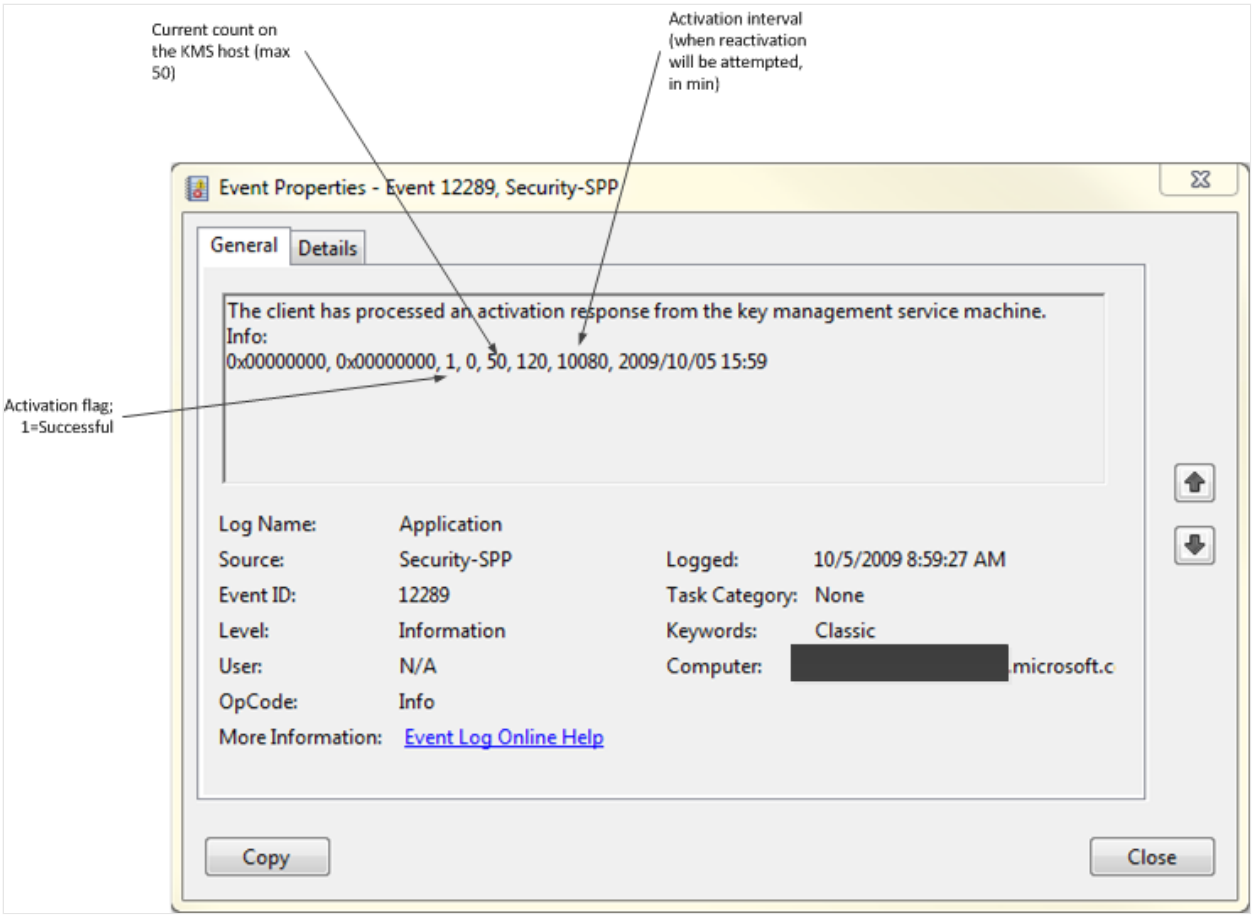
KMS 客户端成功激活或重新激活时，客户端会记录两个事件：事件 ID 12288 和事件 ID 12289。 以下屏幕截图显示事件 ID 12288 条目中来自 KMS 客户端的密钥管理服务事件日志的段。



如果你只看到事件 ID 12288，而没有相应的事件 ID 12289，则可能是 KMS 客户端无法访问 KMS 主机、KMS 主机未响应，或者客户端未收到主机的响应。 在这种情况下，必须验证 KMS 主机是否可发现，以及 KMS 客户端是否可以联系该主机。

事件 ID 12288 中最相关的信息是“*信息*”字段中的数据。 例如，“信息”显示客户端的当前状态以及客户端尝试激活时使用的 FQDN 和 TCP 端口。 可以使用 FQDN 来解决 KMS 主机上的计数不增加的问题。 例如，如果客户端可用的 KMS 主机过多（合法的或不受支持的系统），则计数可能会分布在所有这些主机上。

激活失败并不总是意味着客户端有事件 ID 12288，而没有 12289。 激活或重新激活失败可能也有这两个事件。 在这种情况下，必须检查第二个事件来验证失败的原因。



事件 ID 12289 的信息部分提供以下信息：

- *激活标志*，指示激活是成功 (**1**) 还是失败 (**0**)。
- *KMS 主机上的当前计数*，显示客户端尝试激活时 KMS 主机上的计数值。 如果激活失败，则可能是因为此客户端操作系统的计数不足，或者环境中没有足够的系统来生成计数。

支持人员需要你提供什么信息?

如果激活在故障排除后未按预期工作，你可以联系 Microsoft 支持 寻求技术帮助。 支持工程师通常会要求提供以下信息：

- 来自 KMS 主机和 KMS 客户端系统的 `slmgr.vbs /dlv` 输出。
- 来自 KMS 主机的事件日志（密钥管理服务日志）和来自 KMS 客户端系统的事件日志（应用程序日志）。

后续步骤

- 询问核心团队：#激活

用于获取批量激活信息的 Slmgr.vbs 选项

项目 • 2023/08/30 • 适用于: Windows Server 2012 R2, Windows 10, Windows 8.1

下面介绍了 Slmgr.vbs 脚本的语法，本文的表介绍了每个命令行选项。

Windows 命令提示符

```
slmgr.vbs [<ComputerName> [<User> <Password>]] [<Options>]
```

ⓘ 备注

在本文中，方括号 [] 括起来的是可选参数，尖括号 <> 括起来的是占位符。 键入这些语句时，请省略括号，并使用相应的值替换占位符。

ⓘ 备注

有关使用批量激活的其他软件产品的信息，请参阅专门为这些应用程序编写的文档。

在远程计算机上使用 Slmgr

若要管理远程客户端，请使用批量激活管理工具 (VAMT) 版本 1.2 或更高版本，或创建意识到平台之间差异的自定义 WMI 脚本。 有关批量激活的 WMI 属性和方法的详细信息，请参阅批量激活的 WMI 属性和方法。

ⓘ 重要

由于 Windows 7 和 Windows Server 2008 R2 中的 WMI 更改，因此 Slmgr.vbs 脚本不适用于跨平台工作。 不支持使用 Slmgr.vbs 从 Windows Vista® 操作系统管理 Windows 7 或 Windows Server 2008 R2 系统。 尝试从 Windows 7 或 Windows Server 2008 R2 中管理较旧系统将生成特定版本不匹配错误。 例如，运行脚本 **cscript slmgr.vbs <vista_machine_name> /dlv** 将产生以下输出：

> Microsoft (R) Windows Script Host Version 5.8 版权所有 (C) Microsoft Corporation。 保留所有权利。
>
> 远程计算机不支持此版本的 SLMgr.vbs

常规 Slmgr.vbs 选项

选项	说明
[<ComputerName>]	远程计算机的名称（默认为本地计算机）
[<User>]	具有远程计算机上所需权限的帐户
[<Password>]	具有远程计算机上所需权限的帐户的密码

全局选项

选项	说明
/ipk <ProductKey>	尝试安装 5×5 产品密钥。 确认参数提供的产品密钥有效且适用于已安装的操作系统。 如果没有，则返回错误。 如果密钥有效且适用，则安装密钥。 如果已安装一个密钥，则静默替换它。 若要防止许可证服务中的不稳定性，应重新启动系统或软件保护服务。 必须从提升的“命令提示符”窗口下运行此操作，或必须将“标准用户操作”注册表值设置为允许非特权的用户额外访问软件保护服务。
/ato [<Activation ID>]	对于安装了 KMS 主机密钥或多个激活密钥 (MAK) 的零售版和卷系统，/ato 提示 Windows 尝试联机激活。 对于安装了通用批量许可证密钥 (GVLK) 的系统，这提示尝试 KMS 激活。 当运行 /ato 时，已设置为挂起自动 KMS 激活尝试 (/stao) 的系统仍然尝试 KMS 激活 。 **注意：** 从 Windows 8（和 Windows Server 2012）开始，/stao 选项已弃用。 请改用 /act-type 选项。 参数 <Activation ID> 扩展 /ato 支持，以标识在计算机上安装的 Windows 版本。 指定 <Activation ID> 参数隔离与该激活 ID 相关联版本的选项的影响。 运行所有 Slmgr.vbs /dlv 以获取已安装版本的 Windows 的激活 ID。 如果必须支持其他应用程序，请参阅该应用程序提供的指南，以获取进一步说明。 KMS 激活不需要提升的权限。 但是，联机激活需要提升，或必须将标准用户操作注册表值设置为允许非特权的用户额外访问软件保护服务。
/dli [<Activation ID> | All]	显示许可证信息。 默认情况下， **/dli** 显示已安装的活动 Windows 版本的许可证信息。 指定 <Activation ID> 参数可显示与该激活 ID 相关联的指定版本的许可证信息。 将 All 指定为参数将显示所有适用的已安装产品的许可证信息。 此操作不需要提升的权限。
/dlv [<Activation ID> | All]	显示详细的许可证信息。 默认情况下， **/dlv** 显示已安装操作系统的许可证信息。 指定 <Activation ID> 参数可显示与该激活 ID 相关联的指定版本的许可证信息。 指定 All 参数将显示所有适用的已安装产品的许可证信息。 此操作不需要提升的权限。

选项	说明
/xpr [<Activation ID>]	显示产品的激活到期日期。 默认情况下，因为 MAK 和零售激活是永久性的，所以这指的是当前 Windows 版本，主要用于 KMS 客户端。 指定 <Activation ID> 参数可显示与该激活 ID 相关联的指定版本的激活到期日期。此操作不需要提升的权限。

高级选项

选项	说明
/cpky	某些服务操作要求产品密钥在全新体验 (OOBE) 操作期间在注册表中可用。 **/cpky** 选项从注册表中删除产品密钥以防止恶意代码盗用此密钥。 对于部署密钥的零售安装，最佳做法建议运行此选项。 因为此选项是这些密钥的默认行为，因此 MAK 和 KMS 主机密钥不需要此选项。 此选项仅是默认行为不是从注册表中清除该密钥的其他密钥类型所必需的。 必须在提升的“命令提示符”窗口中运行此操作。
/ilc <license_file>	此选项安装所需的参数指定的许可证文件。 这些许可证可以作为疑难解答措施安装以支持基于令牌的激活，或者作为上架应用程序的手动安装的一部分安装。 在此过程中，不会验证许可证：许可证验证超出 Slmgr.vbs 的范围。 相反，在运行时验证由软件保护服务处理。 必须从提升的“命令提示符”窗口下运行此操作，或必须将“标准用户操作”注册表值设置为允许非特权的用户额外访问软件保护服务。
/rilc	此选项重新安装存储在 %SystemRoot%\system32\oem 和 %SystemRoot%\System32\spp\tokens 中的所有许可证。 这些许可证是在安装过程中存储的“已知正确”副本。 将替换受信任应用商店中的任何匹配许可证。 任何其他许可证（例如，受信任的颁发机构 (TA) 颁发许可证 (IL)、应用程序的许可证）不会受到影响。 必须在提升的“命令提示符”窗口中运行此操作，或必须将“标准用户操作”注册表值设置为允许非特权的用户额外访问软件保护服务。
/rearm	此选项将重置激活计时器。 **/rearm** 过程也称为 **sysprep /generalize**。 如果 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm 注册表项设为 1，则此操作将不执行任何操作 。 请参阅批量激活的注册表设置详细了解此注册表项。 必须在提升的“命令提示符”窗口中运行此操作，或必须将“标准用户操作”注册表值设置为允许非特权的用户额外访问软件保护服务。
/rearm-app <Application ID>	重置指定应用的许可状态。
/rearm-sku <Application	重置指定 SKU 的许可状态。

选项	说明
ID>	
/upk [<Application ID>]	此选项卸载当前 Windows 版本的产品密钥。 重新启动后，系统将处于未经许可的状态下，除非安装了新产品密钥。 还可以使用 <Activation ID> 参数来指定不同的已安装产品。 必须从提升的“命令提示符”窗口下运行此操作。
/dti [<Activation ID>]	为脱机激活显示安装 ID。
/atp <Confirmation ID>	使用用户提供的确认 ID 激活产品。

KMS 客户端选项

选项	说明
/skms <Name[:Port] | : port> [<Activation ID>]	此选项指定名称，或者要连接的 KMS 主计算机的端口（可选）。 设置此值将禁用 KMS 主机的自动检测。 如果 KMS 主机仅使用 Internet 协议版本 6 (IPv6)，必须采用格式 <hostname>:<port> 指定地址。 IPv6 地址包含冒号 (:)，Slmgr.vbs 脚本会错误地分析它。 必须在提升的“命令提示符”窗口中运行此操作。
/skms-domain <FQDN> [<Activation ID>]	设置特定的 DNS 域，可以在该域中找到所有 KMS SRV 记录。 如果使用 /skms 选项设置特定的单个 KMS 主机，则此设置将不起作用。 使用此选项（特别是在断开连接的命名空间环境中）强制 KMS 忽略 DNS 后缀搜索列表，并改为在指定的 DNS 域中查找 KMS 主机记录。
/ckms [<Activation ID>]	此选项从注册表中删除特定的 KMS 主机名、地址和端口信息，并还原 KMS 自动发现行为。 必须在提升的“命令提示符”窗口中运行此操作。
/skhc	此选项启用 KMS 主机缓存（默认）。 客户端发现工作 KMS 主机之后，此设置可防止域名系统 (DNS) 优先级和权重影响与主机的进一步通信。 如果系统无法再联系工作 KMS 主机，客户端将尝试发现新的主机。 必须在提升的“命令提示符”窗口中运行此操作。
/ckhc	此选项禁用 KMS 主机缓存。 此设置指示客户端在每次尝试 KMS 激活（建议在使用优先级和权重时执行此操作）时使用 DNS 自动发现。 必须在提升的“命令提示符”窗口中运行此操作。

KMS 主机配置选项

选项	说明
/sai <Interval>	此选项为未激活的客户端设置时间间隔（以分钟为单位），以尝试连接 KMS。 激活时间间隔必须介于 15 分钟到 30 天之间，尽管建议采用默认值（2 小时）也是如此。 KMS 客户端最初从注册表中选取此时间间隔，但在接收第一个 KMS 响应后切换到 KMS 设置。 必须在提升的“命令提示符”窗口中运行此操作。
/sri <Interval>	此选项为激活的客户端设置续订时间间隔（以分钟为单位），以尝试连接 KMS。 续订时间间隔必须介于 15 分钟到 30 天之间。 KMS 服务器和客户端上最初都设置了此选项。 默认值为 10,080 分钟（7 天）。 KMS 客户端最初将从注册表中拾取此间隔，但在收到第一个 KMS 响应后将切换到 KMS 设置。 必须在提升的“命令提示符”窗口中运行此操作。
/sprt <Port>	此选项设置在其上侦听客户端激活请求的 KMS 主机的端口。 默认的 TCP 端口为 1688。 必须从提升的“命令提示符”窗口下运行此操作。
/sdns	通过 KMS 主机（默认）启用 DNS 发布。 必须在提升的“命令提示符”窗口中运行此操作。
/cdns	通过 KMS 主机禁用 DNS 发布。 必须在提升的“命令提示符”窗口中运行此操作。
/spri	将 KMS 优先级设置为正常（默认）。 必须在提升的“命令提示符”窗口中运行此操作。
/cpri	将 KMS 优先级设置为低。 使用此选项以最大程度地减少来自共同托管环境中的 KMS 的争用。 请注意这可能导致 KMS 匮乏，具体取决于哪些其他应用程序或服务器角色处于活动状态。 谨慎使用。 必须在提升的“命令提示符”窗口中运行此操作。
/act-type [<Activation-Type>] [<Activation ID>]	此选项将限制批量激活的注册表中的值设置为单个类型。 激活类型 **1** 仅将激活限制为 Active Directory；**2** 将其限制为 KMS 激活；**3** 将其限制为基于令牌的激活。 **0** 选项允许任何激活类型，并为默认值。

基于令牌的激活配置选项

选项	说明
/lil	列出已安装的基于令牌的激活颁发许可证。
/ril <ILID><ILvID>	删除已安装的基于令牌的激活颁发许可证。 必须从提升的“命令提示符”窗口下运行此操作。

选项	说明
/stao	设置 **Token-based Activation Only** 标志，从而禁用自动 KMS 激活。 必须在提升的"命令提示符"窗口中运行此操作。 已在 Windows Server 2012 R2 和 Windows 8.1 中删除此选项。 请改用 **/act–type** 选项。
/ctao	清除**仅基于令牌的激活** 标志（默认），从而启用自动 KMS 激活。 必须在提升的"命令提示符"窗口中运行此操作。 已在 Windows Server 2012 R2 和 Windows 8.1 中删除此选项。 请改用 /act-type 选项。
/ltc	列出基于令牌的有效激活证书，这些证书可激活已安装的软件。
/fta <Certificate Thumbprint> [<PIN>]	使用标识的证书强制执行基于令牌的激活。 如果使用受硬件（例如智能卡）保护的证书，提供可选个人标识号 (PIN) 以解锁私钥，无需 PIN 提示。

基于 Active Directory 的激活配置选项

选项	说明
/ad-activation-online <Product Key> [<Activation Object name>]	使用命令提示符正在运行的凭据收集 Active Directory 数据和启动 Active Directory 林激活。 无需本地管理员访问权限。但需要对该林的根域中的激活对象容器的读/写权限。
/ad-activation-get-IID <Product Key>	此选项在手机模式下启动 Active Directory 林激活。 输出内容是安装 ID (IID)，可用于在 Internet 连接不可用时通过电话激活该林。 在激活电话呼叫中提供 IID 后，将返回用于完成激活的 CID。
/ad-activation-apply-cid <Product Key><Confirmation ID> [<Activation Object name>]	使用此选项时，输入激活电话呼叫中提供的 CID 以完成激活
[/name: <AO_Name>]	或者，你可以将 **/name** 选项附加到其中任何命令，以为存储在 Active Directory 中的激活对象指定名称。 名称不能超过 40 个 Unicode 字符。 使用双引号显式定义名称字符串。 在 Windows Server 2012 R2 和 Windows 8.1 中，可以将该名称直接附加在 /ad-activation-online <Product Key> 和 /ad-activation-apply-cid 之后，而无需使用 /name 选项。
/ao-list	显示可用于本地计算机的所有激活对象。
/del-ao <AO_DN> /del-ao <AO_RDN>	从林中删除指定的激活对象。

其他参考

- 批量激活技术参考
- 批量激活概述

排查 Windows 激活错误代码问题

项目 • 2024/02/19

本文提供故障排除信息，帮助你响应尝试使用多重激活密钥 (MAK) 或密钥管理服务 (KMS) 在一台或多台基于 Windows 的计算机上执行批量激活时可能收到的错误消息。

> **备注**
>
> 本文适用于技术支持代理和 IT 专业人员。 如果你正在寻找有关 Windows 激活错误消息的详细信息，请参阅 **获取有关 Windows 激活错误的帮助**。

在下表中查找错误代码，然后选择链接以查看有关该错误代码以及如何解决该错误代码的详细信息。

有关批量激活的详细信息，请参阅 规划批量激活。

有关当前和最新版本 Windows 的批量激活的详细信息，请参阅 批量激活 [客户端]。

有关旧版 Windows 批量激活的详细信息，请参阅 Windows Vista、Windows Server 2008、Windows Server 2008 R2 和 Windows 7 的批量激活信息。

还可以试用 我们的虚拟代理，这有助于快速识别和排查与 KMS 和 MAK 激活相关的问题。

诊断工具

> **备注**
>
> 此工具旨在解决运行企业版、专业版或服务器版 Windows 的计算机上的 Windows 激活问题。

Microsoft 支持部门和恢复助手 (SaRA) 简化了 Windows KMS 激活故障排除。

下载助手

SaRA 工具通过尝试启动 Windows 进行故障排除。 如果 Windows 返回激活错误代码，该工具会显示以下已知错误代码的目标解决方案：

- 0xC004F038
- 0xC004F039
- 0xC004F041

- 0xC004F074
- 0xC004C008
- 0x8007007b
- 0xC004C003
- 0x8007232B

错误代码摘要

下表列出了 Windows 激活的已知错误代码，并包括本文后面的相关部分的链接，这些部分可帮助你解决相关问题。

展开表

错误代码	错误消息	激活类型
0x8004FE21	此计算机未运行正版 Windows。	麦 KMS 客户端
0x80070005	拒绝访问。 请求的操作需要提升的权限。	麦 KMS 客户端 KMS 主机
0x8007007b	0x8007007b DNS 名称不存在。	KMS 客户端
0x80070490	输入的产品密钥不起作用。 检查产品密钥并重试，或输入其他密钥。	麦
0x800706BA	RPC 服务器不可用。	KMS 客户端
0x8007232A	DNS 服务器故障。	KMS 主机
0x8007232B	DNS 名称不存在。	KMS 客户端
0x8007251D	找不到 DNS 查询的记录。	KMS 客户端
0x80092328	DNS 名称不存在。	KMS 客户端
0xC004B100	激活服务器确定无法激活计算机。	麦

错误代码	错误消息	激活类型
0xC004C001	激活服务器确定指定的产品密钥无效。	麦
0xC004C003	激活服务器确定指定的产品密钥被阻止。	麦
0xC004C008	激活服务器确定无法使用指定的产品密钥。	公里
0xC004C020	激活服务器报告多次激活密钥已超出其限制。	麦
0xC004C021	激活服务器报告已超出多次激活密钥扩展限制。	麦
0xC004F009	软件保护服务报告宽限期已过期。	麦
0xC004F00F	软件许可服务器报告硬件 ID 绑定超出了容错级别。	麦 KMS 客户端 KMS 主机
0xC004F014	软件保护服务报告产品密钥不可用。	麦 KMS 客户端
0xC004F02C	软件保护服务报告脱机激活数据的格式不正确。	麦 KMS 客户端
0xC004F035	软件保护服务报告，无法使用批量许可证产品密钥激活计算机。	KMS 客户端 KMS 主机
0xC004F038	软件保护服务报告无法激活计算机。 密钥管理服务 (KMS) 报告的计数不足。 请与您的系统管理员联系。	KMS 客户端
0xC004F039	软件保护服务报告无法激活计算机。 未启用密钥管理服务 (KMS) 。	KMS 客户端
0xC004F041	软件保护服务确定密钥管理服务器 (KMS) 未激活。 需要激活 KMS。	KMS 客户端
0xC004F042	软件保护服务确定无法使用指定的密钥管理服务 (KMS) 。	KMS 客户端
0xC004F050	软件保护服务报告产品密钥无效。	麦 公里 KMS 客户端

错误代码	错误消息	激活类型
0xC004F051	软件保护服务报告产品密钥被阻止。	麦 公里
0xC004F064	软件保护服务报告非正版宽限期已过期。	麦
0xC004F065	软件保护服务报告应用程序在有效的非正版期限内运行。	麦 KMS 客户端
0xC004F06C	软件保护服务报告无法激活计算机。 密钥管理服务 (KMS) 确定请求时间戳无效。	KMS 客户端
0xC004F074	软件保护服务报告无法激活计算机。 无法联系任何密钥管理服务 (KMS) 。 有关其他信息，请参阅应用程序事件日志。	KMS 客户端

若要解决错误，请参阅每个错误消息的以下原因和故障排除步骤。

0x8004FE21此计算机未运行正版 Windows

收到此错误时，会看到以下错误消息：

> 此计算机未运行正版 Windows。

原因：

出现此问题的原因有多种：

- 运行 Windows 版本的计算机上，用户或程序安装的语言包 (MUI) ，但未获得额外语言包的许可。

  > **备注**
  >
  > 此问题不一定表示篡改。 即使该版本的 Windows 未获得这些语言包的许可，某些应用程序也可以安装多语言支持。

- 当恶意软件修改 Windows 以安装更多功能时。
- 某些系统文件已损坏。

解决方案：

若要解决此问题，必须重新安装操作系统。

0x80070005访问被拒绝

此错误消息的全文为：

> 拒绝访问。 请求的操作需要提升的权限。

原因：

用户帐户控制 (UAC) 禁止激活进程在非提升的命令提示符窗口中运行。

解决方案：

1. 打开“开始”菜单并搜索 “**命令提示符**”。
2. 右键单击“ **命令提示符**”，然后选择“ **以管理员身份运行**”。
3. 在命令提示符下，运行 `slmgr.vbs`。

0x8007007b DNS 名称不存在

遇到此错误时，会看到以下错误消息：

> DNS 名称不存在。

原因：

如果 KMS 客户端在 DNS 中找不到 KMS SRV 资源记录，则可能会出现此问题。

解决方案：

有关排查此类 DNS 相关问题的详细信息，请参阅 KMS 和 DNS 问题的常见故障排除过程。

0x80070490 产品密钥不起作用

遇到此问题时，会看到以下错误消息：

> 输入的产品密钥不起作用。 检查产品密钥并重试，或输入其他密钥。

原因：

遇到此问题的可能原因有两种：

- MAK) 多重激活密钥 (无效。
- Windows Server 2019 中的一个已知问题干扰了产品密钥的身份验证。

解决方案：

若要解决此问题并激活计算机，请执行以下操作：

1. 打开“开始”菜单并搜索 “**命令提示符**”。
2. 右键单击“ **命令提示符**”，然后选择“ **以管理员身份运行**”。
3. 在命令提示符下运行以下命令：

```
控制台
```

```
slmgr -ipk <5x5 key>
```

0x800706BA RPC 服务器不可用

遇到此错误时，会看到以下错误消息：

> RPC 服务器不可用。

原因：

由于以下原因，可能会遇到此问题：

- KMS 主机未配置防火墙设置。
- DNS SRV 记录已过时。

解决方案 1：

在 KMS 主机上，请确保已在 TCP 端口 1688 上为密钥管理服务启用防火墙例外。

解决方案 2：

检查 DNS SRV 记录，并确保它们指向有效的 KMS 主机。

解决方案 3：

如果在执行解决方案 1 和 2 后仍看到此错误，检查网络连接，确保可以访问服务器。

还可以按照 KMS 和 DNS 问题的常见故障排除过程中的说明进行操作。

0x8007232A DNS 服务器故障

遇到此问题时，会看到以下错误消息：

> DNS 服务器故障。

原因：

当系统出现网络或 DNS 问题时，可能会遇到此问题。

解决方案：

若要解决此问题，请按照 KMS 和 DNS 问题的常见故障排除过程中的说明对网络连接和 DNS 进行故障排除。

0x8007232B DNS 名称不存在

遇到此错误时，会看到以下错误消息：

> DNS 名称不存在。

原因：

当 KMS 客户端在 DNS 中找不到 KMS 服务器资源记录 (SRV R) 时，将显示此错误消息。

解决方案 1：

请确保已安装 KMS，并且已启用 DNS 发布 (默认) 。 如果 DNS 不可用，请打开提升的命令提示符并运行以下命令，将 KMS 客户端指向 KMS 主机：

```
控制台
```

```
slmgr.vbs /skms <kms_host_name>
```

解决方案 2：

如果没有 KMS 主机，请获取并安装 MAK，然后再次尝试激活系统。

如果这些解决方案无法解决问题，请参阅 KMS 和 DNS 问题的常见故障排除过程中的说明。

0x8007251D 找不到 DNS 查询的记录

遇到此错误时，会看到以下错误消息：

> 找不到 DNS 查询的记录。

原因：

当 KMS 客户端在 DNS 中找不到 KMS SRV 记录时，将显示此错误消息。

解决方案：

若要解决此问题，请按照 KMS 和 DNS 问题的常见故障排除过程中 的说明对网络连接和 DNS 进行故障排除。

0x80092328 DNS 名称不存在

遇到此错误时，会看到以下错误消息：

> DNS 名称不存在。

原因：

如果 KMS 客户端在 DNS 中找不到 KMS SRV 资源记录，则可能会遇到此问题。

解决方案：

若要解决此问题，请按照 KMS 和 DNS 问题的常见故障排除过程中 的说明对网络连接和 DNS 进行故障排除。

0xC004B100激活服务器确定无法激活计算机

遇到此错误时，会看到以下错误消息：

> 激活服务器确定无法激活计算机。

原因：

当 Microsoft 不支持你正在使用的 MAK 时，可能会遇到此问题。

解决方案：

若要排查此问题，请验证所使用的 MAK 是否与 Microsoft 提供的 MAK 相同。 若要验证 MAK 是否有效，请联系 Microsoft 许可激活中心 。

0xC004C001激活服务器确定指定的产品密钥无效

遇到此错误时，会看到以下错误消息：

> 激活服务器确定指定的产品密钥无效。

原因：

输入的 MAK 无效时，可能会遇到此问题。

解决方案：

可以尝试重新输入 MAK 以确保输入了正确的信息。 否则，请通过联系 Microsoft 许可激活中心 来验证你使用的 MAK 是否有效。

0xC004C003激活服务器确定指定的产品密钥被阻止

遇到此错误时，会看到以下错误消息：

> 激活服务器确定指定的产品密钥被阻止。

原因：

如果在激活服务器上阻止 MAK，则可能会遇到此问题。

解决方案：

请联系 Microsoft 许可激活中心 以获取新的 MAK。 获取新的 MAK 后，请尝试再次安装和激活 Windows。

0xC004C008激活服务器确定无法使用指定的产品密钥

遇到此错误时，会看到以下错误消息：

> 激活服务器确定无法使用指定的产品密钥。

原因：

当 KMS 密钥超过其激活限制时，将显示此错误消息。 最多只能在不超过 6 台不同的计算机上激活 KMS 主机密钥 10 次。

解决方案：

请联系 Microsoft 许可激活中心 ，请求更多激活服务器权限。

0xC004C020激活服务器报告多次激活密钥已超出其限制

遇到此错误时，会看到以下错误消息：

> 激活服务器报告多次激活密钥已超出其限制。

原因：

当 MAK 超出其激活限制时，将显示此错误消息。 根据设计，只能激活 MAK 的次数有限。

解决方案：

请求更多激活以增加限制。 如果需要更多激活，请联系 Microsoft 许可激活中心。

0xC004C021超出多次激活密钥扩展限制

遇到此错误时，会看到以下错误消息：

> 激活服务器报告已超出多次激活密钥扩展限制。

原因：

当 MAK 超出其激活限制时，将显示此错误消息。 根据设计，只能激活 MAK 的次数有限。

解决方案：

请求更多激活以提高扩展限制。 如果需要更多激活，请联系 Microsoft 许可激活中心。

0xC004F009软件保护服务报告宽限期已过期

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告宽限期已过期。

原因：

激活系统之前宽限期过期时，会出现此错误消息。 系统当前处于“通知”状态。

解决方案：

如需帮助，请联系 Microsoft 许可激活中心。

0xC004F00F硬件 ID 绑定超出容错级别

遇到此错误时，会看到以下错误消息：

> 软件许可服务器报告硬件 ID 绑定超出了容错级别。

原因：

当系统硬件更改或其驱动程序更新时，将显示此错误消息。

解决方案 1：

如果使用 MAK 激活，请在“容错 (OOT) 宽限期内使用联机激活或电话激活来重新激活系统电话。

解决方案 2：

如果使用 KMS 激活，请尝试以下操作之一：

- 重启 Windows。
- 打开提升的命令提示符并运行以下命令：

```
控制台
slmgr.vbs /ato
```

0xC004F014软件保护服务报告产品密钥不可用

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告产品密钥不可用。

原因：

当系统上未安装产品密钥时，会出现此问题。

解决方案：

如果使用 MAK 激活，请安装 MAK 产品密钥。

如果使用 KMS 激活：

1. 检查位于 *\sources* 文件夹中安装介质上的 *Pid.txt* 文件以获取 KMS 安装密钥。
2. 安装密钥。

0xC004F02C脱机激活数据的格式不正确

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告脱机激活数据的格式不正确。

原因：

当系统检测到在手机激活期间输入的数据无效时，将显示此错误消息。

解决方案：

若要解决此问题，请确保正确输入呼叫方 ID (CID) 。

0xC004F035批量许可证密钥无效

遇到此错误时，会看到以下错误消息：

> 错误：批量许可证密钥无效。 若要激活，需要将产品密钥更改为有效的多重激活密钥 (MAK) 或零售密钥。 你必须拥有合格的操作系统许可证和批量许可证 Windows 7 升级许可证，或零售来源的 Windows 7 的完整许可证。 该软件的任何其他安装都违反了你的协议和适用的版权法。

此错误消息指示计算机的 BIOS 中没有 Windows 标记，该标记将其标识为运行合格版本的 Windows 的 OEM 系统。 简而言之，此消息表示批量许可证密钥无效。 KMS 客户端激活需要此信息。

原因：

Microsoft 仅许可 Windows 7 批量版本进行升级。 Microsoft 不支持在尚未安装合格操作系统的计算机上安装卷操作系统。

解决方案：

使用以下步骤激活批量许可证密钥：

1. 将产品密钥更改为有效的多次激活密钥 (MAK) 或零售密钥。 若要更改密钥，必须同时具有符合条件的操作系统许可证和批量许可证 Windows 7 升级许可证，或零售来源的 Windows 7 的完整许可证。
2. 尝试再次激活密钥。

如果在尝试再次激活密钥时看到错误消息0x80072ee2，则需要通过电话激活密钥。

若要通过电话激活密钥，请执行以下操作：

1. 打开命令提示符并运行 `slmgr /dti`，然后记录安装 ID 的值。
2. 请联系 Microsoft 许可激活中心 并提供安装 ID，以便接收确认 ID。
3. 若要使用确认 ID 激活，请运行 `slmgr /atp <Confirmation ID>`。

0xC004F038 密钥管理服务 (KMS) 报告的计数不足

遇到此问题时，会看到以下错误消息：

> 软件保护服务报告无法激活计算机。 密钥管理服务 (KMS) 报告的计数不足。 请与您的系统管理员联系。

原因：

当 KMS 主机上的计数不够高时，通常会遇到此问题。 对于 Windows Server，KMS 计数必须大于或等于 5。 对于 Windows (客户端) ，KMS 计数必须大于或等于 25。

解决方案：

将计算机添加到 KMS 池。 必须先在 KMS 池中拥有更多计算机，然后才能使用 KMS 激活 Windows。 若要获取 KMS 主机上的当前计数，请运行 `Slmgr.vbs /dli`。

0xC004F039未启用密钥管理服务 (KMS)

遇到此问题时，会看到以下错误消息：

> 软件保护服务报告无法激活计算机。 未启用密钥管理服务 (KMS) 。

原因：

KMS 不响应 KMS 请求时，会出现此问题。

解决方案：

若要解决此问题，请对 KMS 主机和客户端之间的网络连接进行故障排除。 确保防火墙未阻止或筛选 TCP 端口 1688 (默认) 。

0xC004F041软件保护服务确定密钥管理服务器 (KMS) 未激活

遇到此问题时，会看到以下错误消息：

> 软件保护服务确定密钥管理服务器 (KMS) 未激活。 需要激活 KMS。

原因：

当 KMS 主机尚未激活时，会出现此问题。

解决方案：

若要解决此问题，请使用 联机激活或电话激活来激活 KMS 主机。

0xC004F042无法使用指定的密钥管理服务 (KMS)

遇到此错误时，会看到以下错误消息：

> 软件保护服务确定无法读取指定的密钥管理服务。

原因：

当 KMS 客户端尝试联系无法激活客户端软件的 KMS 主机时，可能会遇到此问题。 此方案在具有特定于应用程序的 KMS 主机和特定于操作系统的 KMS 主机的混合环境中很常见。

解决方案：

若要解决此问题，请确保 KMS 客户端连接到正确的主机，尤其是在使用特定 KMS 主机激活特定应用程序或 OS 时。

0xC004F050软件保护服务报告产品密钥无效

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告产品密钥无效。

原因：

如果存在拼写错误或尝试在操作系统的正式发布版本上使用 Beta 密钥，则可能会遇到问题。

解决方案：

若要解决此问题，请确保在相应版本的 Windows 上安装正确的 KMS 密钥。 请确保输入了正确的字符和数字。 如果要复制并粘贴密钥，请确保剪贴板未将连字符替换为短划线。

0xC004F051软件保护服务报告产品密钥被阻止

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告产品密钥被阻止。

原因：

当 Microsoft 阻止产品密钥时，将显示此错误消息。

解决方案：

若要解决此问题，请获取新的 MAK 或 KMS 密钥，将其安装在系统上，然后再次尝试激活。

0xC004F064软件保护服务报告非正版宽限期已过期

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告非正版宽限期已过期。

原因：

当 Windows 激活工具 (WAT) 确定尝试激活的系统不真实时，会发生此错误。

解决方案：

若要解决此问题，请联系 Microsoft 许可激活中心 以获取帮助。

0xC004F065应用程序在有效的非正版期限内运行

遇到此错误时，会看到以下错误消息：

> 软件保护服务报告应用程序在有效的非正版期限内运行。

原因：

你可能会遇到此错误消息，因为 WAT 已确定尝试激活的系统不是正版系统。 但是，由于存在非正版宽限期，系统将继续运行。

解决方案：

若要解决此问题，必须获取并安装正版产品密钥，然后在宽限期结束前激活系统。 否则，系统会在宽限期结束时进入“通知”状态。

0xC004F06C 请求时间戳无效

遇到此问题时，会看到以下错误消息：

> 软件保护服务报告无法激活计算机。 密钥管理服务 (KMS) 确定请求时间戳无效。

原因：

如果客户端计算机上的系统时间与 KMS 主机上的时间太不同，则可能会遇到此问题。 时间同步对系统和网络安全很重要，因此取消同步可能会导致出现问题。

解决方案：

若要解决此问题，需要更改客户端上的系统时间以匹配 KMS 主机。 建议使用网络时间协议 (NTP) 时间源或Active Directory 域服务进行时间同步。 此问题使用 UTP 时间，因此时区选择不会影响它。

0xC004F074无法联系任何密钥管理服务 (KMS)

遇到此问题时，会看到以下错误消息：

> 软件保护服务报告无法激活计算机。 无法联系任何密钥管理服务 (KMS) 。 有关其他信息，请参阅应用程序事件日志。

原因：

当客户端的所有 KMS 主机系统都厌倦了联系返回错误时，会出现此问题。

解决方案：

若要解决该问题，请执行下列操作：

1. 打开 **应用程序事件日志。**
2. 标识与事件 ID 为 12288 的激活尝试关联的每个事件。
3. 按照 KMS 和 DNS 问题的常见故障排除过程中的说明排查上述每个错误。

反馈

此页面是否有帮助? 是 否

提供产品反馈

KMS 激活：已知问题

项目 • 2023/08/30

试用我们的虚拟代理 - 它可以帮助你快速识别并修复与 KMS 和 MAK 激活相关的常见问题

本文描述在密钥管理服务 (KMS) 激活期间可能产生的常见问题，并提供解决问题的指南。

> **备注**
>
> 如果你怀疑问题与 DNS 相关，请参阅 **KMS 和 DNS 问题的常见排查过程**。

我是否应备份 KMS 主机信息?

KMS 主机无需备份。 但是，如果使用工具定期清理事件日志，则存储在日志中的激活历史记录可能丢失。 如果使用事件日志跟踪或记录 KMS 激活，请定期导出事件查看器的“应用程序和服务日志”文件夹中的密钥管理服务事件日志。

如果使用 System Center Operations Manager，System Center数据仓库数据库会存储用于报告的事件日志数据，因此无需单独备份事件日志。

KMS 客户端计算机是否已激活?

在 KMS 客户端计算机上，打开“系统”控制面板并查找“Windows 已激活”消息 。 或者，运行 Slmgr.vbs 并使用 /dli 命令行选项 。

KMS 客户端计算机未激活

验证是否已达到 KMS 激活阈值。 在 KMS 主机上，运行 Slmgr.vbs 并使用 /dli 命令行选项来确定主机的当前计数 。 在 KMS 主机的计数达到 25 之前，Windows 7 客户端计算机都无法激活。 Windows Server 2008 R2 KMS 客户端需要在 KMS 计数为 5 时才能激活。 有关 KMS 要求的详细信息，请参阅批量激活计划指南。

在 KMS 客户端计算机上，在应用程序事件日志中查找事件 ID 12289。 查看此事件以了解以下信息：

- 结果代码是否为 0？ 其他任何值均为错误。

- 事件中的 KMS 主机名是否正确?
- KMS 端口是否正确?
- 是否可访问 KMS 主机?
- 如果客户端正在运行非 Microsoft 防火墙，是否需要配置出站端口?

在 KMS 主机上，在 KMS 事件日志中查找事件 ID 12290。 查看此事件以了解以下信息：

- KMS 主机是否记录了来自客户端计算机的请求? 验证是否列出了 KMS 客户端计算机名称。 验证客户端和 KMS 主机是否能够通信。 客户端是否收到响应?
- 如果 KMS 客户端未记录任何事件，则请求不会到达 KMS 主机，或者 KMS 主机无法处理该请求。 请确保路由器不会阻止使用 TCP 端口1688（如果使用默认端口）的流量，并允许流向 KMS 客户端的有状态的流量。

此错误代码的含义是什么?

除了包含事件 ID 12290 的 KMS 事件，Windows 将所有激活事件记录到名为 Microsoft-Windows-Security-SPP 的事件提供程序下的应用程序事件日志。 Windows 将 KMS 事件记录到“应用程序和服务”文件夹中的密钥管理服务日志中。 IT 专业人员可以运行 Slui.exe 来显示与大部分激活相关的错误代码说明。 此命令的常规语法如下所示：

Windows 命令提示符

```
slui.exe 0x2a ErrorCode
```

例如，如果事件 ID 12293 包含错误代码0x8007267C，可以通过运行以下命令来显示该错误的描述：

Windows 命令提示符

```
slui.exe 0x2a 0x8007267C
```

有关具体错误代码以及如何解决它们的详细信息，请参阅解决常见激活错误代码。

客户端未添加到 KMS 计数

若要重置客户端计算机 ID (CMID) 和其他产品激活信息，请运行 sysprep /generalize 或 slmgr /rearm 。 否则，每台客户端计算机看起来相同，KMS 主机不会将它们作为单独的 KMS 客户端进行计数。

KMS 主机无法创建 SRV 记录

域名系统 (DNS) 可能会限制写权限，或者可能不支持动态 DNS (DDNS)。 在这种情况下，请向 KMS 主机授予对 DNS 数据库的写权限，或者手动创建服务 (SRV) 资源记录 (RR)。 有关 KMS 和 DNS 问题的详细信息，请参阅 KMS 和 DNS 问题的常见排查过程。

只有第一台 KMS 主机能够创建 SRV 记录

如果组织拥有多台 KMS 主机，其他主机可能无法更新 SRV RR，除非更改 SRV 默认权限。 有关 KMS 和 DNS 问题的详细信息，请参阅 KMS 和 DNS 问题的常见排查过程。

我在 KMS 客户端上安装了 KMS 密钥

KMS 密钥应仅安装在 KMS 主机上，而不是 KMS 客户端上。 运行 slmgr.vbs -ipk <SetupKey> 。 有关可用于将计算机配置为 KMS 客户端的密钥表，请参阅 KMS 客户端安装密钥。 这些密钥是公开的，并且是版本特定的。 请记住从 DNS 中删除任何不必要的 SRV RR，再重启计算机。

KMS 主机出现故障

如果 KMS 主机出现故障，则必须在新主机上安装 KMS 主机密钥，然后再激活该主机。 请确保新的 KMS 主机在 DNS 数据库中具有 SRV RR。 如果使用与出现故障的 KMS 主机相同的计算机名和 IP 地址来安装新的 KMS 主机，则新的 KMS 主机可以使用故障主机的 DNS SRV 记录。 如果新主机具有其他计算机名，则可以手动删除故障主机的 DNS SRV RR，或让 DNS 自动删除它（如果在 DNS 中启用了清理）。 如果网络使用的是 DDNS，则新的 KMS 主机会自动在 DNS 服务器上创建新的 SRV RR。 然后，新的 KMS 主机会开始收集客户端续订请求，并在达到 KMS 激活阈值时立即开始激活客户端。

如果 KMS 客户端使用自动发现，则当原始 KMS 主机不响应续订请求时，它们会自动选择另一台 KMS 主机。 如果客户端不使用自动发现，则必须通过运行 slmgr.vbs /skms 手动更新已分配给故障 KMS 主机的 KMS 客户端计算机 。 若要避免这种情况，请将 KMS 客户端配置为使用自动发现。 有关详细信息，请参阅批量激活部署指南。

MAK 激活：已知问题

项目 • 2023/08/30

试用我们的虚拟代理 - 它可以帮助你快速识别并修复与 KMS 和 MAK 激活相关的常见问题

本文描述在多次激活密钥 (MAK) 激活期间可能发生的常见问题，并提供解决这些问题的指南。

我如何判断我的计算机是否已激活?

在计算机上，打开“系统”控制面板并查找“Windows 已激活” 。 或者，运行 Slmgr.vbs 并使用 /dli 命令行选项 。

计算机不能通过 Internet 激活

请确保在防火墙中打开必需的端口。 要获取端口列表，请参阅批量激活部署指南。

Internet 和电话激活失败

请联系当地的 Microsoft 激活中心。 有关全球 Microsoft 激活中心的电话号码，请转到全球 Microsoft 许可激活中心电话号码 。 拨打电话时，请务必提供批量许可协议信息和购买证明。

Slmgr.vbs /ato 将返回错误代码

如果 Slmgr.vbs 返回十六进制错误代码，请通过运行以下脚本确定相应的错误消息：

Windows 命令提示符

```
slui.exe 0x2a 0x <ErrorCode>
```

有关具体错误代码以及如何解决它们的详细信息，请参阅解决常见激活错误代码。

用于排查 DNS 相关激活问题的指南

项目 • 2023/08/02

如果符合下面的一个或多个条件，则可能必须使用这其中的某些方法：

- 使用批量许可介质和批量许可常规产品密钥安装下述操作系统之一：
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows 2008 Server
  - Windows 10
  - Windows 8.1
  - Windows 8
- 激活向导不能连接到 KMS 主机。

当你尝试激活客户端系统时，激活向导使用 DNS 来查找相应的运行 KMS 软件的计算机。 如果向导在查询 DNS 后没有找到 KMS 主机的 DNS 条目，则会报告错误。

请查看以下列表，找到适合自己情况的方法：

- 如果不能安装 KMS 主机或不能使用 KMS 激活，请尝试将产品密钥更改为 MAK 过程。
- 如果必须安装并配置 KMS 主机，请使用配置客户端激活时所使用的 KMS 主机过程。
- 如果客户端找不到现有 KMS 主机，请使用以下过程来排查路由配置问题。 这些过程按照从简单到复杂的顺序进行排列。
  - 验证到 DNS 服务器的基本 IP 连接
  - 验证 KMS 主机配置
  - 确定路由问题的类型
  - 验证 DNS 配置
  - 手动创建 KMS SRV 记录
  - 手动为 KMS 客户端分配 KMS 主机
  - 将 KMS 主机配置为在多个 DNS 域中发布

将产品密钥更改为 MAK

如果不能安装 KMS 主机，或者因为某个其他的原因而不能使用 KMS 激活，请将产品密钥更改为 MAK。 如果从 Microsoft Developer Network (MSDN) 或 TechNet 下载

Windows 映像，则在介质下列出的库存单位 (SKU) 通常为批量许可介质，提供的产品密钥为 MAK 密钥。

若要将产品密钥更改为 MAK，请执行以下步骤：

1. 打开提升的命令提示符窗口。 为此，请按 Windows 徽标键+X，右键单击“命令提示符”，然后选择“以管理员身份运行” 。 如果收到管理员密码提示或确认提示，请键入密码或进行确认。
2. 在命令提示符处运行以下命令：

Windows 命令提示符

```
slmgr -ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

> ⓘ **备注**
>
> **xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** 占位符表示 MAK 产品密钥。

返回到过程列表。

配置客户端激活时所使用的 KMS 主机

KMS 激活要求配置客户端激活时所使用的 KMS 主机。 如果环境中没有配置的 KMS 主机，请使用适当的 KMS 主机密钥安装并激活一个。 在网络上配置用于托管 KMS 软件的计算机以后，请发布域名系统 (DNS) 设置。

若要了解 KMS 主机配置过程，请参阅使用密钥管理服务进行激活和安装和配置 VAMT。

返回到过程列表。

验证到 DNS 服务器的基本 IP 连接

使用 ping 命令验证到 DNS 服务器的基本 IP 连接。 为此，请在遇到错误的 KMS 客户端上和 KMS 主机上执行以下步骤：

1. 打开提升的命令提示符窗口。
2. 在命令提示符处运行以下命令：

Windows 命令提示符

```
ping <DNS_Server_IP_address>
```

> **备注**
>
> 如果此命令的输出不包含“来自...的回复”短语，则表明存在网络问题或 DNS 问题，必须解决该问题后才能使用本文中的其他过程。 若要详细了解在不能 ping DNS 服务器的情况下如何排查 TCP/IP 问题，请参阅**针对 TCP/IP 问题的高级故障排除**。

返回到过程列表。

验证 KMS 主机的配置

检查 KMS 主机服务器的注册表，确定是否已将它注册到 DNS。 默认情况下，KMS 主机服务器每 24 小时动态注册 DNS SRV 记录一次。

> **重要**
>
> 请认真遵循本部分所述的步骤。 如果注册表修改不正确，可能会发生严重问题。 在修改注册表之前，请**备份注册表**，以便在出现问题时可以还原。

若要检查此设置，请执行以下步骤：

1. 启动“注册表编辑器”。 为此，请右键单击“开始”，选择“运行”，键入 **regedit**，然后按 Enter。
2. 找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform 子项（Windows Server 2008 和 Windows Vista 中以前为 SL，而不是 SoftwareProtectionPlatform），然后查看 DisableDnsPublishing 条目的值。 此条目有以下可能值：
   - **0** 或未定义（默认值）：KMS 主机服务器每 24 小时注册 SRV 记录一次。
   - **1**：KMS 主机服务器不自动注册 SRV 记录。 如果实现不支持动态更新，请参阅手动创建 KMS SRV 记录。
3. 如果 **DisableDnsPublishing** 条目缺失，请创建它（类型为 DWORD）。 如果可以接受动态注册，请将此值保留为未定义或设置为 **0**。

返回到过程列表。

确定路由问题的类型

可使用以下命令来确定这是名称解析问题还是 SRV 记录问题。

1. 在 KMS 客户端上，打开提升的命令提示符窗口。
2. 在命令提示符处运行以下命令：

   Windows 命令提示符

   ```
   cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
   cscript \windows\system32\slmgr.vbs -ato
   ```

   > **备注**
   >
   > 在此命令中，<KMS_FQDN> 表示 KMS 主机的完全限定的域名 (FQDN)，<port> 表示 KMS 使用的 TCP 端口。

   如果这些命令解决了此问题，则表明这是 SRV 记录问题。 排查其问题时，可以使用手动为 KMS 客户端分配 KMS 主机过程中记录的某个命令。
3. 如果此问题仍然存在，请运行以下命令：

   Windows 命令提示符

   ```
   cscript \windows\system32\slmgr.vbs -skms <IP Address>:<port>
   cscript \windows\system32\slmgr.vbs -ato
   ```

   > **备注**
   >
   > 在此命令中，<IP Address> 表示 KMS 主机的 IP 地址，<port> 表示 KMS 使用的 TCP 端口。

   如果这些命令解决了此问题，则表明这很可能是名称解析问题。 有关其他故障排除信息，请参阅验证 DNS 配置过程。
4. 如果这些命令都无法解决此问题，请检查计算机的防火墙配置。 在 KMS 客户端和 KMS 主机之间进行的任何激活通信均使用 1688 TCP 端口。 KMS 客户端与 KMS 主机上的防火墙都必须允许通过端口 1688 进行通信。

返回到过程列表。

验证 DNS 配置

> **备注**

除非另有说明，否则请在遇到相应错误的 KMS 客户端上执行以下步骤。

1. 打开提升的命令提示符窗口
2. 在命令提示符处运行以下命令：

```
Windows 命令提示符

IPCONFIG /all
```

3. 注意命令结果中的以下信息：

   - KMS 客户端计算机的已分配 IP 地址
   - KMS 客户端计算机使用的主 DNS 服务器的 IP 地址
   - KMS 客户端计算机使用的默认网关的 IP 地址
   - KMS 客户端计算机使用的 DNS 后缀搜索列表

4. 验证 KMS 主机 SRV 记录是否已在 DNS 中注册。 要实现这一点，请执行下列操作：
   a. 打开提升的命令提示符窗口。
   b. 在命令提示符处运行以下命令：

```
Windows 命令提示符

nslookup -type=all _vlmcs._tcp>kms.txt
```

   c. 打开此命令生成的 KMS.txt 文件。 此文件应该包含一个或多个类似于以下条目的条目：

```

_vlmcs._tcp.contoso.com SRV service location:
priority = 0
weight = 0
port = 1688 svr hostname = kms-server.contoso.com
```

> **备注**
>
> 在此条目中，contoso.com 表示 KMS 主机的域。

   i. 验证 KMS 主机的 IP 地址、主机名、端口和域。
   ii. 如果这些 **_vlmcs** 条目存在且包含预期的 KMS 主机名，请转到手动为 KMS 客户端分配 KMS 主机。

> **备注**

> 即使 **nslookup** 命令找到了 KMS 主机，也并不意味着 DNS 客户端能够找到 KMS 主机。 如果 **nslookup** 命令找到了 KMS 主机，但你仍然不能使用 KMS 主机进行激活，请检查其他 DNS 设置，例如主 DNS 后缀以及 DNS 后缀的搜索列表。

5. 验证主 DNS 后缀的搜索列表是否包含与 KMS 主机相关联的 DNS 域后缀。 如果搜索列表不包含该信息，请转到将 KMS 主机配置为在多个 DNS 域中发布过程。

返回到过程列表。

手动创建 KMS SRV 记录

若要手动为使用 Microsoft DNS 服务器的 KMS 主机创建 SRV 记录，请执行以下步骤：

1. 在 DNS 服务器上，打开 DNS 管理器。 若要打开 DNS 管理器，请依次选择“开始”、“管理工具”、“DNS”。
2. 选择必须在其上创建 SRV 资源记录的 DNS 服务器。
3. 在控制台树中，展开“正向查找区域”，右键单击域，然后选择“其他新记录”。
4. 在列表中向下滚动，选择“服务位置(SRV)”，然后选择“创建记录”。
5. 键入以下信息：

    - 服务：**_VLMCS**
    - 协议： **_TCP**
    - 端口号：**1688**
    - 提供服务的主机： ***<KMS 主机的 FQDN>***

6. 完成这些操作后，请选择“确定”，然后选择“完成”。

若要手动为使用兼容 BIND 9.x 的 DNS 服务器的 KMS 主机创建 SRV 记录，请按该 DNS 服务器的说明操作，并提供以下 SRV 记录信息：

- 名称：_vlmcs._TCP
- 类型：SRV
- 优先级：**0**
- 权重：**0**
- 端口：**1688**
- 主机名：***<KMS 主机的 FQDN 或 A-Name>***

若要将兼容 BIND 9.x 的 DNS 服务器配置为支持 KMS 自动发布功能，请将 DNS 服务器配置为允许从 KMS 主机进行资源记录更新。 例如，将以下行添加到 Named.conf 或 Named.conf.local 的区域定义中：

Windows 命令提示符

```
allow-update { any; };
```

手动为 KMS 客户端分配 KMS 主机

默认情况下，KMS 客户端使用自动发现过程。 根据此过程的要求，KMS 客户端会查询 DNS 中的一系列服务器，这些服务器已在客户端的成员身份区域中发布了 `_vlmcs` SRV 记录。 DNS 以随机顺序返回 KMS 主机的列表。 客户端会选取一个 KMS 主机并尝试在其上建立一个会话。 如果该尝试成功，客户端会缓存 KMS 主机的名称并尝试在下一次续订尝试时使用它。 如何会话设置失败，客户端会随机选取另一个 KMS 主机。 强烈建议使用自动发现过程。

但是，你可以手动为特定的 KMS 客户端分配 KMS 主机。 为此，请按照以下步骤操作。

1. 在 KMS 客户端上，打开提升的命令提示符窗口。
2. 根据实现情况执行以下步骤之一：

   - 若要使用 KMS 主机的 FQDN 来分配该主机，请运行以下命令：

     Windows 命令提示符

     ```
     cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
     ```

   - 若要使用 KMS 主机的版本 4 IP 地址来分配该主机，请运行以下命令：

     Windows 命令提示符

     ```
     cscript \windows\system32\slmgr.vbs -skms <IPv4Address>:<port>
     ```

   - 若要使用 KMS 主机的版本 6 IP 地址来分配该主机，请运行以下命令：

     Windows 命令提示符

     ```
     cscript \windows\system32\slmgr.vbs -skms <IPv6Address>:<port>
     ```

   - 若要使用 KMS 主机的 NETBIOS 名称来分配该主机，请运行以下命令：

     Windows 命令提示符

     ```
     cscript \windows\system32\slmgr.vbs -skms <NETBIOSName>:<port>
     ```

   - 若要在 KMS 客户端上恢复为自动发现，请运行以下命令：

     Windows 命令提示符

```
cscript \windows\system32\slmgr.vbs -ckms
```

> **备注**
>
> 这些命令使用以下占位符：
> - <KMS_FQDN> 表示 KMS 主机的完全限定的域名 (FQDN)
> - **<IPv4Address>** 表示 KMS 主机的 IPv4 地址
> - **<IPv6Address>** 表示 KMS 主机的 IPv6 地址
> - **<NETBIOSName>** 表示 KMS 主机的 NETBIOS 名称
> - **<port>** 表示 KMS 使用的 TCP 端口。

将 KMS 主机配置为在多个 DNS 域中发布

> **重要**
>
> 请认真遵循本部分所述的步骤。 如果注册表修改不正确，可能会发生严重问题。 在修改注册表之前，请**备份注册表**，以便在出现问题时可以还原。

如手动为 KMS 客户端分配 KMS 主机中所述，KMS 客户端通常使用自动发现过程来标识 KMS 主机。 此过程要求必须在 KMS 客户端计算机的 DNS 区域中提供 `_vlmcs` SRV 记录。 DNS 区域对应于计算机的主 DNS 后缀，或者对应于以下项之一：

- DNS 系统（例如 Active Directory 域服务 (AD DS) DNS）分配的计算机域（适用于已加入域的计算机）。
- 动态主机配置协议 (DHCP) 分配的计算机域（适用于工作组计算机）。 根据征求意见文档 (RFC) 2132 中的定义，此域名由代码值为 15 的选项定义。

默认情况下，KMS 主机将其 SRV 记录注册到 DNS 区域中，该区域对应于 KMS 主机的域。 例如，假定 KMS 主机加入 contoso.com 域。 在这种情况下，KMS 主机会将其 `_vlmcs` SRV 记录注册到 contoso.com DNS 区域。 因此，记录会将服务标识为 `_VLMCS._TCP.CONTOSO.COM`。

如果 KMS 主机和 KMS 客户端使用不同的 DNS 区域，则必须将 KMS 主机配置为自动在多个 DNS 域中发布其 SRV 记录。 要实现这一点，请执行下列操作：

1. 在 KMS 主机上启动注册表编辑器。
2. 找到并选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform 子项（Windows Server 2008 和

Windows Vista 中以前为 SL，而不是 SoftwareProtectionPlatform）。

3. 在“详细信息”窗格中右键单击空白区域，选择“新建”，然后选择“多值字符串值”。
4. 输入 **DnsDomainPublishList** 作为新条目的名称。
5. 右键单击这个新的 **DnsDomainPublishList** 条目，然后选择“修改”。
6. 在“编辑多值字符串”对话框中，键入 KMS 在单独的行中发布的每个 DNS 域后缀，然后选择“确定”。

> ⓘ **备注**
>
> Windows Server 2008 R2 的 **DnsDomainPublishList** 的格式有所不同。 有关详细信息，请参阅“批量激活技术参考指南”。

7. 使用服务管理工具重启软件保护服务（以前为 Windows Server 2008 和 Windows Vista 中的软件授权服务）。 此操作创建 SRV 记录。
8. 验证 KMS 客户端是否可以使用典型的方法来联系已配置的 KMS 主机。 验证 KMS 客户端是否可以按名称和按 IP 地址来正确标识 KMS 主机。 如果这两个验证中的任一验证失败，请调查此 DNS 客户端解析程序问题。
9. 若要清除以前在 KMS 客户端上缓存的 KMS 主机名，请在 KMS 客户端上打开已提升权限的命令提示符窗口，然后运行以下命令：

Windows 命令提示符

```
cscript C:\Windows\System32\slmgr.vbs -ckms
```

重新生成 Tokens.dat 文件

项目 • 2023/08/30

解决 Windows 激活问题时，可能需要重新生成 Tokens.dat 文件。 本文详细介绍如何完成此操作。

解决方法

若要重新生成 Tokens.dat 文件，请执行以下步骤：

1. 打开提升的命令提示符窗口：**对于 Windows 10**
   a. 打开“开始”菜单，然后输入cmd 。
   b. 在搜索结果中，右键单击“命令提示符”，然后选择“以管理员身份运行” 。

   对于 Windows 8.1
   a. 从屏幕右边缘轻扫，然后点击“搜索” 。 或者，如果使用鼠标，请指向屏幕右下角，然后选择“搜索” 。
   b. 在搜索框中，输入 cmd 。
   c. 轻扫或右键单击显示的“命令提示符”图标 。
   d. 点击或单击“以管理员身份运行” 。

   对于 Windows 7
   a. 打开“开始”菜单，然后输入cmd 。
   b. 在搜索结果中，右键单击“cmd.exe”，然后选择“以管理员身份运行” 。

2. 输入适用于你的操作系统的命令列表。

   对于 Windows 10、Windows Server 2016 及更高版本的 Windows，按顺序输入以下命令：

   Windows 命令提示符

   ```
   net stop sppsvc
   cd %Systemdrive%\Windows\System32\spp\store\2.0\
   ren tokens.dat tokens.bar
   net start sppsvc
   cscript.exe %windir%\system32\slmgr.vbs /rilc
   ```

   对于 Windows 8.1、Windows Server 2012 和 Windows Server 2012 R2，按顺序输入以下命令：

   Windows 命令提示符

```
net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

对于 Windows 7、Windows Server 2008 和 Windows Server 2008 R2，按顺序输入以下命令：

Windows 命令提示符

```
net stop sppsvc
cd
%Systemdrive%\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

3. 重新启动计算机。

详细信息

重新生成 Tokens.dat 文件后，必须使用以下方法之一重新安装产品密钥：

- 在同一提升的提示符命令下，键入以下命令，然后按 Enter：

  Windows 命令提示符

  ```
  cscript.exe %windir%\system32\slmgr.vbs /ipk <Product key>
  ```

  > **重要**
  >
  > 请勿使用 /upk 开关来卸载产品密钥 。 若要在现有产品密钥上安装产品密钥，请使用 /ipk 开关 。

- 右键单击“我的计算机”，选择“属性”，然后选择“更改产品密钥” 。

有关 KMS 客户端安装密钥的详细信息，请参阅 KMS 客户端安装密钥。

排查未激活的基于 Active Directory 的激活 (ADBA) 客户端的问题

项目 • 2024/02/19

> **备注**
>
> 本文最初于 2018 年 3 月 26 日作为 TechNet 博客发布。

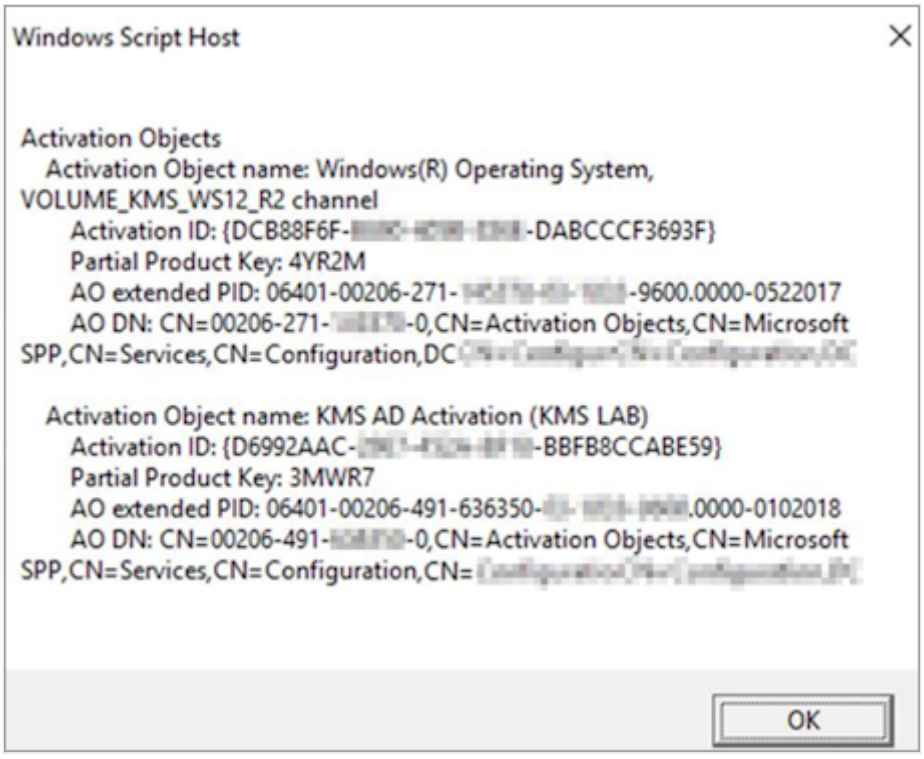
我最近帮助客户在其环境中部署了Windows Server 2016。 我们还借此机会将其激活方法从 KMS 服务器迁移到 基于 Active Directory 的激活。

作为进行所有更改的正确过程，我们在客户的测试环境中开始迁移。 我们按照 活动 Directory-Based 激活与密钥管理服务 中的说明开始部署。 测试环境中的域控制器都 Windows Server 2012 R2 运行，因此无需准备林。 我们在Windows Server 2012 R2 域控制器上安装角色，并选择了“基于 Active Directory 的激活”作为批量激活方法。 我们安装了 KMS 密钥，并为其命名为“KMS AD 激活 (** LAB) ”。我们逐步关注博客文章。

我们首先构建了四个虚拟机、两个 Windows 2016 Server Standard 和两个 Windows 2016 Server Datacenter。 在这一点上，一切都很棒。 我们构建了一个运行 Windows 2016 Server Standard 的物理服务器，并且计算机已正确激活。

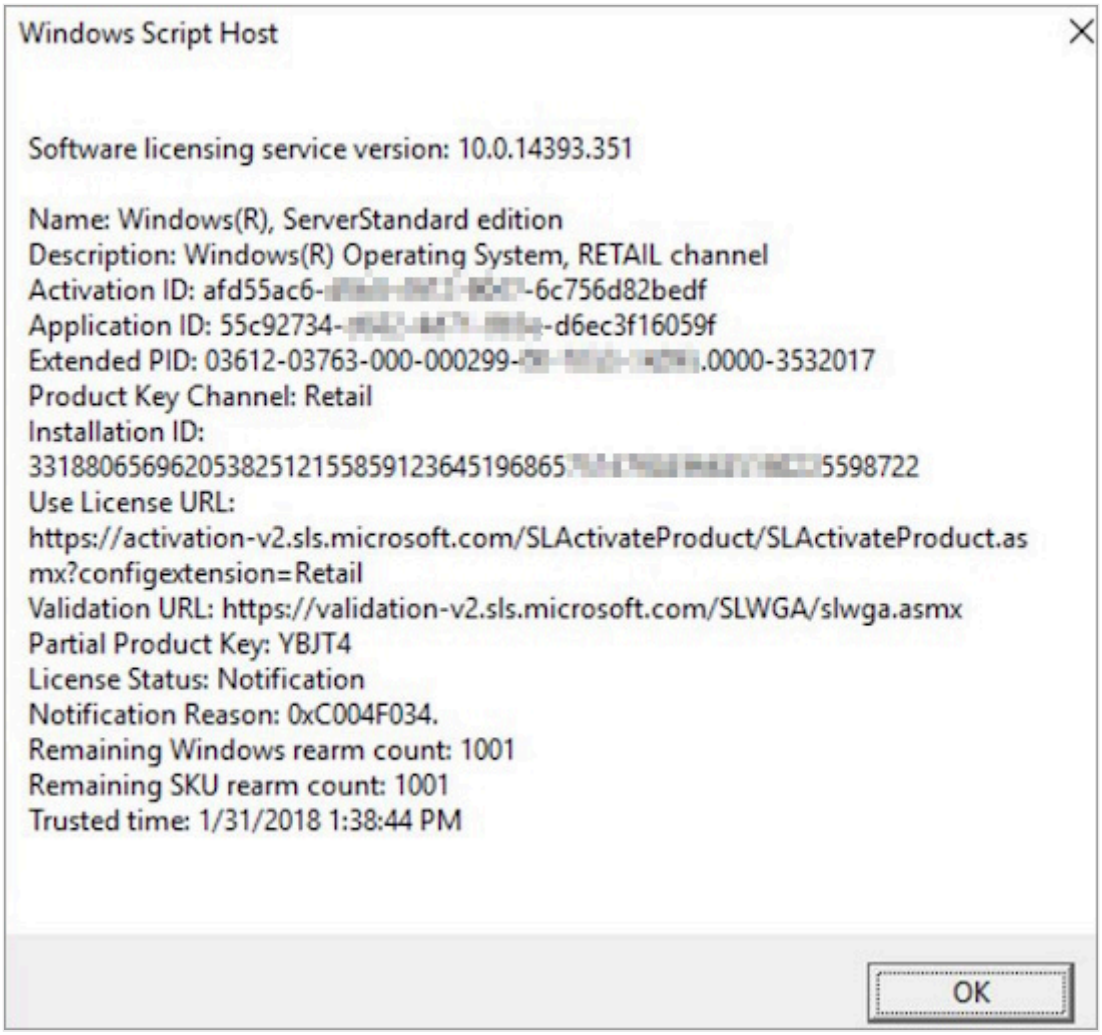
说实话，设置和配置是超级容易，所以部分是简单和直接的。 但是，我之前一周构建的所有虚拟机都显示它们未激活。 我回到物理机，很好。 我去找客户讨论发生了什么事。 第一个问题是“周末有什么变化？”和往常一样，答案是“什么都没有”。这一次，什么都没有改变，我们必须弄清楚发生了什么。

我去了其中一个有问题的服务器，打开了命令提示符，并检查了命令的 `slmgr /ao-list` 输出。 开关 `/ao-list` 显示 Active Directory 中的所有激活对象。



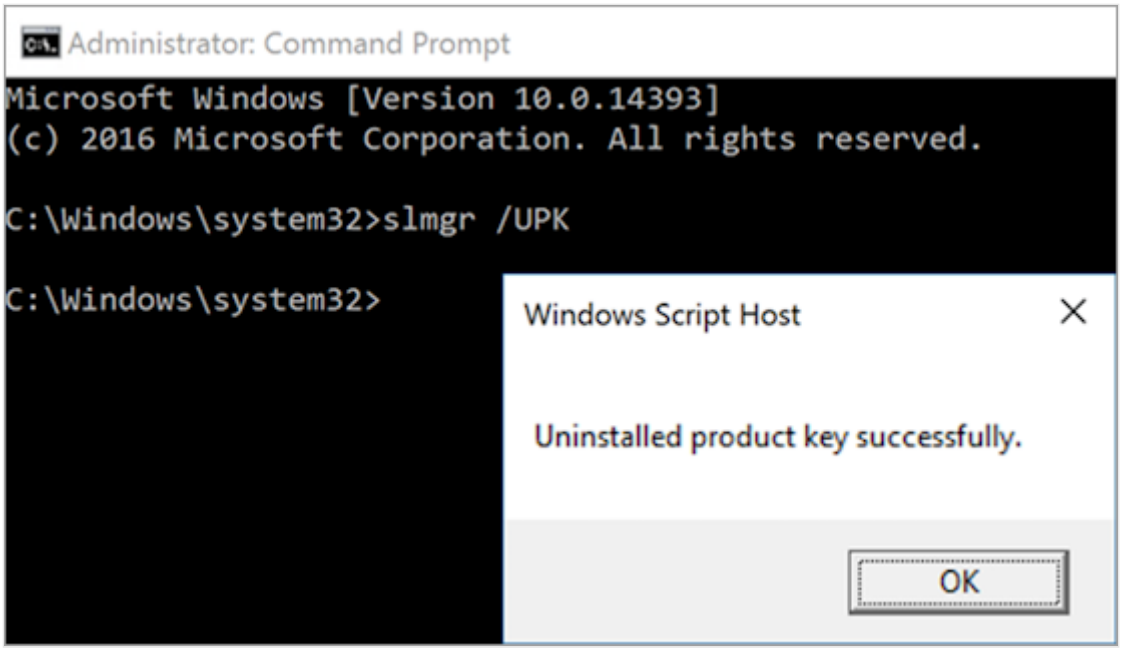
结果显示，我们有两个激活对象：一个用于Windows Server 2012 R2，一个用于新创建的KMS AD 激活 (** LAB) （即Windows Server 2016许可证）。 这确认 Active Directory 已正确配置为激活 Windows KMS 客户端。

知道命令 `slmgr` 用于许可证激活，我继续使用不同的选项。 我尝试了 `/dlv` 开关，该开关将显示详细的许可证信息。 这看起来很好，我运行的是标准版Windows Server 2016，有激活 ID、安装 ID、验证 URL，甚至是部分产品密钥。

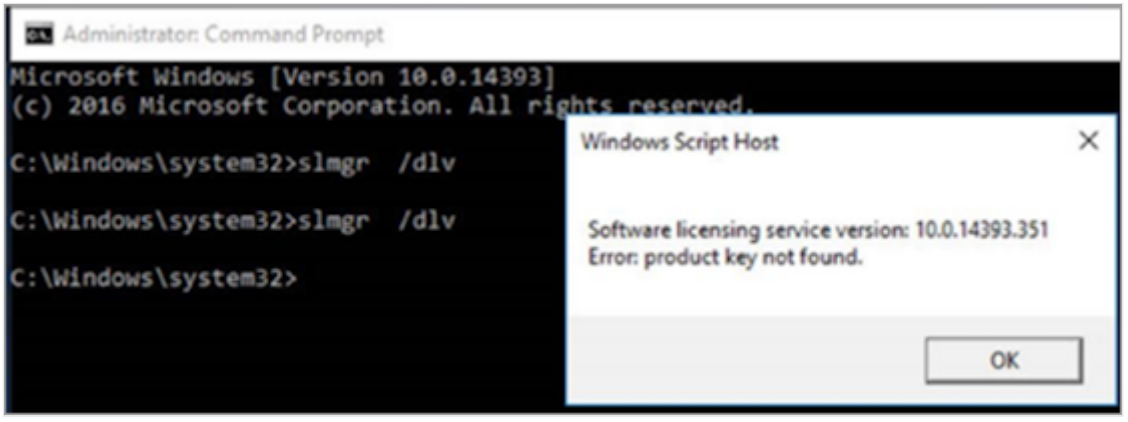


有人看到我在这一点上错过了什么吗？ 在完成其他故障排除步骤后，我们将返回它，但足以说明答案在此屏幕截图中。

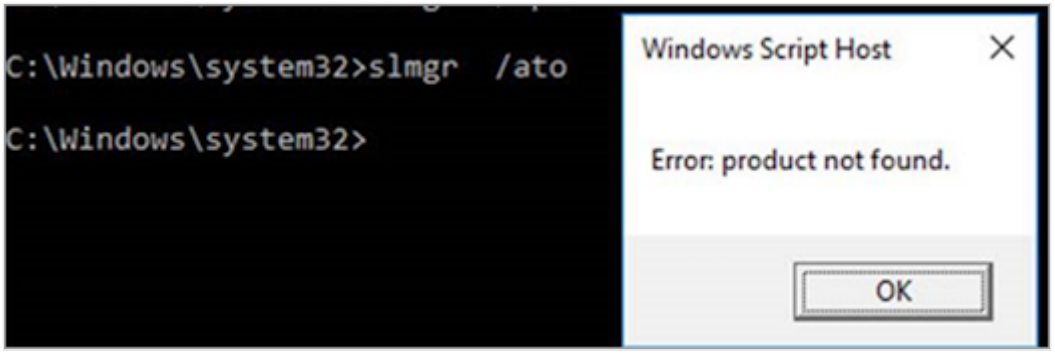
我现在的想法是，由于某种原因，密钥已损坏，因此我使用 `/upk` 开关来卸载当前密钥。 虽然这在删除密钥方面是有效的，但通常不是最好的方法。 如果服务器在获取新密钥之前重新启动，它可能会使服务器处于错误状态？ 我发现使用 `/ipk` 开关 (我稍后在故障排除) 会覆盖现有密钥，并且是一种更安全的路线。



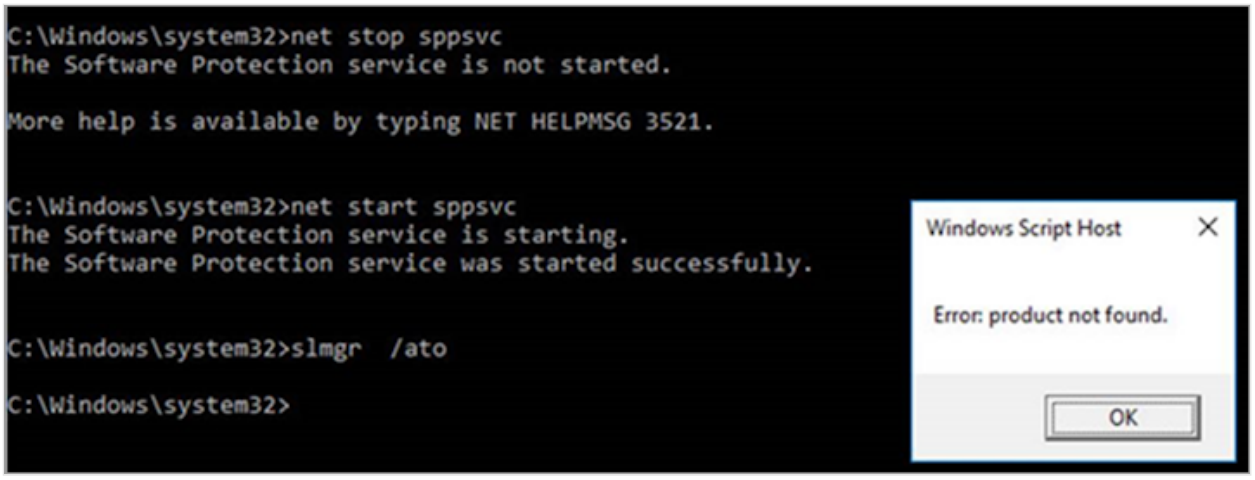
我再次运行开关 `/dlv` ，以查看详细的许可证信息。 遗憾的是，这并没有给我任何有用的信息，只是产品密钥未找到错误。 因为没有密钥，因为我刚刚卸载了它。



我认为这是一个长枪，但我尝试了 `/ato` 开关，它应该激活 Windows 针对已知的 KMS 服务器 (或 Active Directory，因为情况可能) 。 同样，只是一个产品未找到错误。

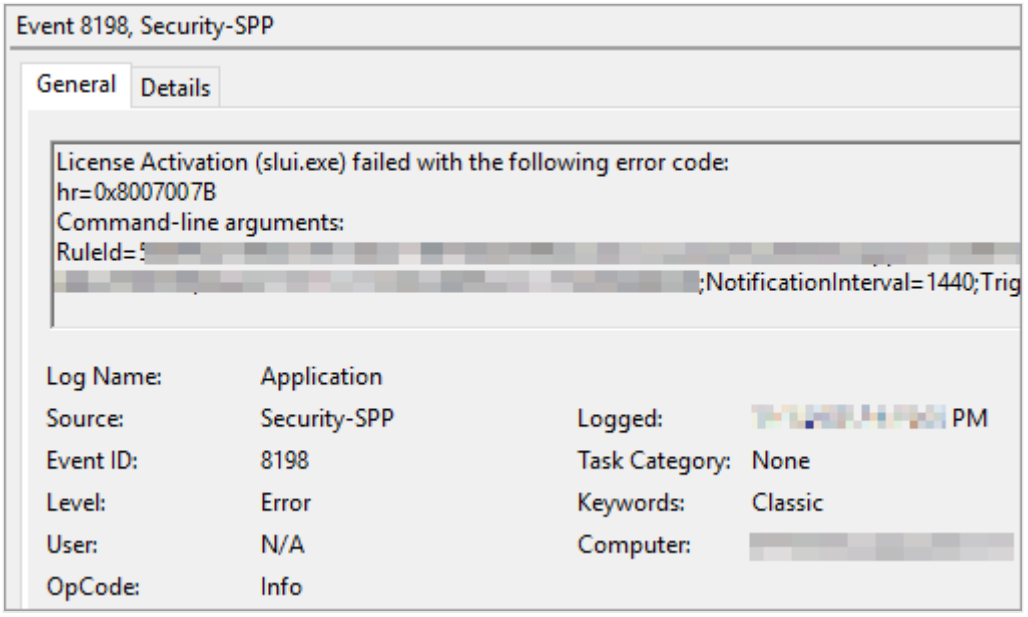


下一个想法是，有时停止和启动服务会起到作用，所以我接下来尝试了。 我需要停止并启动 Microsoft 软件保护平台服务 (SPPSvc 服务) 。 在管理命令提示符下，我使用 trusty `net stop` 和 `net start` 命令。 我一开始注意到该服务未运行，所以我认为这一定是它。



但是，在启动服务并尝试再次激活 Windows 后，我仍然收到“找不到产品”错误。

然后，我查看了其中一个故障服务器上的应用程序事件日志。 我发现一个与许可证激活相关的错误，事件 ID 为 8198，该错误的代码为0x8007007B。



在查找此代码时，我发现一篇文章指出错误代码表示文件名、目录名称或卷标签语法不正确。 通读本文中所述的方法，似乎其中任何方法都不适合这种情况。 运行 `nslookup -type=all _vlmcs._tcp` 命令时，我发现现有的 KMS 服务器 (环境中仍有大量 Windows 7 和 Server 2008 计算机，因此有必要将其保留在) 周围，以及五个域控制器。 这表明这不是 DNS 问题，问题也位于其他位置。

```
nslookup -type=all _vlmcs._tcp>kms.txt

Server:  labdns1.CONTOSO.COM
Address:  10.10.14.11

_vlmcs._tcp.CONTOSO.COM    SRV service location:
          priority       = 0
          weight         = 0
          port           = 1688
          svr hostname   = labKMS.CONTOSO.COM

_tcp.CONTOSO.COM   nameserver = labDC2.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = remDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC4.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC3.CONTOSO.COM
labKMS.CONTOSO.COM  internet address = 10.10.14.100
labDC1.CONTOSO.COM   internet address = 10.10.14.26
remDC1.CONTOSO.COM   internet address = 10.10.20.88
labDC4.CONTOSO.COM   internet address = 10.10.14.27
labDC3.CONTOSO.COM   internet address = 10.10.14.34
labDC2.CONTOSO.COM   internet address = 10.10.14.44
```

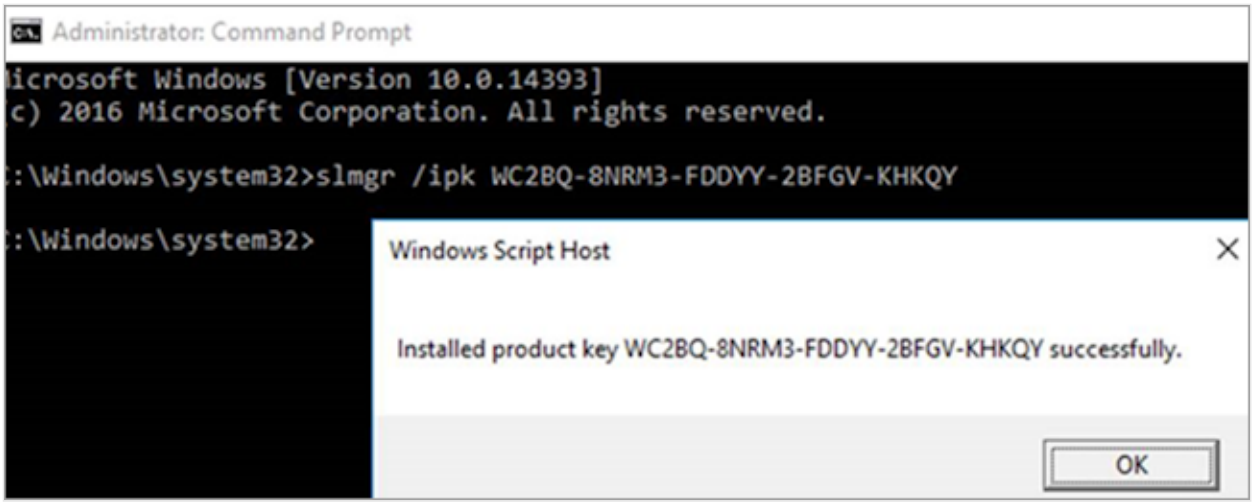
因此，我知道 DNS 正常。 Active Directory 已正确配置为 KMS 激活源。 物理服务器已正确激活。 这是否只是 VM 的问题？ 作为一个有趣的旁注，此时，我的客户通知我，不同部门的某人也决定构建十几台虚拟Windows Server 2016计算机。 因此，现在我假设我还有十几台服务器要处理，这些服务器不会激活。 但是，这些服务器激活正常。

嗯，我回到命令， `slmgr` 找出如何激活这些怪物。 这一次，我将使用 `/ipk` 开关，这将允许我安装产品密钥。 我已访问附录 A：KMS 客户端设置密钥，以获取适用于标准版Windows Server 2016的密钥。 有些服务器是数据中心服务器，但我需要先修复此服务器。

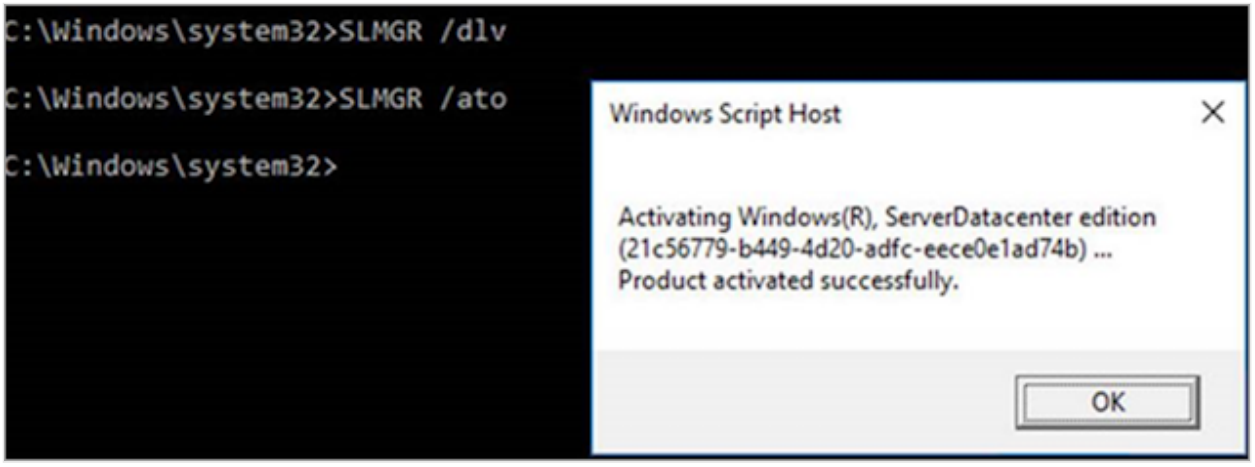
Windows Server 2016

Operating system edition	KMS Client Setup Key
Windows Server 2016 Datacenter	CB7KF-BWN84-R7R2Y-793K2-8XDDG
Windows Server 2016 Standard	WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY
Windows Server 2016 Essentials	JCKRF-N37P4-C2D82-9YXRT-4M63B

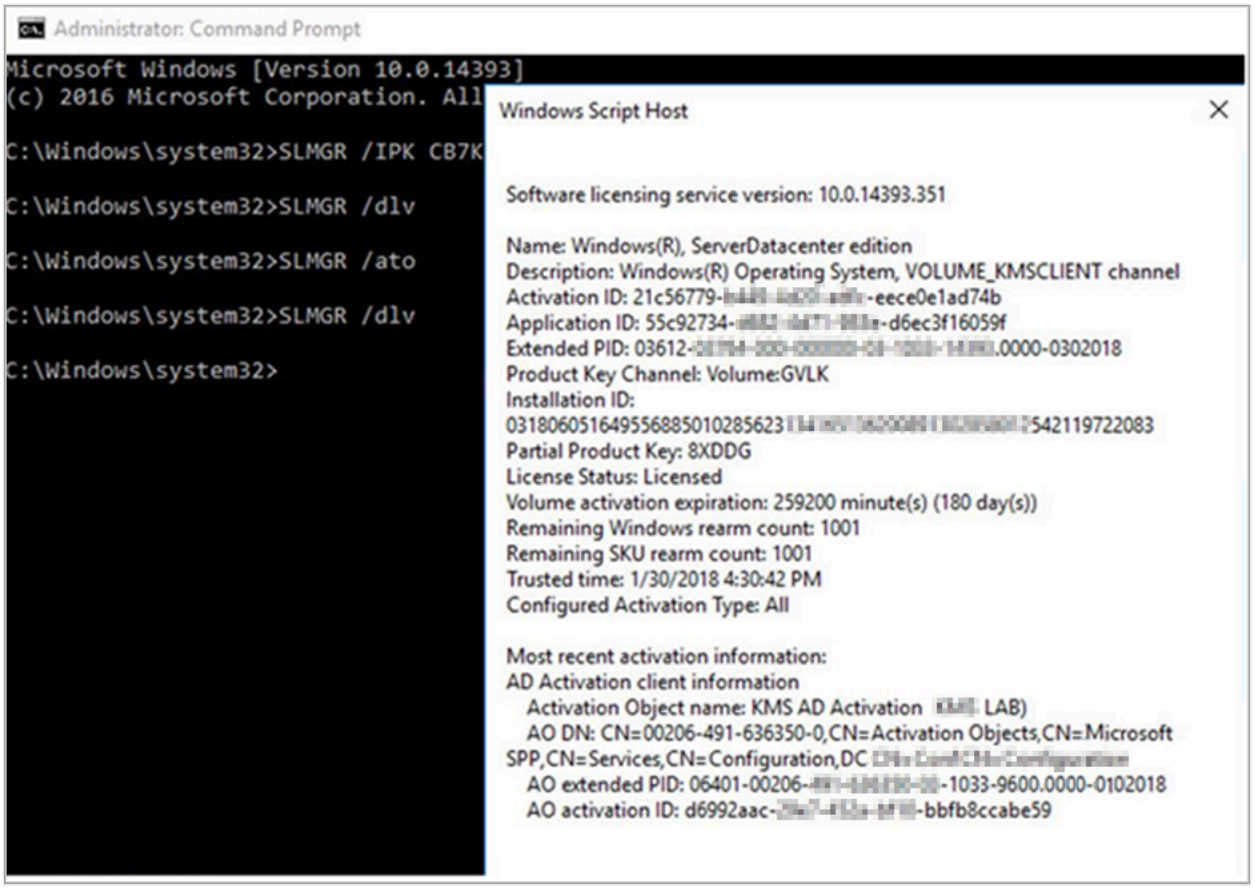
我使用 `/ipk` 开关安装产品密钥，并选择了Windows Server 2016标准密钥。



从此处开始，我只从数据中心体验中捕获了结果，但它们是相同的。 我使用 开关 `/ato` 强制激活。 我们收到产品已成功激活的真棒消息。

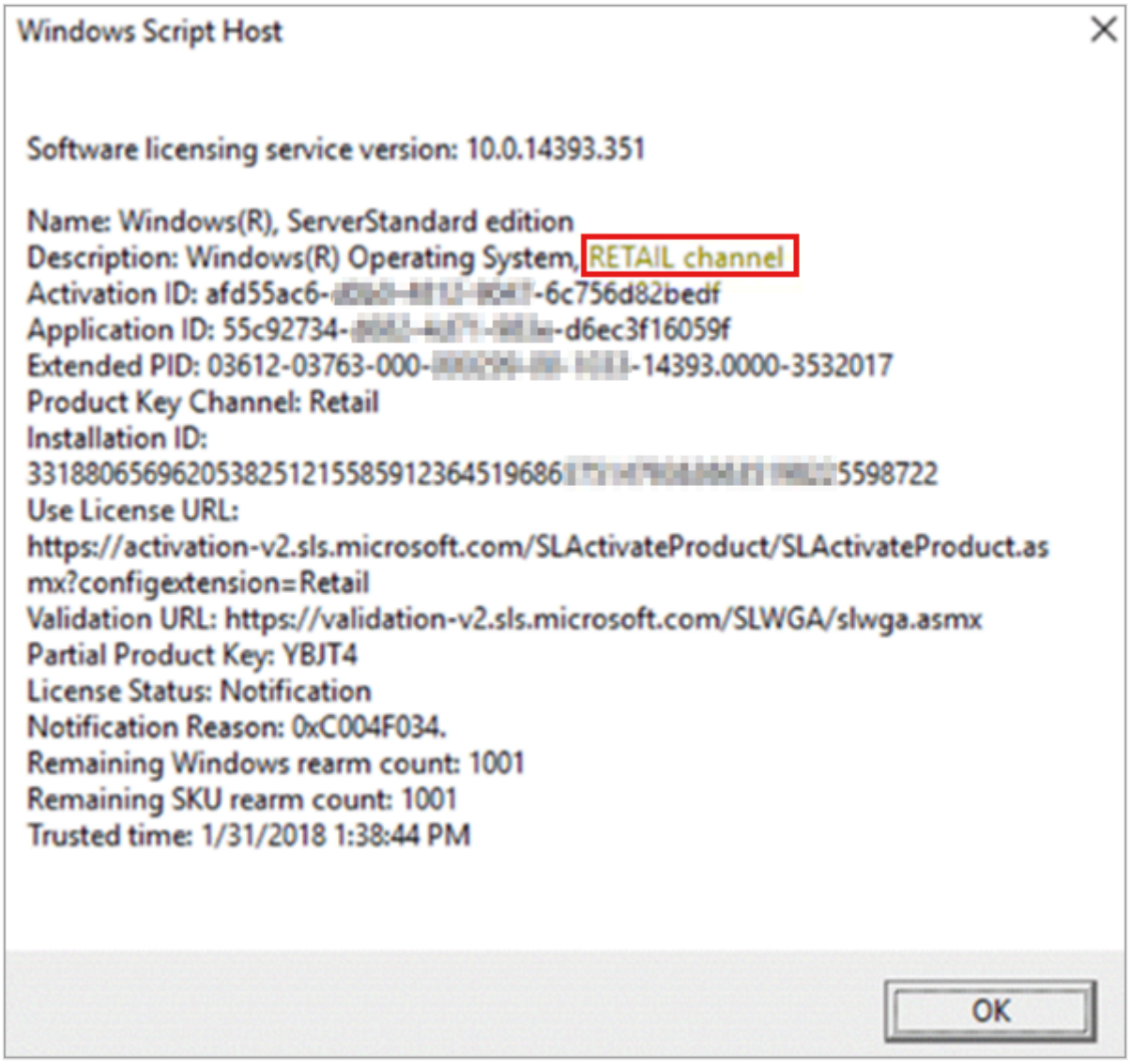


再次使用该 `/dlv` 开关，我们可以看到，现已由 Active Directory 激活。

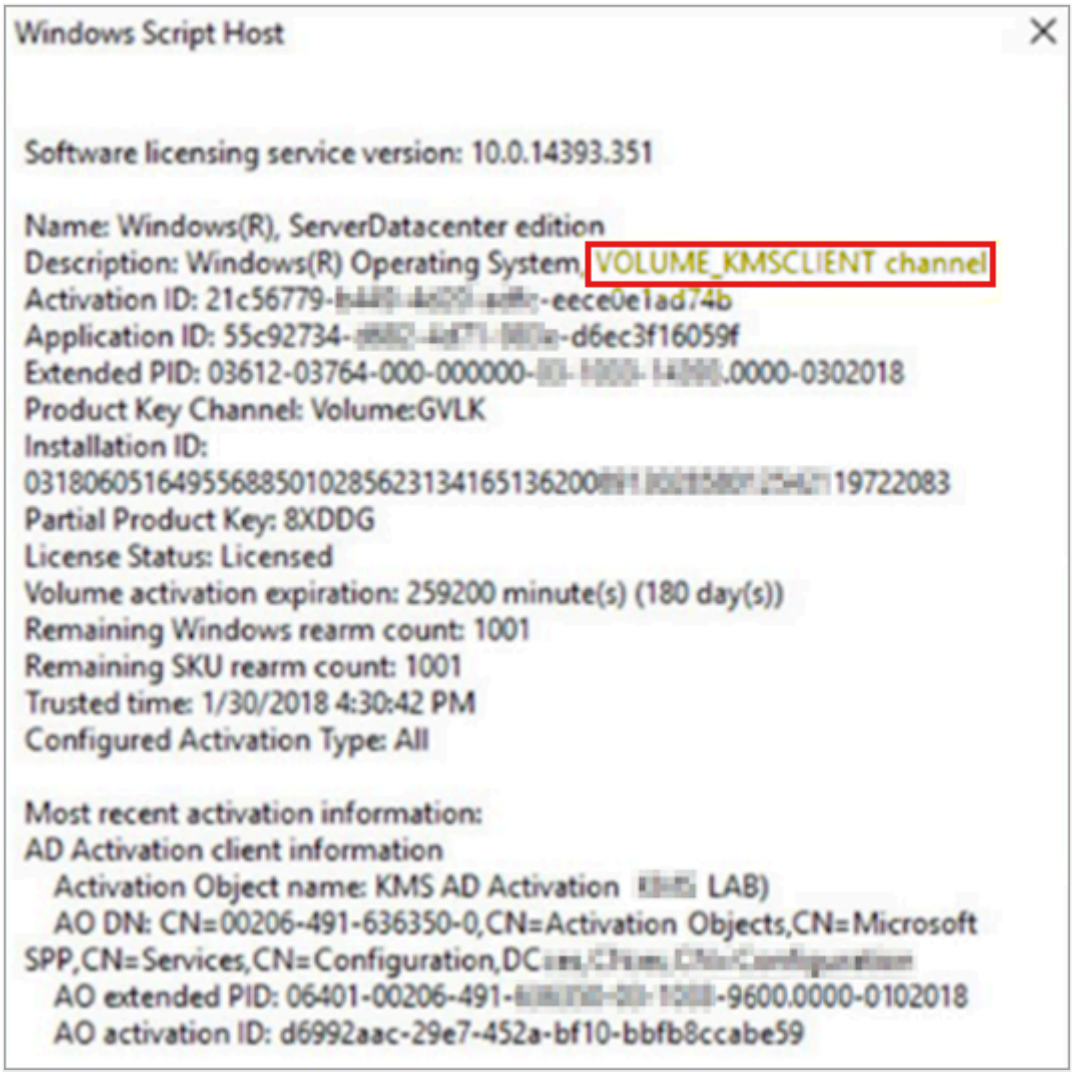


现在，出了什么问题？ 为什么必须删除已安装的密钥并添加这些通用密钥才能使这些计算机正确激活？ 为什么其他十几台计算机在激活时没有问题？ 正如我前面所说，在研究这个问题的最初阶段，我错过了一些关键的东西。 我完全迷惑不解，所以从最初的博客中向海报伸出手来。 海报立即看到了问题，帮助我理解我早就错过了什么。

当我运行第一个 `/dlv` 开关时，说明中的键。 说明为 Windows® 操作系统零售频道。 我看过这个，认为零售频道意味着它已经购买，是一个有效的密钥。



当我们查看正确激活的 `/dlv` 服务器的交换机输出时，请注意，说明现在指出了VOLUME_KMSCLIENT通道。 这让我们知道，它确实是一个批量许可证。



那么，零售渠道意味着什么呢？ 嗯，这意味着用于安装操作系统的介质是 MSDN ISO。 我回到我的客户那里，询问是否有第二个Windows Server 2016 ISO 在网络中浮动。 事实证明，是的，网络上有另一个 ISO，它已用于创建其他十几台计算机。 他们比较了这两个 ISO，并确信提供给我构建虚拟服务器的 ISO 实际上是 MSDN ISO。 他们从其网络中删除了 MSDN ISO，现在我们激活了所有现有服务器，并且不再担心在将来的版本中激活失败。

反馈

此页面是否有帮助？ 是 否

提供产品反馈

Windows 版本运行状况

有关 Windows 版本和服务里程碑的官方信息，加上资源、工具和已知问题及安全措施的相关新闻，可帮助你规划下一次更新。 需要最新的 Windows 版本运行状况更新？ 关注 @WindowsUpdate X (以前称为 Twitter) 。

GET STARTED
如何获取 Windows 11 2023 更新

WHAT'S NEW
探索最个性化的 Windows 11体验

WHAT'S NEW
如何获取最新的 Windows 11创新

REFERENCE
设备有可用更新时立即获取更新

REFERENCE
Windows 11 版本信息

OVERVIEW
了解 Windows 月度更新

消息中心

- Windows 11中的新创新使创建和完成工作变得更加容易
- 2024 年 2 月 Windows 非安全预览版更新现已推出
- 扩展邀请以移动到Windows 11到更多人

查看更多 >

Windows 11 版本 23H2

- 已知问题
- 已解决的问题
- 发行说明
- Windows 11 版本信息
- 如何获取Windows 11版本 23H2

Windows 11 版本 22H2

- 已知问题
- 已解决的问题
- 发行说明
- Windows 11 版本信息
- 如何获取Windows 11版本 22H2

Windows 11 版本 21H2

- 已知问题
- 已解决的问题
- 发行说明
- Windows 11 版本信息
- 如何获取 Windows 11

Windows 10 版本 22H2

- 已知问题
- 已解决的问题
- 发行说明
- Windows 10 版本信息
- 如何获取Windows 10版本 22H2

Windows 10 版本 21H2

- 已知问题
- 已解决的问题
- 发行说明
- Windows 10 发布信息
- 如何获取 Windows 10 版本 21H2

Windows Server 2022

- 已知问题
- 已解决的问题
- 发行说明
- Windows Server 版本信息
- Windows Server 2022 中的新增功能

其他版本

查看其它受支持 Windows 和 Windows Server 版本的已知和已解决问题的详细信息。

- 已知问题：早期版本

有疑问？ 在工作时间加入

获取自定义指南、提示和技巧以及问题答案。

提交反馈

通过反馈中心共享与现有功能相关的看法或新功能创意。

获取帮助

在 Windows 设备中打开“获取帮助”应用，查找用于排查常见问题的资源。

Windows Server - 许可条款

项目 • 2023/09/05

查看我们 Windows Server 相关的许可条款。

- Windows Server 2016 的附加软件
- Windows Server Technical Preview 到期
- Windows Server 2016 Technical Preview 许可条款
- Microsoft 软件许可条款 - MICROSOFT.WINDOWSSERVER.SYSTEMINSIGHTS
- Microsoft 软件许可条款 - MICROSOFT.WINDOWSSERVER.SYSTEMINSIGHTS.CAPABILITIES
- Windows Admin Center - 许可条款