

Contents

Exchange 混合

[Office 365 邮件迁移顾问](#)

[混合配置向导](#)

[混合配置向导常见问题解答](#)

[混合部署先决条件](#)

[证书要求](#)

[传输选项](#)

[传输路由](#)

[混合管理](#)

[共享闲/忙](#)

[服务器角色](#)

[IRM](#)

[权限](#)

[边缘传输服务器](#)

[单一登录](#)

[ActiveSync 设置](#)

[性能最佳做法](#)

[关于最佳做法分析器 \(BPA\)](#)

[取消本地 Exchange](#)

[混合部署](#)

[混合代理](#)

[部署混合](#)

[移动邮箱](#)

[设置旧版混合公用文件夹](#)

[设置新式混合公用文件夹](#)

[设置 EXO 混合公用文件夹](#)

[设置委派邮箱权限](#)

[设置文档协作](#)

[设置 Office 365 组](#)

[创建基于云的存档](#)

[简化 OWA URL](#)

[解决混合部署故障](#)

[Exchange 2013 和 2007 混合](#)

[服务器角色](#)

[混合管理](#)

[边缘传输服务器](#)

[传输选项](#)

[传输路由](#)

[Exchange 2013 和 2010 混合](#)

[服务器角色](#)

[混合管理](#)

[边缘传输](#)

[传输选项](#)

[传输路由](#)

[关于 Exchange 文档](#)

[辅助功能](#)

[第三方版权声明](#)

[组织配置传输属性](#)

[可用同步设备访问规则属性](#)

[可用同步邮箱策略](#)

[ActiveSync 组织设置属性](#)

[地址列表属性](#)

[Dlp 策略属性](#)

[恶意软件筛选器策略属性](#)

[移动设备邮箱策略](#)

[组织配置](#)

[OWA 邮箱策略](#)

[策略提示配置属性](#)

[保留策略标记](#)

[保留策略](#)

Exchange Server 混合部署

2019/6/5 •

摘要: 规划 Exchange 混合部署需要了解的内容。

混合部署使组织可以将随其现有内部部署 Microsoft Exchange 组织提供的功能丰富的体验和管理控制扩展到云。混合部署可在内部部署 Exchange 组织与 Microsoft Office 365 中的 Exchange Online 之间提供单个 Exchange 组织的无缝观感。此外，混合部署还可以充当中间步骤，以完全移动到 Exchange Online 组织。

Exchange 混合部署功能

混合部署支持以下功能：

- 内部部署组织与 Exchange Online 组织之间的安全邮件路由。
- 使用共享域命名空间的邮件路由。例如，内部部署与 Exchange Online 组织都使用 @contoso.com SMTP 域。
- 统一全局地址列表 (GAL)，也称为“共享地址簿”。
- 内部部署组织与 Exchange Online 组织之间的忙/闲状态共享和日历共享。
- 集中控制入站和出站邮件流。可以将所有入站和出站 Exchange Online 邮件配置为通过内部部署 Exchange 组织路由。
- 用于内部部署和 Exchange Online 组织的单个 Web 上的 Outlook URL
- 可以将现有内部部署邮箱移到 Exchange Online 组织。如果需要，还可以将 Exchange Online 邮箱移回内部部署组织。
- 使用内部部署 Exchange 管理中心 (EAC) 集中管理邮箱。
- 内部部署组织和 Exchange Online 组织之间的邮件跟踪、邮件提醒和多邮箱搜索。
- 内部部署 Exchange 邮箱基于云的邮件存档。Exchange Online Archiving 可以与混合部署一起使用。了解 exchange online 存档中的存档功能的 Exchange online 存档的详细信息。

Exchange 混合部署的注意事项

在实施 Exchange 混合部署之前，请考虑以下事项：

- **混合部署要求：**在配置混合部署之前，您需要确保您的内部部署组织满足成功部署所需的所有先决条件。有关详细信息，请参阅[混合部署先决条件](#)。
- **Exchange ActiveSync 客户端：**将邮箱从内部部署 Exchange 组织移动到 Exchange online 时，访问该邮箱的所有客户端都需要更新以使用 Exchange online；这包括 Exchange ActiveSync 设备。大多数 Exchange ActiveSync 客户端现在都会在邮箱移到 Exchange Online 中时自动重新配置，但是，某些旧的设备可能不会正确升级。有关详细信息，请参阅[Exchange ActiveSync 设备设置与 exchange 混合部署](#)。
- **邮箱权限迁移：**内部部署邮箱权限（如“代理发送”、“完全访问”、“代表发送”和“文件夹权限”）将迁移到 Exchange Online。不会迁移继承（非明确）邮箱权限和授予给 Exchange Online 中未启用邮件的对象的权限。在迁移之前，请务必明确授予所有权限，并确保所有对象都启用邮件。因此，需要进行规划以在 Office 365 中配置这些权限（若适用于你的组织）。在代理发送权限情况下，如果尝试代理发送的用户和资源没有同时移动，则需要使用 **Add-RecipientPermission** cmdlet 在 Exchange Online 中显式添加代理发送权限。

- **对跨界邮箱权限的支持:** Exchange 混合部署支持使用完全访问权限, 并代表位于本地 Exchange 组织中的邮箱和位于 Office 365 中的邮箱之间的发送权限。"发送方式"权限需要其他步骤。此外, 可能需要一些额外的配置来支持跨界邮箱权限, 具体取决于在本地组织中安装的 Exchange 版本。有关详细信息, 请参阅[Exchange 混合部署中的权限](#)和[配置 Exchange 以支持混合部署中的委派邮箱权限](#)中的委派邮箱权限。
- **脱离:** 作为日常收件人管理的一部分, 您可能必须将 Exchange Online 邮箱移回到您的本地环境中。

有关如何在基于 Exchange 2010 的混合部署中移动邮箱的详细信息, 请参阅[Move an Exchange Online mailbox to the on-premises organization](#)。

有关如何在基于 Exchange 2013 或更高版本的混合部署中移动邮箱的详细信息, 请参阅在[混合部署中的内部部署组织](#)和[Exchange Online 组织之间移动邮箱](#)。

- **邮箱转发设置:** 可以将邮箱设置为自动将发送给它们的邮件转发到另一个邮箱。虽然 Exchange Online 支持邮箱转发, 但转发配置未随邮箱迁移一起复制到 Exchange Online 中。将邮箱迁移到 Exchange Online 前, 请务必先导出各个邮箱的转发配置。转发配置存储在每个邮箱 `DeliverToMailboxAndForward` 的 `ForwardingAddress`、和 `ForwardingSmtptAddress` 属性中。

Exchange 混合部署组件

混合部署涉及多个不同的服务和组件:

- **Exchange 服务器:** 如果要配置混合部署, 必须在您的内部部署组织中配置至少一个 Exchange 服务器。如果您运行 Exchange 2013 或更低版本, 您需要至少安装一台运行邮箱角色和客户端访问角色的服务器。如果您运行 Exchange 2016 或更新版本, 至少必须安装一台运行邮箱角色的服务器。如果需要, 也可以在外围网络中安装 Exchange 边缘传输服务器, 并支持与 Office 365 的安全邮件流。

NOTE

我们不支持在外围网络中安装运行邮箱服务器角色或客户端访问服务器角色的 Exchange 服务器。

- **Microsoft office 365:** office 365 服务将 Exchange Online 组织作为其订阅服务的一部分包括在其中。配置混合部署的组织需要为迁移到 Exchange Online 组织或者在 Exchange Online 组织中创建的每个邮箱购买一个许可证。
- **"混合配置" 向导:** Exchange 包括 "混合配置" 向导, 该向导为您提供了在内部部署 Exchange 和 Exchange Online 组织之间配置混合部署的简化的过程。

有关详细信息, 请参阅 ["混合配置"向导](#)。

- **AZURE AD 身份验证系统:** Azure Active DIRECTORY (AD) 身份验证系统是一项基于云的免费服务, 充当本地 exchange 2016 组织与 Exchange Online 组织之间的信任代理。配置混合部署的本地组织必须具有与 Azure AD 身份验证系统之间的联合信任。可手动创建联合信任作为配置内部部署 Exchange 组织和其他联合 Exchange 组织之间的联合共享功能的一部分, 或使用混合配置向导配置混合部署的一部分。Office 365 租户的 Azure AD 身份验证系统联合信任是在激活 Office 365 服务帐户时自动配置的。

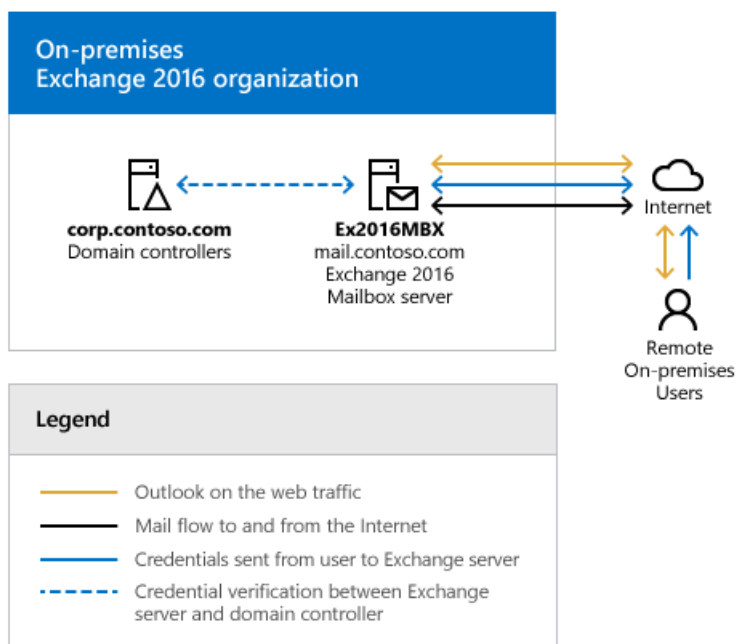
有关详细信息, 请参阅[什么是 AZURE AD Connect?](#)。

- **Azure Active Directory 同步:** azure ad 同步使用 Azure ad Connect 将已启用邮件的对象的本地 Active Directory 信息复制到 Office 365 组织, 以支持统一全局地址列表 (GAL) 和用户身份验证。配置混合部署的组织需要在单独的内部部署服务器上部署 Azure AD Connect 以将您的内部部署 Active Directory 与 Office 365 同步。

有关详细信息, 请参阅: [AZURE AD Connect 的先决条件](#)。

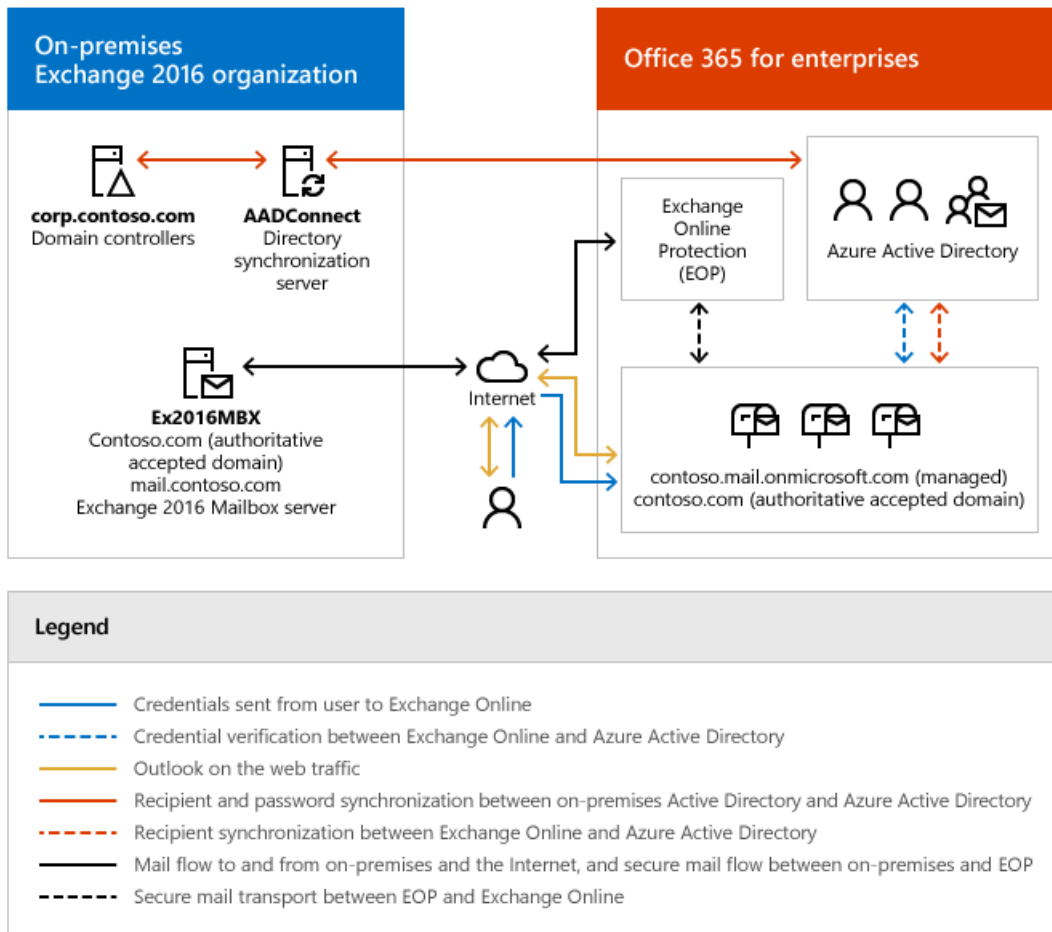
混合部署示例

看一下下面的情况。这是一个拓扑示例，概述了典型的 Exchange 2016 部署。Contoso, Ltd. 是一个单林单域组织，安装了两台域控制器和一台 Exchange 2016 服务器。远程 Contoso 用户使用 Web 上的 Outlook 通过 Internet 连接到 Exchange 2016 以检查其邮箱和访问其 Outlook 日历。



假设您是 Contoso 的网络管理员，同时对配置混合部署感兴趣。您部署与配置符合要求的 Active Directory 同步服务器，同时还决定使用 Azure AD Connect 密码同步功能让用户对其内部部署网络帐户和其 Office 365 帐户使用相同的凭据。完成混合部署先决条件，以及使用混合配置向导选择了混合部署的选项之后，新的拓扑具有以下配置：

- 用户将使用相同的用户名和密码登录到内部部署组织和 Exchange Online 组织 ("单一登录")。
- 位于内部部署组织和 Exchange Online 组织中的用户邮箱将使用相同的电子邮件地址域。例如，位于内部部署组织和 Exchange Online 组织中的邮箱都将在用户电子邮件地址中使用 @contoso.com。
- 所有出站邮件都将通过内部部署组织传递到 Internet。内部部署组织控制所有邮件传输，并充当 Exchange Online 组织的中继 ("集中邮件传输")。
- 内部部署组织用户和 Exchange Online 组织用户可以相互共享日历忙/闲信息。为这两个组织配置的组织关系还将启用跨内部部署邮件跟踪、邮件提示和邮件搜索。
- 内部部署用户和 Exchange Online 用户使用相同的 URL 通过 Internet 连接到其邮箱。



如果将 Contoso 的现有组织配置与混合部署配置进行比较，可以看到通过配置混合部署，添加了支持其他通信和功能的服务器和服务，这些通信和功能在内部部署组织和 Exchange Online 组织之间共享。下面概述了混合部署相对于初始内部部署 Exchange 组织所发生的变化。

配置	混合部署前	混合部署之后
邮箱位置	邮箱仅位于内部部署组织中。	内部部署邮箱与 Office 365 中的邮箱。
邮件传输	内部部署邮箱服务器处理所有入站和出站邮件路由。	内部部署邮箱服务器处理内部部署组织与 Office 365 组织之间的内部邮件路由。
Web 上的 Outlook	内部部署邮箱服务器接收所有 Web 上的 Outlook 请求并显示邮箱信息。	内部部署邮箱服务器将 Web 上的 Outlook 请求重定向到内部部署 Exchange 2016 邮箱服务器或提供登录 Office 365 的链接。
用于两个组织的统一 GAL	不适用;仅限单个组织。	内部部署 Active Directory 同步服务器将已启用邮件的对象的 Active Directory 信息复制到 Office 365。
用于两个组织的单一登录	不适用;仅限单个组织。	内部部署 Active Directory 和 Office 365 对位于内部部署或 Office 365 中的邮箱使用相同的用户名和密码。
与 Azure AD 身份验证系统建立的组织关系和联合信任	可以配置与 Azure AD 身份验证系统的信任关系以及与其他联合 Exchange 组织的组织关系。	必须与 Azure AD 身份验证系统建立信任关系。内部部署与 Office 365 之间建立组织关系。

配置	混合部署前	混合部署之后
忙/闲共享	仅在内部部署用户之间共享忙/闲信息。	在内部部署用户之间和 Office 365 用户之间共享忙/闲信息。

配置混合部署之前要考虑的事项

现在，您已对什么是混合部署有了进一步的了解，该认真考虑一些重要的问题了。配置混合部署可能会影响您当前网络和 Exchange 组织中的多个方面。

目录同步和单一登录

内部部署组织和 Office 365 组织之间的 Active Directory 同步 (由运行 Azure Active Directory Connect 的服务器每三小时执行一次) 是配置混合部署的一项要求。目录同步使任一组织中的收件人可以在全局地址列表中看到彼此。它还将同步用户名和密码，使用户可以在内部部署组织和 Office 365 组织中使用相同凭据登录。

NOTE

如果您选择使用 AD FS 配置 Azure AD Connect，默认情况下，内部部署用户的用户名和密码将仍会同步到 Office 365。但是，用户将通过 AD FS 对内部部署 Active Directory 进行身份验证，作为其主要身份验证方法。如果出于任何原因，AD FS 无法连接到您的内部部署 Active Directory，客户端将尝试回退并对同步到 Office 365 的用户名和密码进行身份验证。

Azure Active Directory 和 Office 365 的所有客户都有 50000 个对象 (用户、启用邮件的联系人和组) 的默认限制，这些对象决定了您可以在 Office 365 组织中创建的对象数。在验证第一个域后，此限制会自动增加到 500000 个对象 (适用于 Azure Active Directory Free) 或无限数量的 Azure Active Directory 基本或高级对象。有关详细信息，请参阅 [Azure Active Directory 定价](#)。

如果选择配置 AD FS，除了运行 Azure AD Connect 的服务器，您还需要部署 Web 应用程序代理服务器。此服务器应置于外围网络中，并将充当内部 Azure AD Connect 服务器和 Internet 之间的中介。Web 应用程序代理服务器需要接受 Internet 上使用 TCP 端口 443 的客户端和服务器的请求进行的连接。

混合部署管理

通过单个统一管理控制台，您可以管理 Exchange 2016 的混合部署，允许同时管理您的内部部署和 Office 365 Exchange Online 组织。替换 Exchange 管理控制台和 Exchange 控制面板的 Exchange 管理中心 (EAC) 允许您连接和配置两个组织的功能。当首次运行混合配置向导时，将提示您连接 Exchange Online 组织。您需要使用作为组织管理角色组之一的 Office 365 帐户连接 EAC 到您的 Exchange Online 组织。

证书

安全套接字层 (SSL) 数字证书对配置混合部署非常重要。这些证书有助于保证内部部署混合服务器与 Exchange Online 组织之间的通信安全。证书是配置几个服务类型的要求。如果您的 Exchange 组织中已在使用数字证书，可能需要修改证书以包括其他域或者从受信任的证书颁发机构 (CA) 购买其他证书。如果未使用证书，则需要从受信任的 CA 购买一个或多个证书。

可在以下位置了解详细信息: [混合部署的证书要求](#)

带宽

与 Internet 的网络连接会直接影响内部部署组织与 Office 365 组织之间的通信性能。尤其是在将邮箱从内部部署 Exchange 2016 服务器移到 Office 365 组织时。可用的网络带宽量以及邮箱大小和同时移动的邮箱数会导致完成邮箱移动的时间有所不同。此外，其他 Office 365 服务 (例如 SharePoint Server 2016 和 Skype for Business) 也可能影响可用于邮件服务的带宽。

将邮箱移动到 Office 365 之前，您应该完成以下事项：

- 确定将移动到 Office 365 的邮箱的平均大小。
- 确定从内部部署组织连接到 Internet 的平均连接速度和吞吐速度。

- 计算预期的平均传输速度，然后相应地制定邮箱移动计划。

可在以下位置了解详细信息：[网络](#)

统一消息

NOTE

统一消息在 Exchange 2019 中不可用。

内部部署组织与 Office 365 组织之间的混合部署中支持统一消息 (UM)。内部部署电话解决方案必须能与 Office 365 组织进行通信。这可能需要购买其他硬件和软件。

如果要移动邮箱从内部部署组织移至 Office 365，并且为这些邮箱配置了 UM 功能，则应先在混合部署中配置 UM，然后再移动这些邮箱。如果先移动邮箱，然后再在混合部署中配置 UM，则这些邮箱将无法再访问 UM 功能。

有关详细信息，请参阅：[在混合部署中设置统一消息](#)

信息权限管理

通过信息权限管理 (IRM)，用户可将 Active Directory 权限管理服务 (AD RMS) 模板应用于其发送的邮件。AD RMS 模板可通过允许用户控制谁可打开受权限保护的邮件及其打开邮件后可对邮件执行什么操作，从而帮助防止信息泄漏。

混合部署中的 IRM 需要进行规划、手动配置 Office 365 组织，并要了解客户端应根据其邮箱是位于内部部署组织还是 Exchange Online 组织中而如何使用 AD RMS 服务器。

有关详细信息，请参阅：[IRM In Exchange 混合部署](#)

移动设备

混合部署中支持移动设备。如果现有服务器已经启用 Exchange ActiveSync，它们会继续将来自移动设备的请求重定向到位于内部部署邮箱服务器的邮箱。对于连接到从内部部署组织移到 Office 365 的现有邮箱的设备，将会自动更新 Exchange ActiveSync 配置文件以连接至大多电话上的 Office 365。支持 Exchange ActiveSync 的所有移动设备应与混合部署兼容。

可在以下位置了解详细信息：[移动电话](#)

客户端要求

建议您的客户端使用 Outlook 2016 或 Outlook 2013，以便在混合部署中实现最佳体验和性能。Outlook 2010 之前的客户端在混合部署中或者 Office 365 中不受支持。

Office 365 的许可

若要在 Office 365 中创建邮箱或将邮箱移至 Office 365，需要注册用于企业的 Office 365 并且必须具有可用的许可证。注册 Office 365 后，您将会收到特定数量的许可证，可以将这些许可证分配给新邮箱或从内部部署组织移动的邮箱。Office 365 中的每个邮箱都必须有许可证。

防病毒和反垃圾邮件服务

对于移至 Office 365 的邮箱，系统会自动通过 Exchange Online Protection (EOP) 为其提供防病毒和反垃圾邮件保护，一种 Office 365 提供的服务。如果选择通过 EOP 服务路由所有传入的 Internet 邮件，则可能需要为您的内部部署用户购买其他 EOP 许可证。我们建议您仔细评估您的 Office 365 中的 EOP 保护是否也适合满足内部部署组织的防病毒和反垃圾邮件需要。如果您已经实施了内部部署组织保护，则可能需要升级或配置您的内部部署防病毒和反垃圾邮件解决方案，以期在整个组织中实现最大程度的保护。

可在以下位置了解详细信息：[Anti-Spam and Anti-Malware Protection](#)

公用文件夹

Office 365 支持公用文件夹，同时内部部署公共文件夹可迁移到 Office 365。此外，Office 365 中的公共文件夹可

以移动到内部部署 Exchange 2016 组织。内部部署和 Office 365 用户均可以使用 Web 上的 Outlook、Outlook 2016、Outlook 2013 或 Outlook 2010 SP2 或更新版本访问位于两个组织中的公用文件夹。配置混合部署时不会改变现有的内部部署公用文件夹配置和对内部部署邮箱的访问权限。

可在以下位置了解详细信息: [Public Folders](#)

辅助功能

有关可能适用于此检查表中的过程的键盘快捷方式的信息, 请参阅 [Exchange 管理中心的键盘快捷方式](#)。

关键术语

以下列表提供了与 Exchange 2013 中的混合部署关联的核心组件的定义。

集中邮件传输

混合配置选项, 其中所有 Exchange Online 入站和出站 Internet 邮件都通过内部部署 Exchange 组织路由。此路由选项在混合配置向导中配置。有关详细信息, 请参阅 [Transport options in Exchange hybrid deployments](#)。

共存域

一种接受域, 添加到内部部署组织中用于 Office 365 服务的混合邮件流和自动发现请求。此域将作为辅助代理域添加到在混合配置向导中为其选择了 "域" 的 " *PrimarySmtptAddress* " 模板的任何电子邮件地址策略中。默认情况下, 此域是 <域>.mail.onmicrosoft.com。

_HybridConfiguration_Active Directory 对象

内部部署组织中的 Active Directory 对象, 其中包含按混合配置向导中选择的内容定义的所需混合部署配置参数。混合配置引擎在配置内部部署和 Exchange Online 设置时使用这些参数来启用混合功能。每次运行 "混合配置" 向导时, _HybridConfiguration_ 对象的内容都会重置。

混合配置引擎

混合配置引擎 (HCE) 运行配置和更新混合部署所需的核心操作。HCE 将 _HybridConfiguration_Active Directory 对象的状态与当前的内部部署 Exchange 和 Exchange Online 配置设置进行比较, 然后执行任务以将部署配置设置与参数进行匹配在 _HybridConfiguration_Active Directory 对象中定义。有关详细信息, 请参阅 [混合配置引擎](#)。

混合配置向导 (HCW)

Exchange 提供的一种自适应工具, 可指导管理员完成内部部署组织和 Exchange Online 组织之间的混合部署配置。向导定义 _HybridConfiguration_ 对象中的混合部署配置参数, 并指示混合配置引擎运行所需的配置任务, 以启用定义的混合功能。有关详细信息, 请参阅 ["混合配置"向导](#)。

基于 Exchange 2010 的混合部署

一种混合部署, 配置时使用 Exchange Server 2010 Service Pack 3 (SP3) 内部部署服务器作为 Office 365 和 Exchange Online 服务连接终结点。一种混合部署选项, 适用于内部部署 Exchange 2010、Exchange Server 2007 和 Exchange Server 2003 组织。

基于 Exchange 2013 的混合部署

一种混合部署, 配置时使用 2013 内部部署服务器作为 Office 365 和 Exchange Online 服务连接终结点。一种

混合部署选项, 适用于内部部署 Exchange 2013、Exchange 2010 和 Exchange 2007 组织。

基于 Exchange 2016 的混合部署

一种混合部署, 配置时使用 2016 内部部署服务器作为 Office 365 和 Exchange Online 服务连接终结点。一种混合部署选项, 适用于内部部署 Exchange 2016、Exchange 2013 和 Exchange 2010 组织。

安全邮件传输

一种自动配置的混合部署功能, 可实现内部部署组织与 Exchange Online 组织之间的安全邮件传递。邮件使用传输层安全性 (TLS) 进行加密和身份验证, 采用混合部署向导中选择的证书。Office 365 租户是源于内部部署组织的混合传输连接的终结点, 是从 Exchange Online 到内部部署组织的混合传输连接的来源。

Exchange 混合部署文档

下表包含主题链接, 这将帮助您学习和管理 Microsoft Exchange 的混合部署。

主题	说明
"混合配置"向导	了解混合配置向导和混合配置引擎如何配置混合部署的信息。
混合部署先决条件	了解混合部署先决条件的详细信息, 包括兼容 Exchange Server 组织、Office 365 要求和其他内部部署配置要求。
混合部署的证书要求	了解有关混合部署数字证书要求的详细信息。
Exchange 混合部署的传输选项	了解有关混合部署中的入站和出站邮件传输选项的详细信息。
Exchange 混合部署中的传输路由	了解有关混合部署中的入站和出站邮件路由选项的详细信息。
Exchange 混合部署中的混合管理	了解有关使用 Exchange 管理中心和 Exchange 命令行管理程序管理混合部署的详细信息。
Exchange 混合部署中共享的忙/闲信息	了解有关混合部署中的内部部署和 Exchange Online 组织之间的日历闲/忙共享的详细信息。
Exchange 混合部署中的服务器角色	了解混合部署中的 Exchange 服务器角色如何运行的详细信息。
Exchange 混合部署中的 IRM	了解有关混合部署中的信息权限管理如何运行的详细信息。
Exchange 混合部署中的权限	了解有关混合部署如何使用基于角色的访问控制 (RBAC) 控制权限的详细信息。
混合部署中的边缘传输服务器	了解 Exchange 边缘传输服务器以及如何在混合部署中部署和运营的详细信息。
混合部署中的单一登录	了解如何使用混合部署中的密码同步和 AD FS 功能进行单一登录的详细信息。
混合部署过程	探索创建和修改 Exchange 内部部署和 Exchange Online 组织的混合部署的程序。

主题	说明
Exchange 2013 和 Exchange 2010 的混合部署	了解有关针对 Exchange 2010 组织进行基于 Exchange 2013 的混合部署的详细信息。
Exchange 2013 和 Exchange 2007 的混合部署	了解有关针对 Exchange 2007 组织进行基于 Exchange 2013 的混合部署的详细信息。

使用 Office 365 邮件迁移顾问

2019/6/5 •

若要从现有本地 Exchange Server 环境迁移,您可以将用户邮箱中的所有电子邮件、日历和联系人迁移到 Office 365。Office 365 提供了一个[邮件迁移顾问](#),可帮助你将邮箱从当前邮件系统移动到 Office 365 中的 Exchange Online,并提供了自动化的工具和分步指南。Advisor 将根据您当前的邮件系统、要迁移的邮箱数以及计划管理用户和用户访问的方式为您的组织建议最佳迁移路径。

如何运行迁移顾问?

若要运行 Office 365 迁移顾问,您需要以下各项:

- 包含 Exchange Online 的 Office 365 订阅计划。若要查看哪些计划支持 Exchange Online,请参阅[Office 365 计划选项](#)和[Exchange Online 服务说明](#)。
- 具有全局管理员权限的 Office 365 帐户。

拥有所需的一切后,即可通过转到[Office 365 邮件迁移顾问](#)打开邮件迁移顾问。打开此链接时,需要登录 Office 365 租户。

运行迁移顾问时,我将会有哪些选项?

运行 advisor 时,它会询问有关现有本地环境的问题,以帮助您确定将电子邮件发送到 Office 365 的最佳方式。根据您的回答,advisor 将选择以下迁移选项之一:

- **混合:** 混合迁移采用几种不同的风格-完整、最小和快速。
 - 完全混合迁移最适用于具有数千个邮箱的大型组织,并且需要在其本地 Exchange 组织和 Office 365 之间实现完全集成。Active Directory 与 Office 365 同步,可以交换忙/闲信息,增强的邮件流选项变得可用,等等。若要了解有关完全混合迁移的详细信息,请参阅[Exchange 混合部署](#)。
 - 最小混合迁移最适用于中等规模的组织,这些组织的数量几百到一千个邮箱,希望在几个月内完成其迁移。与完全混合一样,最小混合迁移设置了与 Office 365 的日常 Active Directory 同步,以帮助实现收件人管理。但是,如忙/闲同步和其他增强功能等功能不可用。若要了解有关最小混合迁移的详细信息,请参阅[最小混合配置](#)。
 - 快速迁移最适用于希望在几个星期内完成其迁移的小型组织。快速迁移执行与 Office 365 的一次性 Active Directory 同步,以设置收件人,然后帮助将其邮箱移动到 Office 365。没有可用的增强功能。若要了解有关快速混合迁移的详细信息,请参阅[Express 混合迁移](#)。
- **暂存:** 暂存迁移最适用于运行 exchange 2003 或 exchange 2007 的组织,他们希望在数周内通过批移动邮箱,从而减少邮箱数少于2000的 exchange。虽然您可以使用更高版本的 Exchange 进行暂存迁移,但强烈建议您改用**最小混合迁移**选项。通过暂存迁移,您可以执行与 Office 365 的一次性 Active Directory 同步,以在 Office 365 中创建收件人。完成后,您可以选择一次移动到 Office 365 的邮箱批处理。移动邮箱后,会向用户提供新的登录凭据,并需要重新配置其 Outlook 和其他邮件应用程序配置文件。有关暂存迁移的详细信息,请查看[有关将暂存电子邮件迁移到 Office 365 的需要了解的信息](#)。
- ****** 转换:** 直接转换迁移最适用于运行 exchange 2003 或 exchange 2007 的组织,他们希望在几天内移动邮箱,但邮箱数少于2000个。虽然您可以使用更高版本的 Exchange 进行直接转换迁移,但强烈建议您改为使用**"Express混合迁移"**选项。通过直接转换迁移,Office 365 读取 Active Directory 并在 Office 365 中创建新的收件人。完成后,Office 365 会将所有用户邮箱的内容复制到 Office 365 中的新邮箱。完成后,将向用户提供新的登录凭据,并需要重新配置其 Outlook 和其他邮件应用程序配置文件。有关直接转换迁移的详细信息,请查看[有关直接转换电子邮件迁移到 Office 365 的需要了解的信息](#)。

若要了解有关这些选项的详细信息或需要更多帮助来决定使用哪个选项, 请查看[将多个电子邮件帐户迁移到 Office 365 的方法](#), 并[决定迁移路径](#)。

“混合配置”向导

2019/6/5 •

本主题概括介绍了 Exchange 混合部署配置过程、可供您使用的混合部署功能和选项以及混合配置引擎, 该引擎将执行配置和更新过程中所需的核心操作。混合部署。

有关混合部署的详细信息, 请查看[Exchange Server 混合部署](#)。

混合配置过程

以下是混合配置向导过程的快速概述。首先, 向导在本地 Active Directory 中创建 **HybridConfiguration** 对象。此 Active Directory 对象存储混合部署的混合配置信息, 并由 “混合配置” 向导更新。其次, 向导将收集现有内部部署 Exchange 和 Active Directory 拓扑配置数据, Office 365 租户和 Exchange Online 配置数据, 定义几个组织参数, 然后同时在内部部署组织和 Exchange Online 组织中执行大量配置任务。

IMPORTANT

使用“混合配置”向导之前您需要考虑一些重要因素和满足一些前提条件。您需要满足[混合部署先决条件](#)中所述的混合部署的要求。然后, 您将准备好使用 “混合配置” 向导为混合部署配置 Exchange 组织。

混合部署配置过程的一般阶段是:

1. 验证先决条件并执行拓扑检查: “混合配置” 向导将验证您的内部部署组织和 Exchange Online 组织是否可以支持混合部署。向导在内部部署组织和 Exchange Online 组织中验证和检查的一些项目如下:
 - 内部部署 Exchange 服务器版本
 - Exchange Online 版本
 - Active Directory 同步状态和配置
 - 联盟与接受域
 - 现有联合身份验证信任和组织的关系
 - Web 服务虚拟目录
 - Exchange 证书
2. 测试帐户凭据: 指定的本地和 Office 365 混合管理帐户可访问内部部署组织和 Exchange Online 组织, 以收集先决条件验证信息并建立组织参数后用混合部署功能的配置更改。“混合配置” 向导将检查帐户是否具有适当的凭据, 以及是否可以连接到内部部署组织和 Exchange Online 组织。内部部署和 Office 365 组织的混合部署管理帐户必须是“混合配置”向导的组织管理角色组成员, 才能成功完成这些任务。
3. 进行混合部署配置更改: 测试混合管理帐户后, 进行验证和拓扑检查, 并收集在向导过程中定义的配置信息, 混合配置向导进行配置更改, 以创建和启用混合部署。对混合配置进行的所有更改会自动记录在混合配置日志中。默认情况下, 混合配置日志位于的内部部署邮箱服务器上

%UserProfile%\AppData\Roaming\Microsoft\Exchange Hybrid Configuration 。

IMPORTANT

入站邮件流由您的组织的 MX 记录控制。混合部署的入站 Internet 电子邮件不是由 “混合配置” 向导配置的。

混合配置功能

“混合配置”向导每次运行时，在默认情况下会自动启用所有混合部署功能。如果要禁用特定的混合配置功能, 则需要使用 Exchange 命令行管理程序和 **HybridConfiguration** cmdlet。默认情况下，该向导会启用以下混合部署功能：

- **忙/闲共享:** 闲/忙共享功能允许在内部部署组织用户和 Exchange Online 组织用户之间共享日历信息。忙/闲共享会在针对内部部署组织和 Exchange Online 组织的联合共享和组织关系配置中启用。有关详细信息，请参阅 [Understanding Federated Delegation](#)。
- **邮件提示:** 邮件提示是在用户撰写邮件时向其显示的信息性消息。通过在混合部署中启用邮件提示，内部部署和 Exchange Online 的发件人可以调整所撰写的邮件，以避免组织之间出现不利情况或未送达报告 (NDR)。有关详细信息，请参阅 [MailTips](#)。
- **在线存档:** 在线存档使 Exchange online 组织能够承载内部部署用户和 Exchange online 用户的用户电子邮件存档。有关详细信息，请参阅[配置 Exchange Online 存档](#)。
- **Web 上的 outlook 重定向:** outlook on the web 重定向提供了访问本地和 Exchange Online 邮箱的单一、通用的 URL。客户端访问服务器会自动将 web 上的 Outlook 请求重定向到内部部署邮箱服务器, 或为 Exchange Online 组织中的邮箱提供用户的链接。
- **Exchange ActiveSync 重定向:** 将邮箱从内部部署 exchange 组织移动到 Exchange online 时, 需要更新访问该邮箱的所有客户端以使用 Exchange online;这包括 Exchange ActiveSync 设备。大多数 Exchange ActiveSync 客户端将在邮箱移动到 Exchange Online 时自动重新配置。有关详细信息, 请参阅[Exchange ActiveSync 设备设置与 exchange 混合部署](#)。
- **安全邮件:** 安全邮件通过传输层安全性 (TLS) 协议启用内部部署组织和 Exchange Online 组织之间的安全邮件传递。内部部署组织和 Exchange Online 组织通过数字证书主题互相进行身份验证，电子邮件头和 RTF 邮件格式会在组织间保留。

混合配置选项

“混合配置”向导允许选择某些方面的特定选项进行混合部署。如果要在最初配置混合部署后更新特定的混合配置选项, 可以使用 “混合配置” 向导或 Exchange 命令行管理程序来选择不同的配置选项。

下表概括了“混合配置”向导修改和配置的主要选项。

配置方面	说明
域	<p>向导会将一个接受的域添加到内部部署组织以实现云组织的混合邮件流和自动发现请求。此域称为共存域, 作为辅助代理域添加到在混合配置向导中选择了 " <i>PrimarySmtptAddress</i> " 域模板的任何电子邮件地址策略中。默认情况下，此域是 <域>.mail.onmicrosoft.com。您可以通过在 exchange Online 中的 Exchange 命令行管理程序中运行以下命令来查看接受</p> <div><pre>Get-AcceptedDomain Format-List DomainName, IsCoexistenceDomain</pre></div> <p>的域。</p>
安全邮件证书	<p>向导要求选择由第三方证书颁发机构 (CA) 颁发的特定证书。该机构负责验证和确保在内部部署与 Exchange Online 组织之间发送的邮件是安全的。</p>

配置方面	说明
Exchange 联合共享	向导将检查内部部署组织的 Azure Active Directory 身份验证系统是否存在现有的 OAuth 身份验证关系或联合身份验证信任。如果存在, 则现有 OAuth 身份验证或联合身份验证信任将用于支持混合部署。如果不存在, 则向导将配置 OAuth 身份验证, 或为具有 Azure AD 身份验证系统的内部部署组织创建联合信任, 具体取决于本地 Exchange 配置的类型。如果需要, 向导还会将在混合配置向导中选择的任何域添加到联合身份验证信任中。除了 OAuth 身份验证或联合身份验证信任配置之外, 向导还会为内部部署组织和 Exchange Online 组织创建和配置组织关系。这些组织关系允许向导启用多种混合部署功能, 包括忙/闲共享、Outlook 在 web 上的重定向和邮件提示。
邮件流	<p>向导允许您选择和配置要在本地环境与 Exchange Online 组织之间处理安全邮件传输的 Exchange 服务器。在 Exchange 2010 中为集线器传输服务器。在 Exchange 2013 中为客户端访问服务器。在 Exchange 2016 和更高版本中, 这是一个邮箱服务器。向导为混合邮件路由配置内部部署 Exchange 和 Exchange Online 组织。通过配置内部部署组织中新的和现有的发送与接收连接器以及 Exchange Online 中的入站与出站连接器, 向导使您可以选择从 Exchange Online 组织传递到 Internet 的出站邮件是直接发送到外部邮件收件人, 还是通过混合部署包含的内部部署 Exchange 服务器进行路由。</p> <p>重要说明: 入站邮件流由您的组织的 MX 记录控制。混合部署的入站 Internet 电子邮件不是由 "混合配置" 向导配置的。</p>

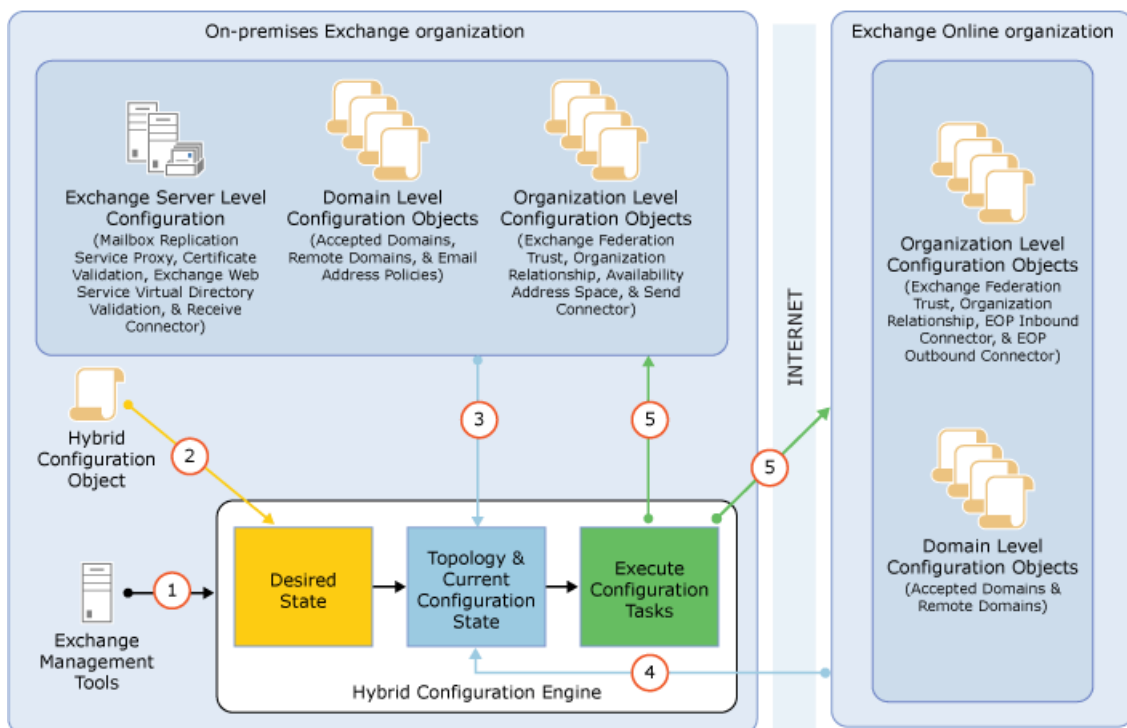
混合配置引擎

混合配置引擎运行配置和更新混合部署所需的核心操作。负责处理 `Update-HybridConfiguration` cmdlet 操作, 混合配置引擎将 `_HybridConfiguration_` Active Directory 对象的状态与当前的内部部署 exchange 和 Exchange Online 配置设置进行比较, 然后运行任务以将部署配置设置与 `_HybridConfiguration_` Active Directory 对象中定义的参数相匹配。如果当前的内部部署 Exchange 和 Exchange Online 部署配置状态已与 `_HybridConfiguration_` Active Directory 对象中定义的设置相匹配, 则混合配置引擎不会对内部部署组织或 Exchange Online 组织。

当更新现有混合部署时, 混合配置引擎会执行以下步骤:

1. `Update-HybridConfiguration` cmdlet 触发混合配置引擎启动。
2. 混合配置引擎会读取 `HybridConfiguration` Active Directory 对象上存储的 "所需状态"。
3. 混合配置引擎从内部部署 Exchange 组织中发现拓扑数据和当前配置。
4. 混合配置引擎从 Exchange Online 组织中发现拓扑数据和当前配置。
5. 根据所需的状况、拓扑数据和当前配置, 混合配置引擎将建立内部部署 Exchange 与 Exchange Online 组织之间的 "差异", 然后执行配置任务以建立所需状态。

下图显示了混合配置引擎如何在混合部署过程中检索和修改本地 Exchange server 和 Exchange Online 配置设置的摘要。



混合配置向导 FAQ

2019/6/5 •

Microsoft 已发布了一个新的混合配置向导 (HCW), 该向导简化了混合部署的配置, 使您可以通过混合配置获得更大的灵活性, 并确保您始终运行最新的体验版本。此版本的混合向导内置在于 Exchange 2016 和从累积更新 10 开始的 Exchange 2013 版本中, 但是, 即使正在运行较旧的 Exchange 2013 累积更新 (CU) 或 Exchange 2010 Service Pack 3 (SP3), 仍可以下载新的向导。

有关 Office 365 混合配置向导的详细信息, 请在 Exchange 团队博客上参阅 [Introducing the Microsoft Office 365 Hybrid Configuration Wizard](#) (引入 Microsoft Office 365 混合配置向导) 和 [Office 365 Hybrid Configuration Wizard for Exchange 2010](#) (适用于 Exchange 2010 的 Office 365 混合配置向导)。

若要下载 Office 365 混合配置向导, 请转到 <https://aka.ms/HybridWizard>。

客户提出的常见问题

问: 什么版本的 Exchange 支持新的混合配置向导?

A: 您可以使用以下一个或多个项的组合:

- Exchange 2010 SP3 (强烈建议使用最新的 RU)
- Exchange 2013 CU1 或更高版本
- Exchange 2016 和 Exchange 2019

重要说明: 若要保持受支持的混合配置, 您需要确保为 Exchange 版本运行最新可用的发布的 CU。累积更新按季度有规律地进行发布。如果无法升级到最新的可用的 CU, 则也支持以前的 CU。

有关特定于角色的要求和先决条件, 请参阅[混合部署的先决条件](#)。

问: 此混合配置向导是否适用于 Exchange 2007?

答: 可以在组织中使用 Exchange 2007 配置混合部署。但是, 若要执行此操作, 需要部署至少一台运行满足上述要求的 Exchange 2013 的服务器。

问: 是否可以退出新混合配置向导?

答: 不可以。目前, 新混合配置向导是在 Exchange 2010、Exchange 2013 和 Exchange 2016 中唯一受支持的向导。

问: 是否可以使用新混合配置向导将当前的 Exchange 2010 混合配置升级到 Exchange 2013 或 Exchange 2016?

答: 可以。确保至少有一台服务器满足当前混合配置向导要求, 然后运行该服务器。该向导将会了解混合配置的当前状态, 并无缝指导你完成升级过程。

问: 我的本地组织中的 Exchange 混合服务器是否需要 Exchange 许可证?

答: 可以。在配置混合部署时, 您需要为您的混合服务器授予许可证。现在, HCW 可以在不转到单独的网站或呼叫 Microsoft 支持的情况下, 检测并许可指定的本地 Exchange 2010、Exchange 2013 或 Exchange 2016 混合服务器, 以供免费使用。您可以在[此处](#)访问 HCW。请注意, Exchange 2019 混合服务器不提供免费 Exchange Server 许可证。

混合部署先决条件

2019/6/5 •

摘要: 在设置混合部署之前, 您的 Exchange 环境需要满足的要求。

在使用"混合配置"向导创建和配置混合部署之前, 现有的内部部署 Exchange 组织必须满足特定的要求。如果不满足这些要求, 将无法完成"混合配置"向导中的步骤, 且无法配置内部部署 Exchange 组织与 Exchange Online 之间的混合部署。

混合部署的先决条件

配置混合部署必须满足以下先决条件:

- **内部部署 exchange 组织:** 可以为基于 Exchange 2007 的本地组织或更高版本配置混合部署。

已安装在您的本地组织中的 Exchange 版本决定了您可以安装的混合部署版本。通常应该配置在您组织中支持的最新混合部署版本。例如, 如果您的本地组织运行 Exchange 2007, 则需配置基于 Exchange 2013 的混合部署。有关 Exchange Server 和 Office 365 企业混合部署兼容性的完整列表, 请参阅下表。

内部部署环境	基于 EXCHANGE 2019 的混合部署	基于 EXCHANGE 2016 的混合部署	基于 EXCHANGE 2013 的混合部署	基于 EXCHANGE 2010 的混合部署
Exchange 2019	支持	不支持	不支持	不支持
Exchange 2016	支持	支持	不支持	不支持
Exchange 2013	支持	支持	支持	不支持
Exchange 2010	不支持	支持	支持	支持
Exchange 2007	不支持	不支持	支持	支持

- **内部部署 Exchange 版本:** 混合部署需要可用于在内部部署组织中安装的 Exchange 版本的最新累积更新或更新汇总。如果您无法安装最新的累积更新或更新汇总, 则也支持前一版本。不支持更早的累积更新或更新汇总。

例如, 假设您已在您的本地组织中安装了 Exchange 2013 累积更新 8, 则 Exchange 2013 的最新可用版本就是累积更新 10。为了保持在受支持的混合配置中, 您需要将您的 Exchange 2013 服务器至少升级到累积更新 9。但是, 我们强烈建议您升级到累积更新 10。

累积更新和更新汇总按季度有规律地进行发布, 因此, 如果您定期需要额外一些时间来完成升级, 那么让您的服务器始终使用最新的累积更新或更新汇总就可以使您拥有更多的灵活性。

- **本地服务器角色:** 需要在内部部署组织中安装的服务器角色取决于已安装的 Exchange 版本。
 - **Exchange 2010:** 至少安装了一台邮箱、集线器传输和客户端访问服务器角色的服务器。虽然可以在单独的服务器上安装邮箱服务器角色、集线器传输服务器角色和客户端访问服务器角色, 但我们强烈建议您在每台服务器上都安装所有角色, 这样可以提供额外的可靠性和更好的性能。
 - **Exchange 2013:** 至少有一台安装了邮箱和客户端访问服务器角色的服务器。虽然可以在单独的服务器上安装邮箱服务器角色和客户端访问服务器角色, 但我们强烈建议您在每台服务器上都安装这两种角色, 这样可以提供额外的可靠性和更好的性能。

- **Exchange 2016 和更高版本:** 至少有一台安装了邮箱服务器角色的服务器。

混合部署还支持运行边缘传输服务器角色的 Exchange 服务器。边缘传输服务器还需要更新到最新的累积更新或更新汇总,以便可以用于您已安装的 Exchange 版本。我们强烈建议您将边缘传输服务器部署在外围网络中。无法在外围网络中部署邮箱服务器和客户端访问服务器。

- **Office 365:** 支持 Azure Active Directory 同步的所有 Office 365 计划都支持混合部署。所有 Office 365 商业高级版、业务重点、企业、政府、学术和中型计划都支持混合部署。Office 365 Business 和 Office 365 Home 计划不支持混合部署。

详细了解如何[注册 Office 365](#)。

- **自定义域:** 使用 Office 365 注册要在混合部署中使用的任何自定义域。您可以使用 Office 365 管理入口网站或选择在您的内部部署组织中配置 Active Directory 联合身份验证服务 (AD FS)。

详细了解如何[将域添加到 Office 365](#)。

- **Active directory 同步:** 部署 Azure Active Directory Connect 工具以后用与您的内部部署组织的 Active Directory 同步。

若要了解详细信息,请参阅 [Azure AD Connect 用户登录选项](#)。

- **自动发现 DNS 记录:** 将现有 SMTP 域的自动发现公用 DNS 记录配置为指向本地 Exchange 2010/2013 客户端访问服务器或 Exchange 2016/2019 邮箱服务器。
- **Exchange 管理中心 (EAC) 中的 office 365 组织:** 默认情况下,office 365 组织节点包含在本地 EAC 中,但必须先使用 office 365 管理员凭据将 EAC 连接到 office 365 组织,然后再您可以使用 "混合配置" 向导。这还允许您通过一个管理控制台管理内部部署组织和 Exchange 联机组织。

有关详细信息,请参阅[Exchange 混合部署中的混合管理](#)。

- **证书:** 安装 Exchange 服务并将其分配给从受信任公共证书颁发机构 (CA) 购买的有效数字证书。虽然自签名证书应用于带 Microsoft 联合网关的内部部署联合身份验证信任,但自签名证书不能用于混合部署中的 Exchange 服务。在混合部署中配置的 Exchange 服务器上的 Internet 信息服务 (IIS) 实例必须具有从受信任的 CA 购买的有效数字证书。此外,在公用 DNS 中指定的 EWS 外部 URL 和自动发现终结点必须列在证书的主题备用名称 (SAN) 中。安装在用于混合部署邮件传输的 Exchange 服务器上的证书必须使用相同的证书(即,由同一 CA 颁发并具有相同主题)。

有关详细信息,请参阅 [混合部署的证书要求](#)。

- **EdgeSync:** 如果您已在内部部署组织中部署了边缘传输服务器,并且想要为混合安全邮件传输配置边缘传输服务器,则必须在使用 "混合配置" 向导之前配置 EdgeSync。此外,每次向边缘传输服务器应用新的累积更新或更新汇总时,您都需要运行 EdgeSync。

IMPORTANT

尽管 EdgeSync 是部署边缘传输服务器的要求,但是当为混合安全邮件传输配置边缘传输服务器时,还需要额外的手动传输配置设置。

有关详细信息,请参阅[混合部署中的边缘传输服务器](#)。

- **已启用统一消息 (UM) 的邮箱:** 如果您具有已启用 UM 的邮箱,并且想要将其移动到 Office 365,除了 Exchange 混合部署之外,还需要以下各项。必须满足这些要求 才能将任意已启用 UM 的邮箱移动到 Office 365。
 - Lync Server 2010, Lync Server 2013, or Skype for Business Server 2015 or later integrated with your on-premises telephony system **or**
 - Skype for Business Online integrated with your on-premises telephony system **or**

- 传统的本地 PBX 或 IP-PBX 解决方案。
- 在 Exchange Online 中创建的，镜像本地组织中 UM 邮箱策略名称的 UM 邮箱策略。

NOTE

可以将多个本地 UM 邮箱策略映射到 Exchange Online 中的一个 UM 邮箱策略中。如果要执行此操作，需要使用 Exchange 命令行管理程序，手动将每个本地 UM 邮箱策略映射到 Exchange Online 策略。

有关详细信息，请查看[Telephone System Integration with UM](#)、[Telephony Advisor for Exchange 2013](#) 和 [设置云 PBX 语音邮件](#)。

混合部署协议、端口和终结点

混合部署功能和组件要求特定传入协议、端口和连接终结点必须可供 Office 365 访问，这样才能正常运行。配置混合部署之前，请先确认本地网络和安全配置能否支持下表中的功能和组件。除了允许特定的入站协议、端口和终结点之外，网络上的计算机还需要能够访问 [Office 365 URL 和 IP 地址范围](#) 中列出的 IP 地址和端口和 URL。

传输协议	较高级别的协议	功能/组件	本地终结点	本地路径	身份验证提供程序	授权方法	是否支持预身份验证？
TCP 25 (SMTP)	SMTP/TLS	Office 365 和本地之间的邮件流	Exchange 2019/2016 邮箱/边缘 Exchange 2013 CAS/EDGE Exchange 2010 HUB/EDGE	不适用	不适用	基于证书	否
TCP 443 (HTTPS)	自动发现	自动发现	Exchange 2019/2016 邮箱 Exchange 2013/2010 CAS	/autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc	Azure AD 身份验证系统	WS-Security 身份验证	否
TCP 443 (HTTPS)	EWS	忙/闲、邮件提示、邮件跟踪	Exchange 2019/2016 邮箱 Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity	Azure AD 身份验证系统	WS-Security 身份验证	否

传输协议	较高级别的协议	功能/组件	本地终结点	本地路径	身份验证提供程序	授权方法	是否支持预身份验证？
TCP 443 (HTTPS)	EWS	多邮箱搜索	Exchange 2019/2016 邮箱 Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc	身份验证服务器	WS-Security 身份验证	否
TCP 443 (HTTPS)	EWS	邮箱迁移	Exchange 2019/2016 邮箱 Exchange 2013/2010 CAS	/ews/mrsproxy.svc	NTLM	Basic	是
TCP 443 (HTTPS)	自动发现 EWS	OAuth	Exchange 2019/2016 邮箱 Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc	身份验证服务器	WS-Security 身份验证	否
TCP 443 (HTTPS)	不适用	AD FS(包括在 Windows 中)	Windows 2012 R2/2016 服务器	/adfs/*	Azure AD 身份验证系统	根据配置而异。	双重
TCP 443 (HTTPS)	不适用	Azure Active Directory Connect 和 AD FS	Windows 2012 R2/2016 服务器	/adfs/*	Azure AD 身份验证系统	根据配置而异。	双重

推荐的工具和服务

除了前面介绍的必备先决条件外，在使用“混合配置”向导配置混合部署时，还可使用一些其他的工具和服务：

- **Exchange Server 部署助理**: Exchange Server 部署助理是一个免费的基于 web 的工具，可帮助您在内部部署组织中部署 Exchange，在您的内部部署组织和 Office 365 之间配置混合部署，或完全迁移到 Office 365。该工具会询问您一组简单的问题，并根据您的回答创建一个自定义检查表，其中包含部署或配置 Exchange Server 的说明。部署助理可以准确提供您配置混合部署所需要的信息。

有关详细信息，请参阅[Microsoft Exchange Server 部署助理](#)。

- **远程连接分析器工具**: Microsoft 远程连接分析器工具可检查本地 Exchange 组织的外部连接，并确保您已

准备好配置混合部署。强烈建议在使用“混合配置”向导配置混合部署之前，使用远程连接分析工具检查内部部署组织。

可在以下位置了解详细信息：[Microsoft Remote Connectivity Analyzer](#)。

- **单一登录：**单一登录使用户可以使用一个用户名和密码访问内部部署组织和 Exchange Online 组织。它向用户提供了一种熟悉的登录体验，并允许管理员使用内部部署 Active Directory 管理工具轻松控制 Exchange Online 组织邮箱的帐户策略。

部署单一登录时有多个选项：密码同步和 Active Directory 联合身份验证服务。这两个选项均由 Azure Active Directory Connect 提供。密码同步使几乎任何组织（不论大小）都能轻松实现单一登录。由于这个原因，并且由于混合部署中的用户体验在启用单一登录后会得到极大的改善，因此我们强烈建议您实现单一登录。对于超大型组织，例如具有多个需要加入混合部署的 Active Directory 林的组织，需要 Active Directory 联合身份验证服务。

有关详细信息，请参阅[混合部署中的单一登录](#)。

混合部署的证书要求

2019/6/5 •

在混合部署中，数字证书是保护内部部署 Exchange 组织和 Office 365 之间通信的重要部分。证书允许每个 Exchange 组织信任另一个组织的身份。证书还有助于确保每个 Exchange 组织与正确的源通信。

在混合部署中，许多服务都使用证书：

- **Azure Active Directory Connect (AZURE AD connect) 与 Active Directory 联合身份验证服务 (AD FS)**: 如果你选择在混合部署中部署 Azure ad CONNECT 与 AD FS, 则由受信任的第三方证书颁发机构颁发的证书。(CA) 用于在 web 客户端和联合服务器代理之间建立信任, 以对安全令牌进行签名以及解密安全令牌。

有关更多信息，请参阅[证书](#)。

- **Exchange 联合身份验证**: 自签名证书用于在内部部署 Exchange 服务器和 Azure Active Directory 身份验证系统之间创建安全连接。

有关详细信息，请参阅 [Understanding Federated Delegation](#)。

- **Exchange 服务**: 受信任的第三方 CA 颁发的证书用于帮助保护 Exchange 服务器和客户端之间的安全套接字层 (SSL) 通信。使用证书的服务包括 Web 上的 Outlook、Exchange ActiveSync、Outlook Anywhere 和安全邮件传输。

- **现有的 exchange 服务器**: 现有的 exchange 服务器可能使用证书, 以帮助保护 Outlook 在 web 通信、邮件传输等方面的安全。根据在 Exchange 服务器上使用证书的方式，可以使用自签名证书或受信任第三方 CA 颁发的证书。

混合部署的证书要求

当配置混合部署时，您必须使用和配置从受信任的第三方 CA 购买的证书。必须在所有内部部署邮箱 (Exchange 2016 及更高版本)、邮箱和客户端访问 (Exchange 2013 及之前版本) 服务器上安装用于混合安全邮件传输的证书。

IMPORTANT

如果在多个 Active Directory 林中部署了 Exchange 服务器的组织中配置混合部署，必须对每个 Active Directory 林使用单独的第三方 CA 证书。

当在本地组织中部署 Exchange 边缘传输服务器时，此证书还必须安装在所有边缘传输服务器上。每个传输服务器必须使用共享相同颁发 CA 和相同主题的证书，以便混合安全邮件正常运行。

多种服务，如 AD FS、Exchange 联合身份验证、服务和 Exchange，各自都需要证书。根据组织，可以决定执行以下操作之一：

- 跨多个服务器使用由所有服务使用的第三方证书。
- 对提供服务的每部服务器使用第三方证书。

是选择对所有服务使用相同证书还是对每种服务使用专用证书，取决于您的组织和要实现的服务。下面是针对每个选项需要考虑的一些事项：

- **跨多个服务器的第三方证书**: 在多个服务器之间的服务使用的第三方证书可能会略有不同，但它们可能会使续订和替换变得复杂。出现这种复杂性是因为：当证书需要替换时，您需要在安装证书的每部服务器上

都替换证书。

- **每个服务器的第三方证书:** 对承载服务的每台服务器使用专用证书, 可以为该服务器上的服务专门配置证书。如果需要替换证书或续订证书, 则只需在安装服务的服务器上进行替换。其他服务器不会受到影响。

建议您对任何可选 AD FS 服务器使用专用第三方证书, 对混合部署的 Exchange 服务使用另一个证书, 并对其他所需服务或功能的 Exchange 服务器使用另一个证书(如果需要)。默认情况下, 在混合部署联合共享中配置的内部部署联合信任使用自签名证书。除非您有特定要求, 否则无需对混合部署中配置的联合身份验证信任使用第三方证书。

安装在单个服务器上的服务可能需要您为该服务器配置多个完全限定域名 (FQDN)。应该购买允许使用最大所需 FQDN 数目的证书。证书包含主题(也称为主体名称)以及一个或多个主题备用名称 (SAN)。主题名称是向其颁发证书的 FQDN, 并应该使用在内部部署与 Exchange Online 组织之间共享的主 SMTP 域。SAN 是除了主题名称之外, 可以添加到证书的其他 FQDN。如果需要证书支持五个 FQDN, 请购买允许向证书添加五个域的证书: 一个主题名称和四个 SAN。

下表概括了在混合部署中使用的配置证书应包括的最小建议 FQDN。

服务	建议的 FQDN	字段
主要共享 SMTP 域	contoso.com	使用者名称
自动发现	与 Exchange 2013 客户端访问服务器的外部自动发现 FQDN 相匹配的标签, 如 autodiscover.contoso.com	使用者替代名称
传输	与边缘传输服务器的外部 FQDN 匹配的标签, 如 edge.contoso.com	使用者替代名称

Exchange 混合部署的传输选项

2019/6/5 •

在混合部署中，可以具有既驻留在本地 Exchange 组织中也驻留在 Exchange Online 组织中的邮箱。为了使这两个单独组织对用户及在他们之间交换的邮件表现为一个合并的组织，关键组件是混合传输。通过混合传输，在任一组织中的收件人之间发送的邮件会经过身份验证、加密并使用传输层安全性 (TLS) 传输。这些邮件向 Exchange 组件（如传输规则、日记和反垃圾邮件策略）显示为“内部”。混合传输由混合配置向导自动配置。

为了在混合配置向导中使用混合传输配置，接受来自 Exchange Online 的连接的本地的 SMTP 终结点必须是邮箱服务器 (Exchange 2016 及更高版本)、客户端访问服务器 (Exchange 2013)、集线器传输服务器 (Exchange 2010 及之前版本) 或边缘传输服务器 (Exchange 2010 及更高版本)。

IMPORTANT

不要在处理或修改 SMTP 通信的内部部署 Exchange 服务器和 Office 365 之间放置任何服务器、服务或设备。内部部署 Exchange 组织和 Office 365 之间的安全邮件流取决于组织之间发送的邮件中包含的信息。支持允许 TCP 端口 25 上的 SMTP 通信通过而无需修改的防火墙。如果服务器、服务或设备处理内部部署 Exchange 组织和 Office 365 之间发送的邮件，此信息将被删除。如果发生这种情况，该邮件将不再被视为组织内部邮件，并且将会对其应用反垃圾邮件筛选、传输和日记规则以及可能不适用于它的其他策略。

从外部 Internet 发件人发送到两个组织中的收件人的入站邮件会采用通用入站路由。从组织发送到外部 Internet 收件人的出站邮件可以采用通用出站路由，也可以通过独立的路由发送。

在计划和配置混合部署时需要选择如何路由入站和出站邮件。发送到和发送自内部部署和 Exchange Online 组织中收件人的入站和出站邮件采用的路由取决于以下因素：

- 您是否希望通过 Exchange Online 组织或通过本地组织路由本地邮箱和 Exchange Online 邮箱的入站 Internet 邮件？

这两个组织采用的入站邮件路由取决于多种因素，例如大部分邮箱位于何处，是否想要保护您使用 Office 365 反恶意软件和反垃圾邮件扫描的本地组织，您的合规性基础结构的配置位置等等。

- 是要通过内部部署组织（集中邮件传输）路由来自 Exchange Online 组织的出站邮件到外部收件人，还是要将其直接路由到 Internet？

使用集中邮件传输，可以先通过本地组织路由来自 Exchange Online 组织中邮箱的所有邮件，然后再将这些邮件传递到 Internet。此方法用于合规性方案，在这类方案中，发送到和发送自 Internet 的所有邮件都必须由本地服务器进行处理。或者，可以配置 Exchange Online 以将外部收件人的邮件直接传递到 Internet。

NOTE

仅对具有与合规性相关的特定传输需求的组织推荐使用集中式邮件传输。我们对典型的 Exchange 组织的建议是不启用集中式邮件传输，因为它可以极大地增加您的本地服务器处理的邮件数量、增加使用的带宽和在本地服务器上创建不必要的依赖项。

- 是否要在内部部署组织中部署边缘传输服务器？

如果您不想将加入域的内部 Exchange 服务器直接向 Internet 公开，则可在外围网络中部署边缘传输服务器。有关向混合部署添加边缘传输服务器的详细信息，请参阅[混合部署中的边缘传输服务器](#)。

无论如何路由发送到和发送自 Internet 的邮件，在内部部署与 Exchange Online 组织之间发送的所有邮件都使用安全传输进行发送。有关详细信息，请参阅本主题后面的[受信任通信](#)。

有关这些选项如何影响贵组织的邮件路由的详细信息，请参阅 [Exchange 混合部署中的传输路由](#)。

混合部署中的 Exchange Online Protection

EOP 是 Microsoft 提供的联机服务，由许多公司用于保护其内部部署组织免受病毒、垃圾邮件、欺诈邮件和策略违规的危害。在 Office 365 中，EOP 用于保护 Exchange Online 组织免受相同威胁的危害。在注册 Office 365 时，会自动创建与您的 Exchange Online 组织关联的 EOP 公司。

EOP 公司包含一些邮件传输设置，可以为 Exchange Online 组织配置这些设置。可以指定哪些 SMTP 域必须来自特定 IP 地址，需要 TLS 和安全套接字层 (SSL) 证书，可以绕过反垃圾邮件筛选或合规性策略，等等。EOP 是 Exchange Online 组织的前门。所有邮件（无论其来源如何）都必须先经过 EOP，然后才能到达 Exchange Online 组织中的邮箱。而且，从 Exchange Online 组织发送的所有邮件都必须先经过 EOP，然后才能到达 Internet。

在使用混合配置向导配置混合部署时，会在内部部署组织以及为 Exchange Online 组织设置的 EOP 公司中自动配置所有传输设置。混合配置向导会在此 EOP 公司中配置所有入站和出站连接器及其他设置，以保护在内部部署与 Exchange Online 组织之间发送的邮件并将邮件路由到正确目标。如果要为 Exchange Online 组织配置自定义传输设置，则也会在此 EOP 公司中配置这些设置。

受信任通信

为了帮助保护本地和 Exchange Online 组织中的收件人，并帮助确保不会截获和读取组织之间发送的邮件，本地组织与 EOP 之间的传输会配置为使用强制 TLS。安全邮件传输使用受信任第三方证书颁发机构 (CA) 提供的 TLS/SSL 证书。EOP 与 Exchange Online 组织之间的邮件也使用 TLS。

当使用强制 TLS 传输时，发送和接收服务器会检查在其他服务器上配置的证书。对证书配置的使用者名称或使用替代名称 (SAN) 之一，必须与管理员在其他服务器上显式指定的 FQDN 匹配。例如，如果 EOP 配置为接受并保护从 mail.contoso.com FQDN 发送的邮件，则发送内部部署客户端访问或边缘传输服务器必须具有在主题名称或 SAN 中包含 mail.contoso.com 的 SSL 证书。如果不满足此要求，则 EOP 会拒绝连接。

NOTE

使用的 FQDN 无需与收件人的电子邮件域名匹配。唯一要求在于证书主题名称或 SAN 中的 FQDN 必须与接收或发送服务器配置为接受的 FQDN 匹配。

除了使用 TLS 以外，还可将组织之间的邮件作为“内部”邮件处理。此方法使邮件可以绕过反垃圾邮件设置和其他服务。

有关 SSL 证书和域安全性的详细信息，请参阅 [混合部署的证书要求](#) 和 [了解 TLS 证书](#)。

Exchange 混合部署中的传输路由

2019/6/5 •

本主题讨论来自 Internet 的进站邮件和发送到 Internet 的出站邮件的路由选项。

IMPORTANT

不要在处理或修改 SMTP 通信的内部部署 Exchange 服务器和 Office 365 之间放置任何服务器、服务或设备。内部部署 Exchange 组织和 Office 365 之间的安全邮件流取决于组织之间发送的邮件中包含的信息。支持允许 TCP 端口 25 上的 SMTP 通信通过而无需修改的防火墙。如果服务器、服务或设备处理内部部署 Exchange 组织和 Office 365 之间发送的邮件，此信息将被删除。如果发生这种情况，该邮件将不再被视为组织内部邮件，并且将会对其应用反垃圾邮件筛选、传输和日记规则以及可能不适用于它的其他策略。

NOTE

本主题中的示例不包括向混合部署添加边缘传输服务器。邮件在内部部署组织、Exchange Online 组织与 Internet 之间采用的路由不会随着添加边缘传输服务器而更改。只有内部部署组织中的路由会更改。有关向混合部署添加边缘传输服务器的详细信息，请参阅[混合部署中的边缘传输服务器](#)。

来自 Internet 的进站邮件

作为计划和配置混合部署的一部分，需要决定是否想要通过 Exchange Online 或本地组织路由来自 Internet 发件人的所有邮件。所有来自 Internet 发件人的邮件最初会传递到所选的组织，然后根据收件人邮箱所在的位置路由。是否选择通过 Exchange Online 或本地组织路由邮件取决于各种因素，包括是否想要对发送到两种组织的所有邮件应用合规性策略以及每个组织中的邮箱数等。

本地和 Exchange Online 组织中发送到收件人的路径取决于在混合部署中决定如何配置 MX 记录。首选方法是配置 MX 记录，使其指向 Office 365 中的 Exchange Online Protection (EOP)，因为该配置提供最准确的垃圾邮件筛选。混合邮件配置向导不配置本地或 Exchange Online 组织的进站 Internet 邮件的路由。如果想要更改进站 Internet 邮件传递的方式，则必须手动配置 MX 记录。

- 如果您将 MX 记录更改为指向 Office 365 中的 Exchange Online Protection 服务：这是混合部署的推荐配置。所有发送到任一组织中的任何收件人的邮件都将首先通过 Exchange Online 组织路由。发往位于本地组织中的收件人的邮件会首先通过 Exchange Online 组织路由，随后传递到本地组织中的收件人。如果您的 Exchange Online 组织中的收件人数量比本地组织中的多，则推荐该路由。Exchange Online Protection 需要该配置选项，以提供对垃圾邮件的扫描和阻止。
- 如果您决定将 MX 记录保留为您的内部部署组织：则所有发送到任一组织中的任何收件人的邮件都将首先通过您的内部部署组织进行路由。发往位于 Exchange Online 中的收件人的邮件会首先通过本地组织进行路由，随后传递到 Exchange Online 中的收件人。对于具有合规性策略（该策略要求日记解决方案检查发送到和发送至组织的邮件）的组织，此路由可能很有帮助。如果选取了该选项，则 Exchange Online Protection 将不能有效地扫描垃圾邮件。

有关详细信息，请参阅 [Mail flow best practices for Exchange Online and Office 365 \(Overview\)](#)。

阅读下面与您计划将从 Internet 收件人发送的邮件路由到内部部署和 Exchange Online 收件人的方式相匹配的章节。在每个部分中，“内部部署 Exchange 服务器”可以是 Exchange 2013 客户端访问服务器，也可以是 Exchange 2016 邮箱服务器。

通过 Exchange Online 组织路由入站 Internet 邮件

以下步骤和图表举例说明了在指向 MX 记录到 Office 365 组织中的 EOP 服务的情况下，混合部署中出现的入站邮件路径。邮件路径因是否选择启用集中邮件传输而异。

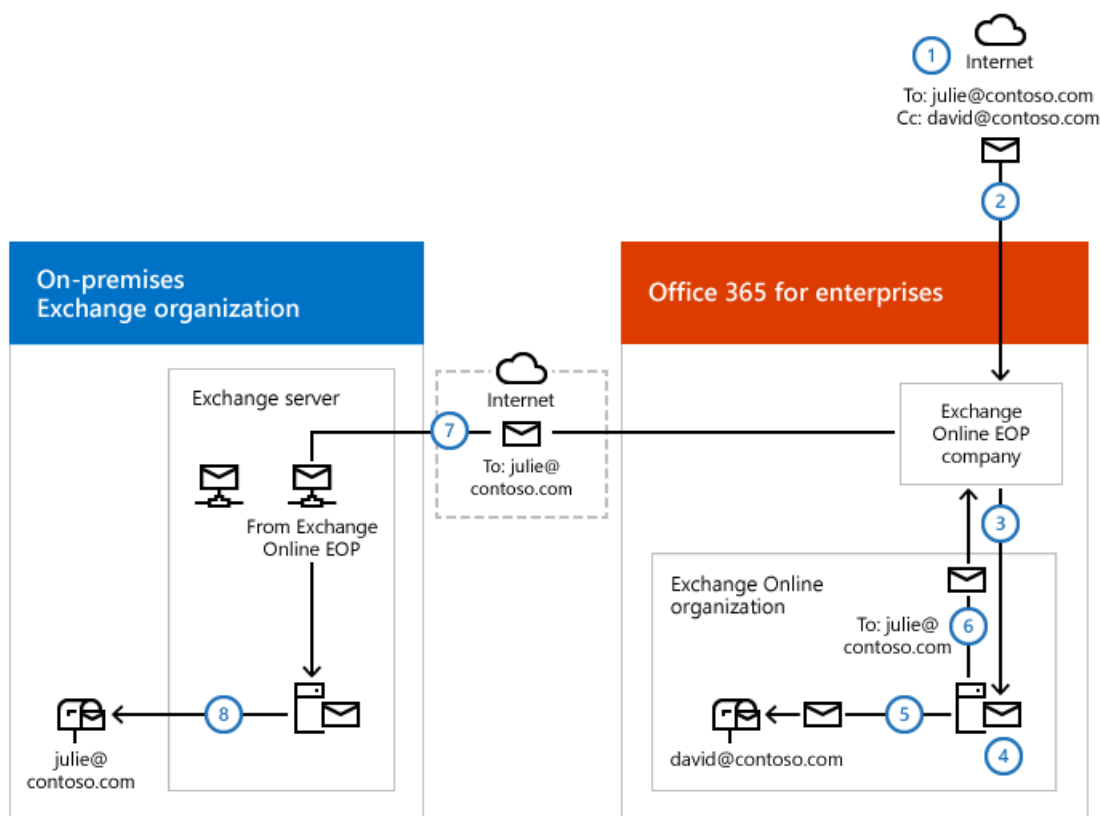
IMPORTANT

对于接收首先传递到 EOP 然后通过 Exchange Online 组织进行路由的邮件的每个内部部署邮箱，可能需要购买 EOP 许可证。有关详细信息，请与您的 Microsoft 经销商联系。

当集中邮件传输被 **禁用**（默认配置）时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 julie@contoso.com 和 david@contoso.com。Julie 的邮箱位于内部部署组织中的 Exchange 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 contoso.com 电子邮件地址，并且 contoso.com 的 MX 记录指向 EOP，所以邮件会传递到 EOP。
3. EOP 将两个收件人的邮件都路由到 Exchange Online。
4. Exchange Online 对邮件进行病毒扫描并对每个收件人执行查找。通过查找，确定 Julie 的邮箱位于内部部署组织中，而 David 的邮箱位于 Exchange Online 组织中。
5. Exchange Online 将邮件拆分为两个副本。将邮件的一个副本传递到 David 的邮箱。
6. 将第二个副本从 Exchange Online 发送回 EOP。
7. EOP 发送邮件到内部部署组织中的内部部署 Exchange 服务器。
8. Exchange 将发送邮件到 Exchange 邮箱服务器，该服务器会将其传递到 Julie 的邮箱。

通过 **Exchange Online** 组织为内部部署组织和 **Exchange Online** 组织路由邮件，同时禁用集中邮件传输（默认配置）

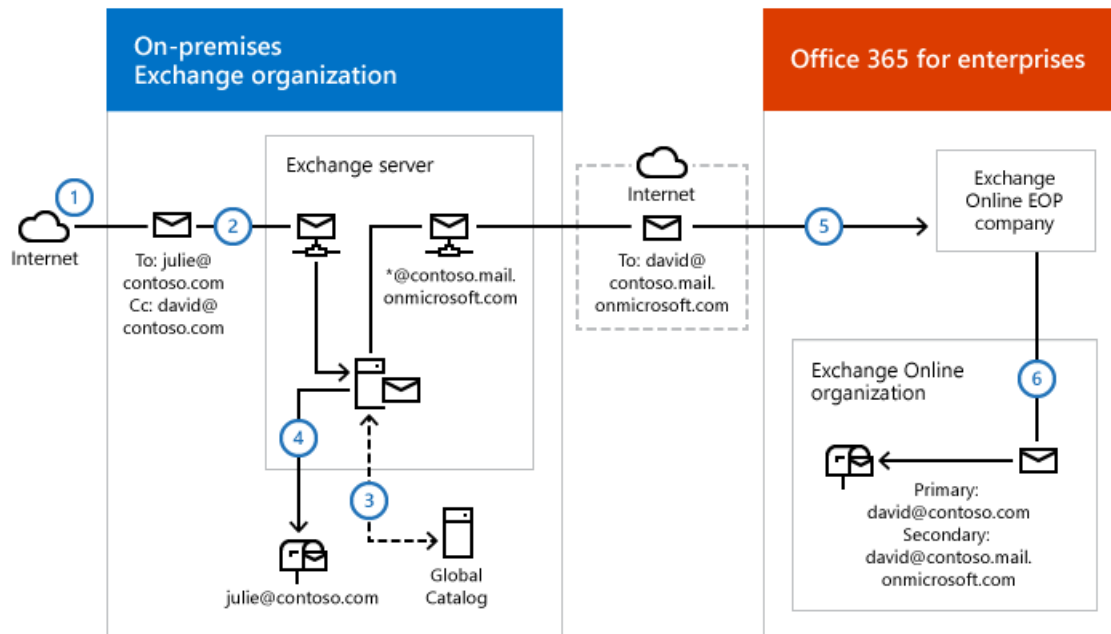


当集中邮件传输被 **启用** 时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 julie@contoso.com 和 david@contoso.com。Julie 的邮箱位于内

4. 内部部署 Exchange 服务器将邮件拆分为两个副本。邮件的一个副本会发送给内部部署 Exchange 邮箱服务器, 在该服务器中它会传递给 Julie 的邮箱。
5. 邮件的第二个副本被内部部署 Exchange 服务器发送到 EOP, 这将使用配置为使用 TLS 的发送连接器接收发送到 Exchange Online 组织的邮件。
6. EOP 将邮件发送到 Exchange Online 组织, 在该组织中对邮件进行病毒扫描并将其传递到 David 的邮箱。

通过内部部署组织为内部部署组织和 Exchange Online 组织路由邮件



发送到 Internet 的出站邮件

除了选择如何对发送给组织中的收件人的进站邮件进行路由之外, 还可以选择如何对从 Exchange Online 收件人发送的出站邮件进行路由。运行“混合配置”向导时, 可以选择两个选项之一:

- **不启用集中邮件传输:** 默认情况下, 在“混合配置”向导中选择此选项可将从 Exchange Online 组织发送的出站邮件直接路由到 Internet。如果无需将任何内部部署合规性策略或其他处理规则应用于从 Exchange Online 组织中的收件人发送的邮件, 请使用此选项。
- **启用集中邮件传输:** 选择此选项可通过内部部署组织路由从 Exchange Online 组织发送的出站邮件。除了向同一个 Exchange Online 组织中的其他收件人发送的邮件之外, 从 Exchange Online 组织中的收件人发送的所有邮件都会通过内部部署组织发送。这使您可以将合规性规则应用于这些邮件以及必须应用于所有收件人(无论这些收件人是处于 Exchange Online 组织中还是处于内部部署组织中)的任何其他过程或要求。

NOTE

仅对具有与符合性相关的特定传输需求的组织推荐使用集中式邮件传输。我们建议典型的 Exchange 组织不要启用集中式邮件传输。

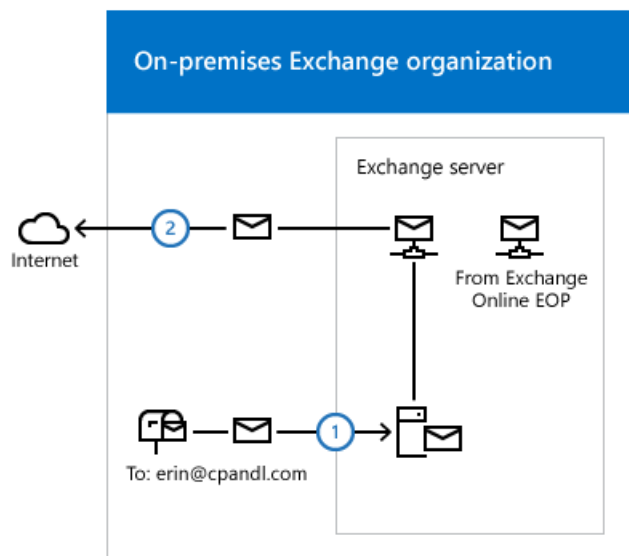
从内部部署收件人发送的邮件会始终使用 DNS 直接发送到 Internet 收件人(无论在“混合配置”向导中选择了以上哪个选项)。

以下步骤和图表说明从内部部署收件人发送的邮件的出站邮件路径。

1. 在内部部署 Exchange 邮箱服务器上拥有一个邮箱的 Julie 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange 服务器会在 MX 记录中查找 cpandl.com, 并将邮件发送给位于 Internet 上的 cpandl.com 邮件服

务器。

从内部部署发件人发送给 Internet 收件人的邮件



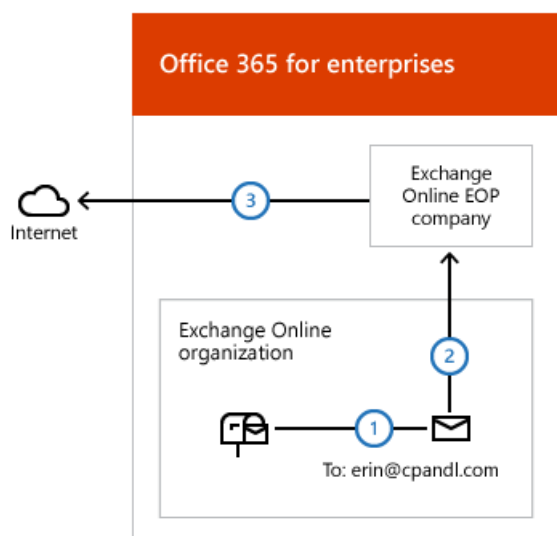
阅读下面与您计划将从 Exchange Online 组织中收件人发送的邮件路由到 Internet 收件人的方式相匹配的章节。

使用 DNS (集中式邮件传输已禁用) 传递来自 Exchange Online 的 Internet 邮件。

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 Exchange Online EOP 公司。
3. EOP 会在 MX 记录中查找 cpandl.com, 并将邮件发送给位于 Internet 上的 cpandl.com 邮件服务器。

来自 Exchange Online 发件人的邮件将直接路由到 Internet, 同时禁用集中邮件传输 (默认配置)

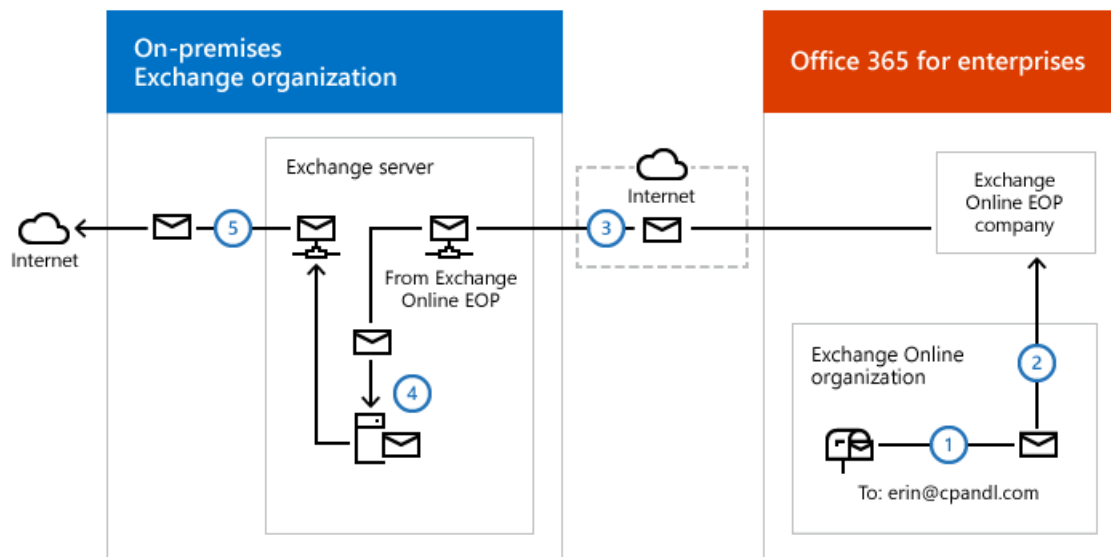


通过内部部署组织 (启用集中邮件传输) 路由从 Exchange Online 发送到 Internet 的邮件

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 EOP。
3. EOP 配置为将所有 Internet 出站邮件发送给内部部署服务器，因此邮件会路由到内部部署 Exchange 服务器。邮件使用 TLS 发送。
4. 内部部署 Exchange 服务器对 David 的邮件执行遵从性、防病毒以及管理员配置的任何其他过程。
5. 内部部署 Exchange 服务器会在 MX 记录中查找 cpandl.com，并将邮件发送给位于 Internet 上的 cpandl.com 邮件服务器。

通过内部部署组织路由的来自 Exchange Online 发件人的邮件(启用集中邮件传输)



Exchange 混合部署中的混合管理

2019/6/5 •

安装 Exchange 服务器时，会自动在该服务器上安装 Exchange 管理工具。您将使用以下工具来配置和管理本地 Exchange 和 Exchange Online 组织：

- **Exchange 管理中心**: EAC 是一种基于 web 的管理控制台，可简化使用，并针对内部部署、在线或混合 Exchange 部署进行了优化。EAC 替换了 Exchange 管理控制台 (EMC) 和 Exchange 控制面板 (ECP)，它们是用于管理 Exchange Server 2010 的界面。
- **Exchange 命令行管理程序**: exchange 命令行管理程序是基于 Windows PowerShell 的命令行界面。

Exchange 管理中心

EAC 允许您同时在本地的 Exchange 服务器和 Exchange Online 组织上执行许多部署任务和最常见的日常管理任务。默认情况下，它将在每个 Exchange 2013 或更高版本的服务器上安装。此外，由于它是基于 Web 的管理控制台，您还可以使用网络中的其他计算机的 Web 浏览器或通过使用 ECP 虚拟目录 URL 访问它。

您可以通过选择 Office 365 跨界导航选项卡来访问 EAC 中的 Exchange Online 组织。跨界导航允许您在 Exchange Online 和内部部署 Exchange 组织之间轻松切换。如果您已经配置混合部署，选择 Office 365 选项卡将允许您管理 Exchange Online 组织和收件人对象。如果您没有 Exchange Online 组织，选择 Office 365 链接会将您转到 Office 365 注册页面。

有关 EAC 的详细信息，请参阅 [Exchange Administration Center](#)。

Exchange 命令行管理程序

Exchange 命令行管理程序可以执行 EAC 执行的任何任务，以及只能在 Exchange 命令行管理程序中执行的某些其他任务。Exchange 命令行管理程序是安装 Exchange 管理工具时安装在计算机上的 Windows PowerShell 脚本和 cmdlet 的集合。只有在使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，才会加载这些脚本和 cmdlet。如果你直接打开 Windows PowerShell，则不会加载 Exchange 脚本和 cmdlet，并且你将无法管理内部部署组织。

NOTE

你可以创建到本地内部部署组织的手动 Windows PowerShell 连接，方式与手动连接到以下 Exchange Online 组织类似。但是，强烈建议你使用 Exchange 命令行管理程序图标来打开 Exchange 命令行管理程序，以管理内部部署 Exchange 服务器。

当你在安装了管理工具的计算机上使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，可以管理内部部署组织。但是，在使用此图标打开 Exchange 命令行管理程序时不能管理 Exchange Online 组织。这是因为使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序会自动连接到本地 Exchange 服务器。

如果要使用 Windows PowerShell 管理 Exchange Online 组织，必须直接打开 Windows PowerShell，而不要通过 Exchange 命令行管理程序图标打开。打开 Windows PowerShell 后，你便可以手动指定要连接的位置。当你创建手动连接时，可在 Office 365 租户组织中指定一个管理员帐户，然后运行命令以创建连接。建立该连接后，你即可使用有权运行的 Exchange cmdlet。有关更多信息，请参阅[使用 Windows PowerShell](#)。

如果你不熟悉 Exchange 命令行管理程序，请查看 [Exchange Management Shell](#)，以了解有关 Exchange 命令行管理程序的工作方式的基本信息、命令语法及更多内容。

Exchange 混合部署中共享的忙/闲信息

2019/6/5 •

在位于内部部署和 Exchange Online 组织中的用户之间共享忙/闲(日历可用性)信息是混合部署的主要好处之一。两种组织中的用户都可以查看彼此的日历,就如同这些用户位于同一个物理组织中一样。如此便可以方便且高效地进行会议和资源调度。

需要混合部署中的几个组件在本地 Exchange 组织和 Exchange Online 组织之间启用共享忙/闲功能。

- **联合身份验证信任:** 内部部署和 Office 365 服务组织都需要与 Azure AD 身份验证系统建立联合身份验证信任。联合身份验证信任是与 Azure AD 身份验证系统的一对一关系,该关系会定义 Exchange 组织的参数。该系统在充当本地组织与 Office 365 服务组织之间的信任代理时,使用这些参数在本地组织用户与 Exchange Online 组织用户之间交换忙/闲信息。

在创建帐户时,将自动为 Office 365 服务组织配置与该系统的联合信任。混合配置向导会自动查看对于本地组织,是否存在与 Azure AD 身份验证系统之间的现有联合身份验证信任。如果存在,则现有联合身份验证信任将用于支持混合部署。如果不存在,则向导会为本地组织创建与 Azure AD 身份验证系统之间的联合身份验证信任。该向导还会将在"混合配置"向导中选择的所有域都添加到本地组织联合身份验证信任中。

有关详细信息,请参阅 [Understanding Federated Sharing](#)。

- **组织关系:** 内部部署组织和 Exchange Online 组织都需要组织关系,并且由"混合配置"向导自动配置。组织关系将定义组织共享的忙/闲信息级别。

默认情况下,"闲/忙"数据访问共享级别是"闲/忙"访问共享级别,同时包含本地和 Exchange Online 组织关系的主题和位置。如果需要修改内部部署组织用户与 Exchange Online 组织用户之间的忙/闲共享访问,可以在完成"混合配置"向导后手动配置组织关系访问级别。

有关详细信息,请参阅 [Understanding Federated Sharing](#)。

为组织部署混合部署时,在所有情况下,"混合配置"向导都会自动配置共享忙/闲日历访问。混合部署要求创建与 Azure AD 身份验证系统的联合身份验证信任,并为本地组织和 Exchange Online 组织配置组织关系。如果不希望内部部署组织用户与 Exchange Online 组织用户在混合部署中共享忙/闲信息,则可手动禁用忙/闲共享,方法是:在完成"混合配置"向导后使用 Exchange 命令行管理程序和 [Set-HybridConfiguration](#) cmdlet。

下表中显示的混合部署功能依赖于联合身份验证信任和组织关系。

邮件传递区域	功能
电子邮件客户端	邮件跟踪 邮件提示 多邮箱搜索
合规性	Exchange 联机存档 Exchange 就地电子数据展示

Exchange 混合部署中的服务器角色

2019/6/5 •

您可以配置基于 Exchange 2013 和 Exchange 2016 的混合部署。支持混合部署需要配置的角色取决于您使用的 Exchange 版本。

Exchange 2016 混合部署

在 Exchange 2016 组织中配置混合部署时，无需在现有 Exchange 组织中安装任何额外的 Exchange 服务器。您的邮箱服务器将协调现有 Exchange 2016 组织和 Exchange Online 组织之间的通信。此通信包括本地组织与 Exchange Online 组织之间的邮件传输和消息功能。我们强烈建议在本地组织中安装多个 Exchange 服务器，以帮助提高混合部署功能的可靠性和可用性。

Exchange 2016 只有一个必需的服务器角色 - 邮箱角色。除了托管本地收件人邮箱，邮箱角色还执行所有使用 Exchange Online 支持混合部署所必需的功能。这包括处理本地组织和 Exchange Online 组织之间的安全邮件以及处理传输规则、日志记录策略和向用户的混合部署邮箱中执行的邮件传递操作。所有客户端连接和组织的关系功能（如忙/闲共享）也由邮箱服务器处理。

了解有关 [Exchange 2016 部署的大小调整](#) 的 Exchange 2016 容量规划的详细信息。

Exchange 2013 混合部署

在 Exchange 2013 组织中配置混合部署时，无需在现有 Exchange 组织中安装任何额外的 Exchange 服务器。您的客户端访问和邮箱服务器将协调现有 Exchange 2013 组织和 Exchange Online 组织之间的通信。此通信包括内部部署组织与 Exchange Online 组织之间的邮件传输和消息功能。我们强烈建议在内部部署组织中安装多个 Exchange 服务器，以帮助提高混合部署功能的可靠性和可用性。

下面是混合部署中的 Exchange 2013 服务器角色的快速概述：

- **客户端访问服务器角色：**客户端访问服务器角色继续提供基本上与 Exchange 2013 组织中的客户端访问服务器提供的相同功能，此外，还提供了支持混合部署所需的一些附加功能。客户端访问服务器还处理在内部部署和 Exchange Online 组织之间发送的所有安全邮件消息，以及处理混合部署中的传输规则、日记策略和到用户邮箱的邮件传递。默认情况下，在客户端访问服务器上配置有专门的接收连接器以支持安全混合邮件传输。所有客户端连接（包括 Outlook 客户端访问、Outlook Web App 和 Outlook Anywhere）都通过客户端访问服务器角色进行。内部部署组织与 Exchange Online 组织之间的组织关系功能（如忙/闲共享）也由客户端访问服务器角色处理。

有关详细信息，请参阅 [Client Access Server](#)。

- **邮箱服务器角色：**邮箱服务器角色托管本地收件人邮箱，并通过代理通过内部部署客户端访问服务器与 Exchange Online 组织进行通信。默认情况下，在邮箱服务器角色上配置有专门的发送连接器以支持安全混合邮件传输。

有关详细信息，请参阅 [Mailbox Server](#)。

根据所需的混合部署配置，Exchange 2013 服务器需要安装一个或两个服务器角色：

- **单一 exchange server：**如果选择在内部部署组织中安装一台 Exchange 服务器，则需要在单台服务器上同时安装客户端访问和邮箱服务器角色。
- **多个 exchange 服务器：**如果选择在内部部署组织中安装多个 exchange 服务器，则可以在内部部署组织中的不同服务器上安装服务器角色。例如，可以安装一个安装了邮箱和客户端访问服务器角色的 Exchange 服务器，同时也再安装一个仅安装了客户端访问服务器角色的 Exchange 服务器。但是，最佳实践及推荐的服

务器配置是在内部部署组织中部署的 每个服务器上同时安装客户端访问和邮箱服务器。

有关 Exchange 2013 容量规则的详细信息, 请参阅[了解容量规划中的多个服务器角色配置](#)。

混合部署中的 Exchange 服务器功能

Exchange 服务器为混合部署中的内部部署组织提供了几个重要功能:

- **联合:** Exchange 服务器使您能够为内部部署组织创建与 Microsoft 联合网关的联合身份验证信任。Microsoft 联合网关是 Microsoft 提供的一项基于云的免费服务, 该服务可充当本地组织与 Office 365 组织之间的信任代理。联合身份验证是关于在本地组织与 Exchange Online 组织之间创建组织关系的要求。

有关详细信息, 请参阅[Understanding Federation](#)。

- **组织关系:** 通过具有客户端访问角色的 exchange 2013 服务器和具有邮箱角色的 Exchange 2016 服务器, 可以在内部部署组织和 exchange Online 组织之间创建组织关系关系。混合部署中的许多其他服务(包括日历/闲信息共享、邮件跟踪以及内部部署组织与 Exchange Online 组织之间的邮箱移动)需要组织关系。

有关详细信息, 请参阅 [Understanding Federated Sharing](#)。

- **邮件传输:** 具有客户端访问和邮箱服务器角色的 Exchange 服务器负责混合部署中的邮件传输。通过使用发送和接收连接器, 这些服务器可用作传入外部邮件的连接终结点, 并提供到 Internet 和 Exchange Online 组织的出站邮件传递。

有关详细信息, 请参阅[Exchange 混合部署中的传输选项](#)。

- **邮件传输安全性:** 具有客户端访问和邮箱服务器角色的 Exchange 服务器通过使用 Exchange 中的域安全功能, 帮助保护内部部署组织与 Exchange Online 组织之间的邮件通信安全。可以通过将相互传输层安全性身份验证和加密用于邮件通信, 来增强安全。

有关详细信息, 请参阅[了解域安全性](#)。

- **Outlook 网页版 (即 exchange 2013 中的 Outlook Web App):** 具有客户端访问角色的 exchange 2013 服务器和具有邮箱角色的 exchange 2016 服务器支持将单个 URL 终结点配置为与内部部署和 exchange 的外部连接联机邮箱。对于本地邮箱, Exchange 服务器被配置为 Web 上的 Outlook 请求。对于 Exchange Online 组织邮箱, Exchange 服务器被配置为自动显示到 Exchange Online 组织上的 Web 上的 Outlook 终结点的链接。

有关详细信息, 请参阅[web 上的 Outlook](#)。

Exchange 混合部署中的 IRM

2019/6/5 •

摘要: IRM 在 Exchange 混合环境中的工作方式, 以及如何配置 IRM 以在 Exchange Online 和内部部署 Exchange 服务器之间工作。

信息权限管理 (IRM) 通过对电子邮件和附件提供持久联机保护和脱机保护来帮助防止敏感信息泄露。内部部署组织中的 Exchange 以及 Office 365 企业版中的 Exchange Online 都支持 IRM。但是, 这两种实现之间有一些不同; 您必须在 Exchange Online 组织中配置 IRM, 然后该组织中的用户才能使用该功能。

IRM 将使用作为 Windows Server 2008 及更高版本的一个组件的 Active Directory Rights Management Services (AD RMS)。AD RMS 允许用户创建受权限保护的内容, 如电子邮件和附件, 并控制内容的使用方式以及分发对象。用户可以指定模板以确定内容的使用方式。例如, 用户可以指定不能将某封电子邮件转发给其他收件人, 或不能复制邮件中的信息。

进一步了解 Exchange 2010 中的 IRM: [Understanding Information Rights Management](#) (了解信息权限管理)。

在 [Information Rights Management](#) 进一步了解 Exchange 2013 和 Exchange 2016 中的 IRM。

有关 AD RMS 的详细信息, 请参阅 [Active Directory 权限管理服务](#)。

IRM 在 Exchange 内部部署和 Exchange Online 之中的差别

内部部署 Exchange 组织中提供的 IRM 功能可能不同于 Exchange Online 组织中提供的功能。下表汇总了在每个组织中可用的功能。(进一步了解这些功能: [Understanding Information Rights Management](#))

可用的 IRM 功能

功能	在 EXCHANGE 2007 及之前版本中可用	在 EXCHANGE 2010 中是否可用	在 EXCHANGE ONLINE 和 EXCHANGE 2013 及更高版本中可用
手动保护 Outlook 中的邮件	是	是	是
手动保护 Outlook Web App 中的邮件	否	可访问	是
查看 Outlook 中受 IRM 保护的邮件	是	是	是
查看 Outlook Web App 中受 IRM 保护的邮件	否	可访问	是
IRM 预许可代理	是	是	是
RMS 策略模板	否	可访问	是
传输解密	否	可访问	是
日记报告解密	否	可访问	是
Exchange 搜索和发现解密	否	可访问	是

功能	在 EXCHANGE 2007 及之前版本中可用	在 EXCHANGE 2010 中是否可用	在 EXCHANGE ONLINE 和 EXCHANGE 2013 及更高版本中可用
自动 Outlook 保护规则	否	否	可访问
自动传输保护规则	否	可访问	是

混合部署中的 IRM

Exchange 将使用安装有 Exchange 服务器的 Active Directory 林中的 AD RMS 服务器。对于内部部署 Exchange 服务器，使用内部部署 AD RMS 服务器。对于 Exchange Online 组织，使用在 Office 365 数据中心的维护的 AD RMS 服务器。每个 Exchange 组织使用的 AD RMS 配置独立于任何其他 AD RMS 部署。

AD RMS 配置不会在内部部署 Exchange 组织和 Exchange Online 组织之间自动进行复制，因而 IRM 配置也是如此。所定义的任何 AD RMS 模板不会自动复制到 Exchange Online 组织。如果希望相同的 AD RMS 模板在 Exchange Online 组织中可用，必须手动将模板从内部部署组织中导出，并将其应用于 Office 365 组织。请参阅本主题后面的[在混合部署中配置 IRM](#)。

用户体验

应用于用户的 IRM 配置取决于用户使用的客户端以及用户邮箱的位置。下表列出了用户可使用的 AD RMS 服务器。

Active AD RMS 服务器

客户端	内部部署邮箱	EXCHANGE ONLINE 邮箱
Outlook 桌面客户端	内部部署 AD RMS	内部部署 AD RMS
Web 上的 Outlook	内部部署 AD RMS	Exchange Online AD RMS
ActiveSync 设备	内部部署 AD RMS	Exchange Online AD RMS

根据在内部部署和基于 Exchange Online 组织中配置的 AD RMS 配置，使用 Outlook 2007 和 Web 上的 Outlook 的用户可能会看到不同的 AD RMS 模板。因此，我们强烈建议您对内部部署和 Exchange Online 组织应用相同的模板。

对于 Outlook 客户端用户，无论其邮箱是在内部部署组织中还是在 Exchange Online 组织中，其 IRM 体验应该没有任何差别。

其邮箱位于 Exchange 内部部署服务器上的 Web 上的 Outlook 用户在安装了用于 Internet Explorer 的权限管理外接程序后只能打开受权限保护的邮件，并且不能答复或新建受权限保护的邮件。

其邮箱位于 Exchange Online 中的 Web 上的 Outlook 用户无需任何附加软件便可打开受权限保护的邮件，并且可以答复和新建受权限保护的邮件。

服务器功能

内部部署 Exchange 服务器使用 AD RMS 预许可代理来解密受权限保护的邮件，这样用户不必提供凭据便可打开这些邮件。内部部署 Exchange 服务器将联系内部部署 AD RMS 服务器来核查使用策略和权限，并请求授权以解密邮件。

Exchange Online 组织还提供了几个与 IRM 相关的功能，这些功能使用了 Exchange Online AD RMS。通过这些功能(如日记报告解密)，Exchange 服务可对受权限保护的邮件内容进行额外的处理。例如，可以与原始受权限保护的邮件一起保存已解密的日记邮件内容，以便更有利于发现。此外，使用 Outlook 保护规则或传输规则，IRM 模板可以自动应用于邮件，以确保邮件符合组织在信息保护方面的策略。

在混合部署中配置 IRM

Exchange 中的 IRM 依赖于在 Exchange 服务器所在的 Active Directory 林中部署的 AD RMS。AD RMS 配置不会自动在内部部署组织和 Exchange Online 组织之间进行同步。您必须从内部部署 AD RMS 服务器手动导出已知是受信任发布域 (TPD) 的 AD RMS 配置, 并将该配置导入到 Exchange Online 组织中。TPD 包含 Exchange Online 组织使用 IRM 时所需要的 AD RMS 配置, 包括模板。

有关更多信息, 请参阅 [AD RMS 受信任发布域的注意事项](#)。

除了对 Exchange Online 组织应用内部部署 AD RMS 配置外, 您还必须确保内部部署网络之外的 Outlook 和 ActiveSync 客户端能够联系到 AD RMS 服务器。如果您希望这些客户端能够访问内部部署网络之外的受权限保护的邮件, 就必须做到这一点。

配置了内部部署网络并导出了 TPD 数据后, 您需要通过导入 TPD 数据并启用 IRM 来配置 Exchange Online 组织。

NOTE

每当修改内部部署 AD RMS 配置时, 都必须手动在 Exchange Online 组织中应用新配置。为此, 请从内部部署 AD RMS 服务器导出 TPD 数据, 并将其导入到 Exchange Online 组织中。

如何在 Exchange 混合部署中配置 IRM

如果在内部部署 Exchange 组织中使用 IRM, 并且希望 Exchange Online 用户也使用 IRM, 则需要执行以下操作:

1. 配置内部部署 Active Directory Rights Management Services (AD RMS) 服务器。
2. 在 Exchange Online 组织中启用 IRM。
3. 将导入的 AD RMS 模板分发给 Exchange Online 组织中的用户。

如何配置内部部署 AD RMS 服务器？

若要在混合部署中配置 IRM, 需要使用 Windows PowerShell 来访问内部部署 AD RMS 服务器。有关详细信息, 请参阅[使用 Windows PowerShell 管理 AD RMS](#)

执行以下操作, 从内部部署 AD RMS 服务器导出受信任的发布域 (TPD) 数据, 然后配置外部客户端对 AD RMS 服务器的访问。

1. 从内部部署组织导出 TPD 数据。有关详细信息, 请参阅[导出受信任的发布域](#)
2. 配置外部客户端对 AD RMS 服务器的访问。有关详细信息, 请参阅[添加 Extranet 群集 URL](#)

如何在 Exchange Online 组织中启用 IRM？

从内部部署 AD RMS 服务器导出 TPD 数据后, 需要将这些数据导入到 Exchange Online 组织中, 然后启用 IRM。

1. 在 Exchange Online 组织中, 导入 TPD 数据。

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Content -Encoding Byte -Path "<Path to exported TPD file>" -ReadCount 0))
```

2. 在 Exchange Online 组织中启用 IRM。

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

如何在 Exchange Online 组织中分发 AD RMS 模板？

在 Exchange Online 组织中启用了 IRM 之后, 必须分发导入的 AD RMS 模板。以下 Exchange Online 用户和功能

使用 AD RMS 模板：

- Web 上的 Outlook 用户
- Exchange ActiveSync 用户
- 传输规则
- 日记报告解密
- Outlook 保护规则

1. 在 Exchange Online 组织中，检索 AD RMS 模板的列表。

```
Get-RMSTemplate -Type All
```

2. 将 AD RMS 模板分发给 Exchange Online 组织中的用户和功能。

```
Set-RMSTemplate <template name> -Type Distributed
```

NOTE

无法修改“不要转发”AD RMS 模板。

3. 对要分发的每个 AD RMS 模板重复步骤 2。

我如何知道这有效？

Web 上的 Outlook 用户应能够将 AD RMS 模板应用于新邮件。Web 上的 Outlook 和 Exchange ActiveSync 用户应能够阅读应用了 AD RMS 模板的邮件。此外，运行 **Get-RMSTemplate** cmdlet 时，应列出从内部部署组织导入的所有 AD RMS 模板。

在 Exchange Online 组织中运行以下命令：

```
Get-RMSTemplate
```

可在以下位置了解详细信息：[Understanding Information Rights Management in Outlook Web App](#)

Exchange 混合部署中的权限

2019/6/5 •

Office 365 组织中的 Exchange Online 基于 Exchange Server, 与内部部署组织一样, 它还使用基于角色的访问控制 (RBAC) 来控制权限。使用管理角色组向管理员授予权限, 而使用管理角色分配策略向最终用户授予权限。

若要详细了解 Exchange Online 和本地 Exchange 中的权限, 请访问[权限](#)

管理员权限

默认情况下, 用于创建 Office 365 租户的用户成为 Exchange Online 组织中的 "组织管理" 角色组的成员。此用户可以管理整个 Exchange Online 组织, 包括组织级别设置的配置和 Exchange Online 收件人的管理。

您可以在 Exchange Online 组织中添加其他管理员, 具体取决于需要进行的管理。例如, 可以添加其他组织管理员和收件人管理员、使专家用户可以执行合规性任务 (如发现)、配置自定义权限等。必须使用 Exchange 管理中心 (EAC) 或远程 PowerShell 在 Exchange Online 组织中执行所有 Office 365 管理员的 Exchange Online 权限管理。

IMPORTANT

在内部部署组织与 Office 365 组织之间不会进行任何权限传输。在内部部署组织中定义的权限都必须在 Office 365 组织中重新创建。

有关详细信息, 请参阅[Manage Role Groups](#)和[Manage Role Group Members](#)。

委派邮箱权限

在本地 Exchange 部署中, 可以向用户授予对其他用户的邮箱的各种权限。这称为委派邮箱权限, 在管理助理需要管理其他用户的邮箱的某些部分时非常有用; 例如, 管理总经理的日历。Exchange 混合部署支持使用内部部署 Exchange 组织中的邮箱和位于 Office 365 中的邮箱之间的某些 (而非全部) 邮箱权限。以下各节详细介绍了受支持的和不受支持的权限。支持混合邮箱权限所需的其他配置; 以及如何在您的内部部署组织和 Office 365 之间同步邮箱权限。

混合环境中支持的邮箱权限

支持以下权限****:

- **完全访问:** 可以向本地 Exchange 服务器上的邮箱授予对 Office 365 邮箱的完全访问权限, 反之亦然。例如, 可以向 Office 365 邮箱授予对内部部署共享邮箱的 "完全访问"**** 权限。用户需要使用 Outlook 桌面客户端打开邮箱。Web 上的 Outlook 不完全支持跨界邮箱权限。用户可以使用在 web 上的 Outlook 中打开另一个邮箱, 以打开其他邮箱, 在该邮箱中有完全访问权限。但是, 这将在用户可以访问邮箱之前生成重定向链接和凭据提示。

NOTE

当用户第一次访问其他组织中的邮箱并将其添加到其 Outlook 配置文件时, 他们可能会收到额外的凭据提示。

- **代表发送:** 本地 Exchange 服务器上的邮箱可被授予对 Office 365 邮箱的 "代表发送" 权限, 反之亦然。例如, 可以向 Office 365 邮箱授予对本地共享邮箱的 "代表发送" 权限。用户需要使用 Outlook 桌面客户端打开邮箱; web 上的 Outlook 不支持跨界邮箱权限。

您的 Azure Active Directory Connect server 需要进行一些更改, 以便在本地 Exchange 服务器和 Exchange Online 之间同步的 "代表发送" 权限。有关详细信息, 请参阅本主题后面的在[Azure Active Directory](#)

Connect 中启用对混合邮箱权限的支持一节。

- **私人项目**: 当您授予对邮箱的完全访问权限时, 您可以决定是否允许代理查看邮箱中的私人项目 (私人会议、约会、联系人或任务)。

不支持以下权限或功能:

- **"代理发送"**: 允许用户像好像来自其他用户的邮箱一样发送邮件。"代理发送" 权限不会自动通过内部部署和 Office 365 之间的 Azure Ad Connect 进行同步。这就是为什么在这种情况下, 不支持跨界发送权限。但是, 如果在两个环境中手动添加 "代理发送" 权限, 则在大多数情况下都可以使用 "代理发送" 权限。

例如, 您想要向名为 ONPREM1 的本地邮箱授予对名为 EXO1 的云邮箱的 "代理发送" 权限。

首先在本地服务器上运行以下命令-

```
Add-adpermission-Identity EXO1-User ONPREM1-AccessRights ExtendedRight-ExtendedRights "Send As"
```

然后, 从 Exchange Online PowerShell 运行相应的命令-

```
Add-recipientpermission-Identity "EXO1"-受信者 ONPREM1-AccessRights SendAs
```

- **自动映射**: 使 Outlook 能够在启动时自动打开用户已被授予完全访问权限的任何邮箱。
- **文件夹权限**: 授予对特定文件夹内容的访问权限。

从另一个邮箱接收这些权限的所有邮箱都需要与授予邮箱的时间同时移动。如果邮箱从多个邮箱接收权限, 该邮箱以及向其授予权限的所有邮箱需同时移动。有关详细信息, <https://support.microsoft.com/en-us/help/3064053> 可参阅。

配置内部部署 Exchange 服务器以支持混合邮箱权限

若要在混合部署中启用 "完全访问" 和 "代表发送" 权限, 则可能需要进行其他配置更改, 具体取决于已安装的 Exchange 版本。下表显示了哪些版本的 Exchange 支持在混合部署中使用 Office 365 委派邮箱权限以及所需的其他配置。有关如何配置 Exchange 2013 和 2010 服务器和邮箱以支持 Acl 的步骤, 请参阅[配置 Exchange 以在混合部署中支持委派邮箱权限](#)。

EXCHANGE 版本	先决条件
Exchange 2016	不需要其他配置。
Exchange 2013	Exchange 2013 服务器需要以下各项: <ul style="list-style-type: none">• 安装了最新的累积更新 (CU) 或直接的以前的 CU。运行旧版 Cu 的 Exchange 2013 服务器不受支持, 并且可能无法在混合部署中与委派邮箱权限一起使用。• 将 Exchange 组织配置为允许在邮件对象上标记访问控制列表 (Acl), 并将其与 Office 365 同步。• 与 Exchange 2013 之前移动到 Office 365 的邮箱相关联的本地远程邮箱 CU10 需要手动配置为支持 Acl。在运行 Exchange 2013 CU10 或更高版本的服务器上创建的远程邮箱, 以及在将 Exchange 组织设置为允许 Acl 后, 会自动配置这些邮箱。
Exchange 2010	Exchange 2010 SP3 服务器需要以下各项: <ul style="list-style-type: none">• 已安装最新的更新汇总 (RU) 或上一次的 RU。不支持运行旧 RU 的 Exchange 2010 SP3 服务器, 也不能在混合部署中使用委派邮箱权限。• 需要将 Office 365 邮箱关联的本地远程邮箱配置为支持 Acl。需要为与 Office 365 邮箱相关联的每个本地远程邮箱执行此操作。
Exchange 2007 或更早版本	不支持。

在 Azure Active Directory Connect 中启用混合邮箱权限支持

除了配置本地 Exchange 服务器之外, 还需要确保已将 Azure Active Directory Connect (AAD Connect) 服务器设置为同步混合邮箱权限。若要确保 AAD 连接服务器已准备好支持这些权限, 您需要执行以下操作:

- **UPGRADE Aad connect:** aad connect 需要升级到至少版本1.1.553.0。您可以从[Microsoft Azure Active Directory connect](#)下载 AAD Connect 的最新版本。
- **在 AAD Connect 中启用 Exchange 混合:** 若要同步启用混合邮箱权限的属性 (尤其是 "代表发送" 权限), 您需要确保**Exchange 混合部署**配置选项为在 AAD Connect 中启用。有关如何再次运行 AAD 连接安装向导更新其配置的信息, 请参阅[AZURE AD Connect sync: 第二次运行安装向导](#)

最终用户权限

与管理员权限一样, 可以向 Exchange Online 中的最终用户授予权限。默认情况下, 会通过默认角色分配策略向最终用户授予权限。此策略将应用于 Exchange Online 组织中的每个邮箱。如果默认情况下授予的权限足够使用, 则您无需更改任何内容。

如果确实需要自定义最终用户权限, 则可以修改现有默认角色分配策略, 也可以创建新分配策略。如果创建多个分配策略, 则可以向不同邮箱组分配不同策略, 从而使您可以根据每个组的要求控制向每个组授予的权限。Exchange Online 最终用户的所有权限管理都必须使用 EAC 或远程 PowerShell 在 Exchange Online 组织中执行。

与管理员权限一样, 最终用户权限不会在内部部署组织和 Exchange Online 组织之间进行传输。必须在 Exchange Online 组织中重新创建在内部部署组织中定义的任何权限。

有关详细信息, 请参阅[Manage Role Assignment Policies](#)和[Change the Assignment Policy on a Mailbox](#)。

下表列出了由 Exchange Online 组织中的默认角色分配策略授予的权限。

默认角色分配策略权限

管理角色	说明
MyTeamMailboxes	<code>MyTeamMailboxes</code> 管理角色使各个用户能够创建网站邮箱并将其连接到 Microsoft SharePoint 网站。
我的市场应用程序	<code>My Marketplace Apps</code> 管理角色使各个用户能够查看和修改其 Microsoft Office 市场应用程序。
MyBaseOptions	<code>MyBaseOptions</code> 管理角色使各个用户能够查看和修改自己的邮箱和关联设置的基本配置。
MyContactInformation	<code>MyContactInformation</code> 管理角色使各个用户能够修改其联系人信息 (包括地址和电话号码)。
MyDistributionGroupMembership	<code>MyDistributionGroupMembership</code> 管理角色使各个用户能够在组织中查看和修改其在通讯组中的成员身份, 前提是这些通讯组允许操作组成员身份。
MyDistributionGroups	<code>MyDistributionGroups</code> 管理角色使各个用户能够创建、修改和查看通讯组, 并将成员修改、查看、删除和添加到其拥有的通讯组中。
MyMailSubscription	该 <code>MyMailSubscription</code> 角色使各个用户能够查看和修改其电子邮件订阅设置, 如邮件格式和协议默认设置。

管理角色	说明
MyProfileInformation	<code>MyProfileInformation</code> 管理角色使各个用户能够修改其名称。
MyRetentionPolicies	<code>MyRetentionPolicies</code> 管理角色使各个用户能够查看其保留标记, 并查看和修改其保留标记设置和默认值。
通过 mytextmessaging	<code>MyTextMessaging</code> 管理角色使各个用户能够创建、查看和修改其短信服务设置。
MyVoiceMail	<code>MyVoiceMail</code> 管理角色使各个用户能够查看和修改其语音邮件设置。
我的 ReadWriteMailbox 应用程序	<code>My ReadWriteMailbox Apps</code> 管理角色使用户能够使用 ReadWriteMailbox 权限安装应用程序。
我的自定义应用程序	<code>My Custom Apps</code> 管理角色使用户能够查看和修改其自定义应用程序。

混合部署中的边缘传输服务器

2019/6/5 •

边缘传输服务器角色是通常部署在位于 Exchange 组织外围网络中的计算机上的可选角色，旨在使组织的受攻击面降到最小。边缘传输服务器角色处理所有面向 internet 的邮件流，该流为组织中的内部部署 Exchange 服务器提供 SMTP 中继和智能主机服务。

基于 Exchange 的混合部署组织中的边缘传输服务器

要使用边缘传输服务器的 Exchange 2016 组织可以选择部署运行最新版本 Exchange 2010 或更高版本的边缘传输服务器。如果您不想直接向 internet 公开内部 Exchange 服务器，请使用边缘传输服务器。在混合部署中部署边缘传输服务器时，Exchange Online 将通过 Exchange Online Protection 服务连接到边缘传输服务器传送邮件。然后，边缘传输服务器将把邮件传递到收件人邮箱所在的内部部署 Exchange 邮箱服务器。

IMPORTANT

不要在处理或修改 SMTP 通信的内部部署 Exchange 服务器和 Office 365 之间放置任何服务器、服务或设备。内部部署 Exchange 组织和 Office 365 之间的安全邮件流取决于组织之间发送的邮件中包含的信息。支持允许 TCP 端口 25 上的 SMTP 通信通过而无需修改的防火墙。如果服务器、服务或设备处理内部部署 Exchange 组织和 Office 365 之间发送的邮件，此信息将被删除。如果发生这种情况，该邮件将不再被视为组织内部邮件，并且将会对其应用反垃圾邮件筛选、传输和日记规则以及可能不适用于它的其他策略。

Exchange 混合需要边缘订阅。如果您在其他位置具有其他 Exchange 边缘传输服务器，但是这些服务器不处理混合传输，那么这些服务器进行升级以支持混合部署。但是，如果将来您希望 EOP 连接到其他边缘传输服务器以进行混合传输，则它们必须运行最新版本的 Exchange 2010 或更高版本。

向混合部署添加边缘传输服务器

配置混合部署时，您可以视需要选择在内部部署组织中部署边缘传输服务器。配置混合部署时，您可以使用混合配置向导，选择一个或多个内部部署 Exchange 服务器，或选择一个或多个内部部署边缘传输服务器处理 Exchange Online 组织的混合邮件传输。

在将边缘传输服务器添加到混合部署时，混合配置向导将代表内部 Exchange 服务器与 EOP 进行通信。边缘传输服务器作为内部 Exchange 服务器和 EOP 之间的中继，用于从内部部署组织到 Exchange Online 组织的出站邮件。边缘传输服务器还作为内部 Exchange 服务器之间的中继，用于从 Exchange Online 组织到内部部署组织的进站邮件。所有以前由内部 Exchange 服务器处理的连接安全性由边缘传输服务器处理。收件人查询、遵从性策略和其他邮件检查继续由内部 Exchange 服务器处理。

如果将边缘传输服务器添加到混合部署，则无需在本地用户和 internet 收件人之间路由发送的邮件。只有在内部部署与 Exchange Online 组织之间发送的邮件才会通过边缘传输服务进行路由。

IMPORTANT

如果需要删除并重新创建用于在本地组织和 Exchange Online 之间进行通信的边缘订阅，请确保再次运行“混合配置”向导。重新创建边缘订阅将删除内部部署组织与 Exchange Online 之间的通信所需的配置更改。重新运行“混合配置”向导将再次应用这些更改。

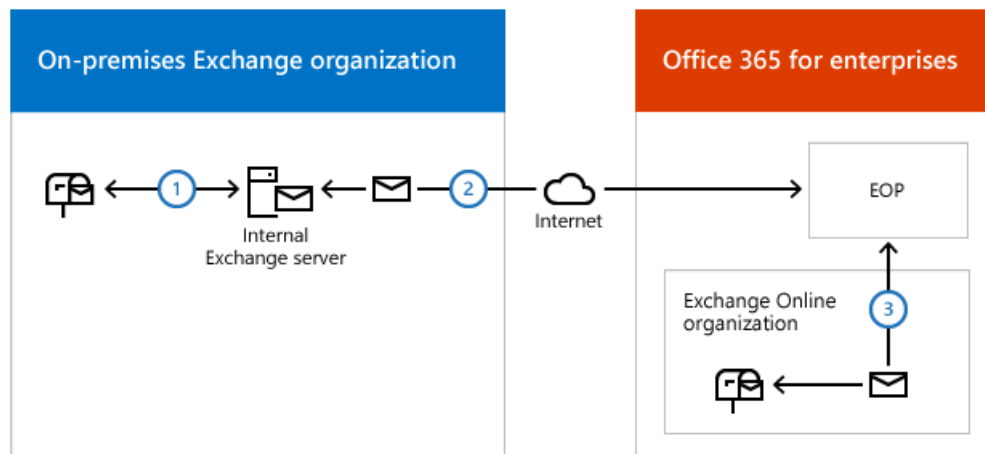
不使用边缘传输服务器的邮件流

下面的流程和图表展示了在没有部署边缘传输服务器时，本地组织与 Exchange Online 之间的邮件路径：

1. 从内部部署组织到 Exchange Online 组织中的收件人的出站邮件从内部 Exchange 服务器上的邮箱进行发送。
2. Exchange 服务器直接将邮件发送至 EOP。
3. EOP 将邮件传递到 Exchange Online 组织。

从 Exchange Online 组织发送到本地组织中收件人的邮件遵循相反的路由。

未部署边缘传输服务器的混合部署中的邮件流



使用边缘传输服务器的邮件流

以下流程介绍了在部署边缘传输服务器后，邮件在内部部署组织与 Exchange Online 之间采用的路径。从内部部署组织到 Exchange Online 组织中收件人的邮件是从内部 Exchange 服务器发送的：

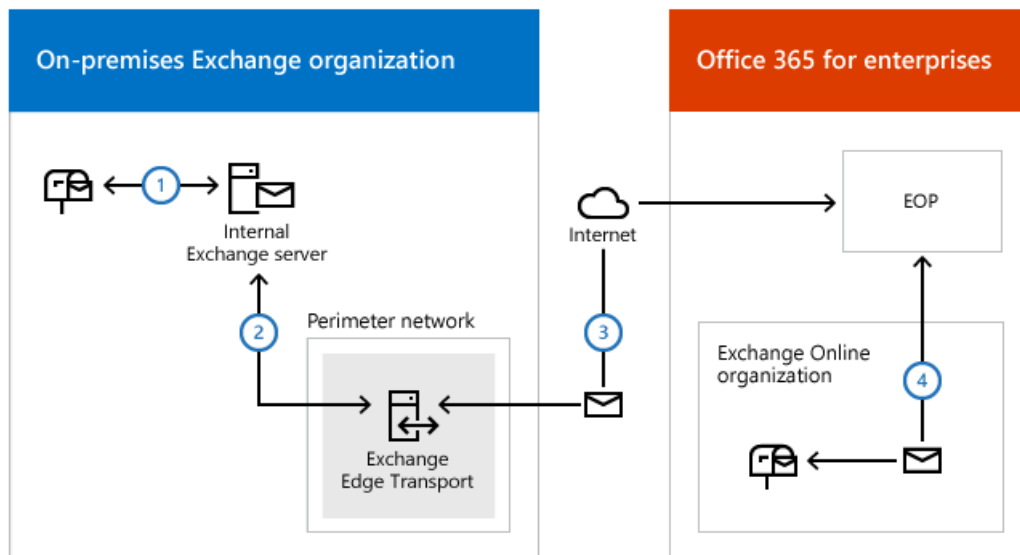
1. 从内部部署组织到 Exchange Online 组织中的收件人的邮件从内部 Exchange 服务器上的邮箱进行发送。
2. Exchange 服务器将邮件发送到运行版本受支持的 Exchange 发行版边缘传输服务器。
3. 边缘传输服务器将邮件发送至 EOP。
4. EOP 将邮件传递到 Exchange Online 组织。

从 Exchange Online 组织发送到本地组织中收件人的邮件遵循相反的路由。

NOTE

安装边缘服务器并建立边缘订阅将影响您的邮件流。此过程会自动为 internet 邮件流创建两个发送连接器：一个用于向所有 internet 域发送电子邮件，另一个用于将电子邮件从边缘传输服务器发送到内部 Exchange 组织。如果这不是你预期的邮件流方案，请查看连接器和邮件流。

部署了边缘传输服务器的混合部署中的邮件流



Exchange Server 部署助理

混合部署中的单一登录

2019/6/5 •

单一登录 (SSO) 使用户可以使用一个用户名和密码访问内部部署组织和 Office 365 组织。它向用户提供了一种熟悉的登录体验, 并能够允许管理员使用内部部署 Active Directory 管理工具轻松控制 Exchange Online 组织邮箱的帐户策略。尽管您不需要启用单一登录来配置混合部署, 但我们强烈建议您这样做。如果不使用单一登录, 用户将需要记住两组不同的凭据, 一组用于您的内部部署组织, 另一组用于 Office 365。下面是单一登录的其他几个优点:

- **Exchange Online 存档:** 部署单一登录时, 在首次访问 Exchange Online 组织中的存档内容时, 系统会提示本地 Outlook 用户提供其凭据。不过, 用户可以通过选择"保存密码"而暂时避免以后的凭据提示, 只会在更改内部部署帐户密码以后才再次收到提供凭据的提示。如果 Exchange 组织中没有部署单一登录, 且启用了 Exchange Online Archiving, 则内部部署用户主体名称 (UPN) 必须与 Exchange Online 帐户匹配, 且用户在访问存档内容时始终会收到提供内部部署凭据的提示。
- **策略控制:** 您可以通过 Active Directory 控制帐户策略, 这使您能够管理密码策略、工作站限制、锁定控件等, 而无需在 Office 365 中执行其他任务。组织。
- **减少了支持呼叫:** 忘记密码是所有公司的支持呼叫的常见来源。如果用户要记住的密码较少, 则他们忘记密码的可能性就较低。

部署单一登录时有三个选项: 密码哈希同步、传递身份验证和联合, 例如 Active Directory 联合身份验证服务 (AD FS)。所有选项均由 Azure Active Directory Connect 实现。强烈建议使用密码哈希同步方法, 除非您有需要联合的特定需求。密码哈希同步提供了很多与联合部署不复杂的联合的好处。

若要了解有关每个选项的详细信息, 请参阅[为你的 Azure Active Directory 混合标识解决方案选择正确的身份验证方法](#)。

Exchange ActiveSync 设备设置与 Exchange 混合部署

2019/6/5 •

当邮箱从 Exchange 内部部署组织移动到 Office 365 时，Exchange ActiveSync 设备将立即自动重新配置。Exchange ActiveSync 将在 Office 365 中查找新邮箱位置，并更新其配置，从而直接与 Office 365 通信。当 Exchange ActiveSync 设备成功重定向到 Office 365 后，此设备不会尝试与内部部署 Exchange 服务器联系。仅少数例外情况外（详情如下），用户不再需要手动设置设备来继续处理邮件。

如果要移动邮箱到 Office 365，请参阅在[混合部署中的内部部署组织和 Exchange Online 组织之间移动邮箱](#)。

有关混合部署的更多信息，请参阅[Exchange Server 混合部署](#)。

若要使用自动重定向，内部部署服务器应运行 Exchange 2010、Exchange 2013、Exchange 2016 或更高版本的最新发行版。您还需要已使用["混合配置"向导](#)设置好混合部署。Exchange ActiveSync 重定向功能将使用在组织关系对象上设置的 Web 上的 Outlook 目标 URL。运行混合配置向导时，将配置此对象。

如果您的组织满足上面列出的要求，当用户的邮箱移动时，移动设备应自动被重定向到 Office 365，无需任何其他配置。若要获得最佳体验，请确保您用户的移动设备正在运行其操作系统和电子邮件客户端的最新版本。某些移动设备（如运行 Android 操作系统的设备）可能需要相当长的时间重定向。此外，某些设备可能不正确地解释由 Exchange 发送的 Exchange ActiveSync 451 重定向说明。对于这些设备，用户仍需要手动重新配置或重新创建其设备上的电子邮件帐户。如果您对设备是否支持 Exchange ActiveSync 451 重定向有疑问，请与设备制造商联系。

在下列方案中不支持自动 Exchange ActiveSync 重定向：

- 将邮箱从 Office 365 移动到内部部署 Exchange 组织。
- 在内部部署 Exchange 组织之间移动邮箱。
- 将邮箱从 Exchange 2007 服务器移动到 Office 365。

混合迁移的性能因素和最佳做法

2019/6/5 •

在 Office 365 中有许多途径可以将本地电子邮件组织中的数据迁移到 Office 365。在计划迁移到 Office 365 时，一个常见的问题是如何提高数据迁移的性能并优化迁移速度。本文讨论了 Exchange 混合部署的迁移性能，有关其他迁移方法的性能信息，请参阅 [Office 365 迁移性能和最佳做法](#)。

混合迁移的性能因素和最佳做法

混合部署迁移支持本地 Exchange 服务器和 Office 365 中的 Exchange Online 之间的顺利迁移。

混合部署迁移是到目前为止将邮箱数据迁移到 Office 365 的最快迁移方法。我们看到在实际客户部署期间吞吐量高达 100 GB/小时。下表列出了适用于本机 Office 365 混合迁移方案的因素。

如果你的本地环境在分散的地理位置中包含多个站点，可以通过创建地理位置邻近感应的迁移终结点来提高迁移性能。这是因为在这样的情况下迁移使用 Microsoft 的网络，而不使用集中式迁移终结点（使用本地网络）。

因素 1: 数据源 (Exchange Server)

清单	说明	最佳做法
系统性能	数据提取是一项非常占用资源的任务。源系统必须具有足够的资源（如 CPU 时间和内存）才能提供更佳的迁移性能。在迁移时，源系统通常接近全部容量以满足定期最终用户工作负载。由于缺少系统资源，额外的迁移工作负载有时甚至会导致最终用户的访问量下降。	<p>在试点迁移测试过程中监视系统性能。如果系统繁忙，我们建议不要对特定系统执行很占用资源的迁移计划，因为这可能导致迁移变慢和服务可用性问题。如果可能，应通过增加硬件资源和减少系统中的负载（通过将任务和用户移至迁移未涉及的其他服务器）提高源系统性能。</p> <p>有关详细信息，请参阅： 询问性能专家：Sizing Exchange 2016 Deployments（调整 Exchange 2016 部署的大小） Exchange Server 运行状况和性能 了解 Exchange 2010 性能</p> <p>当从存在多个邮箱服务器和多个数据库的本地 Exchange 组织迁移时，我们建议创建在多个邮箱服务器和数据库之间均匀分布的迁移用户列表。根据各个服务器的性能，可以对该列表进一步微调以最大限度地增加吞吐量。</p> <p>例如，如果服务器 A 的资源可用性比服务器 B 高 50%，那么在同一个迁移批次中让服务器 A 中多迁移 50% 的用户较为合理。类似的做法可应用于其他源系统。</p> <p>在服务器具有最大资源可用性时（如下班后或周末和假日）执行迁移。</p>
后端任务	在迁移期间运行的其他后端任务。最佳做法是在下班之后执行迁移，因此经常会遇到迁移与您的内部部署服务器上运行的其他维护任务（如数据备份）相冲突的情况。	<p>查看在迁移期间可能会运行的其他系统任务。我们建议在没有运行其他占用资源较多的任务时执行数据迁移。</p> <p>注意：对于使用本地 Microsoft Exchange 的客户，常见的后端任务是备份解决方案和 Exchange 存储维护。</p>

因素 2: 迁移服务器

混合部署迁移是云发起的数据提取/推送迁移, Exchange 混合服务器充当迁移服务器。而这一点经常被忽略, 且客户会使用规模较小的虚拟机充当混合服务器。这会导致迁移性能降低

最佳做法

除了应用之前描述的最佳做法之外, 我们还测试了以下最佳做法, 这些做法提高了实际客户迁移的迁移性能:

- 为 Exchange 混合服务器使用强大的服务器类物理计算机来替代虚拟机。
- 使用多台位于客户的网络负载均衡器之后的混合服务器。

例如, 在实际客户迁移中, 我们已通过以下配置达到了一致的 30 GB/小时的吞吐量:

- **网络:** 500-mb 出站管道到 Internet; 使用 10 GB 光纤主干的 1 GB 内部网络。
- **硬件:** 两个客户端访问/中心 (物理) 服务器的规范为:
 - CPU: Intel® Xeon® CPU E5520 @ 2.27 GHz 2.26 GHz (两个处理器)。
 - RAM: 24 GB。
 - 磁盘: 每个磁盘 8×146 GB。RAID 5 配置 = 960 GB 总原始空间。
- **MRSProxy:** 配置了 100 的并发性。

因素 3: 迁移引擎

混合部署迁移使用本机 Office 365 工具。它受 Office 365 迁移服务限制的约束。

Exchange 2003 和更高版本的 Exchange

从 Exchange 2003 进行迁移时, 存在最终用户体验的重大差异。与 Exchange 的更高版本不同, Exchange 2003 最终用户无法在迁移数据时访问其邮箱。因此, Exchange 2003 客户通常更关注何时安排迁移以及迁移所需的时间 (尤其是在因邮箱较大或网速较慢而导致迁移性能降低时)。

Exchange 2003 迁移对中断也非常敏感。例如, 在实际客户迁移中, 在 10 GB 邮箱迁移期间, 在邮箱迁移完成 50% 时发生了服务事件。处理数据迁移的 Office 365 客户端访问服务器必须重新启动才能解决问题。在这种情况下, 必须重新启动邮箱迁移, 这意味着客户必须重新迁移所有 10 GB 的数据。不能从停止的点恢复迁移。但 Exchange 2010 和更高版本的 Exchange 却能在中断后恢复迁移。

最佳做法

有些客户选择对规模较大且敏感的 Exchange 2003 邮箱执行两跳迁移:

- **第一个跃点:** 将邮箱从 exchange 2003 迁移到 exchange 2010 或更高版本的服务器 (通常为混合服务器)。第一个跃点是脱机移动, 但通常是通过本地网络执行的速度极快的迁移。
- **第二跃点:** 将邮箱从 Exchange 2010 或更高版本迁移到 Office 365。

第二个跃点是联机移动, 会提供更好的用户体验和容错功能。这两个跃点方法需使用临时本地用户邮箱的 Exchange 许可证。

邮箱复制服务代理 (MRSProxy)

MRS 代理是与 Office 365 端运行的邮箱复制服务结合使用的本地迁移功能。有关详细信息, 请参阅[了解移动请求](#)。

最佳实践 *

可以为本地 Exchange 混合服务器 配置最大数量的 MRSProxy 连接。运行以下 Windows PowerShell 命令。

```
Set-WebServicesVirtualDirectory -Identity "EWS (Default Web Site)" -MRSMaxConnections <number between 0 and unlimited; default is 100>
```

NOTE

对于大多数客户迁移, 无需更改默认 MRSMAXConnections 值。如果需要保护源服务器以免迁移负载过大, 客户可以减少连接数。此设置按每个 MRSPROXY 服务器进行设置。如果客户有两个 MRSPROXY 服务器, 每个服务器都设置为 10 个连接, 它们的总 MRSPROXY 连接数将为 20 (2 x 10)。有关在本地 Exchange 2010 组织中配置 MRSPROXY 服务的详细信息, 请参阅[在远程客户端访问服务器上启动 MRSPROXY 服务](#)。

因素 4: 网络

验证测试

对于运行 Exchange 2010 或更高版本的客户, 可通过执行多个测试邮箱迁移完成对混合迁移网络性能的测试。或者, 也可以使用 -SuspendWhenReadyToComplete 选项迁移实际用户邮箱, 以满足迁移性能指标。测试完成时, 删除移动请求, 以避免影响最终用户。

有关移动请求的详细信息, 请参阅 [New-MoveRequest](#)。

因素 5: Office 365 服务

基于 Office 365 资源运行状况的限制将影响使用 Office 365 混合部署迁移的迁移。请参阅上面的基于 Office 365 资源运行状况的限制部分, 以了解更多详细信息。

关于 Exchange Server 的 Office 365 最佳实践分析工具

2019/6/5 •

Office 365 最佳实践分析工具是一个自动化的工具,可评估本地 Exchange 环境的运行状况和就绪情况。您可以随时在 Exchange 服务器上运行 Office 365 最佳实践分析工具,以评估 Exchange 配置的状态。

概述

您可以在以下环境中使用 Office 365 最佳实践分析工具:

- 仅限本地 Exchange server (Exchange 2013 或更高版本)
- 混合配置 (使用 Exchange 2013 或更高版本)

您将需要 Office 365 或 Azure Active Directory 帐户来安装和使用此工具。在安装并运行该工具后,无需登录到 Office 365 管理中心即可重新运行检查 (尽管可能会提示您再次登录的话)。

先决条件

若要在 Exchange 服务器上运行 Office 365 最佳实践分析工具,您需要满足以下要求。我们将自动验证你是否已准备好在下载该工具时运行检查。

- Exchange Server 2013 或更高版本。
- Internet Explorer 9.0 或更高版本。
- Windows Management Framework (WMF) 版本3.0 或更高版本 (包括 Windows PowerShell 和 Windows 远程管理或 WinRM)。Windows Server 2012 或更高版本已具有所需的 WMF 版本。请注意,在 Exchange 2013 或更高版本的服务器上,安装不支持单独的可下载版本的 WMF。
- 适用于 Windows PowerShell 的 Microsoft Azure Active Directory 模块和 Microsoft Online Services 登录助手的64位版本。您可以按照[此处](#)所述安装它们。
- 最小屏幕分辨率为 1024 x 768 (XGA)。

如何使用 Office 365 最佳实践分析工具

任务	ACTIONS
步骤 1: 登录并登录。	<p>远程桌面到本地 Exchange 服务器,然后打开 Exchange 管理中心 (EAC)。例如, https://localhost/ecp。</p> <p>如果你是 Office 365 企业版或 Office 365 中型企业版管理员,请打开 Internet Explorer,并通过 Office 365 帐户浏览关于 office 365 管理中心的信息。</p> <p>如果你还没有安装 Office 365,你可以在此处注册。</p>

任务	ACTIONS
步骤 2: 安装最佳实践分析工具。	<ol style="list-style-type: none"> 1. 在 EAC 中, 转到 "工具 > 检查", 然后单击 "使用 Office 365 最佳实践分析工具检查内部部署 Exchange 服务器"。 2. 当系统提示您下载或运行该工具时, 请单击 "运行"。 3. 针对所需的每个必备组件 (Microsoft Online Services 登录助手、.NET Framework 和 windows PowerShell 的 Windows Azure Active Directory 模块), 单击最终用户许可协议上的 "接受"。 4. 在 "应用程序安装-安全警告" 对话框中, 单击 "安装"。 5. 在 Office 365 最佳实践分析工具的使用条款中, 单击 "接受"。
步骤 3: 运行最佳实践分析工具。	<p>在第一次安装 Office 365 最佳实践分析工具之后, 它应自动启动。您还可以在以后通过从 Windows "开始" 菜单中选择 "Microsoft Office 365 最佳实践分析工具" 来运行它。</p> <ol style="list-style-type: none"> 1. 在 "欢迎" 页上, 单击 "下一步"。 2. 在 "新建最佳实践扫描" 页上, 单击 "开始扫描"。 3. 如果显示 "office 365 凭据" 对话框, 请输入 office 365 帐户和密码。 4. 等待扫描完成。
步骤 4: 了解有关任何警告或故障的详细信息。	<ol style="list-style-type: none"> 1. 在最佳实践扫描结果摘要页上, 单击 "查看详细信息" 以打开 "详细扫描结果" 页, 或单击 "保存扫描结果", 将结果保存到 HTML 文件中, 然后打开该文件。 2. 单击检测到的任何问题旁边的 "了解更多" 链接。 <p>注意: 如果保存了结果, 但无法看到 HTML 文件中的 "了解更多" 链接, 请单击弹出菜单中的 "允许阻止的内容: Internet Explorer 限制此网页运行脚本或 ActiveX 控件"。</p>

后续步骤

在解决任何报告的问题后, 您可以通过 Exchange 服务器再次运行 Office 365 最佳实践分析工具。

如何以及何时在混合部署中停止使用内部部署 Exchange 服务器

2019/6/5 •

如果您已准备好从 Exchange 混合部署移动至全云实现, 请阅读本文。

将公司与 Exchange Online 相关的一种更有吸引力的选择是使用 Exchange 混合部署中介绍的混合部署方法和 [Office 365](#) 中的迁移。这是唯一能让您轻松加入和退出邮箱的选项(所有其他本机选项都仅为加入)。除了能够脱离板载之外, 混合配置还具有以下关键选项。

本主题将帮助您了解停止使用 Exchange 的选项, 以及每个选项应何时实现。何时以及如何停止使用 Exchange 混合服务器存在很多差异。花点时间了解其含义并正确计划内部部署服务器的完全或部分停止使用, 这一点非常重要。

- **跨界可用性。**允许您在计划会议时查看用户的空闲/忙碌信息, 不论其邮箱位置如何。
- **跨界存档。**允许客户仅将用户的存档邮箱移动到云。这通常是客户试用 Office 365, 更具体地说是试用 Exchange Online 的第一步。
- **跨界发现搜索。**允许客户执行电子数据展示搜索, 对两个位置的邮箱和存档进行爬网(这需要配置 OAuth 身份验证)。
- **Outlook Web App URL 重定向。**允许用户被重定向到正确的位置以访问 Outlook Web App。
- **移动后不重新创建配置文件。**与其他迁移选项不同, 邮箱 GUID 不会更改。这意味着您在移动邮箱后不必重新创建配置文件或重新下载 OST。

根据您的组织的需求, 混合部署是用于提供最无缝的用户和共存体验的最佳选项。

迁移到 Exchange Online 的其他方法

混合部署不适合每个人;事实上, 通常有更好的选择。很多选择部署混合配置的租户具有 50 个以下座席。混合部署的优点众多, 听上去非常有吸引力, 但随着而来的是高额价格和复杂性。有些小型租户需要混合部署的功能, 但是对于大多数租户来说, 使用直接转换、暂存或 IMAP 迁移选项将会带来更好的体验。我们有一个 FastTrack 计划, 您可以使用这个计划来决定要采取的迁移方法。有关 FastTrack 的信息, 请参阅[Office 365 FastTrack 页面](#)。

使用下表可决定您的组织的迁移类型。(有关详细信息, 请参阅[将多个电子邮件帐户迁移到 Office 365 的方法](#)。)

现有组织	要迁移的邮箱数	是否要管理内部部署组织中的用户帐户?	迁移类型
Exchange 2013、Exchange 2010、Exchange 2007 或 Exchange 2003	少于 2,000 个邮箱	否	直接转换 Exchange 迁移
Exchange 2007 或 Exchange 2003	少于 2,000 个邮箱	否	暂存 Exchange 迁移
Exchange 2007 或 Exchange 2003	多于 2,000 个邮箱*	是	暂存 Exchange 迁移或 Exchange 混合部署中的远程移动迁移
Exchange 2013 或 Exchange 2010	多于 2,000 个邮箱*	是	Exchange 混合部署中的远程移动迁移

现有组织	要迁移的邮箱数	是否要管理内部部署组织中的用户帐户？	迁移类型
Exchange 2000 Server 或更早版本	无最大值	是	IMAP 迁移
非 Exchange 本地邮件系统	无最大值	是	IMAP 迁移

*有些邮箱数少于 2,000 的组织可能会从仅混合部署提供的特征和功能中受益。必须认真考虑混合部署的优势及其带来的复杂性。我们强烈建议邮箱数少于 2,000 的客户在进行混合部署之前，先考虑直接转换或暂存迁移。

为什么您不想从内部部署停止使用 Exchange 服务器

使用混合配置的客户在一段时间后通常会发现他们的所有邮箱均已迁移到 Exchange Online。此时，他们可能会决定将 Exchange 服务器从内部部署中移除。但是，他们发现自己不能再管理自己的云邮箱。

当为租户启用目录同步且从内部部署同步用户时，大部分属性都无法从 Exchange Online 管理，而必须从内部部署管理。这并非是由于混合配置，而是由于目录同步所致。此外，即使您已在不运行混合配向导的情况下进行了目录同步，您仍然无法从云管理大部分收件人任务。有关详细信息，请参阅此 [TechNet 博客](#)。

能否使用第三方管理工具？

一个常见问题是能否使用第三方管理工具或 ADSIEDIT。答案是可以使用，但不受支持。Exchange 管理控制台、Exchange 管理中心 (EAC) 和 Exchange 命令行管理程序是用于管理 Exchange 收件人和对象的唯一受支持的工具。如果您决定使用第三方管理工具，您需自行承担风险。第三方管理工具通常可以正常运行，但未经过 Microsoft 验证。

常见应用场景

将混合配置移动到云并不简单。实现混合配置通常需要耗费大量时间才能完成。尽管存在各种问题，但我们将实现混合这样一项几乎不可能的任务变成一个非常简单的基于向导的过程，我们认为自己已经做得很好了。

但是，我们几乎没有费力考虑如何将您从混合配置转变为仅云配置。根据您的短期目标，此过程可能非常简单，我们提供了一些指导。下面是三个常见混合方案以及我们对于如何正确实现客户最终目标的建议。

由于混合客户群非常的多样化，试图将所有客户都归纳到“常见”方案中非常困难。我们尝试在下面提供了一些用于停止使用内部部署 Exchange Server 的高级方案，因为在您阅读这些方案并制定停止使用计划时，您将需要确定最适合您需求的方案。

方案一

问题: 我的组织已在混合配置中运行，并且我的所有邮箱都在 Exchange Online 中。我不需要从内部部署管理我的用户，并且不再需要进行目录同步或密码同步。

解决方案: 由于所有用户都将在 Office 365 中进行管理，且没有其他的目录同步要求，您可以安全地禁用目录同步并将 Exchange 从内部部署环境中移除。



禁用目录同步并卸载 Exchange 混合

1. 运行 `Get-OrganizationConfig | Format-List PublicFoldersEnabled` 并确保未将其设置为“远程”。如果将其设置为“远程”，并且公用文件夹是您想要继续访问的内容，则需要将其迁移到 Exchange Online。有关详细信息，

请参阅 [Use batch migration to migrate legacy public folders to Office 365 and Exchange Online](#)。

2. 假定您已将所有邮箱迁移至 Exchange Online, 您可以将 MX 和自动发现 DNS 记录指向 Exchange Online, 而不是内部部署。有关详细信息, 请参阅[参考:Office 365 的外部域名系统记录](#)。

IMPORTANT

确保同时更新内部和外部 DNS, 否则可能会出现不一致的客户端连接行为。

3. 接下来, 您应该移除 Exchange 服务器上的服务连接点 (SCP) 值。这可以确保不会返回 SCP, 且客户端将改为使用 DNS 方法进行自动发现。下面是一个示例:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri $Null
```

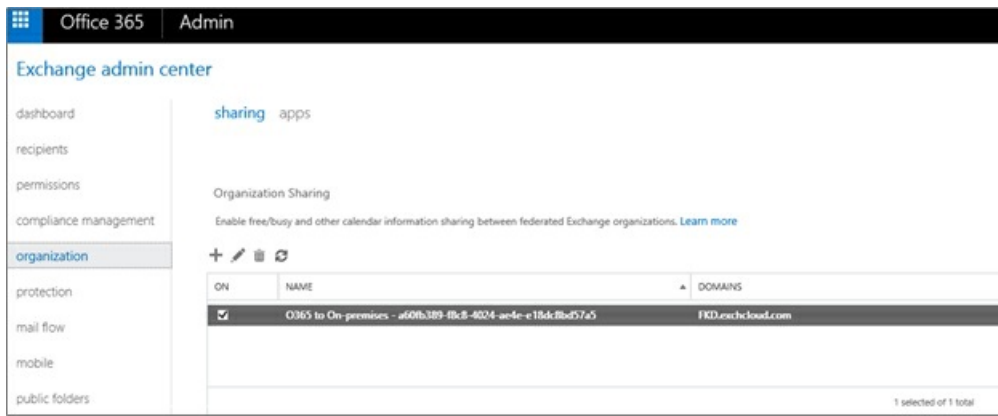
NOTE

如果您的环境中具有 Exchange 2007 服务器, 您将需要在 Exchange 2007 服务器上运行类似的命令以清空设置。

4. 混合配置向导创建了一些入站和出站连接器, 您可能需要将其删除。为此, 请执行以下步骤:
 - a. 登录到 [Office 365 管理门户](#) 并以租户管理员身份注册。
 - b. 选择管理 **Exchange** 的选项。
 - c. Navigate to **Mail Flow** -> **Connection**.
 - d. 现在您可以禁用或删除入站和出站连接器。HCW 使用唯一的命名空间 **inbound from <唯一标识符>** 和 **outbound from <唯一标识符>** 创建连接器, 如下图中所示。



5. 删除混合配置向导创建的组织关系。为此, 请执行以下步骤:
 - a. 登录到 [Office 365 管理门户](#) 并以租户管理员身份注册。
 - b. 选择管理 Exchange 的选项。
 - c. Navigate to **Organization**.
 - d. Under **Organization Sharing**, remove the organization named **O365 to On-Premises - <unique identifier>** as shown in the graphic below.



6. 如果为 Exchange 混合部署配置了 OAuth，您可能需要从内部部署和 Office 365 中禁用此配置。在大部分环境中，可以跳过这些步骤，因为只有一小部分客户配置了 OAuth。

禁用内部部署配置：

- 从 Exchange 2013 服务器，打开 Exchange 命令行管理程序。
- 运行以下命令：

```
Get-IntraorganizationConnector -Identity ExchangeHybridOnPremisesToOnline | Set-IntraOrganizationConnector -Enabled $False
```

禁用 Exchange Online 配置：

- 将 Windows PowerShell 连接到 Exchange Online。
- 运行以下命令：

```
Get-IntraorganizationConnector -Identity ExchangeHybridOnlineToOnPremises | Set-IntraOrganizationConnector -Enabled $False
```

注意：_Identity_ 参数假定您已使用 "混合配置" 向导配置 OAuth。如果不是，您可能需要调整为连接器标识指定的值。

- 为租户禁用目录同步。完成此步骤后，即表示将从 Office 365 管理工具完成所有用户管理任务。这意味着您不能再使用 Exchange 管理控制台或 Exchange 管理中心 (EAC)。有关如何禁用目录同步的详细信息，请参阅[停用目录同步](#)。
- 现在您可以从内部部署服务器安全地卸载 Exchange。

方案二

问题：我的组织已经运行混合配置大约一年的时间，并且已经将我的最后一个邮箱移动到云。我计划保留 Active Directory 联合身份验证服务 (AD FS)，以便对我的 Exchange Online 邮箱进行用户身份验证。（此方案将适用于任何计划保留目录同步的客户）。

解决方案：由于客户计划保留 AD FS，则也必须保留目录同步，因为这是必备条件。因此，他们无法从内部部署环境完全移除 Exchange 服务器。但是，他们可以停止使用大多数 Exchange 服务器，仅留下几台服务器进行用户管理。请记住，保留运行的服务器可以在虚拟机上运行，因为工作负荷已几乎完全转移到 Exchange Online。

下图显示了所需的最终状态：



下图显示了实际的最终状态：



保留 AD FS 和目录同步并停止使用大多数 Exchange 服务器

1. 运行 `Get-OrganizationConfig | fl PublicFoldersEnabled` 并确保未将其设置为 "远程"。如果设置为远程, 并且您需要继续访问公用文件夹, 您可能需要将其迁移到 Exchange Online。有关如何执行此操作的信息, 请参阅 [Use batch migration to migrate legacy public folders to Office 365 and Exchange Online](#)。

IMPORTANT

如果将公用文件夹迁移到 Exchange Online 不是选项, 并且您仍需要将其用于用户, 则不应继续。

2. 将所有邮箱迁移到 Exchange Online 后, 停止使用大多数 Exchange 服务器需执行的第一个操作是将 MX 和自动发现 DNS 记录指向 Exchange Online, 而不是内部部署。有关详细信息, 请参阅 [参考: Office 365 的外部域名系统记录](#)。

IMPORTANT

确保同时更新内部和外部 DNS, 否则可能会出现不一致的客户端连接和邮件流行为。

3. 接下来, 您应该移除 Exchange 服务器上的服务连接点 (SCP) 值。这可以确保不会返回 SCP, 且客户端将改为使用 DNS 方法进行自动发现。下面是一个示例:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri $Null
```

NOTE

如果您的环境中具有 Exchange 2007 服务器, 您将需要在 Exchange 2007 服务器上运行类似的命令以清空设置。

4. 为防止在将来重新创建混合配置对象, 您应该将混合配置对象从 Active Directory 中移除。为此, 请打开 Exchange 命令行管理程序并运行以下命令:

```
Remove-HybridConfiguration
```

5. 移除所有 Exchange 服务器, 除了需要保留用于用户管理和创建的服务器以外。两台服务器应足以用于用户管理, 一台服务器可能也可以实现此目的。此外, 没有必要保留数据库可用性组或任何其他高可用性选项。
6. 如果为 Exchange 混合部署配置了 OAuth, 您可能需要从内部部署和 Office 365 中禁用此配置。在大部分环境中, 可以跳过这些步骤, 因为只有一小部分客户配置了 OAuth。

禁用内部部署配置：

- a. 从 Exchange 2013 服务器, 打开 Exchange 命令行管理程序。
- b. 运行以下命令：

```
Set-IntraorganizationConnector -Identity ExchangeHybridOnPremisesToOnline | Set-IntraOrganizationConnector -Enabled $False
```

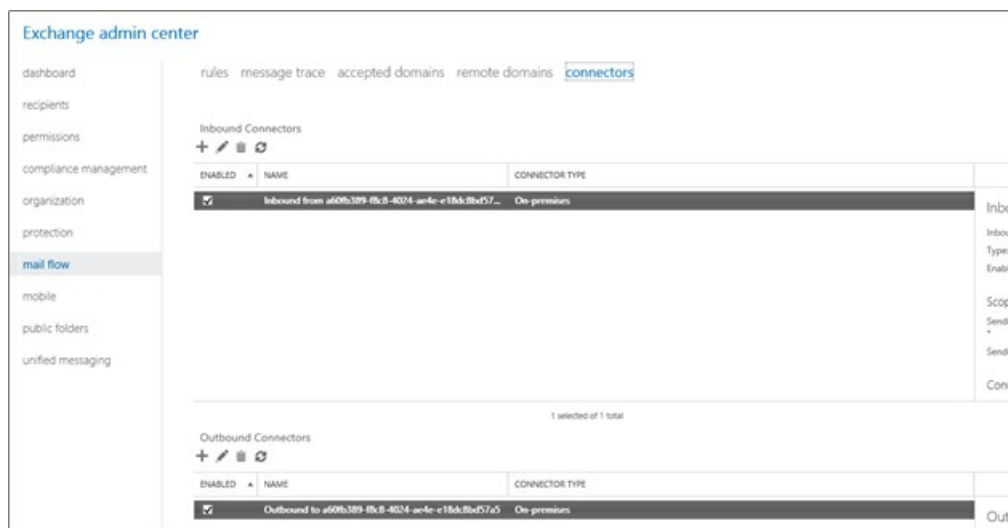
禁用 Exchange Online 配置：

- a. 将 Windows PowerShell 连接到 Exchange Online。
- b. 运行以下命令：

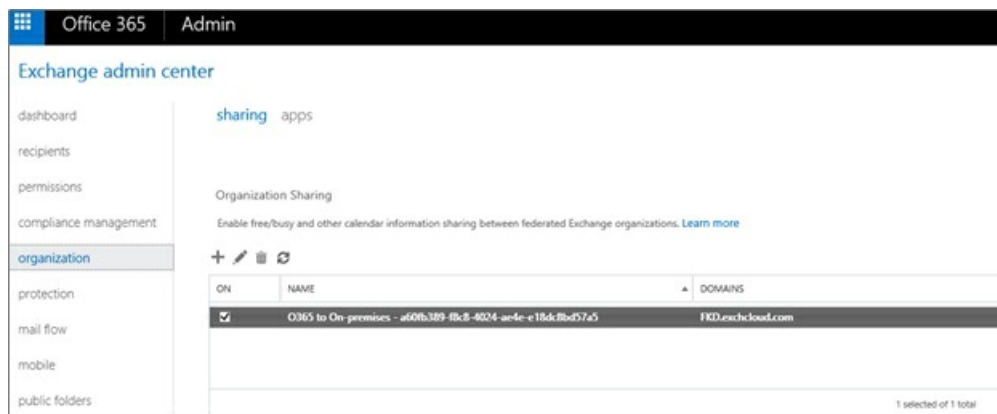
```
Get-IntraorganizationConnector -Identity ExchangeHybridOnlineToOnPremises | Set-IntraOrganizationConnector -Enabled $False
```

注意：Identity 参数假定您已使用“混合配置”向导配置 OAuth。如果不是，您可能需要调整为连接器标识指定的值。

7. 混合配置向导创建了一些入站和出站连接器，您可能需要将其删除。为此，请执行以下步骤：
 - a. 登录到 [Office 365 管理门户](#) 并以租户管理员身份注册。
 - b. 选择管理 **Exchange** 的选项。
 - c. Navigate to **Mail Flow** -> **Connectors**.
 - d. 现在您可以禁用或删除入站和出站连接器。HCW 使用唯一的命名空间 **inbound from <唯一标识符>** 和 **outbound from <唯一标识符>** 创建连接器，如下图中所示。



8. 删除混合配置向导创建的组织关系。为此，请执行以下步骤：
 - a. 登录到 [Office 365 管理门户](#) 并以租户管理员身份注册。
 - b. 选择管理 **Exchange** 的选项。
 - c. Navigate to **Organization**.
 - d. Under **Organization Sharing**, remove the organization named **O365 to On-Premises - <unique identifier>** as shown in the graphic below.



方案三

问题: 在将所有邮箱移动到 exchange Online 后, 我想要删除本地 Exchange 服务器。但是, 我们发现它们将 Exchange 用于其他目的, 例如用于应用程序的简单邮件传输协议 (SMTP) 中继或用于访问公用文件夹。如果您需要内部部署 Exchange 服务器以满足组织的当前需求, 移除内部部署服务器可能不是对您最有利的选项。

解决方案: 我们建议在这种情况下不要移除 Exchange 和混合配置。如果您刚刚通过将自动发现记录指向 Exchange Online 启动了此过程, 您可能会立即破坏一些功能, 如混合公用文件夹访问。您可以将 MX 记录改为指向 Exchange Online Protection (如果尚未就绪), 您甚至可以移除一些内部部署 Exchange 服务器。但是, 您需要保留足够的空间以处理其余的混合功能。通常, 这会导致占用少量的内部部署空间。

混合部署过程

2019/6/5 •

随着混合配置向导的最新改进，配置和管理混合部署变得更加简单。无论是否希望连接您的 Exchange 内部部署和 Exchange Online 组织用于长期共存，或作为云迁移战略的一部分，配置混合部署都是 Exchange 组织的第一步。

选择以下一个主题开始：

[使用混合配置向导创建混合部署](#)

[在混合部署中的内部部署组织和 Exchange Online 组织之间移动邮箱](#)

[Configure legacy on-premises public folders for a hybrid deployment](#)

[Configure Exchange 2013 public folders for a hybrid deployment](#)

[Configure Exchange Online public folders for a hybrid deployment](#)

[将 Exchange 配置为支持混合部署中的委派邮箱权限](#)

[通过 OneDrive for Business 和本地 Exchange 2016 配置新式附件](#)

[使用本地 Exchange 混合配置 Office 365 组](#)

[在 Exchange 混合部署中为本地主邮箱创建基于云的存档](#)

[为 Office 365 混合简化 Outlook Web App URL](#)

[混合部署故障排除](#)

[在混合部署中配置 IRM](#)

Microsoft 混合代理-预览

2019/6/5 •

混合代理删除了配置 Exchange 混合环境时可以面对的一些挑战。与 Azure 应用程序代理在同一技术的基础上构建的代理将删除对外部 DNS 条目、证书更新、通过防火墙的入站网络连接等一些要求,以便您可以使用 Exchange 混合功能。这些功能包括忙/闲共享和联机邮箱移动。混合代理仅支持忙/闲和邮箱迁移;不包括邮件流、目录同步和其他混合功能。

代理安装位置 & 要求

在设计为 "代理服务器" 的独立计算机上支持通过 "混合配置" 向导进行的代理安装和混合配置。您还可以使用客户端访问角色在 Exchange 2010、2013、2016或2019服务器上安装它。

系统要求

混合代理具有以下要求:

- 安装它的计算机需要具备以下条件:
 - 使用 .NET Framework 4.6.2 (或更高版本,由您在其上安装的 Exchange 版本支持) 运行 Windows Server 2012 R2 或2016
 - 加入到 Active Directory 域
 - TLS 1.2 已启用
 - Azure 应用程序代理文档:<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application>
 - 能够建立到 Internet 的出站 HTTPS 连接
 - 能够与为混合配置选择的客户端访问服务器 (CAS) 建立 HTTPS 和远程 PowerShell 连接。
- 使用支持 ClickOnce 技术的浏览器 (如 Microsoft Edge)。
- 你登录的本地 Active Directory 帐户必须:
 - 是本地 Exchange 组织中的 "组织管理" 角色组的成员
 - 是正在安装混合代理的计算机上本地 Administrators 组的成员。
- 用于连接到 Office 365 租户的帐户必须是全局管理员。

端口和协议要求

- 在安装了混合代理的计算机与 Internet 之间,必须打开出站端口 HTTPS (TCP) 443 和 80,如下所示:
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-enable>
- 端口 HTTPS (TCP) 443、80、5985和5986必须在混合代理在混合配置向导中所选的 CAS 上安装了混合代理的计算机之间打开。

IMPORTANT

所有客户端访问服务器都必须能够通过 HTTPS (TCP) 443 访问出站到 Office 365 终结点, 将本地用户的忙/闲请求发送到 Office 365 用户不会遍历混合代理。这些请求仍要求您的 Exchange 服务器具有到 Office 365 终结点的出站连接。Office 365 Url 和 IP 地址范围描述从-本地到服务的必需 (和混合) 端口和 Ip 出站: <https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges>。

代理服务器注意事项

如果您的网络环境使用出站代理服务器, 则需要其他配置和要求。此列表可能不详尽。

代理

代理支持出站代理服务器, 但在安装后需要进行其他配置。有关详细信息, 请参阅[使用现有的本地代理服务器](#)。

IMPORTANT

阻止注册的代理服务器会导致连接器安装失败。建议您允许连接器绕过代理, 直到可以进行应用程序配置更改。

客户端访问服务器

HCW 建立从客户端访问服务器到 domains.live.com 的连接, 以交换元数据并建立信任关系。由于连接源于 CAS 服务器, 因此该服务器上的代理设置 (from `Get-ExchangeServer | Format-List InternetWebProxy`) 必须正确设置, 否则出站的忙/闲可能会失败。除了连接故障之外, 如果代理设置不正确, 则 HCW 将无法配置委派身份验证。

预览限制

在安装混合代理之前, 请注意以下问题:

- 混合代理不支持[混合新式身份验证](#)。客户将需要利用经典 Exchange 混合拓扑, 并发布自动发现、EWS、MAPI 和 OAB 终结点, 以便与各种 Outlook 客户端配合使用来运行混合新式身份验证。
- 邮件提示、邮件跟踪和多邮箱搜索不会遍历混合代理。这些混合功能需要经典连接模型, 其中 Exchange Web 服务 (EWS) 和自动发现在本地发布且在外部可用于 Office 365。
- 公共预览版仅支持 Exchange 组织的单个混合代理安装。支持多个代理安装以实现冗余, 但尚不可用。如果安装了混合代理的服务器脱机, 则从租户到内部部署组织的忙/闲查找以及从租户到或来自你的租户的邮箱迁移将无法工作。如果安装了代理的服务器是永久性脱机、已重建或卸载了代理, 则可以重新运行混合配置向导, 以便在新服务器上直接重新安装混合代理。

WARNING

请勿尝试在你的环境中使用此预览版安装多个活动混合代理, 这可能会导致意外问题。

- 混合代理在 Azure 应用程序代理中运行 "混合配置" 向导时, 注册所选 CAS 服务器的内部完全限定域名 (FQDN)。如果注册的 CAS 脱机, 则从你的租户到本地的忙/闲外观, 以及从你的租户到/的邮箱迁移将无法工作。如果所选的 CA 是永久性脱机的, 则必须注册新的 CAS 服务器。再次运行 "混合配置" 向导, 以注册新的 CAS 服务器。
- 混合代理预览提供了一些支持限制, 这些限制是在安装功能之前必须同意的术语文档中调用的。

NOTE

SMTP 不会遍历混合代理, 并且仍需要 Office 365 和内部部署组织之间的邮件流的公共证书。SMTP 流量超出混合代理的范围, 现在和通过常规可用性。

运行安装程序

HCW 是负责安装混合代理的应用程序, 即内部部署组织和 Office 365 租户中的配置。您必须从要安装代理的计算机运行 HCW。在安装并配置代理之后, HCW 将找到要连接到的首选服务器并运行标准混合配置步骤。您无需直接从 Exchange 服务器运行 HCW, 但如前所述, 运行 HCW 的计算机必须能够连接到在 ["端口和协议"](#) 部分中指定的端口上的 CAS 服务器。

NOTE

仅当您从未运行 "混合配置" 向导时, 才会显示 "新式混合" 选项。如果你已在租户的 "经典 config" 中成功或完全建立了混合, 则不会向你显示此新选项。

安装先决条件

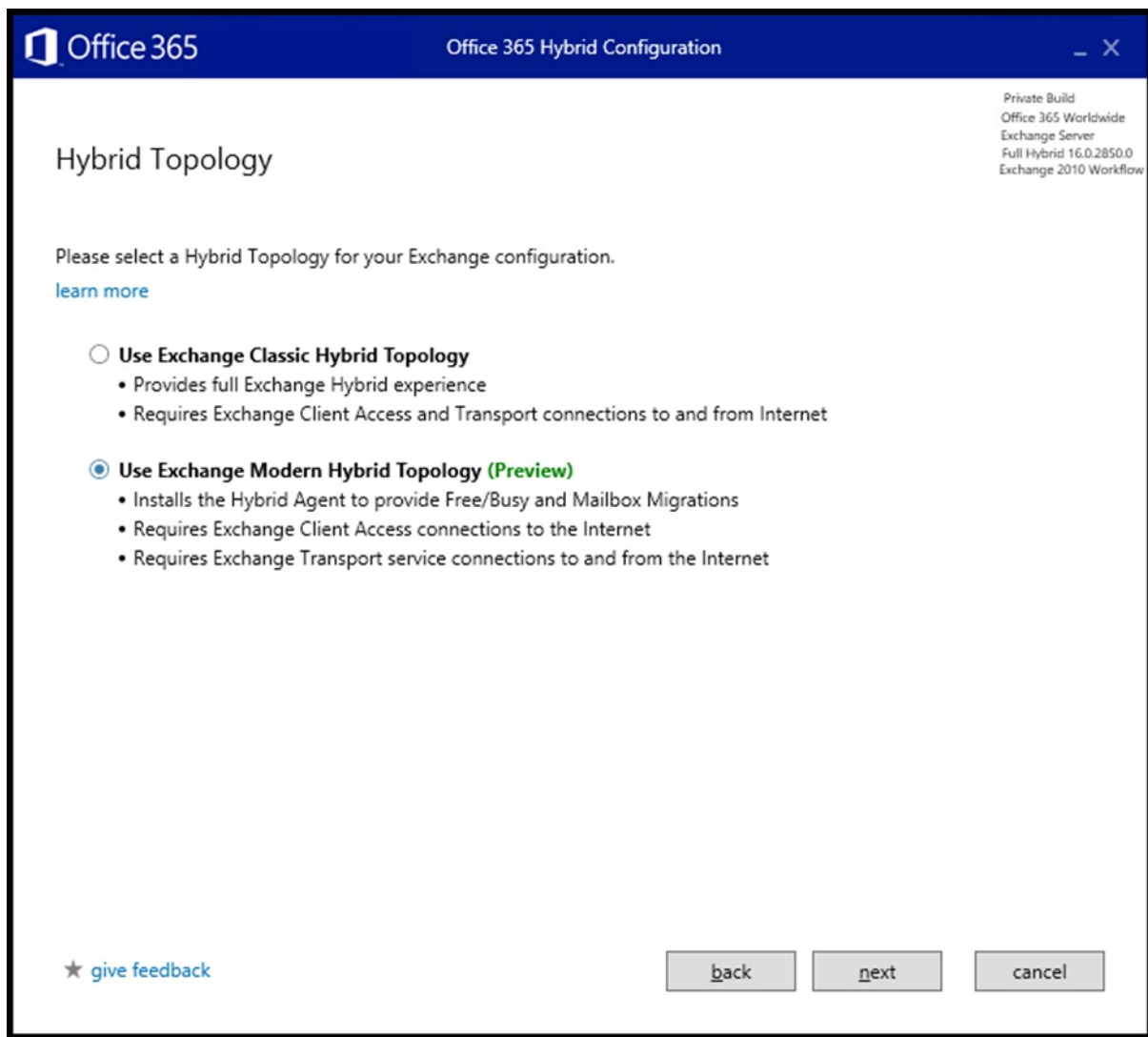
1. 若要允许安装混合代理并在 Office 365 租户中执行邮箱迁移, 请使用以下命令在 EWS 虚拟目录上启用邮箱复制服务 (MRS) 代理。

```
Set-WebServicesVirtualDirectory -Identity "EWS (Default Web Site)" -MRSProxyEnabled $true
```

2. 转到 **"程序和功能"**, 并验证是否尚未安装早期版本的 Microsoft Office 365 "混合配置" 向导。如果是, 请将其卸载。
3. 在运行 HCW 的计算机上安装 .NET Framework 版本 4.6.2。您可能需要安装更高版本的 .NET Framework, 具体取决于已安装的 Exchange 版本。或者, 如果未安装此版本, HCW 将提示您安装它或升级您的计算机上已安装的版本。

安装步骤

1. 登录到本地 Exchange 管理中心 (EAC), 导航到 **"混合"** 节点, 然后单击 **"配置"**。
2. 选择要在其中运行传统混合安装程序的 Exchange 服务器。选择 HCW 提供的默认服务器, 或在第二个单选按钮中指定特定服务器。选择 **"下一步"**。****
3. 输入你的本地 Exchange 凭据和 Office 365 全局管理员凭据。单击 **"下一步"**。****
4. 等待, 同时 HCW 收集有关您的环境的信息和配置。完成后, 单击 **"下一步"**。
5. 选择 **"最小"** 或 **"完全"** 混合配置。您还可以选择 **"组织配置转移"**。有关详细信息, 请参阅 [混合组织配置转移](#)。单击 **"下一步"**。****
6. 按照启用联盟的步骤操作。单击 **"下一步"**。****
7. 选择 **"使用 Exchange 新式混合"**



单击“下一步”。****

8. HCW 安装混合代理。有四个基本阶段:

- a. 下载代理安装包
- b. 在本地计算机上安装代理 (注意: 这将再次提示您输入 Office 365 全局管理员凭据)
- c. 在 Azure 中注册代理, 包括创建用于代理请求的 URL。URL 的格式 `uniqueGUID.resource.mailboxmigration.his.msapproxy.net` 为。
- d. 通过代理, 通过代理将 Office 365 租户的迁移生存能力测试到本地 Exchange 组织。

NOTE

混合代理安装过程最长可能需要10分钟才能完成。

其余的 HCW 步骤与传统的混合部署相同。在 HCW 的最后阶段中, HCW 将创建具有自定义 URL 的迁移终结点。然后, 它设置 `TargetSharingEPR` 组织关系和/或 `IntraOrganization` 连接器上的值。仅在 Office 365 端上设置新 `TargetSharingEPR` 的迁移终结点值和值。新 URL 用于将来自 Office 365 租户的请求发送到内部部署 Exchange 组织, 以实现忙/闲和迁移。您可以通过运行 `Get-MigrationEndpoint` Office 365 租户并 `Get-OrganizationRelationship` 从 Exchange Online PowerShell 连接 o 中查看为每个配置的特定值。下面的示例显示在运行 `Get-MigrationEndpoint` cmdlet 时可能会看到的输出:

```
Get-MigrationEndpoint | Format-List Identity,RemoteServerIdentity
```

Identity : Hybrid Migration Endpoint - EWS (Default Web Site)

RemoteServer :
087f1c2e-8711-4176-ab4f-4b1c1777a350.resource.mailboxmigration.his.msapproxy.net

```
Get-OrganizationRelationship | Format-List Name,TargetSharingEpr
```

Name : 0365 to On-premises - c6d22e11-2340-4432-9122-19097bacf0c1

TargetSharingEpr :
https://087f1c2e-8711-4176-ab4f-4b1c1777a350.resource.mailboxmigration.his.msapproxy.net/EWS/Exchange.asmx

其他信息

可以在安装了混合代理的服务器上的以下位置查看该混合代理的安装详细信息。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Hybrid Service :

"添加/删除程序":

测试混合代理的 & 验证

成功部署混合代理和混合配置后, 以下两个简单测试可用于通过代理验证闲/忙和邮箱迁移流。

在安装了混合代理的服务器上, 打开 "性能监视器"。将对象 " **Microsoft AD 应用程序代理连接器** " 和 " ** #请求 *** " 计数器添加到视图中。

迁移

打开与 Office 365 租户的 Exchange Online PowerShell 连接, 并运行以下测试 cmdlet:

```
Test-MigrationServerAvailability -ExchangeRemoteMove: $true -RemoteServer '<your customguid>.resource.mailboxmigration.his.msapproxy.net' -Credentials (Get-Credential)
```

在出现的对话框中, 输入您的本地凭据。在测试返回成功结果后, 切换回性能监视器, 并确认请求数已增加。

若要执行从内部部署 Exchange 组织到 Office 365 租户的测试邮箱移动, 也可以选择执行此项。

闲/忙

若要对忙/闲信息执行相同的验证, 请登录到租户中的 Office 365 邮箱, 创建测试会议邀请, 并将其发送到内部部署邮箱。

卸载混合代理

若要卸载混合代理, 请从运行安装的同台计算机重新运行混合配置向导, 并选择 "经典连接"。选择 "经典连接" 将从计算机和 Azure 中卸载并注销混合代理。在注销混合代理之后, 可以在经典模式下恢复安装程序并配置混合。

使用混合配置向导创建混合部署

2019/6/5 •

通过建立混合部署，您可以将随其现有内部部署 Exchange Server 组织提供的功能丰富的体验和管理控制扩展到云。混合部署还使用 Exchange Online 存档，为内部部署邮箱的基于云的存档解决方案提供支持，同时还可作为完全迁移您的内部部署邮箱到 Exchange Online 的中间步骤。

本主题包括使用混合配置向导在面向企业的 Office 365 中为内部部署 Exchange 组织与 Exchange Online 组织配置混合部署。在本主题中，将为以下组织配置创建混合部署：

- 内部部署组织为单林内部部署 Exchange 组织。
- 内部部署组织不使用现有 Microsoft Exchange Online Protection (EOP) 服务用于内部部署保护。
- 内部部署组织并不部署边缘传输服务器。作为混合部署的一部分，混合配置向导支持配置边缘传输服务器。但是本主题并不包括在向导中配置边缘传输服务器。

IMPORTANT

使用混合配置向导配置混合部署要求某些重要的先决条件，这些先决条件有助于向导成功完成任务，以及有助于混合部署功能的正常工作。必须完成在 [混合部署先决条件](#) 中概括的先决条件后，才可使用混合配置向导创建与配置混合部署。 > 此外，[Exchange Server 部署助理](#)是一款免费的 Web 工具，可帮助您在内部部署组织和 Office 365 之间配置混合部署，或完全迁移到 Office 365。该工具会询问您一些简单的问题，然后根据您的回答，创建一个自定义检查表，其中包含配置混合部署的说明。我们强烈建议您使用部署助理生成针对特定组织需求的自定义混合部署检查表。

关于混合部署的更多管理任务，参阅 [混合部署过程](#)。

有关混合部署的详细信息，请参阅 [Exchange Server 混合部署](#)。有关 Office 365 的更多信息，请参阅[什么是 Office 365？](#)。

在开始之前，您需要知道什么？

- 估计完成时间:30 分钟

IMPORTANT

该主题概述了完成混合配置向导步骤的估计完成时间。配置混合部署要求将会花费比估计完成时间长得多的时间。例如，注册企业 Office 365、配置 Active Directory 同步、分配 Exchange Online 许可证要求巨大的时间投资，并且可能也包括网络拓扑更改。考虑到完成端到端混合部署配置需要的整体时间，您应该计划出比所列的完成该步骤需要的时间更长的时间。

- 您必须先获得权限，然后才能执行此过程或多个过程。若要查看所需的权限，请参阅 [Exchange and Shell infrastructure permissions](#)主题中的"混合部署"条目。
- 您需要通过运行且版本受支持的最新 Exchange 发行版的计算机运行混合配置向导。配置 Exchange OAuth 身份验证的混合配置向导中的最后步骤要求从内部部署 Exchange 服务器或从任何连接域的服务器或工作站执行这些步骤。此外，OAuth 身份验证进程在使用 Internet Explorer 11 或更高版本的桌面版时效果最佳。
- 检查 [Exchange Server 混合部署](#) 主题，并确保您清楚会受到配置混合部署影响的方面。
- 检查并完成 [混合部署先决条件](#) 概括的所有混合部署要求。
- Microsoft 远程连接分析工具可以检查内部部署 Exchange 组织的外部连接，确保做好配置混合部署的准备。

强烈建议在使用混合配置向导配置混合部署之前, 使用远程连接分析工具检查内部部署组织。有关更多信息, 请参阅[远程连接分析工具](#)。

- 我们强烈建议使用 Azure Active Directory Connect 的密码同步配置单一登录。单一登录使用户可以使用一个用户名和密码访问内部部署组织和 Exchange Online 组织。单一登录也确保用户在使用 "Exchange Online Archiving" 访问 Exchange Online 组织中的存档内容时, 不会获得凭据提示。有关密码同步的详细信息, 请参阅 [Azure AD Connect 同步: 实施密码同步](#)
- 有关可能适用于本主题中的过程的键盘快捷方式的信息, 请参阅[Exchange 管理中心的键盘快捷方式](#)。

TIP

是否有任何疑问? 在 Exchange 论坛中寻求帮助。请访问以下论坛:[Exchange Server](#)、[Exchange Online](#)或 [Exchange Online Protection](#)。

使用 Exchange 管理中心与混合配置向导创建混合部署

使用以下过程来创建和配置混合部署:

1. 在您的内部部署组织中的 Exchange 服务器上的 EAC 中, 导航到 "混合" 节点。
2. 在****"混合"节点中, 单击"配置"**** 以输入您的 Office 365 凭据。

IMPORTANT

如果您的内部部署组织位于中国并且您的 Office 365 租户由世纪互联托管, 则必须选中"我的 Office 365 组织由世纪互联托管"**** 复选框。如果您的 Office 365 租户由世纪互联托管但未选中此复选框, 混合配置向导将无法连接到世纪互联服务, 您的 Office 365 帐户凭据不会被识别, 因此无法正确完成向导。

3. 提示您登录到 Office 365 时, 选择"登录到 Office 365"**** 并输入帐户凭据。您登录到的帐户需要是 Office 365 中的全局管理员。
4. 单击"配置"**** 以启动"混合配置"向导。
5. 在"Microsoft Office 365 混合配置向导下载"**** 页面上, 单击"单击此处" **** 下载向导。系统提示时, 在"应用程序安装"**** 对话框上单击"安装"****。
6. 单击"下一步"****, 然后在"本地 Exchange Server 组织"**** 部分中, 选择"检测运行 Exchange 2013 CAS 或 Exchange 2016 的服务器"****。该向导将尝试检测内部部署 Exchange 服务器。如果向导未检测到 Exchange 服务器, 或者如果要使用其他服务器, 请选择 "指定运行 **Exchange 2013** 或 **exchange 2016** 的服务器", 然后指定 exchange 邮箱服务器的内部 FQDN。
7. 在 **Office 365 Exchange Online** 部分中, 选择 **Microsoft Office 365**, 然后单击"下一步"****。
8. 在 "凭据" 页上的 "输入内部部署帐户凭据" 部分, 选择 "使用当前 Windows 凭据" 以让向导使用登录的帐户访问本地 Active Directory 并 Exchange 服务器。如果您想要指定一组不同的凭据, 则取消选择"使用当前的 Windows 凭据"****, 并指定您要使用的 Active Directory 帐户的用户名和密码。无论选择哪种方式, 使用的帐户都需要为企业管理员安全组的成员。
9. 在"输入您的 Office 365"**** 凭据部分中, 指定具有全局管理员权限的 Office 365 帐户的用户名和密码。单击"下一步"****。
10. 在"验证连接和凭据"**** 页面中, 该向导将连接到您的本地组织和 Office 365 组织来验证凭据并检查这两个组织的当前配置。完成时单击"下一步"****。
11. 在"混合域"**** 中, 选择您想要在混合部署中包含的域。在大多数部署中, 对于每个域, 您可以将"自动发现"**** 列设置为 **False**。如果您需要强制向导使用特定域中的自动发现信息, 只能选择域旁边的 **True**。单

击“下一步”****。

IMPORTANT

当您运行向导时，混合配置向导的这一域选择步骤可能不会显示。如果出现以下情况，则不会显示此步骤：

- 仅将一个内部部署接受域添加到 Office 365 租户。由于这是混合部署配置可用的唯一域，该域将自动选定，同时向导中的步骤将跳过。
- 不会向您的 Office 365 租户添加任何本地接受的域。在这种情况下，您将收到错误，同时需要在继续之前添加至少一个域到 Office 365 租户。可以通过使用 Office 365 管理门户完成此操作，也可以通过在内部部署组织中有选择地配置 Active Directory 联合身份验证服务 (AD FS) 完成此操作。

如果您添加了不少于一个内部部署接受的域到 Office 365 租户，该步骤将显示。

12. 在“联合身份验证信任”**** 页面上，单击“启用”****，然后单击“下一步”****。
13. 在“域所有权”页面上，单击“复制到剪贴板”以复制已选择要包含在混合部署中的域的域证明令牌信息。打开文本编辑器，如“记事本”，并粘贴这些域的令牌信息。在混合配置向导继续运行之前，必须使用该信息为公共 DNS 中的每个域创建一个 TXT 记录。请参考 DNS 主机的帮助，了解有关如何将 TXT 记录添加到 DNS 区域的信息。在创建 TXT 记录以及复制 DNS 记录后，单击“下一步”****。
14. 在“传输证书”页面上的“选择引用服务器”字段中，选择具有您在检查表中之前配置的证书的 Exchange 服务器。
15. 在“选择证书”字段中，选择要用于安全邮件传输的证书。该列表显示了安装在在上一步所选的邮箱服务器上的，由第三方证书颁发机构 (CA) 颁发的数字证书。单击“下一步”****。
16. 在“组织 FQDN”页上，为面向 Internet 的 Exchange 服务器输入外部可访问的 FQDN。Office 365 使用该 FQDN 来为 Exchange 组织之间的安全邮件传输配置服务连接器。例如，输入“mail.contoso.com”。单击“下一步”。****
17. 混合部署配置选择已经更新，且您已准备好进行 Exchange 服务改变与混合部署配置。单击“更新”**** 以开始配置过程。在混合配置过程进行时，向导显示正在为混合部署进行配置的各功能与服务方面，就如其已经更新过。
18. 向导将显示完成消息和“关闭”**** 按钮。单击“关闭”**** 以完成混合部署配置过程，并关闭向导。

配置 Exchange 和 Exchange Online 组织之间的 OAuth 身份验证

对于 Exchange 2013/2010 与 Exchange 2013/2007 混合部署，Office 365 和内部部署组织之间基于新混合部署 OAuth 的身份验证连接不由混合配置向导配置。默认情况下，这些部署继续使用联合身份验证信任过程。但是，邮件记录管理 (MRM)、Exchange 就地存档和就地电子数据展示等特定 Exchange 2013 功能仅当使用新的 Exchange OAuth 身份验证协议时，才在组织中完全可用。对于希望将这些功能作为 Exchange Online 混合部署一部分来实施的所有混合 Exchange 2013/2010 与 Exchange 2013/2007 组织，我们建议在使用混合配置向导配置混合部署后再配置 Exchange OAuth 身份验证。

有关详细的配置步骤，请参阅[Configure OAuth Authentication Between Exchange and Exchange Online Organizations](#)

有关使用 OAuth 身份验证的 Exchange 安全与合规性功能的详细信息，请参阅：

- [Using OAuth authentication to support Archiving in an Exchange hybrid deployment](#)
- [Using OAuth Authentication to Support eDiscovery in an Exchange Hybrid Deployment](#)

您如何知道这有效？

混合配置向导的成功完成会是混合配置步骤按预期进行的第一个指示。

为了进一步确认您已经成功创建与配置了混合部署，请执行下列操作：

- 在 Exchange 命令行管理程序中为内部部署组织运行以下命令。该命令会显示混合部署配置值与设置、混合功能与传输终结点。确认这些值正确无误。

```
Get-HybridConfiguration
```

- 通过检查混合配置日志来确认混合配置向导是否完成了所有配置步骤。默认情况下，日志位于内部部署邮箱服务器的以下位置：C:\Program Files\Microsoft\Exchange Server\V15\Logging\Update-HybridConfiguration。
- 将现有内部部署邮箱移至 Exchange Online 组织，以测试邮箱的移动功能支持；或在 Exchange Online 组织中创建新的用户邮箱，以测试两个组织之间共享的忙/闲日历信息。任一邮箱操作也会允许您测试与确认内部部署与 Exchange Online 组织之间的邮件传递是否正在与现有的邮箱一起正常工作，以及到 Exchange 组织的邮件传递是否为安全的，且是否在按内部邮件进行处理。
 - 使用 EAC 并导航到 "企业 > 收件人 > 邮箱"，在 Exchange Online 中创建新的远程邮箱。
 - 使用 EAC 并导航到 "Office 365 > 收件人 > 迁移" 以将现有邮箱移动到 Exchange Online。

在混合部署中的内部部署组织和 Exchange Online 组织之间移动邮箱

2019/6/5 •

只要具备了基于 Exchange 的混合部署，您可以选择将内部部署 Exchange 邮箱移动到 Exchange Online 组织或将 Exchange Online 邮箱移动到 Exchange 组织。当您在内部部署和 Exchange Online 组织间移动邮箱时，使用迁移批处理执行远程邮箱移动请求。这个方法不必创建用户邮箱和导入用户信息就可以移动现有邮箱。这个方法与将内部部署 Exchange 组织中的用户邮箱迁移到 Exchange Online 作为 Exchange 完整迁移到云中的一部分不同。在本话题中讨论的邮箱移动在内部部署 Exchange 和 Exchange Online 组织间的长期共存关系中是管理的 Exchange 管理的一部分。

有关将本地 Exchange 组织迁移至 Exchange Online 的详细信息，请参阅[将多个电子邮件帐户迁移至 Office 365 的方法](#)。

IMPORTANT

必须在内部部署和 Exchange Online 组织间配置一个混合部署以完成本话题中的邮箱移动过程。有关混合部署的更多信息，请参阅[Exchange Server 混合部署](#)。

IMPORTANT

在将统一消息启用 (UM) 邮箱移动到 Exchange Online 之前，您需要确保本地 Skype for Business 2015、Skype for Business Online 和 Exchange Online 都符合混合部署中指定的要求。[先决条件](#)。有关如何将本地 UM 邮箱策略映射到 Exchange Online 中的策略的信息，请参阅[Set-UMMailboxPolicy](#)。

开始前，有必要了解什么？

- 估计完成时间：用 10 分钟的时间来配置迁移批处理，但是完成迁移的总时间取决于每个迁移批处理所包括的邮箱数量。
- 您必须先获得权限，然后才能执行此过程或多个过程。若要查看所需的权限，请参阅[Recipients permissions](#)主题中的“邮箱移动和迁移权限”部分。
- 在您的内部部署和 Exchange Online 组织间配置混合部署。
- 如果您运行的是 Exchange 2013，确保已在您的内部部署 Exchange 2013 客户端访问服务器上启用了邮箱复制服务代理 (MRSPProxy)。
- 有关可能适用于本主题中的过程的键盘快捷方式的信息，请参阅[Exchange 管理中心的键盘快捷方式](#)。

TIP

是否有任何疑问？在 Exchange 论坛中寻求帮助。请访问以下论坛：[Exchange Server](#)、[Exchange Online](#)或 [Exchange Online Protection](#)。

步骤 1: 创建迁移终结点

在 Exchange 混合部署中执行场内传输和场外传输远程移动迁移前，建议您创建 Exchange 远程迁移终结点。迁移终结点包含运行 MRS 代理服务的内部部署 Exchange 服务器的连接设置，这需从 Exchange Online 执行远程移

动迁移和执行远程移动迁移到 Exchange Online。

步骤 2: 启用 MRSPProxy 服务

如果没有启用内部部署 Exchange 2013 客户端访问服务器上的 MRSPProxy 服务, 则按照 Exchange 管理中心 (EAC) 中的步骤操作:

1. 打开 EAC, 然后导航到 **服务器 > "虚拟目录"**。
2. 选择客户端访问服务器, 然后选择 **"EWS"** 虚拟目录, 然后****✎编辑图标"。
3. 选择**"已启用 MRS 代理"****** 复选框, 然后单击**"保存"******。

步骤 3: 使用 EAC 移动邮箱

您可以使用 Exchange 服务器上 EAC 中的 **"Office 365"** 选项卡上的远程移动迁移向导, 将内部部署组织中的现有用户邮箱移动到 Exchange online 组织, 或将 Exchange Online 邮箱移动到内部部署组织。选择下列过程之一:

将内部部署邮箱移动到 Exchange Online

您可以在 Exchange 服务器上的 EAC 中的 **"Office 365"** 选项卡上使用远程移动迁移向导, 将内部部署组织中的现有用户邮箱移动到 exchange Online 组织。请按以下步骤操作:

1. 打开 EAC, 然后导航到**Office 365 > 收件人 > 迁移**。
2. 单击 **"添加+添加"** 图标, 然后选择 **"迁移到 Exchange Online"**。
3. 在 **"选择迁移类型"** 页上, 选择 **"远程移动迁移"**, 然后单击 **"下一步"**。
4. 在 **"选择用户"** 页上, ****+添加图标", 然后选择要移到 Office 365 的内部部署用户并单击 **"添加"**, 然后单击 **"确定"**。单击**"下一步"**。****

NOTE

如果 **"用户选择"** 列表中未显示共享邮箱帐户, 则需要使用 Azure AD Connect 将共享邮箱本地 AD 帐户同步到 Office 365。共享邮箱 AD 帐户将在 Office 365 门户中显示为阻止的帐户, 您将能够从用户列表中选择这些帐户。""

5. 在**"输入 Windows 用户帐户凭据"****** 页上的**"本地管理员名称"****** 文本字段中, 输入本地管理员帐户名称, 然后在**"本地管理员密码"****** 文本字段中输入与此帐户关联的密码。例如, **"corp\administrator"**和密码。单击**"下一步"**。****

NOTE

如果您已经创建了一个迁移终结点, 那么就会收到此步骤的终结点确认提示。如果您创建了两个或多个迁移终结点, 那么您必须在迁移终结点下拉菜单中选择一个终结点。

6. 在 **"确认迁移终结点"** 页上, 验证向导确认迁移终结点时, 是否列出了本地 Exchange SERVER 的 FQDN。例如, **"mail.contoso.com"**。单击**"下一步"**。****

NOTE

当选择将多个邮箱移动到 Exchange Online 时, Exchange 服务器上的 MRSPProxy 服务会自动限制邮箱移动请求。完成邮箱移动操作的总时间取决于选定邮箱的总数、邮箱大小和 MRSPProxy 的配置。若要了解有关自定义 MRSPProxy 的详细信息, 请参阅[Message Throttling](#)。

7. 在 **"移动配置"** 页上的 **"新迁移批量名称"** 文本字段中, 输入迁移批处理的名称。使用向下箭头↓选择要迁

移到 **Office 365** 的邮箱的目标传递域。在大多数混合部署中, 这是用于 Exchange Online 组织邮箱的主 SMTP 域。例如, contoso.mail.onmicrosoft.com。确认已选中“移动主邮箱及存档邮箱”**** 选项, 然后单击“下一步”****。

- 在“启动批处理”**** 页上, 至少选择一个接收批处理完成报告的收件人。确认已选中“自动启动批处理”**** 选项, 然后选中“自动完成迁移批处理”**** 复选框。单击“新建”****。

NOTE

如果在步骤8中选择“手动完成批次”, Exchange Online 将仅同步该批处理中每个邮箱的 95%。Exchange Online 将定期同步批次, 以在 95% 同步时保留每个邮箱, 直到通过单击“完成此迁移批处理”手动完成批处理, 然后再单击迁移剩余 5% 的位置。

将 Exchange Online 邮箱移至内部部署组织

您可以在 Exchange 服务器上的 EAC 中的“**Office 365**”选项卡上使用远程移动迁移向导, 将内部部署组织中的现有用户邮箱移动到 exchange Online 组织:

- 打开 EAC 并导航到“**Office 365 > 收件人 > 迁移**”。
- 单击“添加+”添加图标, 然后选择“从 Exchange Online 迁移”。
- 在“选择用户”页上, 选择“选择要移动的用户”, 然后单击“下一步”。
- 在“选择用户”页上, ****+添加图标, 然后选择要移到内部部署组织的 Exchange Online 用户, 单击“添加”, 然后单击“确定”。单击“下一步”。****
- 在“确认迁移终结点”页上, 验证向导确认迁移终结点时, 是否列出了本地 Exchange SERVER 的 FQDN。例如, “mail.contoso.com”。单击“下一步”。****

NOTE

当选择将多个邮箱移动到 Exchange Online 时, Exchange 服务器上的 MRSPProxy 服务会自动限制邮箱移动请求。完成邮箱移动操作的总时间取决于选定邮箱的总数、邮箱大小和 MRSPProxy 的属性。若要了解有关自定义 MRSPProxy 的详细信息, 请参阅[Message Throttling](#)。

- 在“移动配置”页上的“新迁移批量名称”文本字段中, 输入迁移批处理的名称。然后在迁移到 **Office 365** 域的邮箱的目标传递域中输入目标传递域。在大多数混合部署中, 这是用于本地和 Exchange Online 组织邮箱的主 SMTP 域。例如, contoso.com。
- 选择是否还要移动所选用户的存档邮箱, 并在“目标数据库”文本字段中输入要将此邮箱移动到的数据库名称。例如, 邮箱数据库 123456789。单击“下一步”。****
- 在“启动批处理”**** 页上, 至少选择一个接收批处理完成报告的收件人。确认“自动启动批处理”已选中, 然后选中“自动完成迁移批处理”复选框。单击“新建”。

步骤 4: 删除已完成的迁移批处理

在邮箱移动完成后, 我们建议删除已完成的迁移批处理, 以在相同的用户再次移动时将错误的可能性降到最低。

若要删除已完成的迁移批处理, 请执行下列操作:

- 打开 EAC 并导航到“**Office 365 > 收件人 > 迁移**”。
- 单击已完成的迁移批处理, 然后单击“删除”图标。
- 在“删除警告确认”对话框中, 单击“是”。

步骤 5: 为 Web 上的 Outlook 重新启用脱机访问

当不能连接到网络时, Web 上的 Outlook 中的脱机访问(以前称为 Outlook Web App)允许用户访问他们的邮箱。如果你将 Exchange 邮箱迁移到 Exchange Online, 用户需要重置浏览器中的脱机访问设置以脱机使用 Web 上的 Outlook。有关在 Web 上的 Outlook 中脱机访问、支持脱机访问的浏览器和如何打开的详细信息, 请参阅[脱机使用 Outlook Web App](#)。

您如何知道这有效?

当在内部部署和 Exchange Online 组织间移动现有用户邮箱时, 成功完成远程移动向导初步表示, 移动邮箱按预期完成。

由于邮箱移动过程需要几分钟才能完成, 因此您还可以通过打开 EAC 并选择 " **Office 365** > 收件人 > 迁移" 来验证移动是否正常工作。迁移以显示移动状态对于在远程移动向导中选择的邮箱。在邮箱移动过程中同步****状态的值, 并在邮箱已成功移动到内部部署或 Exchange Online 组织中时完成。

邮箱移动完成后, 您可以通过验证邮箱属性来检查是否已成功移动了位于内部部署或 Exchange Online 组织中的远程邮箱。为此, 请导航到 EAC 中的 "收件人 > "邮箱, 以获取内部部署组织或 Exchange Online 组织。用户邮箱应显示适用于 Exchange Online 邮箱的**Office 365**的邮箱类型和用于本地邮箱的用户。

您也可以运行 Exchange 命令行管理程序中的以下 cmdlet 来确认迁移批处理的状态。

```
Get-MigrationBatch -Identity <batch name>
```

有疑问吗? 请在 Office 365 论坛中寻求帮助。若要访问论坛, 必须使用已拥有对基于云的服务的管理员访问权限的帐户进行登录。请访问以下论坛:[Office 365 论坛](#)

为旧版本本地公用文件夹配置混合部署

2019/6/5 •

摘要: 使用本文中的步骤在 Office 365 与 Exchange Server 2010 本地部署之间同步公用文件夹。

在混合部署中, 您的用户可以位于 Exchange Online 中或本地内, 或同时位于两者中, 并且您的公用文件夹位于 Exchange Online 中或本地内。公用文件夹只能驻留在一个位置, 因此您必须决定是否将公用文件夹放在 Exchange Online 或本地中。他们无法同时位于两者中。目录同步服务可以将公用文件夹邮箱同步至 Exchange Online 上。但是, 已启用邮件的公用文件夹无法跨界同步。

本主题介绍如果您的用户在 Office 365 中, 并且您的 Exchange Server 2010 SP3 公用文件夹是本地的, 则如何同步已启用邮件的公用文件夹。但是, 不是由内部部署的 MailUser 对象 (本地到目标公用文件夹层次结构) 未表示的 Office 365 用户不能访问旧版或新式的本地公用文件夹。

NOTE

本主题将 Exchange Server 2010 SP3 服务器称为旧版 Exchange server。

您将使用以下脚本同步已启用邮件的公用文件夹, 这些脚本由在本地环境中运行的 Windows 任务启动:

- `Sync-MailPublicFolders.ps1`: 此脚本将已启用邮件的公用文件夹对象从本地 Exchange 内部部署与 Office 365 同步。该脚本将本地 Exchange 本地部署用作主机来确定需要应用于 O365 的更改。该脚本将基于本地 Exchange 部署中存在的內容创建、更新或删除 O365 Active Directory 中已启用邮件的公用文件夹对象。
- `SyncMailPublicFolders.strings.ps1`: 这是前面的同步脚本使用的支持文件, 应将其复制到与上述脚本相同的位置。

当您完成此过程时, 您的本地和 Office 365 用户将可以访问相同的本地公用文件夹基础结构。

Exchange 的哪个混合版本可以和公用文件夹一起使用?

下表介绍了用户邮箱和受支持的公用文件夹的版本和位置组合。"混合不适用"仍然是一个受支持的方案, 但是由于公用文件夹和用户驻留在相同位置, 因此它不再被认为是一个混合方案。

	内部部署 EXCHANGE 2010 用户邮箱	内部部署 EXCHANGE 2013 用户邮箱	EXCHANGE ONLINE 用户邮箱
内部部署 Exchange 2010 公用文件夹	混合不适用	混合不适用	支持
内部部署 Exchange 2013 公用文件夹	混合不适用	混合不适用	支持
Exchange Online 公用文件夹	不支持	支持	混合不适用

不支持包含 Exchange 2003 公用文件夹的混合配制。如果您的组织中运行的是 Exchange 2003, 则必须将所有公用文件夹数据库和副本移动到 Exchange 2010 SP3 或更高版本。Exchange 2003 中不能保留公用文件夹副本。

NOTE

Outlook 2016 不支持访问 Exchange 2007 旧版公用文件夹。如果您有使用 Outlook 2016 的用户, 则必须将公用文件夹移动到 Exchange Server 的更新版本。可在[本文](#)找到有关 Outlook 2016 和 Office 2016 与 Exchange 2007 及更早版本兼容性的详细信息。

步骤 1: 开始之前, 您必须知道什么?

- 这些说明假定您已使用 "混合配置" 向导来配置和同步内部部署和 Exchange Online 环境, 并且大多数用户使用的用于自动发现服务的 DNS 记录都引用本地终结点。有关详细信息, 请参阅["混合配置"向导](#)。
 - 这些说明假定 Outlook 无处不在所有本地旧版 Exchange 公用文件夹服务器上启用并正常运行。有关如何启用 Outlook 无处不在的信息, 请参阅[Outlook 无处不在](#)。
 - 对 Exchange 与 Office 365 的混合部署实施旧公用文件夹共存可能需要在导入过程中解决冲突。发生冲突的原因是分配给启用邮件的公用文件夹的非路由电子邮件地址与 Office 365 中的其他用户和组冲突, 以及其他原因。
 - 这些说明假定您的 Exchange Online 组织已升级到支持公用文件夹的版本。
 - 在 Exchange Online 中, 您必须是"组织管理"角色组的成员。该角色组与订阅 Exchange Online 时分配给您的权限不同。有关如何启用 "组织管理" 角色组的信息, 请参阅[Manage Role Groups](#)。
 - 在 Exchange 2010 中, 您必须是"组织管理"或"服务器管理"RBAC 角色组的成员。有关详细信息, 请参阅[向角色组添加成员](#)。
 - 若要跨内部部署访问公用文件夹, 用户必须将其 Outlook 客户端升级到2012年11月的 Outlook 公共更新或更高版本。
1. 若要下载 2012 年 11 月发布的适用于 Outlook 2010 的 Outlook 更新程序, 请参阅 [Microsoft Outlook 2010 更新 \(KB2687623\) 32 位版本](#)。
 2. 若要下载 2012 年 11 月发布的适用于 Outlook 2007 的 Outlook 更新程序, 请参阅 [Microsoft Office Outlook 2007 更新 \(KB2687404\)](#)。
- 不支持使用 Outlook 2016 for Mac(及早期版本)和适用于 Office 365 的 Outlook for Mac 访问跨界部署旧式公用文件夹。用户必须转到公用文件夹所在的位置, 才能使用 Outlook for Mac 或适用于 Office 365 的 Outlook for Mac 访问这些公用文件夹。此外, 邮箱位于 Exchange Online 中的用户将无法使用 Outlook Web App 访问本地公用文件夹。
 - 按照本文中的说明操作, 为混合部署配置内部部署公用文件夹, 除非您执行其他步骤, 否则组织外部的用户将无法向内部部署公用文件夹发送邮件。您可以将公用文件夹的接受域设置为内部中继 (请参阅[在 Exchange Online 中管理接受的域](#)) 或禁用基于目录的边缘阻止 (DBEB) (请参阅[使用基于目录的边缘阻止拒绝发送的邮件收件人无效](#))。

步骤 2: 使远程公用文件夹可见

1. 如果公用文件夹位于 Exchange 2010 或更高版本的服务器上, 则必须在具有公用文件夹数据库的所有邮箱服务器上安装客户端访问服务器 (CAS) 角色。这允许运行 Microsoft Exchange Set-rpcclientaccess 服务, 以便所有客户端都可以访问公用文件夹。有关详细信息, 请参阅[安装 Exchange Server 2010](#)。

NOTE

客户端负载平衡不需要包含此服务器。有关详细信息, 请参阅[了解 Exchange 2010 中的负载平衡](#)。

2. 在每个公用文件夹服务器上创建一个空的邮箱数据库。

对于 Exchange 2010, 运行以下命令。此命令会将邮箱数据库从邮箱配置负载均衡器中排除。这将阻止新邮箱自动添加到此数据库。

```
New-MailboxDatabase -Server <PFServerName_with_CASRole> -Name <NewMDBforPFs> -  
IsExcludedFromProvisioning $true
```

NOTE

我们建议您只将在步骤 3 中创建的代理邮箱添加至此数据库。不应在此邮箱数据库中创建任何其他邮箱。

3. 在新邮箱数据库中创建代理邮箱, 并将邮箱从通讯簿中隐藏。此邮箱的 SMTP 将由自动发现作为 _DefaultPublicFolderMailbox_ SMTP 返回, 因此, 通过解析此 smtp, 客户端可以访问旧版 exchange server 来访问公用文件夹。

```
New-Mailbox -Name <PFMailbox1> -Database <NewMDBforPFs>
```

```
Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled $true
```

4. 对于 Exchange 2010, 启用自动发现以返回代理公用文件夹邮箱。

```
Set-MailboxDatabase <NewMDBforPFs> -RPCClientAccessServer <PFServerName_with_CASRole>
```

5. 对组织中的每个公用文件夹服务器重复执行前面的步骤。

步骤 3: 下载脚本

1. 从[启用邮件的公用文件夹 - 目录同步脚本](#)中下载以下文件:

- Sync-MailPublicFolders.ps1
- SyncMailPublicFolders.strings.psd1

2. 将这些文件保存到将要运行 PowerShell 的本地计算机中。例如, C:\PFScripts。

步骤 4: 配置目录同步

目录同步服务不对启用邮件的公用文件夹进行同步。运行以下两个脚本可以对已启用邮件的跨界公用文件夹进行同步。分配给已启用邮件的公用文件夹的特殊权限将需要在云中重新创建, 因为跨界权限在混合部署方案中不受支持。有关详细信息, 请参阅[Exchange 混合部署文档](#)。

NOTE

已同步的启用邮件的公用文件夹将显示为邮件联系人对象, 用于处理邮件流, 并且不会在 Exchange 管理中心 中显示。请参阅 Get-MailPublicFolder 命令。要重新创建云中的 SendAs 权限, 请使用 Add-RecipientPermission 命令。

1. 在旧版 Exchange 服务器上, 运行以下命令将启用邮件的公用文件夹从本地 Active Directory 同步到 O365 中。

```
Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile:sync_summary.csv
```

其中 `Credential` , 是您的 Office 365 用户名和密码, `CsvSummaryFile` 是您希望以 .csv 格式记录同步操作和错误的位置的路径。

NOTE

在运行脚本之前, 我们建议您首先模拟脚本在您的环境中执行的操作, 如上面的 `-WhatIf` 开关所述。我们还建议您每天都运行此脚本以同步启用邮件的公用文件夹。

步骤 5: 配置 Exchange Online 用户以访问本地公用文件夹

此过程中的最后一步是配置 Exchange Online 组织并允许访问旧版本本地公用文件夹。

允许 Exchange Online 组织访问本地公用文件夹。您可以指向在 [步骤 2: 使远程公用文件夹可见](#) 中创建的所有代理公用文件夹邮箱。

在 **Windows PowerShell** 中运行以下命令：

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicFolderMailboxes  
PFMailbox1,PFMailbox2,PFMailbox3
```

您必须等待 ActiveDirectory 同步完成才能查看更改。此过程可能需要 3 个小时才能完成。如果您不想等待每隔三小时进行一次定期同步, 可以随时强制执行目录同步。有关强制执行目录同步的详细步骤, 请参阅[强制执行目录同步](#)。Office 365 随机选择此命令中提供的一个公用文件夹邮箱。

IMPORTANT

不是由 MailUser 本地对象代表的 Office 365 用户(对目标公用文件夹层次结构是本地的)不能访问旧版或 Exchange 2013 本地公用文件夹。请参阅知识库文章 [Exchange 联机用户不能访问旧版本本地公用文件夹](#) 查找解决方案。

我如何知道这有效？

1. 登录到适用于 Exchange Online 中的用户的 Outlook, 然后运行以下公用文件夹测试:

- 查看层次结构。
- 检查权限。
- 创建和删除公用文件夹。
- 发布内容到公用文件夹并从公用文件夹删除内容。

为 Exchange 2013 公用文件夹配置混合部署

2019/6/5 •

摘要：允许 Exchange Online 用户访问 Exchange 2013 环境中的本地公用文件夹的说明。

在混合部署中，您的用户可以位于 Exchange Online 中，或内部部署内，或同时位于两者中，并且您的公用文件夹位于 Exchange Online 中或内部部署内。有时，您的联机用户可能需要访问 Exchange Server 2013 内部部署环境中的公用文件夹。同样，Exchange 2013 用户可能需要访问 Office 365 或 Exchange Online 中的公用文件夹。

NOTE

如果您有 Exchange 2010 公用文件夹，请参阅[配置旧版本本地公用文件夹以进行混合部署](#)。

本文介绍如何允许 Exchange Online/Office 365 用户访问 Exchange 2013 中的公用文件夹。若要允许本地 Exchange 2013 用户访问 Exchange Online 中的公用文件夹，请参阅[配置 Exchange Online 公用文件夹以实现混合部署](#)。

必须由 Exchange 本地环境中的 MailUser 对象来表示 Exchange Online/Office 365 用户，才能访问 Exchange 2013 公用文件夹。此 MailUser 对象还必须是目标 Exchange 2013 公用文件夹层次结构的本地对象。如果你的 Office 365 用户目前不是由 MailUser 对象进行本地表示，请参阅 Microsoft 知识库文章 3106618“[Exchange Online 用户无法访问旧的本地公用文件夹](#)”来创建匹配的本地实体。

开始前，有必要了解什么？

1. 这些说明假定您已经使用混合配置向导对您的内部部署和 Exchange Online 环境进行配置和同步，并且假定用于多数用户的自动发现的 DNS 记录可以引用一个内部部署终结点。有关详细信息，请参阅[“混合配置”向导](#)。
2. 无法使用 OWA 访问此配置中的公用文件夹。
3. 对 Exchange 与 Office 365 的混合部署实施公用文件夹共存可能需要在导入过程中解决冲突。冲突可能是由于分配给启用邮件的公用文件夹的不可路由电子邮件地址，或者与 Office 365 中的其他用户和组冲突及其他属性所致。
4. 为了能够跨界访问公用文件夹，用户必须将其 Outlook 客户端升级至 2012 年 11 月的 Outlook 公共更新或更高版本。
5. 若要下载 2012 年 11 月发布的适用于 Outlook 2010 的 Outlook 更新程序，请参阅[Microsoft Outlook 2010 更新 \(KB2687623\) 32 位版本](#)。
6. Outlook 2011 for Mac 和 Outlook for Mac for Office 365 不受跨界公用文件夹的支持。用户必须与公用文件夹位于相同位置，才能通过 Outlook 2011 for Mac 或 Outlook for Mac for Office 365 访问这些公用文件夹。此外，使用 Exchange Online 邮箱的用户将无法使用 Outlook Web App 访问本地公用文件夹。

NOTE

Outlook 2016 for Mac 支持跨界部署公用文件夹。如果组织中的客户使用 Outlook 2016 for Mac，请确保他们安装了 2016 年 4 月发布的更新程序。否则，这些用户将无法访问混合拓扑中的公用文件夹。有关详细信息，请参阅[通过 Outlook 2016 for Mac 访问公用文件夹](#)。

步骤 1: 下载脚本

1. 从[启用邮件的公用文件夹 - 目录同步脚本](#)中下载以下文件：

- `Sync-MailPublicFolders.ps1`
- `SyncMailPublicFolders.strings.ps1`

2. 将这些文件保存到将要运行 PowerShell 的本地计算机中。例如，C:\PFScripts。

步骤 2: 配置目录同步

目录同步服务不对启用邮件的公用文件夹进行同步。运行以下两个脚本可以对已启用邮件的跨界和 Office 365 公用文件夹进行同步。分配给已启用邮件的公用文件夹的特殊权限将需要在云中重新创建，因为跨界权限在混合部署方案中不受支持。有关详细信息，请参阅[Exchange 混合部署文档](#)。

NOTE

已同步的启用邮件的公用文件夹将显示为邮件联系人对象，用于处理邮件流，并且不会在 EExchange 管理中心 中显示。请参阅 `Get-MailPublicFolder` 命令。要重新创建云中的 SendAs 权限，请使用 `Add-RecipientPermission` 命令。

在 Exchange 2013 服务器上，运行以下命令将启用邮件的公用文件夹从内部部署 Active Directory 同步到 O365 中。

```
.\Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile:sync_summary.csv
```

其中 `Credential`，是您的 Office 365 用户名和密码，`CsvSummaryFile` 是您希望以 .csv 格式记录同步操作和错误的位置的路径。

NOTE

在运行脚本之前，我们建议您首先模拟脚本在您的环境中执行的操作，如上面的 `-WhatIf` 开关所述。我们还建议您每天都运行此脚本以同步启用邮件的公用文件夹。

步骤 3: 配置 Exchange Online 用户以访问 Exchange 2013 本地公用文件夹

该程序的最后一步是配置 Exchange Online 组织并允许访问 Exchange 2013 公用文件夹。

允许 Exchange Online 组织访问本地公用文件夹。您将指向所有本地公用文件夹邮箱。

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicFolderMailboxes  
PFMailbox1,PFMailbox2,PFMailbox3
```

NOTE

您必须等待 ActiveDirectory 同步完成才能查看更改。此过程可能需要 3 个小时才能完成。如果您不想等待每隔三小时进行一次定期同步，可以随时强制执行目录同步。有关强制执行目录同步的详细步骤，请参阅[强制执行目录同步](#)。

我如何知道这有效？

1. 登录到位于 Exchange Online 内的用户的 Outlook，并执行以下公用文件夹测试：

- 查看层次结构。

- 检查权限
- 创建和删除公用文件夹。
- 发布内容到公用文件夹并从公用文件夹删除内容。

为 Exchange Online 公用文件夹配置混合部署

2019/6/5 •

摘要: 有关允许本地 Exchange 2013 用户访问 Exchange Online 中的公用文件夹的说明。

在混合部署中, 您的用户可以位于 Exchange Online 中, 或内部部署内, 或同时位于两者中, 并且您的公用文件夹位于 Exchange Online 中或内部部署内。有时, 您的联机用户可能需要访问 Exchange Server 2013 内部部署环境中的公用文件夹。同样, Exchange 2013 用户可能需要访问 Office 365 或 Exchange Online 中的公用文件夹。

本文介绍了如何允许 Exchange 2013 本地环境中的用户访问 Exchange Online/Office 365 公用文件夹。若要允许 Exchange Online/Office 365 用户访问本地 Exchange 2013 公用文件夹, 请参阅[针对混合部署配置 Exchange 2013 公用文件夹](#)。

NOTE

如果您有 Exchange 2010 公用文件夹, 请参阅[配置旧版本本地公用文件夹以进行混合部署](#)。

开始前, 有必要了解什么?

1. 这些说明假定您已经使用混合配置向导对您的内部部署和 Exchange Online 环境进行配置和同步, 并且假定用于多数用户的自动发现的 DNS 记录可以引用一个内部部署终结点。有关详细信息, 请参阅["混合配置"向导](#)。
2. 这些说明假定 Outlook 无处不在已启用, 并且在内部部署 Exchange Server 上正常运行。有关如何启用 Outlook 无处不在的信息, 请参阅[Outlook 无处不在](#)。
3. 对 Exchange 与 Office 365 的混合部署实施公用文件夹共存可能需要在导入过程中解决冲突。冲突可能是由于分配给启用邮件的公用文件夹的不可路由电子邮件地址, 或者与 Office 365 中的其他用户和组冲突及其他属性所致。
4. 为了能够跨界访问公用文件夹, 用户必须将其 Outlook 客户端升级至 2012 年 11 月的 Outlook 公共更新或更高版本。
5. 若要下载 2012 年 11 月发布的适用于 Outlook 2010 的 Outlook 更新程序, 请参阅[Microsoft Outlook 2010 更新 \(KB2687623\) 32 位版本](#)。
6. 若要下载 2012 年 11 月发布的适用于 Outlook 2007 的 Outlook 更新程序, 请参阅[Microsoft Office Outlook 2007 更新 \(KB2687404\)](#)。
7. Outlook 2011 for Mac 和 Outlook for Mac for Office 365 不受跨界公用文件夹的支持。用户必须与公用文件夹位于相同位置, 才能通过 Outlook 2011 for Mac 或 Outlook for Mac for Office 365 访问这些公用文件夹。此外, 使用 Exchange Online 邮箱的用户将无法使用 Outlook Web App 访问内部部署公用文件夹。

NOTE

Outlook 2016 for Mac 支持跨界部署公用文件夹。如果组织中的客户使用 Outlook 2016 for Mac, 请确保他们安装了 2016 年 4 月发布的更新程序。否则, 这些用户将无法访问共存或混合拓扑中的公用文件夹。有关详细信息, 请参阅[通过 Outlook 2016 for Mac 访问公用文件夹](#)。

步骤 1: 下载脚本

1. 从 [Mail-enabled Public Folders - directory sync from EXO to On-prem script](#) (启用邮件的公用文件夹 - 将目录从 EXO 同步到本地的脚本) 下载以下文件。

- `Import-PublicFolderMailboxes.ps1`
- `ImportPublicFolderMailboxes.strings.psd1`
- `Sync-MailPublicFoldersCloudToOnprem.ps1`
- `Sync-MailPublicFoldersCloudToOnprem.strings.psd1`

2. 将这些文件保存到将要运行 PowerShell 的本地计算机中。例如, C:\PFScripts。

步骤 2: 配置目录同步

运行此脚本 `Sync-MailPublicFoldersCloudToOnprem.ps1` 会在 exchange Online 和 exchange 2013 本地环境之间同步已启用邮件的公用文件夹。必须在云中重新创建分配给启用邮件的公用文件夹的特殊权限, 因为混合部署方案不支持跨界部署权限。有关详细信息, 请参阅[Exchange 混合部署文档](#)。

NOTE

已同步的启用邮件的公用文件夹将显示为邮件联系人对象, 用于处理邮件流, 并且不会在 Exchange 管理中心中显示。请参阅 `Get-MailPublicFolder` 命令。要重新创建云中的 SendAs 权限, 请使用 `Add-RecipientPermission` 命令。

1. 在 Exchange 2013 服务器上, 运行以下命令, 将启用邮件的公用文件夹从 Exchange Online/Office 365 同步到本地 Active Directory。

```
Sync-MailPublicFoldersCloudToOnprem.ps1 -Credential (Get-Credential)
```

其中 *Credential* 是您的 Office 365 用户名和密码。

NOTE

我们建议每天运行一次这段脚本, 以同步启用邮件的公用文件夹。

第 3 步: 将本地用户配置为访问 Exchange Online 公用文件夹

此过程的最后一步是将 Exchange 2013 本地组织配置为允许访问 Exchange Online 公用文件夹。

运行此脚本 `Import-PublicFolderMailboxes.ps1` 会将公用文件夹邮箱对象从云中导入为本地环境中已启用邮件的用户。此脚本还会将导入的对象配置为远程公用文件夹邮箱。

1. 在 Exchange 2013 服务器上, 运行以下命令, 将公用文件夹邮箱对象从云中导入本地 Active Directory。

```
Import-PublicFolderMailboxes.ps1 -Credential (Get-Credential)
```

其中, *Credential* 是你的 Office 365 用户名和密码。

NOTE

我们建议每天运行一次这段脚本, 以导入公用文件夹邮箱对象, 因为只要公用文件夹邮箱达到阈值容量, 就会自动拆分为多个新邮箱。因此, 你总是要确保从云中导入的是最新公用文件夹邮箱。

2. 允许 Exchange 2013 本地组织访问 Exchange Online 公用文件夹。

```
Set-OrganizationConfig -PublicFoldersEnabled Remote
```

NOTE

您必须等待 ActiveDirectory 同步完成才能查看更改。此过程可能需要 3 个小时才能完成。如果您不想等待每隔三小时进行一次定期同步, 可以随时强制执行目录同步。有关强制执行目录同步的详细步骤, 请参阅[强制执行目录同步](#)。

我如何知道这有效？

1. 登录到位于 Exchange Online 内的用户的 Outlook, 并执行以下公用文件夹测试:

- 查看层次结构。
- 检查权限
- 创建和删除公用文件夹。
- 发布内容到公用文件夹并从公用文件夹删除内容。

配置 Exchange 在混合部署支持委派的邮箱权限

2019/6/5 •

委派的邮箱权限使某人能够管理其他用户的邮箱的某些部分。一个常见的例子是行政助理人员需要管理经理的邮箱和日历。内部部署 Exchange 组织与 Office 365 之间的混合部署支持 "完全访问" 和 "代表代理发送" 邮箱权限。但是, 根据已经安装在您的内部组织的 Exchange 的版本, 您可能需要执行其他配置, 以在部署中混合使用委派的邮箱权限。下面列出了支持委派邮箱权限中混合部署, 该版本是否需要额外的配置版本的 Exchange。

- **Exchange 2016:** 需要其他配置。
- **Exchange 2013:** 支持的 exchange 2013 累积更新 (CU) 和其他配置是必需的。
- **Exchange 2010:** 支持的 exchange 2010 更新辑 (RU) 和其他配置是必需的。

有关在混合部署中支持委派邮箱权限的特定要求的详细信息, 请参阅[Exchange 混合部署中的权限](#)。

以下各节将引导您完成配置的 Exchange 2013 和 Exchange 2010 内部部署启用委派的邮箱权限的支持。执行这些步骤之前, 您需要确保您在最新的 Exchange 2013 CU 或 Exchange SP3 RU。有关详细信息, 请参阅[混合部署先决条件](#)。

Exchange 2013 和 Exchange 2016

您需要执行操作来启用委派的邮箱权限的支持取决于几个因素。如果向 Office 365 和当时移动邮箱:

以下被安装...	而该组织中的 ACLABLE 对象同步...	然后您需要...
交换 2013 CU9 或更早版本	此功能不是用交换 2013 CU9 及更早版本。	手动配置每个邮箱, 以支持 Acl
交换 2013 CU10 或更高版本	已禁用	启用在组织级别应用的 ACLable 对象同步 手动启用每个 ACLable 对象同步在组织级别启用之前移动到 Office 365 的邮箱上的 Acl。 邮箱移动到 Office 365, ACLable 对象同步在组织级别启用后才不需要任何额外的配置。
交换 2013 CU10 或更高版本	已启用	不需要进行任何其他配置
Exchange 2016	已禁用	启用在组织级别应用的 ACLable 对象同步 手动启用每个 ACLable 对象同步在组织级别启用之前移动到 Office 365 的邮箱上的 Acl。 邮箱移动到 Office 365, ACLable 对象同步在组织级别启用后才不需要任何额外的配置。
Exchange 2016	已启用	不需要进行任何其他配置

启用 ACLable 对象同步

要启用在组织级别应用的 ACLable 对象同步, 请执行以下操作。

1. 在所有您 AAD 连接的服务器上安装 Azure 活动目录连接 (AAD 连接) 的最新版本。这被需要允许 AAD 连接同步支持混合权限所需的属性。可以从[Microsoft Azure 活动目录连接](#)下载 AAD 连接。
2. 在运行最新可用 CU 的 Exchange 2013 或 Exchange 2016 服务器上打开 Exchange 命令行管理程序, 或直接上一个的 CU。
3. 运行以下命令。

```
Set-OrganizationConfig -ACLableSyncedObjectEnabled $True
```

执行此操作后, 将移到 Office 365 的所有邮箱将正确都配置以支持委派的邮箱的权限。如果邮箱已移动到 Office 365 在您完成这些步骤之前, 您需要手动启用这些邮箱[启用远程邮箱的 Acl](#)中使用步骤上的 Acl。

IMPORTANT

Ad 不启用远程创建 Office 365 中的邮箱。如果您在 Office 365 中创建远程邮箱, 您需要远程邮箱节, 以启用该远程邮箱 Acl 并遵照启用 Acl 中的步骤操作。若要避免此额外步骤, 我们建议您在本地 Exchange 服务器上创建邮箱, 然后将邮箱移动到 Office 365。

启用远程邮箱的 Acl

要启用在组织级别启用 ACLable 对象同步之前移动到 Office 365 的邮箱上的 Acl, 请执行以下操作。

1. 在运行最新可用 CU 的 Exchange 2013 或 Exchange 2016 服务器上打开 Exchange 命令行管理程序, 或直接上一个的 CU。
2. 若要启用单个邮箱上的 Acl, 请运行以下命令:

```
Get-AdUser <Identity> | Set-AdObject -Replace @{msExchRecipientDisplayType=-1073741818}
```

3. 若要在移动到 Office 365 的所有邮箱上启用 Acl, 请运行以下命令:

```
Get-RemoteMailbox -ResultSize unlimited | ForEach {Get-AdUser -Identity $_.Guid | Set-ADObject -Replace @{msExchRecipientDisplayType=-1073741818}}
```

4. 若要验证是否已成功更新邮箱, 请运行以下命令:

```
Get-RemoteMailbox -ResultSize unlimited | ForEach {Get-AdUser -Identity $_.Guid -Properties msExchRecipientDisplayType | Format-Table DistinguishedName,msExchRecipientDisplayType -Auto}
```

Exchange 2010

远程邮箱的 Exchange 2010 SP3 服务器支持的 Acl 配置, 但是, 这种配置需要手动设置每个邮箱。与不同的较新版本的 Exchange 中, Exchange 2010 不提供在组织级别设置此功能的能力。您需要执行下列步骤, 您以前已移动到 Office 365 的所有邮箱和将被移动从 Exchange 2010 SP3 服务器到 Office 365 将来任何邮箱上。

启用远程邮箱的 Acl

要启用移动到 Office 365 的邮箱上的 Acl, 请执行以下操作。

1. 打开 Exchange 管理外壳程序运行最新版本可用 Exchange 2010 SP3 RU 或立即以前 RU 的服务器上。
2. 若要启用单个邮箱上的 Acl, 请运行下面的命令。

```
Get-AdUser <Identity> | Set-AdObject -Replace @{msExchRecipientDisplayType=-1073741818}
```

3. 若要启用对所有邮箱移到 Office 365 的 Acl, 请运行下面的命令。

```
Get-RemoteMailbox -ResultSize unlimited | ForEach {Get-AdUser -Identity $_.Guid | Set-ADObject -Replace @{msExchRecipientDisplayType=-1073741818}}
```

4. 要验证已成功更新邮箱, 请运行下面的命令。

```
Get-RemoteMailbox -ResultSize unlimited | ForEach {Get-AdUser -Identity $_.Guid -Properties msExchRecipientDisplayType | Format-Table DistinguishedName,msExchRecipientDisplayType -Auto}
```

通过 OneDrive for Business 和本地 Exchange 2016 配置新式附件

2019/6/5 •

摘要：如何允许本地 Exchange Server 2016 用户在混合配置期间利用 OneDrive for Business 和 SharePoint Online 的文档协作。

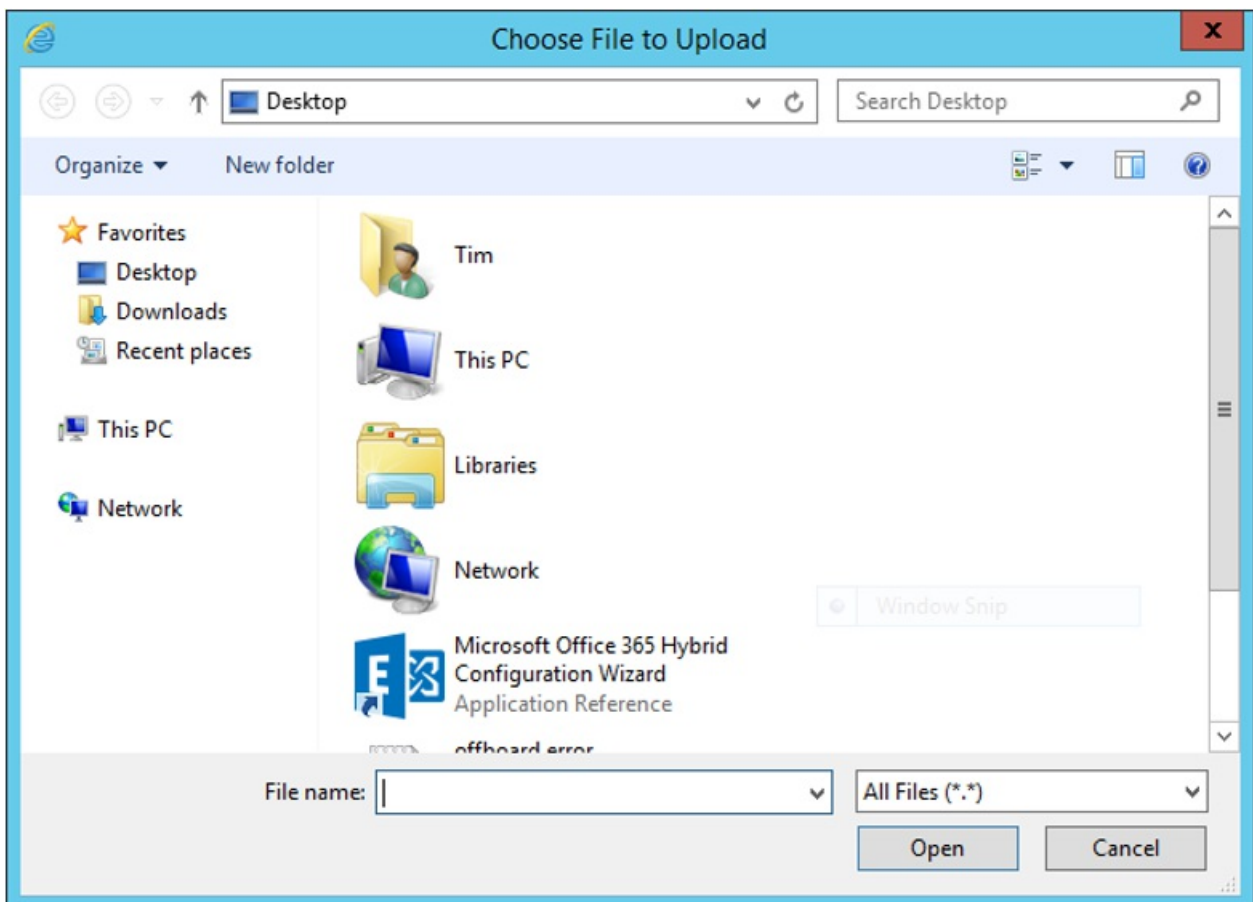
最近，在 Office 365 中推出了新的附件选项。在 Exchange 2016 中，该选项被称为“文档协作”，它允许本地用户将存储在 OneDrive for Business 上的附件与其 Outlook 网页版客户端直接集成。

NOTE

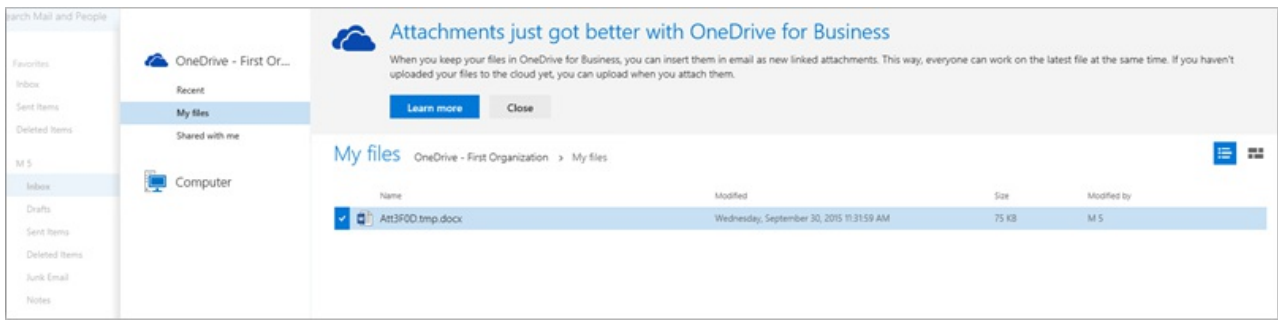
从 Exchange Server 2016 的发布开始，Outlook Web App 现在被称为 Outlook 网页版。

通常情况下，用户通过将文件附加到邮件向他人发送该文件。然后，一个或多个收件人在其各自的文件副本中进行更改，最终需要在某个时刻将所有这些文件进行合并。此外，这些附加的文件会占用每个用户邮箱的存储空间。通过文档协作，用户改为向存储在 OneDrive for Business 帐户中的文件插入链接，以使文件可在相同源位置由多个人人员进行编辑，而无需额外存储。

为文档协作正确配置 Exchange 2016 环境前，Outlook 网页版用户的默认附件对话框将类似于：



使用以下说明配置环境后，Outlook 网页版附件对话框将类似于：



组织中具有本地邮箱的用户以及在 Office 365 中具有 OneDrive for Business 帐户的用户有权使用新式的附件方法，允许他们与多个收件人共享存储在 OneDrive for Business 中的文档。收件人的位置（联机和本地）无关紧要。

在 [Exchange Server 混合部署](#) 中了解有关混合部署的详细信息。

在开始之前，您需要知道什么？

- 估计完成时间：15 分钟
- 检查 [Exchange Server 混合部署](#) 主题，并确保您清楚会受到配置混合部署影响的方面。
- 检查并完成 [混合部署先决条件](#) 概括的所有混合部署要求。
- 有关可能适用于本主题中的过程的键盘快捷方式的信息，请参阅[Exchange 管理中心的键盘快捷方式](#)。

TIP

是否有任何疑问？在 Exchange 论坛中寻求帮助。请访问以下论坛：[Exchange Server](#)、[Exchange Online](#)或 [Exchange Online Protection](#)。

在混合环境中配置 Exchange 2016 以启用文档协作

验证以下先决条件步骤已完成，然后使用下面的过程启用文档协作。

先决条件：

- 使用 ["混合配置"向导 \(HCW\)](#) 配置 Exchange 混合环境。
- Exchange 2016 必须安装在本地组织中。Exchange 2016 可与早期版本的 Exchange 共存，但文档协作适用于 Exchange 2016 服务器上的邮箱。
- 必须安装身份验证服务器并同步所有用户。可使用 [Get-AuthServer](#) cmdlet 查找身份验证服务器。我们建议使用来自 Exchange 2016 服务器的 HCW 对 OAuth 进行必要的配置。

IMPORTANT

需要正确配置 Exchange 2016 和 Office 365 之间的 OAuth。有关详细信息，请参阅 [Configure OAuth Authentication Between Exchange and Exchange Online Organizations](#)。

- 用户必须拥有正确的许可证。具有 OneDrive for Business 帐户的用户需获得 SharePoint Online 或 OneDrive for Business 的授权。可通过在 Office 365 门户中选择用户，并选择“编辑”按钮来验证用户的许可证。

NOTE

有关详细信息，请参阅 [Set up OneDrive for Business in Office 365](#)（在 Office 365 中设置 OneDrive for Business）。

执行以下步骤：

1. 配置默认 Outlook 网页版邮箱策略以设置 OneDrive for Business 宿主 URL。

NOTE

可转到 Office 365 SharePoint Online 租户管理，以检索 OneDrive for Business 宿主 URL。例如，https://contoso-my.sharepoint.com 是 Contoso 的 O365 租户中的“我的网站”URL。> 尽管 Exchange 2016 随附的 Outlook 网页版邮箱策略称为“默认”策略，但它不会自动应用到任何邮箱，除非将其设置为默认策略或直接将其分配到某个邮箱。

使用以下示例作为基础，使用 Exchange 命令行管理程序 在默认 Outlook 网页版邮箱策略上配置内部和外部“我的网站”URL：

```
Set-OwaMailboxPolicy Default -InternalSPMySiteHostURL https://Contoso-my.sharepoint.com -  
ExternalSPMySiteHostURL https://Contoso-my.sharepoint.com
```

2. 接下来，将刚配置的策略设置为默认策略，以使其应用于所有邮箱，或将策略分配到个人用户。

若要将该策略作为 Outlook 网页版邮箱策略的默认策略，请在 Exchange 命令行管理程序 中键入以下命令。

```
Set-OwaMailboxPolicy Default -IsDefault
```

若要向个人邮箱分配策略，请在 Exchange 命令行管理程序 中键入以下命令：

```
Set-CASMailbox <user mailbox> -OwaMailboxPolicy Default
```

3. (可选)在每个 Exchange 2016 服务器上，重启 **OWAApplicationPool**，这将可以使配置立即生效。如果不运行此命令，则 Exchange 2016 服务器需要几分钟应用更新的邮件策略。在 Exchange 命令行管理程序 中，运行：

```
Restart-WebAppPool MSExchangeOWAAppPool
```

配置完成后，Outlook 网页版用户将可以选择想要应用到其邮件的附件类型：传统或新式。

Share with OneDrive or send as attachment




Share with OneDrive

Recipients see the latest changes and can work together in real time.



Send as attachment

Recipients get a copy to review.

☐ Remember my choice for files from OneDrive 

使用本地 Exchange 混合配置 Office 365 组

2019/6/5 •

了解如何使本地 Exchange 用户在混合部署中使用 Office 365 组。

组是 Office 365 的一项服务，它使团队能够更轻松地进行通信、安排会议以及就文档进行协作。任何组成员都可使用与组共享的所有信息，包括从发送到组的电子邮件到存储在组的 OneDrive for Business 或 SharePoint 库中的文件。如果已在本地 Exchange 组织和 Office 365 之间配置了混合部署，则可按照本主题中的步骤使在 Office 365 中创建的组对本地用户可用。

IMPORTANT

对 Exchange 混合部署中的本地用户使用 Office 365 组是一项新功能。因为是新功能，所以可能会在设置时遇到一些问题。请务必查看本主题结尾的[已知问题](#)部分，了解可能遇到的问题的修复方法。

先决条件

开始前，请确保完成以下操作：

- 已为租户购买 Azure Active Directory Premium 许可证。这是在 Azure Active Directory Connect 中启用组写回功能所必需的。
- 已在 Exchange 本地组织和 Office 365 之间配置混合部署并验证它能够正常运行。有关 Exchange 混合部署的详细信息，请参阅以下内容：
 - [Exchange Server 混合部署](#)
 - [混合部署先决条件](#)
- 在 CU1 和较新版本的 Exchange 2016，以及 CU11 和较新版本的 Exchange 2013 中提供了与 Office 365 组集成的安装了受支持 Exchange 版本的本地 Exchange。但是，Exchange 混合需要在本地 Exchange 服务器上安装最新的 Exchange 2013 或 Exchange 2016 累积更新 (CU)。如果不能安装最新的 CU，也可使用当前 CU 的上一发布更新。
- 配置的单一登录使用 Azure Active Directory Connect (Azure AD Connect)。需要这些信息来允许用户单击“查看组文件”或组电子邮件中的云附件链接。

在 Exchange 混合部署中为单一登录配置 Azure AD 连接时，建议使用密码同步。在下列情况下，应仅使用 Active Directory 联合身份验证服务 (AD FS)：你在大型组织中、你有一个复杂的本地 Active Directory 部署（例如，多个 Active Directory 林）、另一个 Microsoft 产品需要 AD FS 与 Office 365 配合使用，或者因为合规性策略无法同步本地网络之外的密码。有关单一登录的详细信息，请参阅[选择用于将本地 Active Directory 与 Azure 集成的解决方案](#)。

启用 Azure AD Connect 中的组写回

1. 打开“Azure AD 连接向导”，选择“配置”，然后单击“下一步”。
2. 选择“自定义同步选项”，然后单击“下一步”。
3. 在“连接到 AZURE AD”页上，输入 Office 365 凭据。单击“下一步”。
4. 在“可选功能”页上，验证以前配置的选项是否仍处于选中状态。最常选择的选项是“Exchange 混合”和“密码哈希同步”。

5. 选择 "组写回 (预览)", 然后单击 "下一步"。
6. 在 "写回" 页上, 选择 Active Directory 组织单位 (OU) 以存储从 Office 365 同步到本地组织的对象, 然后单击 "下一步"。
7. 在 "准备配置" 页上, 单击 "配置"。
8. 完成向导后, 在 "配置完成" 页上单击 "退出"。
9. 在 Active Directory 域控制器上打开 Active Directory 用户和计算机, 并找到以 AAD_ 开头的用户帐户。记下此帐户的名称。您还可以使用 PowerShell cmdlet 来 [确定 AD DS 连接器帐户](#)
10. 在 Azure Active Directory Connect 服务器上打开 Windows PowerShell, 然后运行以下命令。

```
$AzureADConnectWritebackAccountDN = <AAD_ account DN>
Import-Module "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig\AdSyncConfig.psm1"
Set-ADSyncUnifiedGroupWritebackPermissions -ADConnectorAccountDN $AzureADConnectWritebackAccountDN
```

配置组域

Office 365 组的主 SMTP 域称为组域。默认情况下, 组织中默认的接受域会被选作组域。如果想要添加专用组域, 可以使用下列步骤添加域。有关 Office 365 组的多域支持的详细信息, 请查看 [多域支持 \(针对 office 365 组\)](#)。

1. 将新域添加到 Office 365 组织。如果您需要有关将域添加到 Office 365 的帮助, 请查看 [将用户和域添加到 office 365](#)。
2. 使用以下命令, 添加该组域作为本地 Exchange 组织中的接受域。需要执行该操作, 以使用混合发送连接器将出站邮件传递到 Office 365 中的组域。

```
New-AcceptedDomain -Name groups.contoso.com -DomainName groups.contoso.com -DomainType InternalRelay
```

3. 使用 DNS 提供程序创建以下公用 DNS 记录。

DNS 记录名称	DNS 记录类型	DNS 记录值
groups.contoso.com	MX	groups-contoso-com.mail.protection.outlook.com ¹
autodiscover.groups.contoso.com	CNAME	autodiscover.outlook.com

¹此 DNS 记录值的格式为_<域键>_。mail.protection.outlook.com。要找出你的域密钥是什么, 请参阅[收集创建 Office 365 DNS 记录所需的信息](#)。

Caution

如果将组域的 MX DNS 记录设置为本地 Exchange 服务器, 则本地 Exchange 组织用户和 Office 365 组用户之间的邮件流将不能正常工作。

4. 使用以下命令, 将组域添加到由本地 Exchange 组织中的混合配置向导创建的混合发送连接器中。

```
Set-SendConnector -Identity "Outbound to Office 365" -AddressSpaces
"contoso.mail.onmicrosoft.com", "groups.contoso.com"
```

NOTE

如果未更新发送连接器, 或未将组域添加为本地 Exchange 组织中的接受域, 则不会将从本地邮箱发送的邮件传递至组, 除非将该组配置为接收来自外部发件人的邮件。

您如何知道这有效？

若要确保组可以正常使用 Exchange 混合部署, 应使用本地邮箱以及已从本地组织移动到 Office 365 的邮箱对其进行测试。使用以下各部分中的步骤执行每个测试。

使用本地邮箱进行测试

1. 将本地邮箱添加到 Office 365 组。
2. 将 Office 365 邮箱添加到同一 Office 365 组。
3. 使用 Outlook 网页版登录到 Office 365 邮箱。
4. 使用 Office 365 邮箱向组发送邮件。
5. 使用 Outlook 2016 或 Outlook 网页版打开本地邮箱。
6. 验证邮箱收到包含发送到 Office 365 组的文章的电子邮件。
7. 在同一邮箱中, 撰写邮件回复并将其发送到组。
8. 验证邮件可由所有组成员查看。

使用移动到 Office 365 的邮箱进行测试

1. 将邮箱从本地 Exchange 组织移动到 Office 365。
2. 向 Office 365 组添加邮箱。
3. 在新的浏览器会话中, 登录已移动到 Office 365 的邮箱。
4. 在 Outlook 网页版中, 验证该组在左侧导航栏中列出。
5. 向组发送邮件。
6. 验证邮件可由所有组成员查看。

已知问题

- **较旧版本的 AZURE ad connect 不会安装 DSACLs:** 您需要安装 RSAT 或 latest 版本的 Azure ad connect, 以管理组的权限 (如果需要)。
- **将邮箱移动到 office 365 时不显示组:** 当用户从本地 Exchange 组织移动到 office 365 时, 组不会显示在 Outlook 或 web 上的 outlook 的左侧导航窗格中。若要解决此问题, 将该邮箱从其所属的任何组中删除, 并将其重新添加到每个组。
- **新组不会显示在内部部署 Exchange 全局地址列表 (GAL) 中:** 当在 Office 365 中创建新组时, 它不会自动显示在本地 GAL 中。若要解决此问题, 在本地 Exchange 服务器上打开 Exchange 命令行管理程序, 并运行以下命令。

```
Update-Recipient "<group name>"
```

- **组不接收来自本地用户的邮件:** 当满足以下条件时, 本地用户将无法向 Office 365 组发送邮件:
 - 将组域配置为本地 Exchange 组织中的权威域。

- 最近创建了该组, 且其信息尚未写回到本地 Active Directory。

当 Azure AD Connect 在 Office 365 和本地组织间执行其下一同步时, 该问题将自行解决。每隔三十分钟进行一次 Azure AD Connect 同步。

- **内部部署用户无法使用组邮件页脚中包含的链接:** 本地用户无法使用发送给他们的每个组邮件的页脚中包含的 "查看组" 对话或取消订阅链接。若要取消组订阅, 本地用户需要与组管理员联系。
- **发送到组的辅助 SMTP 地址的邮件无法传递:** 将多个电子邮件地址添加到组中时, 仅将主 SMTP 地址写回到您的本地 Active Directory。如果某个本地用户尝试将邮件发送到某个组的辅助 SMTP 地址, 则邮件将无法传递。若要避免此问题, 请仅在每个组上配置一个 SMTP 地址。
- **本地用户不能成为组的管理员:** 本地用户不能直接访问组空间。因此, 不能将他们添加为组管理员。
- **如果已启用集中邮件流, 则向组传递外部邮件可能会失败:** 如果启用了集中邮件流, 则外部用户发送给组的邮件将无法传递, 即使该组允许来自外部发件人的邮件也是如此。
- **本地用户不能以组的形式发送邮件:** 如果本地用户尝试将邮件作为 Office 365 组发送, 即使他们被授予对组的 "代理发送" 权限, 也会收到权限被拒绝的错误。以组发送权限只适合 Exchange Online 邮箱用户。
- **从 Outlook 的左侧导航窗格中选择一个组不会打开组的邮箱:** Outlook 使用自动发现 URL 打开组邮箱。如果一个组的主电子邮件地址在一个不指向 Office 365 的自动发现 URL (autodiscover.outlook.com) 的域中, Outlook 将无法打开组的邮箱。若要解决此问题, 可以使用指向 Office 365 自动发现 URL 的域中的主地址设置组。可以配置电子邮件地址策略, 以将主电子邮件添加至每个指向 Office 365 自动发现 URL 的组邮箱。有关详细信息, 请查阅 [Multi-domain support for Office 365 Groups](#) (Office 365 组的多域支持)

在 Exchange 混合部署中为本地主邮箱创建基于云的存档

2019/6/5 •

在 Exchange 混合部署中，可以在 Exchange Online 中为本地主邮箱配置基于云的存档邮箱。

开始之前

- 拥有本地主邮箱的用户必须在 Office 365 组织中拥有用户帐户。
- Office 365 用户帐户必须分配有 Exchange Server 适用的 Exchange Online Archiving 许可证。第 1 步中的过程包含分配许可证的步骤。
- 在第 1 步中启用基于云的存档邮箱后，最长可能要等 30 分钟，基于云的存档邮箱才能完成预配。这是因为基于云的存档邮箱是在目录同步期间创建。在此期间，本地 Active Directory 与 Office 365 中的 Azure Active Directory (Azure AD) 同步。默认情况下，每 30 分钟运行一次目录同步。

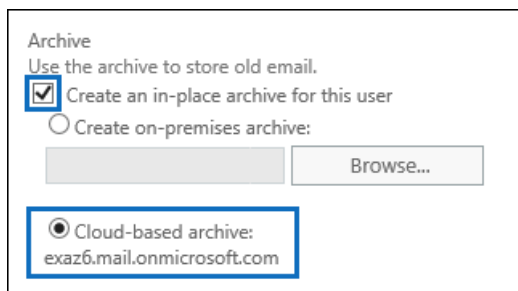
第 1 步：为本地主邮箱启用基于云的存档邮箱

若要为本地主邮箱启用基于云的存档邮箱，请按以下任意一个过程操作。在本地 Exchange 组织的 Exchange 管理中心中和 Office 365 管理中心中按以下步骤操作。

- [为新用户创建基于云的存档邮箱](#)
- [为现有用户创建基于云的存档邮箱](#)

为新用户创建基于云的存档邮箱

1. 在您的本地组织中的 EAC 中，转到“收件人 > ”“邮箱”。
2. 单击“新建+ > 图标用户邮箱”。
3. 在“新建用户邮箱”页上，为新用户或现有用户创建邮箱。For more information about creating a user mailbox, see [Create User Mailboxes](#).
4. 单击“更多选项”，启用基于云的存档邮箱。
5. 在“存档”下，单击选中“为此用户创建就地存档”复选框，然后单击“基于云的存档”。此时，系统会显示要预配存档邮箱的域名。



Archive
Use the archive to store old email.

☒ Create an in-place archive for this user
☐ Create on-premises archive:

Browse...

☒ Cloud-based archive:
exaz6.mail.onmicrosoft.com

6. 单击“保存”，创建邮箱和基于云的存档。


请注意，在“邮箱”页上，选定邮箱的“邮箱类型”列中显示值“用户(存档)”。

7. 最长可能要等 30 分钟，目录同步才能完成。完成后才能在 Office 365 中创建相应的用户帐户。

TIP

在 Office 365 管理中心, 转到 "运行状况 > 目录同步状态", 查看上次目录同步发生的时间。

- 验证在创建新的本地邮箱之后发生目录同步之后, 在 Office 365 管理中心中, 转到 "用户 > 活动用户", 然后选择为其创建的新 Office 365 用户帐户新的本地邮箱。
- 在显示的 "用户属性" 页上, 单击 "产品许可证" 部分中的 "编辑"。

 **Test On-Prem User 1**
TestOnPrem1@exaz6.cpubtest.com

[Reset password](#) [Delete user](#)

User name	TestOnPrem1@exaz6.cpubtest.com	Edit
Product licenses	No products have been assigned	Edit
Group memberships (0)	No groups for the user. Click edit to change group membership.	Edit
Sign-in status	Sign-in allowed	Edit


- 在 "位置" 下拉菜单下, 选择用户的位置。
- 展开 "Office 365 企业版许可证" 列表, 然后分配 exchange **Online 存档 For Exchange Server** 许可证, 然后保存所做的更改。

此时, 在用户列表的 "状态" 列中, 你会发现许可证已分配给用户。

- 同样, 最长可能要等 30 分钟, 目录同步才能完成。完成后才能预配基于云的存档邮箱。转到第 2 步, 了解如何确认基于云的存档邮箱是否已创建。创建存档邮箱后, 用户可以使用 Outlook 或 Web 上的 Outlook 对其进行访问。

为现有用户创建基于云的存档邮箱

- 在 Office 365 管理中心中, 转到 "用户 > 活动用户", 然后选择要为其创建云基础存档邮箱的用户帐户。
- 在显示的 "用户属性" 页上, 单击 "产品许可证" 部分中的 "编辑"。

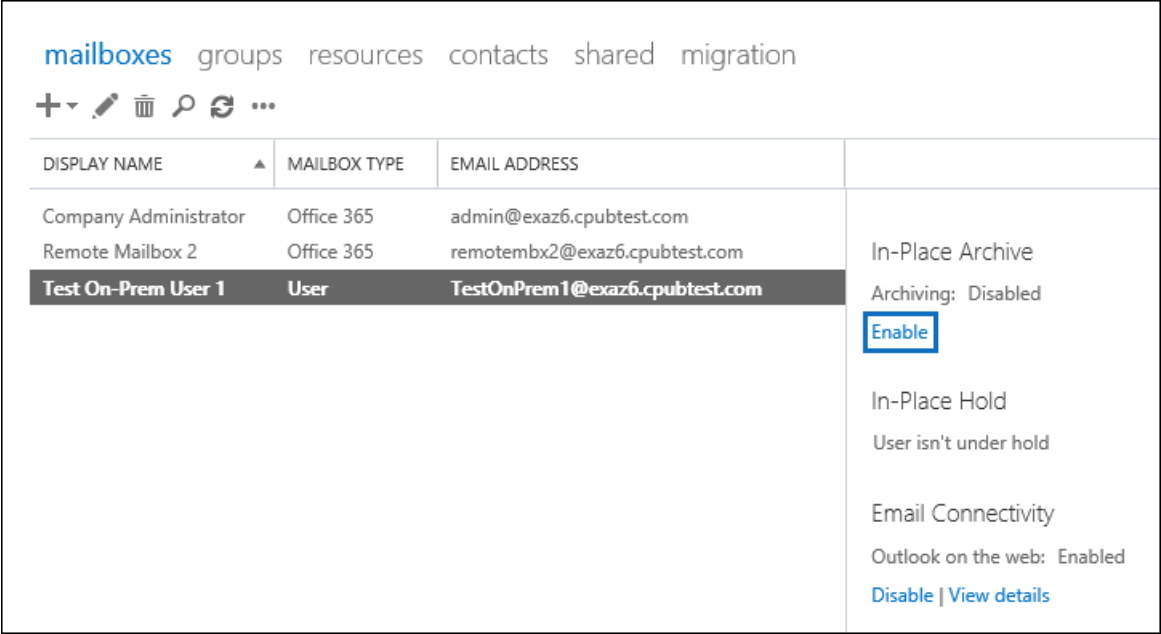
 **Test On-Prem User 1**
TestOnPrem1@exaz6.cpubtest.com

[Reset password](#) [Delete user](#)

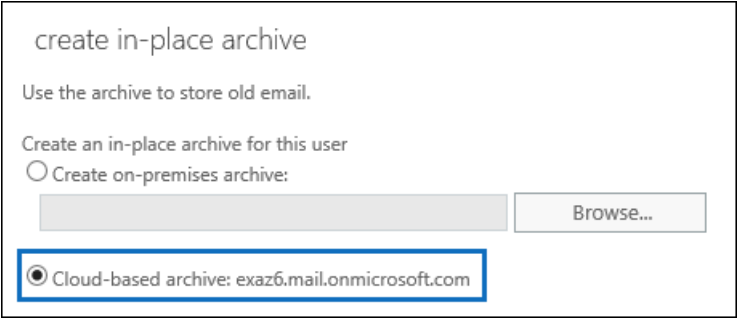
User name	TestOnPrem1@exaz6.cpubtest.com	Edit
Product licenses	No products have been assigned	Edit
Group memberships (0)	No groups for the user. Click edit to change group membership.	Edit
Sign-in status	Sign-in allowed	Edit

- 在 "位置" 下拉菜单下, 选择用户的位置。

4. 展开 "Office 365 企业版许可证" 列表, 然后分配 exchange **Online 存档 For Exchange Server**许可证, 然后保存所做的更改。
- 此时, 在用户列表的"状态"列中, 你会发现许可证已分配给用户。
5. 在您的本地组织中的 EAC 中, 转到 "收件人 > " "邮箱"。
6. 在邮箱列表中, 选择刚刚向其分配许可证的用户。
7. 在详细信息窗格中的"就地存档"**** 下, 单击"启用"****。



8. 在"创建就地存档"页上, 依次单击"基于云的存档"和"确认"。此时, 系统会显示要预配存档邮箱的域名。



请注意, 在"邮箱"页上, 选定邮箱的"邮箱类型"列中显示值"用户(存档)"。

9. 最长可能要等 30 分钟, 目录同步才能完成。完成后才能创建基于云的存档邮箱。转到第 2 步, 了解如何确认基于云的存档邮箱是否已创建。创建存档邮箱后, 用户可以使用 Outlook 或 Web 上的 Outlook 对其进行访问。

TIP

在 Office 365 管理中心, 转到 "运行状况 > 目录同步状态", 查看上次目录同步发生的时间。

第 2 步: 确认基于云的存档邮箱是否已创建

如前所述, 基于云的存档邮箱的启用时间与其实际创建时间之间可能有延迟。这是因为必须运行目录同步才能创建基于云的存档邮箱。下面介绍了几种用于确认基于云的存档邮箱是否已创建的方法。

在 Exchange Online 组织中, 运行以下 PowerShell 命令, 以显示与用户存档邮箱相关的属性。若要连接到使用远程

PowerShell Exchange Online，请参阅[连接到 Exchange 联机 PowerShell](#)。

```
Get-MailUser <cloud mail user> | FL *archive*
```

以下屏幕截图显示了待预配基于云的存档邮箱时和创建存档邮箱后返回的属性。

Mail user properties before the cloud-based archive mailbox is provisioned by directory synchronization

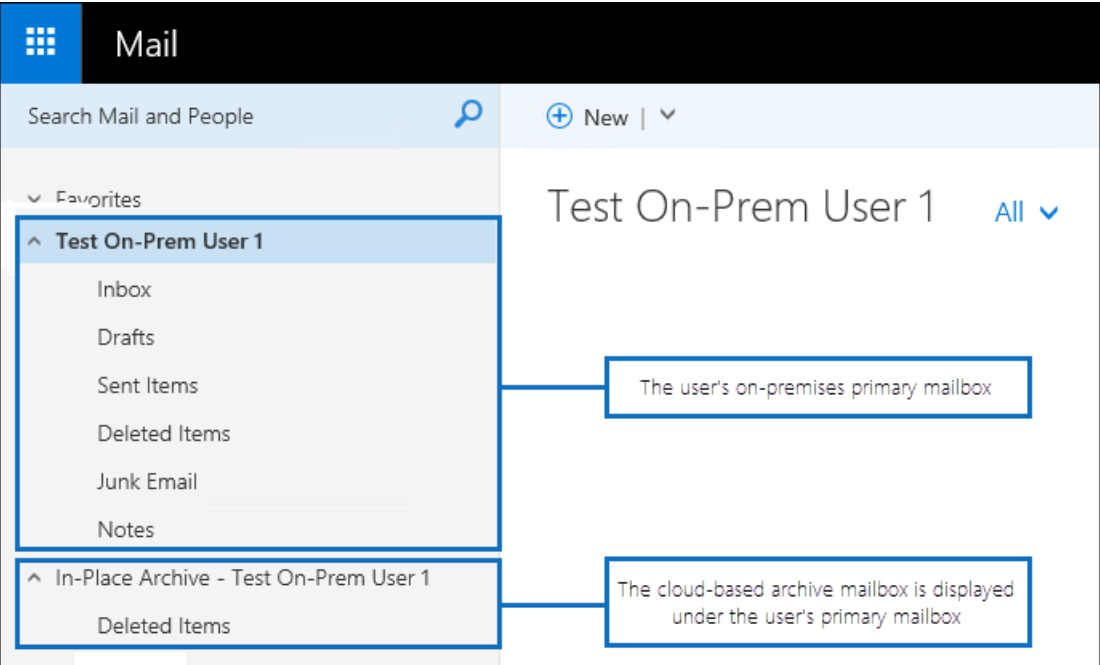
```
ArchiveGuid      : 00000000-0000-0000-0000-000000000000
ArchiveName      : {}
ArchiveQuota     : 100 GB (107,374,182,400 bytes)
ArchiveWarningQuota : 90 GB (96,636,764,160 bytes)
ArchiveDatabase  :
ArchiveStatus    : None
DisabledArchiveDatabase :
DisabledArchiveGuid : 00000000-0000-0000-0000-000000000000
JournalArchiveAddress :
ArchiveRelease   :
```

在目录同步设置基于云的存档之前，_ArchiveStatus_属性设置为 `None`。此外，还请注意，_ArchiveGuid_ 和 _ArchiveName_ 属性为空。

Mail user properties after the cloud-based archive mailbox is provisioned by directory synchronization

```
ArchiveGuid      : 91c2b207-2c46-4d4c-9141-7dcac79a2b3f
ArchiveName      : {In-Place Archive - Test On-Prem User 1}
ArchiveQuota     : 100 GB (107,374,182,400 bytes)
ArchiveWarningQuota : 90 GB (96,636,764,160 bytes)
ArchiveDatabase  : NAMPR14DG094-db094
ArchiveStatus    : Active
DisabledArchiveDatabase :
DisabledArchiveGuid : 00000000-0000-0000-0000-000000000000
JournalArchiveAddress :
ArchiveRelease   :
```

目录同步预配基于云的存档后，_ArchiveStatus_属性设置为 `Active`，并填充 _ArchiveGuid_ 和 _ArchiveName_ 属性。此时，用户可以在 Outlook 或 Web 上的 Outlook 中访问其基于云的存档邮箱。



也可以在本地 Exchange 组织中运行以下 PowerShell 命令，以显示与用户基于云的存档邮箱有关的属性。

```
Get-Mailbox <on-premises user mailbox> | FL *archive*
```

在通过目录同步预配基于云的存档邮箱之前的本地邮箱属性 **

```
ArchiveDatabase      :  
ArchiveGuid         : f3ebb048-abf6-43bc-8138-d44d727a8582  
ArchiveName         : <In-Place Archive - Test On-Prem User 1>  
JournalArchiveAddress :  
ArchiveQuota        : 100 GB (107,374,182,400 bytes)  
ArchiveWarningQuota : 90 GB (96,636,764,160 bytes)  
ArchiveDomain       : exaz6.mail.onmicrosoft.com  
ArchiveStatus       : None  
ArchiveState        : HostedPending  
DisabledArchiveDatabase :  
DisabledArchiveGuid  : 00000000-0000-0000-0000-000000000000  
ArchiveRelease      :
```

在目录同步设置基于云的存档之前, 将_ArchiveStatus_属性设置为 `None` , 并将_ArchiveState_属性设置为 `HostedPending` 。

通过目录同步预配基于云的存档邮箱后的本地邮箱属性 **

```
ArchiveDatabase      :  
ArchiveGuid         : f3ebb048-abf6-43bc-8138-d44d727a8582  
ArchiveName         : <In-Place Archive - Test On-Prem User 1>  
JournalArchiveAddress :  
ArchiveQuota        : 100 GB (107,374,182,400 bytes)  
ArchiveWarningQuota : 90 GB (96,636,764,160 bytes)  
ArchiveDomain       : exaz6.mail.onmicrosoft.com  
ArchiveStatus       : Active  
ArchiveState        : HostedProvisioned  
DisabledArchiveDatabase :  
DisabledArchiveGuid  : 00000000-0000-0000-0000-000000000000  
ArchiveRelease      :
```

在目录同步设置基于云的存档后, _ArchiveStatus_属性设置为 `Active` , 并将_ArchiveState_属性设置为 `HostedProvisioned` 。此时, 用户可以在 Outlook 或 Web 上的 Outlook 中访问其基于云的存档邮箱。

[返回顶部](#)

(可选)运行目录同步

如前所述, 基于云的存档邮箱是在目录同步期间创建。By default, your on-premises Active Directory is synchronized with Azure AD in Office 365 once every 30 minutes. 通过转到 Office 365 管理中心中的运行状况 > 目录同步状态, 可以查看上次目录同步的时间。

在某些情况下, 不妨启动目录同步, 以在运行下一个计划同步前预配基于云的存档邮箱。为此, 可在安装了 Azure AD Connect 的服务器上运行以下 PowerShell 命令。

```
Start-ADSyncSyncCycle -PolicyType Delta
```

有关详细信息, 请参阅 [Azure AD Connect sync:Scheduler](#) (Azure AD Connect 同步: 计划程序)。

[Return to top](#)

为 Office 365 混合简化 Outlook Web App URL

2019/6/5 •

了解如何在混合环境中为云邮箱用户配置 Web 上的 Outlook (Outlook Web App) URL。

对于从本地 Exchange 迁移到 Office 365 的组织, 主要关注的是用户体验。用户需要的是邮箱访问不受中断, 无论邮箱在何时被移动到何处。考虑到这一点, Web 上的 Outlook (旧称"Outlook Web App") 共存情景很重要。

假设应用场景如下: 某公司使用混合部署将一些邮箱从本地 Exchange 迁移到 Office 365。在迁移前的星期五, 用户使用 URL <https://mail.contoso.com/owa> 访问本地邮箱。在迁移后的星期一, 相同用户尝试使用该 URL 访问邮箱时却看到了错误消息。

为了让受影响的用户可以使用 Web 上的 Outlook 连接邮箱, 可以采用下列两种方式之一:

- 告诉用户新 URL (例如, <https://outlook.com/owa/contoso.com>) 此选项的问题如下:
 - URL 非常复杂。
 - 受影响的用户无法获得顺畅体验。
- 在组织关系上配置 **TargetOWAUrl** 设置: 此选项的问题如下:
 - 云邮箱的终结点在外部 (并不在用户所需的域中)。
 - 终结点需要在 URL 中指定域 (以区分 Office 365 商业服务和 outlook.com 使用者服务)。
 - 终结点导致用户看到证书不匹配警告。

若要为有云邮箱的用户解决这些问题, 请按以下步骤操作:

1. 在 DNS 中创建一个指向 **mail.office365.com** 的 **CNAME** 记录 (例如, **cloudowa.contoso.com**):
 - 请务必在内部和外部 (公共) DNS 中创建此 CNAME 记录, 因为用户可能会通过内部或外部 Internet 连接进行连接。
 - 在我们的示例中, 请求中使用的是域 **contoso.com** (舍弃了 **cloudowa** 部分)。也就是说, 无需在 URL 中指定域。
2. 在内部部署组织关系中配置 **web 上的 Outlook 重定向**: 为此, 请在本地 exchange 中的 Exchange 命令行管理程序中使用以下语法:

```
Set-OrganizationRelationship -TargetOWAUrl http://<CNAME value>/owa
```

例如, 如果你在第 1 步中创建的 CNAME 记录为 **cloudowa.contoso.com**, 请运行以下命令:

```
Set-OrganizationRelationship -TargetOWAUrl http://cloudowa.contoso.com/owa
```

注意:

- 请使用 **http**, 而不是 **https**。
- 在组织关系中, 后缀值 **/owa** 是必需的, 但用户不需要在 URL 中输入 **/owa**。

多重身份验证提示

用户可能会收到多重身份验证提示, 具体取决于:

- 连接起始位置(内部还是外部 Internet 连接)。
- 如果他们的计算机已加入或未加入域。
- 是否在混合环境中使用了联合身份验证。

下表介绍了可能会向用户提供的身份验证提示体验。

身份验证方法	客户端计算机	身份验证提示体验
联合身份验证	内部 Internet 连接	单一提示
联合身份验证	外部 Internet 连接	双重提示
无联合身份验证	已加入域(内部或外部)	双重提示
有或无联合身份验证	未加入域(内部或外部)	双重提示

注意:联合身份验证要求在 Internet Explorer 的 Intranet 区域中配置 AD FS 终结点(如 <https://go.microsoft.com/fwlink/p/?linkid=834460> 中的主题所述), 并要求根据常规 Office 365 指导配置 AD FS。

混合部署故障排除

2019/6/5 •

在 Exchange 中使用混合配置向导配置混合部署将极大减少混合部署出现问题的可能性。然而，这里有一些混合配置向导范围之外的典型区域，如果配置不当的话，可能导致混合部署出现问题。本主题将讨论可能出现问题的以下常见区域，并介绍验证或修正问题的基本步骤：

- 本地 Exchange 服务器
- 证书
- 混合配置向导的具体错误

NOTE

本主题中的 "Exchange 服务器" 是指以下内容：> 客户端访问服务器 exchange 2013 和更早版本的 > 邮箱服务器 exchange 2016 及更高版本

有关其他信息，请参阅 [Exchange Server 混合部署](#)。

关于混合部署的更多管理任务，参阅 [混合部署过程](#)。

在开始之前，您需要知道什么？

- 估计完成该任务的时间：因混合部署问题的类型而异
- 您必须先获得权限，然后才能执行此过程或多个过程。若要查看所需的权限，请参阅 [Exchange and Shell infrastructure permissions](#) 主题中的 "混合部署" 条目。
- 本主题中的指导适用于使用混合配置向导配置的混合部署。不支持手动配置的混合部署。
- 有关可能适用于本主题中的过程的键盘快捷方式的信息，请参阅 [Exchange 管理中心的键盘快捷方式](#)。

TIP

是否有任何疑问？在 Exchange 论坛中寻求帮助。请访问以下论坛：[Exchange Server](#)、[Exchange Online](#) 或 [Exchange Online Protection](#)。

要执行什么操作？

内部部署 Exchange 服务器故障排除

内部部署 Exchange 服务器的配置通常是混合配置最有可能出现问题的区域。通常，需要检查的区域包括：

- **可用性：**将内部部署 Exchange 服务器正确发布到 Internet 对于在混合部署中正常运行的功能至关重要。为了使混合功能正常运行，您必须配置内部部署防火墙或其他安全设备，以允许从 Internet 到内部部署 Exchange 服务器上的自动发现和 Exchange Web Services (EWS) 终结点的入站访问。此外，还必须配置 Exchange 服务器以接受入站 SMTP 邮件。如果 Office 365 租户组织中包含的 Microsoft Exchange Online Protection (EOP) 服务无法到达内部部署 Exchange 服务器，从 Exchange Online 组织到内部部署组织的安全邮件可能无法正常运行。
- **证书：**需要将用于在内部部署组织与 exchange online 组织之间进行安全邮件传输的数字证书安装在将与 Exchange Online 通信的所有本地 Internet Exchange 服务器上，必须从第三方证书颁发机构 (CA) 发出，不能

过期, 并且必须分配有 IIS 和 SMTP 服务。如果未满足这些证书要求, 将无法正常运行从 Exchange Online 组织到内部部署组织的安全邮件传输。本主题后面的“解决证书问题”提供了有关证书要求的详细信息。

如何知道您的 Exchange 服务器配置是否正确？

要验证您已成功发布内部部署 Exchange 服务器, 使用 Microsoft Remote Connectivity Analyzer 验证内部部署 Exchange 服务器的入站 Internet 连接。请执行以下操作:

1. 转到[远程连接分析器](#)工具。
2. 该步骤用于 EWS 任务的常规测试, 以确认它们是否正常运行, 同时已配置 EWS 终结点。

在 " **Microsoft Exchange Web 服务连接测试** " 部分运行 "同步、通知、可用性和自动答复 (OOB) " 测试, 并验证没有任何错误。如果发生错误, 更正测试确定的项目。

3. 该步骤用于自动发现服务的常规测试, 以确认它们是否正常运行, 同时已配置自动服务终结点。

运行 " **Microsoft Office Outlook 连接测试** " 部分中的 " **Outlook 自动发现** " 测试, 并验证没有任何错误。如果发生错误, 更正测试确定的项目。

4. 该步骤用于 SMTP 连接性的一般测试, 并确认 Exchange 服务器可以接收入站 Internet 邮件。

运行 " **Internet 电子邮件测试** " 部分中的 " **入站 SMTP 电子邮件测试** ", 并验证没有任何错误。如果发生错误, 更正测试确定的项目。

证书问题故障排除

在内部部署 Exchange 服务器上安装的证书配置可能导致混合部署发生问题。在大多数情况下, 以下证书相关问题将影响混合功能:

- **证书类型:** 用于安全混合传输和在混合配置向导中定义的数字证书必须从第三方 CA 颁发。自签名证书必须不得用于混合传输身份验证。如果无意中选择或分配自签名证书, Exchange Online 和内部部署组织之间的安全邮件传输将无法正常运行。
- **分配的服务:** 应将 Internet 信息服务 (IIS) 和简单邮件传输协议 (SMTP) 服务分配给用于混合传输的数字证书。如果未分配这些服务, Exchange Online 组织和内部部署组织之间的安全邮件传输将无法正常运行。
- **安装:** 必须在所有内部部署 exchange 服务器上安装用于在内部部署和 exchange Online 组织之间进行安全邮件传输的数字证书。如果您正为内部部署边缘传输服务器部署混合部署, 数字证书还必须安装在您的边缘传输服务器上。如果未在内部部署服务器上安装证书, Exchange Online 和内部部署组织之间的安全邮件传输将无法正常运行。
- **过期:** 用于内部部署组织与 Exchange Online 组织之间的安全邮件传输的数字证书不得过期。如果证书到期, Exchange Online 组织和内部部署组织之间的安全邮件传输将无法正常运行。

如何知道您的证书是否正确配置？

要验证用于内部部署 Exchange 服务器的混合邮件传输证书正确配置, 请执行以下操作:

1. 在本地 Exchange 服务器上, 打开 Exchange 命令行管理程序。
2. 在 Exchange 命令行管理程序中, 运行以下命令。

```
Get-ExchangeCertificate| format-list
```

3. 查找您在用于安全邮件传输的混合配置向导中定义证书的信息。
4. 验证已分配以下参数值给证书:

- **IsSelfSigned 参数:** 此参数值应为 `_False_`。
- **RootCAType 参数:** 此参数值应为 `_第三方_`。

- **服务参数**: 此参数值应为_IIS, SMTP_。
- **NotAfter 参数**: 此参数值是证书到期日期。这里列出的日期不应到期。

混合配置向导的具体错误疑难解答

如果您在运行混合配置向导时收到错误, 通常可以通过执行若干简单的检查或操作来解决问题。关于解决在运行混合配置向导时可能遇到的具体消息或问题, 请参阅以下建议。

- **消息: "在 <服务器上找不到默认接收连接器>":** 如果以下属性中列出的任何 Exchange 服务器上的接收连接器没有侦听 IPv4 和 IPv6 的 TCP 端口 25, 则会出现此消息协议:

```
(Get-HybridConfiguration).ReceivingTransportServers。
```

若要验证在运行时列出的 Exchange 服务器上的接收连接器是否

`(Get-HybridConfiguration).ReceivingTransportServers。`具有正确的绑定, 请在 Exchange 命令行管理程序中运行以下命令。

```
Get-ReceiveConnector -Server <Server Name> | Format-Table Identity, Bindings
```

您应该会看到为您的 Exchange 服务器列出的以下条目: `{[::]:25, 0.0.0.0:25}`

如果未列出此绑定, 则需要使用**set-receiveconnector** Cmdlet 的 `_Bindings_` 参数将其添加到您的接收连接器。有关详细信息, 请参阅 [Set-ReceiveConnector](#)。

Exchange 2013 和 Exchange 2007 的混合部署

2019/6/5 •

随着 Microsoft Exchange Server 2013 引入混合配置向导的最新改进和体系结构更改，配置和管理基于 Exchange 2013 的与 Exchange 2007 混合的部署变得更加简单。无论是要将 Exchange 2007 内部部署与 Exchange Online 组织连接以实现长期共存，还是要作为云迁移策略的一部分，了解混合部署概念都十分重要。

选择以下一个主题开始并了解详细信息：

[Exchange 2013/Exchange 2007 混合部署中的服务器角色](#)

[Exchange 2013/Exchange 2007 混合部署中的混合管理](#)

[Exchange 2013/Exchange 2007 混合部署中的边缘传输服务器](#)

[Exchange 2013/Exchange 2007 混合部署中的传输选项](#)

[Exchange 2013/Exchange 2007 混合部署中的传输路由](#)

Exchange 2013/Exchange 2007 混合部署中的服务器角色

2019/6/5 •

在 Exchange 2007 组织中配置了混合部署后，您需要在现有的 Exchange 2007 组织中至少安装一个具有客户端访问服务器角色和邮箱服务器角色的 Exchange 2013 服务器。Exchange 2013 客户端访问服务器和邮箱服务器协调现有的 Exchange 2007 内部部署组织和 Exchange Online 组织之间的通信。此通信包括内部部署组织与 Exchange Online 组织之间的邮件传输和消息功能。

我们强烈建议在内部部署组织中安装多个 Exchange 2013 服务器，以帮助提高混合部署功能的可靠性和可用性。

混合部署中的服务器角色

下面是混合部署中的 Exchange 2013 服务器角色的快速概述：

- **客户端访问服务器角色**：Exchange 2013 客户端访问服务器角色继续提供许多与贵组织中的 Exchange 2007 客户端访问服务器通常一起提供的功能，其中包含支持混合的一些附加功能。Exchange 2007 的部署和共存。客户端访问服务器还处理由 Exchange Online 组织发送到内部部署组织的安全邮件，以及处理混合部署中的传输规则、日记策略和到邮箱服务器的邮件传递。默认情况下，在客户端访问服务器上配置有专门的接收连接器以支持安全混合邮件传输。所有客户端连接（包括 Outlook 客户端访问、Outlook Web App 和 Outlook Anywhere）都通过客户端访问服务器角色进行。内部部署组织与 Exchange Online 组织之间的组织关系功能（如忙/闲共享）也由客户端访问服务器角色处理。

有关详细信息，请参阅[客户端访问服务](#)。

- **邮箱服务器角色**：Exchange 2013 邮箱服务器角色处理从内部部署组织发送到 Exchange Online 组织的安全邮件邮件。尽管不典型，但它也可以托管内部部署收件人邮箱并与通过内部部署客户端访问服务器代理的 Exchange Online 组织通信。默认情况下，在邮箱服务器角色上配置有专门的发送连接器以支持安全混合邮件传输。

有关详细信息，请参阅[Mailbox Server](#)。

根据所需的混合部署配置，Exchange 2013 服务器需要安装一个或两个服务器角色：

- **单一 exchange server**：如果选择在内部部署组织中安装一台 Exchange 服务器，则需要在单台服务器上同时安装客户端访问和邮箱服务器角色。
- **多个 exchange 服务器**：如果选择在内部部署组织中安装多个 exchange 服务器，则可以在内部部署组织中的不同服务器上安装服务器角色。例如，可以安装一个安装了邮箱和客户端访问服务器角色的 Exchange 2013 服务器，同时也再安装一个仅安装了客户端访问服务器角色的 Exchange 服务器。但是，最佳实践及推荐的服务器配置是在内部部署组织中部署的“每个”Exchange 2013 服务器上同时安装客户端访问和邮箱服务器。

有关 Exchange 容量规则的详细信息，请参阅[了解容量规划中的多个服务器角色配置](#)。

混合部署中的 Exchange 服务器功能

Exchange 服务器为混合部署中的内部部署组织提供了几个重要功能：

- **联合**：Exchange 2013 服务器使您能够为内部部署组织创建与 Microsoft 联合网关的联合身份验证信任。Microsoft 联合网关是 Microsoft 提供的一项基于云的免费服务，该服务可充当内部部署组织与 Office 365 租户组织之间的信任代理。联合身份验证是关于在内部部署组织与 Exchange Online 组织之间创建组织关系

的要求。

有关详细信息，请参阅[Understanding Federation](#)。

- **组织关系:** 通过使用客户端访问服务器角色的 Exchange 2013 服务器, 可以在内部部署组织和 Exchange Online 组织之间创建组织关系关系。混合部署中的许多其他服务(包括日历忙/闲信息共享、邮件跟踪以及内部部署组织与 Exchange Online 组织之间的邮箱移动)需要组织关系。

有关详细信息，请参阅 [Understanding Federated Sharing](#)。

- **邮件传输:** 具有客户端访问和邮箱服务器角色的 Exchange 2013 服务器负责混合部署中的邮件传输。通过使用发送和接收连接器，这些服务器可用作传入外部邮件的连接终结点，并提供到 Internet 和 Exchange Online 组织的出站邮件传递。

有关详细信息，请参阅 [Exchange 2013/Exchange 2007 混合部署中的传输选项](#)。

- **邮件传输安全性:** 具有客户端访问和邮箱服务器角色的 Exchange 2013 服务器通过使用 Exchange 中的域安全功能, 可帮助保护内部部署组织与 Exchange Online 组织之间的邮件通信安全。可以通过将相互传输层安全性身份验证和加密用于邮件通信，来增强安全。

有关详细信息，请参阅[了解域安全性](#)。

- **Outlook Web App:** 具有客户端访问服务器角色的 Exchange 2013 服务器支持将单个 URL 终结点配置为与内部部署和 Exchange Online 邮箱的外部连接。对于内部部署邮箱，客户端访问服务器被配置为响应 Outlook Web App 请求。对于 Exchange Online 组织邮箱，客户端访问服务器被配置为自动显示到 Exchange Online 组织上的 Outlook Web App 终结点的链接。

有关详细信息，请参阅[web 上的 Outlook](#)。

Exchange 服务器拓扑

如果添加额外的 Exchange 2013 服务器来支持混合部署，则 Exchange 服务器的部署将与其他任何 Exchange 服务器部署到现有 Exchange 2007 组织的方式非常相似。为混合部署配置现有的内部部署 Exchange 2007 组织不需要任何特殊的 Exchange 服务器拓扑。但是必须在 Exchange 2007 服务器上安装 Exchange 2007 Service Pack 3 (SP3) 更新汇总 10 和 Exchange 2013 累积更新 1 (CU1) 或更高版本，以启用 Office 365 的兼容性和完全混合功能。

下表简要描述配置了混合部署后的服务更改。

服务	混合部署之前	混合部署之后	说明
邮件传输(进站和出站)	Exchange 2007 客户端访问服务器	Office 365 包含 Exchange 2013 客户端访问服务器或 Exchange Online Protection (EOP)	域的 MX(邮件交换器)记录可以保留不变，或者更新为指向 EOP。
Outlook Web App 公用 URL	Exchange 2007 客户端访问服务器	Exchange 2013 客户端访问服务器	Exchange 2013 客户端访问服务器代理内部部署邮箱到 Exchange 2007 客户端访问服务器的 Outlook Web App 请求。在 Outlook Web App Online 上托管邮箱的 Exchange 请求提供到 Exchange Online Outlook Web App URL 的链接。

Exchange 服务器软件

Exchange 2013 CU1 或更高版本通过混合配置向导 (HCW) 启用混合部署功能。在安装其他 Exchange 2013 服务器时，可以使用任何 Exchange 2013 CU1 或更高版本的媒体。

有关如何下载 Exchange Server 的最新版本的信息, 请参阅[Exchange 更新](#)。

IMPORTANT

在配置混合部署时, 您需要为您的混合服务器授予许可证。现在, HCW 可以在不转到单独的网站或呼叫 Microsoft 支持的情况下, 检测并许可指定的本地 Exchange 2010、Exchange 2013 或 Exchange 2016 混合服务器, 以供免费使用。您可以在[此处](#)访问 HCW。请注意, Exchange 2019 混合服务器不提供免费 Exchange Server 许可证。

Exchange 2013/Exchange 2007 混合部署中的混合管理

2019/6/5 •

在 Exchange 2007 内部部署组织中安装运行 Microsoft Exchange Server 2013 的服务器时，会自动在服务器上安装 Exchange 2013 管理工具。您将使用以下工具来配置和管理内部部署 Exchange 和 Exchange Online 组织的混合功能：

- **Exchange 管理中心:** EAC 是一种基于 web 的管理 2013 控制台，它易于使用，并针对内部部署、在线或混合 Exchange 部署进行了优化。EAC 补充了用于管理 Exchange Server 2007 的 Exchange 管理控制台 (EMC) 和 Exchange 控制面板 (ECP) 界面。
- **Exchange 命令行管理程序:** exchange 命令行管理程序是基于 Windows PowerShell 的命令行界面。

Exchange 管理中心

EAC 允许您同时在内部部署 Exchange 服务器和 Exchange Online 组织上执行许多部署任务和最常见的日常管理任务。默认情况下，它将在每个 Exchange 2013 服务器上安装。此外，由于它是基于 Web 的管理控制台，您还可以使用网络中的其他计算机的 Web 浏览器或通过使用 ECP 虚拟目录 URL 访问它。

IMPORTANT

如果想要使用邮箱位于 Exchange 2007 邮箱服务器中的帐户(例如域管理员帐户)访问 EAC，则必须在浏览器中使用以下地址访问 EAC: > `https://<FQDN of Exchange 2013 Client Access server>/ECP? ExchClientVer=15`

您可以通过选择 Office 365 跨界导航选项卡来访问 EAC 中的 Exchange Online 组织。跨界导航允许您在 Exchange Online 和内部部署 Exchange 组织之间轻松切换。如果您已经配置混合部署，选择 Office 365 选项卡将允许您管理 Exchange Online 组织和收件人对象。如果您没有 Exchange Online 组织，选择 Office 365 链接会将您转到 Office 365 注册页面。

有关 EAC 的详细信息，请参阅 [Exchange Administration Center](#)。

Exchange 命令行管理程序

Exchange 命令行管理程序可以执行 EAC 执行的任何任务，以及只能在 Exchange 命令行管理程序中执行的某些其他任务。Exchange 命令行管理程序是安装 Exchange 2013 管理工具时安装在计算机上的 Windows PowerShell 脚本和 cmdlet 的集合。只有在使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，才会加载这些脚本和 cmdlet。如果你直接打开 Windows PowerShell，则不会加载 Exchange 脚本和 cmdlet，并且你将无法管理内部部署组织。

NOTE

你可以创建到本地内部部署组织的手动 Windows PowerShell 连接，方式与手动连接到以下 Exchange Online 组织类似。但是，强烈建议你使用 Exchange 命令行管理程序图标来打开 Exchange 命令行管理程序，以管理内部部署 Exchange 服务器。

当你在安装了管理工具的计算机上使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，可以管理内部部署组织。但是，在使用此图标打开 Exchange 命令行管理程序时不能管理 Exchange Online 组织。这是因为使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序会自动连接到本地 Exchange 服务器。

如果要使用 Windows PowerShell 管理 Exchange Online 组织，必须直接打开 Windows PowerShell，而不要通过

Exchange 命令行管理程序图标打开。打开 Windows PowerShell 后，你便可以手动指定要连接的位置。当你创建手动连接时，可在 Office 365 租户组织中指定一个管理员帐户，然后运行命令以创建连接。建立该连接后，你即可使用有权运行的 Exchange cmdlet。有关更多信息，请参阅[使用 Windows PowerShell](#)。

如果你不熟悉 Exchange 命令行管理程序，请查看 [Exchange Management Shell](#)，以了解有关 Exchange 命令行管理程序的工作方式的基本信息、命令语法及更多内容。

Exchange 2013/Exchange 2007 混合部署中的边缘传输服务器

2019/6/5 •

使用 Microsoft Exchange 部署的边缘传输服务器部署在组织的内部部署外围网络中。它们是未加入域的计算机，可处理面向 Internet 的邮件流，并充当内部网络中的 Exchange 服务器的 SMTP 中继和智能主机。

对于想要使用边缘传输服务器的 Exchange 2013 组织，提供部署 Exchange Server 2013 边缘传输服务器或运行 Exchange 2010 Service Pack 3 (SP3) 的 Exchange 2010 边缘传输服务器的选项。如果您不想将内部 Exchange 2013 客户端访问或邮箱服务器直接暴露给 Internet，请使用边缘传输服务器。

可在以下位置了解 Exchange 2013 边缘传输服务器角色的详细信息：[Overview of the Edge Transport Server Role](#)。

有关 Exchange 2010 边缘传输服务器的详细信息，请参阅[边缘传输服务器角色概述](#)。

基于 Exchange 2013 的混合部署组织中的边缘传输服务器

在内部部署与混合部署中的 Exchange Online 组织之间路由的邮件要求 Microsoft Exchange Online Protection (EOP) 服务代表 Exchange Online 直接连接到运行 Exchange 2013 或 Exchange 2010 SP3 的边缘传输服务器。

IMPORTANT

如果您在其他位置具有其他 Exchange 2010 边缘传输服务器，但是这些服务器不处理混合传输，那么这些服务器无需升级到 Exchange 2010 SP3。然而，如果希望 EOP 在未来连接至混合传输的其他边缘传输服务器，那么这些服务器必须使用 Exchange 2010 SP3 升级或升级到 Exchange 2013 边缘传输服务器。

向混合部署添加边缘传输服务器

当配置混合部署时，在内部部署组织中部署边缘传输服务器是可选项。当配置混合部署时，混合配置向导允许您选择一个或多个客户端访问和邮箱服务器用于混合邮箱传输，或选择一个或多个内部部署边缘传输服务器处理 Exchange Online 组织的混合邮件传输。

在将边缘传输服务器添加到混合部署时，混合配置向导将代表内部 Exchange 2013 客户端访问和邮箱服务器与 EOP 进行通信。边缘传输服务器作为内部部署邮箱服务器和 EOP 之间的中继，用于从内部部署组织到 Exchange Online 的出站邮件。边缘传输服务器还作为内部部署客户端访问服务器之间的中继，用于从 Exchange Online 组织到内部部署组织的入站邮件。所有以前由客户端访问服务器处理的连接安全性由边缘传输服务器处理。收件人查找、合规性策略和其他邮件检查继续由客户端访问服务器处理。

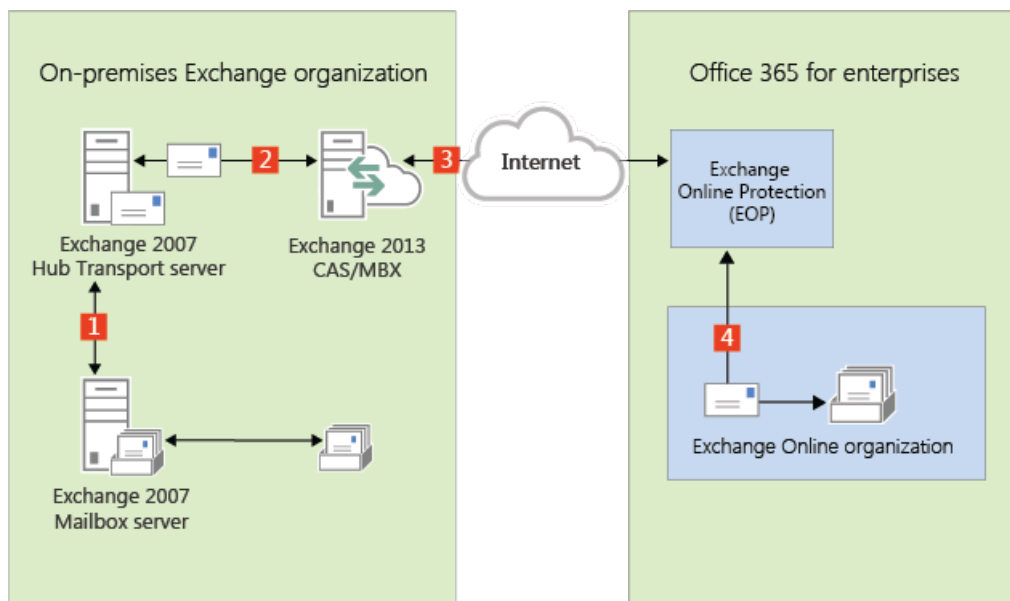
不使用边缘传输服务器的邮件流

以下过程与图表描述了在无边缘传输服务器部署时，内部部署组织与 Exchange Online 之间的邮件的路径：

1. 从内部部署组织到 Exchange Online 组织中收件人的出站邮件将从 Exchange 2007 邮箱服务器中的邮箱发送到 Exchange 2007 集线器传输服务器。
2. Exchange 2007 集线器传输服务器将邮件发送到 Exchange 2013 邮箱服务器。
3. Exchange 2013 邮箱服务器将邮件直接发送至 Exchange Online EOP 公司。
4. EOP 将邮件传送给 Exchange Online 组织。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

从 Exchange Online 组织发送到内部部署组织中的收件人的邮件将遵循相反的路由。

未部署边缘传输服务器的混合部署中的邮件流



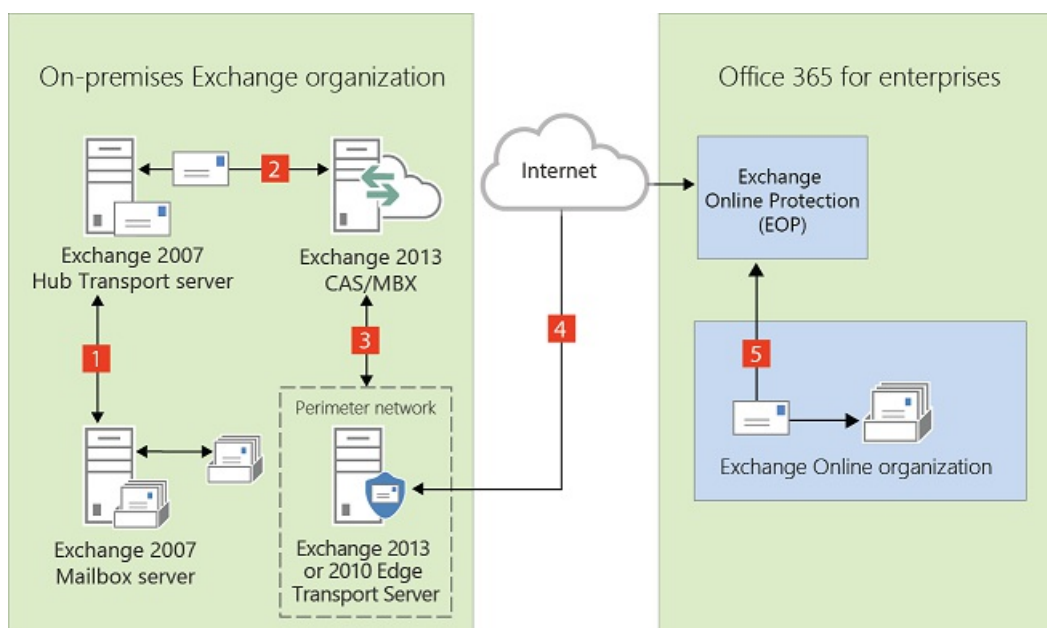
使用边缘传输服务器的邮件流

以下流程介绍了在部署边缘传输服务器后，邮件在内部部署组织与 Exchange Online 之间采用的路径。从内部部署组织到 Exchange Online 组织中收件人的邮件是从 Exchange 2007 邮箱服务器发送的：

1. 从内部部署组织到 Exchange Online 组织中收件人的出站邮件将从 Exchange 2007 邮箱服务器中的邮箱发送到 Exchange 2007 集线器传输服务器。
2. Exchange 2007 集线器传输服务器将邮件发送到 Exchange 2013 邮箱服务器。
3. Exchange 2013 邮箱服务器将邮件发送至 Exchange 2013 或 Exchange 2010 SP3 边缘传输服务器。
4. 边缘传输服务器将邮件发送到 Exchange Online EOP 公司。
5. EOP 将邮件传送给 Exchange Online 组织。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

从 Exchange Online 组织发送到内部部署组织中的收件人的邮件将遵循相反的路由。

部署了 Exchange 2013 或 2010 SP3 边缘传输服务器的混合部署中的邮件流



Exchange 2013/Exchange 2007 混合部署中的传输选项

2019/6/5 •

在混合部署中，可以具有既驻留在本地 Exchange 组织中也驻留在 Exchange Online 组织中的邮箱。为了使这两个单独组织对用户及在他们之间交换的邮件表现为一个合并的组织，关键组件是混合传输。通过混合传输，在任一组织中的收件人之间发送的邮件会经过身份验证、加密并使用传输层安全性 (TLS) 传输，并且向 Exchange 组件 (如传输规则、日记和反垃圾邮件策略) 显示为“内部”。混合传输是由 Exchange 2013 中的混合配置向导自动配置的。

若要使混合传输配置能与混合配置向导一起使用，接受来自 Microsoft Exchange Online 保护 (EOP) (该功能为 Exchange Online 组织处理传输) 的连接的本地的 SMTP 终结点必须为 Exchange 2013 客户端访问服务器、Exchange 2013 边缘传输服务器或者 Exchange Server 2010 Service Pack 3 (SP3) 边缘传输服务器。

IMPORTANT

本地 Exchange 2013 客户端访问服务器或 Exchange 2013/Exchange 2010 SP3 边缘传输服务器与 EOP 之间可以没有任何其他 SMTP 主机或服务。当邮件经过非 Exchange 2013 服务器、预 Exchange 2010 SP3 服务器或 SMTP 主机时，会删除添加到邮件中用于启用混合传输功能的信息。如果在组织中部署了 Exchange 2010 SP2 边缘传输服务器，并且要将这些服务器用于混合传输，则它们必须升级到 Exchange 2010 SP3。

从外部 Internet 发件人发送到两个组织中的收件人的入站邮件会采用通用入站路由。从组织发送到外部 Internet 收件人的出站邮件可以采用通用出站路由，也可以通过独立的路由发送。

在计划和配置混合部署时需要选择如何路由入站和出站邮件。发送到和发送自内部部署和 Exchange Online 组织中收件人的入站和出站邮件采用的路由取决于以下因素：

- 您是否希望通过 Microsoft Office 365 和 EOP 或内部部署组织路由内部部署和 Exchange Online 邮箱的入站 Internet 邮件？

可以选择通过内部部署组织或通过 EOP 和 Exchange Online 组织为两个组织路由入站 Internet 邮件。两个组织入站邮件的路由取决于是否在混合部署中启用了集中邮件传输。

- 是要通过内部部署组织 (集中邮件传输) 路由来自 Exchange Online 组织的出站邮件到外部收件人，还是要将其直接路由到 Internet？

作为集中邮件传输，可以先通过内部部署组织路由来自 Exchange Online 组织中邮箱的所有邮件，然后再将这些邮件传递到 Internet。此方法用于合规性方案，在这类方案中，发送到和发送自 Internet 的所有邮件都必须由内部部署服务器进行处理。或者，可以配置 Exchange Online 以将外部收件人的邮件直接传递到 Internet。

NOTE

仅对具有与符合性相关的特定传输需求的组织推荐使用集中式邮件传输。我们建议典型的 Exchange 组织不要启用集中式邮件传输。

- 是否要在内部部署组织中部署边缘传输服务器？

如果您不想将加入域的内部 Exchange 2013 服务器直接向 Internet 公开，则可在外围网络中部署 Exchange 2013 边缘传输服务器或 Exchange 2010 SP3 边缘传输服务器。有关向混合部署添加边缘传输服务器的详细信息，请参阅 [Exchange 2013/Exchange 2007 混合部署中的边缘传输服务器](#)。

无论如何路由发送到和发送自 Internet 的邮件，在内部部署与 Exchange Online 组织之间发送的所有邮件都使用安全传输进行发送。有关详细信息，请参阅本主题后面的[受信任通信](#)。

有关这些选项如何影响贵组织的邮件路由的详细信息，请参阅 [Exchange 2013/Exchange 2007 混合部署中的传输路由](#)。

混合部署中的 Exchange Online Protection

EOP 是 Microsoft 提供的联机服务，由许多公司用于保护其内部部署组织免受病毒、垃圾邮件、欺诈邮件和策略违规的危害。在 Office 365 中，EOP 用于保护 Exchange Online 组织免受相同威胁的危害。在注册 Office 365 时，会自动创建与您的 Exchange Online 组织关联的 EOP 公司。

EOP 公司包含一些邮件传输设置，可以为 Exchange Online 组织配置这些设置。可以指定哪些 SMTP 域必须来自特定 IP 地址，需要 TLS 和安全套接字层 (SSL) 证书，可以绕过合规性策略，等等。EOP 是 Exchange Online 组织的前门。所有邮件(无论其来源如何)都必须先经过 EOP，然后才能到达 Exchange Online 组织中的邮箱。而且，从 Exchange Online 组织发送的所有邮件都必须先经过 EOP，然后才能到达 Internet。

在使用混合配置向导配置混合部署时，会在内部部署组织以及为 Exchange Online 组织设置的 EOP 公司中自动配置所有传输设置。混合配置向导会在此 EOP 公司中配置所有进站和出站连接器及其他设置，以保护在内部部署与 Exchange Online 组织之间发送的邮件并将邮件路由到正确目标。如果要为 Exchange Online 组织配置自定义传输设置，则也会在此 EOP 公司中配置这些设置。

受信任通信

为了帮助保护内部部署和 Exchange Online 组织中的收件人，并帮助确保不会截获和读取组织之间发送的邮件，内部部署组织与 EOP 之间的传输会配置为使用强制 TLS。TLS 传输使用受信任第三方证书颁发机构 (CA) 提供的安全套接字层 (SSL) 证书。EOP 与 Exchange Online 组织之间的邮件也使用 TLS。

当使用强制 TLS 传输时，发送和接收服务器会检查在其他服务器上配置的证书。对证书配置的使用者名称或使用替代名称 (SAN) 之一，必须与管理员在其他服务器上显式指定的 FQDN 匹配。例如，如果 EOP 配置为接受并保护从 mail.contoso.com FQDN 发送的邮件，则发送内部部署客户端访问或边缘传输服务器必须具有在主题名称或 SAN 中包含 mail.contoso.com 的 SSL 证书。如果不满足此要求，则 EOP 会拒绝连接。

NOTE

使用的 FQDN 无需与收件人的电子邮件域名匹配。唯一要求在于证书主题名称或 SAN 中的 FQDN 必须与接收或发送服务器配置为接受的 FQDN 匹配。

除了使用 TLS 以外，还可将组织之间的邮件作为“内部”邮件处理。此方法使邮件可以绕过反垃圾邮件设置和其他服务。

有关 SSL 证书和域安全性的详细信息，请参阅 [混合部署的证书要求](#) 和 [了解 TLS 证书](#)。

Exchange 2013/Exchange 2007 混合部署中的传输路由

2019/6/5 •

本主题讨论来自 Internet 的进站邮件和发送到 Internet 的出站邮件的路由选项。

IMPORTANT

不要在处理或修改 SMTP 通信的内部部署 Exchange 服务器和 Office 365 之间放置任何服务器、服务或设备。内部部署 Exchange 组织和 Office 365 之间的安全邮件流取决于组织之间发送的邮件中包含的信息。支持允许 TCP 端口 25 上的 SMTP 通信通过而无需修改的防火墙。如果服务器、服务或设备处理内部部署 Exchange 组织和 Office 365 之间发送的邮件，此信息将被删除。如果发生这种情况，该邮件将不再被视为组织内部邮件，并且将会对其应用反垃圾邮件筛选、传输和日记规则以及可能不适用于它的其他策略。

NOTE

本主题中的示例不包括将边缘传输服务器添加到混合部署中。邮件在内部部署组织、Exchange Online 组织与 Internet 之间采用的路由不会随着添加边缘传输服务器而更改。只有内部部署组织中的路由会更改。有关向混合部署添加边缘传输服务器的详细信息，请参阅[Exchange 2013/Exchange 2007 混合部署中的边缘传输服务器](#)。

来自 Internet 的进站邮件

作为计划和配置混合部署的一部分，需要决定是否想要通过 Exchange Online 或本地组织路由来自 Internet 发件人的所有邮件。所有来自 Internet 发件人的邮件最初会传递到所选的组织，然后根据收件人邮箱所在的位置路由。是否选择通过 Exchange Online 或本地组织路由邮件取决于各种因素，包括是否想要对发送到两种组织的所有邮件应用合规性策略以及每个组织中的邮箱数等。

本地和 Exchange Online 组织中发送到收件人的路径取决于在混合部署中决定如何配置 MX 记录。首选方法是配置 MX 记录，使其指向 Office 365 中的 Exchange Online Protection (EOP)，因为该配置提供最准确的垃圾邮件筛选。混合邮件配置向导不配置本地或 Exchange Online 组织的进站 Internet 邮件的路由。如果想要更改进站 Internet 邮件传递的方式，则必须手动配置 MX 记录。

- **如果您将 MX 记录更改为指向 Office 365 中的 Exchange Online Protection 服务：**这是混合部署的推荐配置。所有发送到任一组织中的任何收件人的邮件都将首先通过 Exchange Online 组织路由。发往位于本地组织中的收件人的邮件会首先通过 Exchange Online 组织路由，随后传递到本地组织中的收件人。如果您的 Exchange Online 组织中的收件人数量比本地组织中的多，并且如果您希望邮件被 EOP 筛选，则推荐该路由。Exchange Online Protection 需要该配置选项，以提供对垃圾邮件的扫描和阻止。
- **如果您决定将 MX 记录保留为您的内部部署组织：**则所有发送到任一组织中的任何收件人的邮件都将首先通过您的内部部署组织进行路由。发往位于 Exchange Online 中的收件人的邮件会首先通过本地组织进行路由，随后传递到 Exchange Online 中的收件人。对于具有合规性策略（该策略要求日记解决方案检查发送到和发送至组织的邮件）的组织，此路由可能很有帮助。如果选取了该选项，则 Exchange Online Protection 将不能有效地扫描垃圾邮件。

有关详细信息，请参阅 [Mail flow best practices for Exchange Online and Office 365 \(Overview\)](#)。

阅读下面与您计划将从 Internet 收件人发送的邮件路由到内部部署和 Exchange Online 收件人的方式相匹配的章节。

通过 Exchange Online 组织路由入站 Internet 邮件

以下步骤和图表举例说明了在指向 MX 记录到 Office 365 组织中的 EOP 服务的情况下，混合部署中出现的入站邮件路径。邮件路径因是否选择启用集中邮件传输而异。

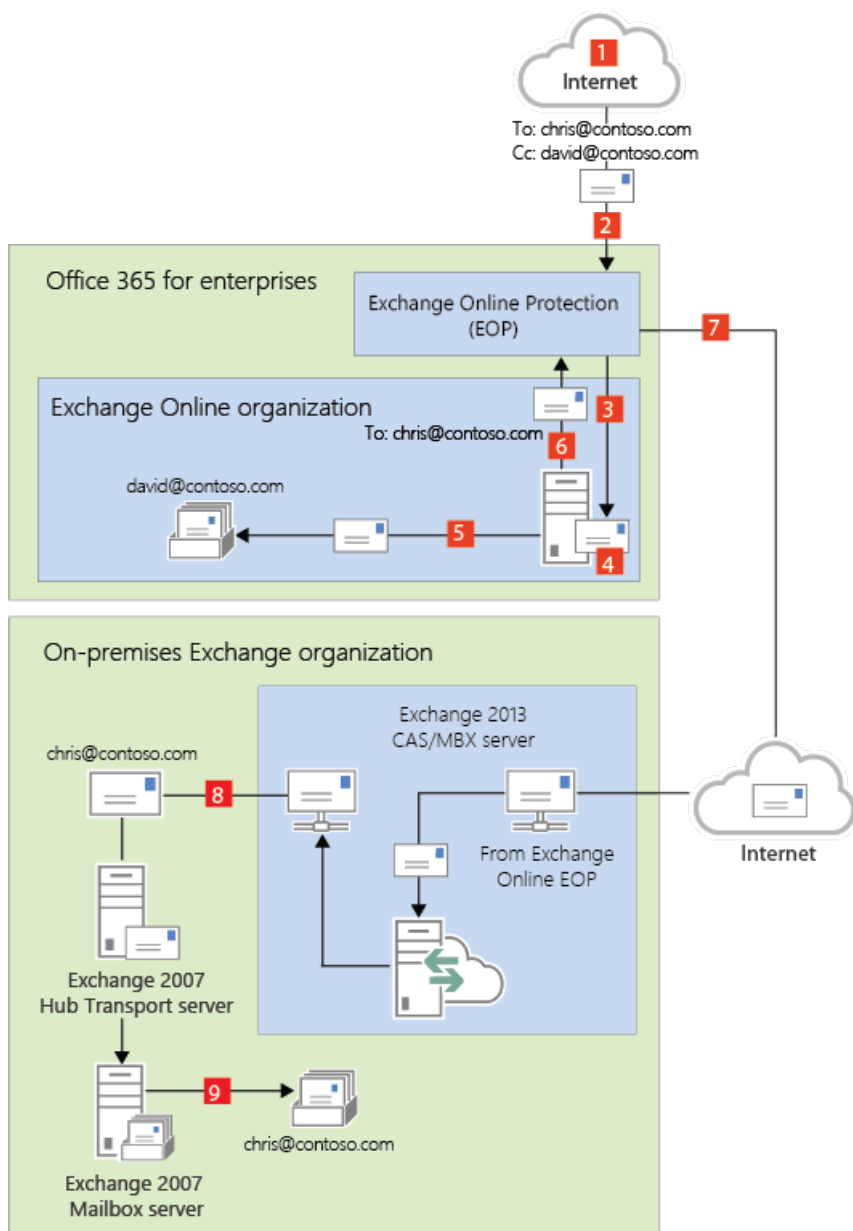
IMPORTANT

对于接收首先传递到 EOP 然后通过 Exchange Online 组织进行路由的邮件的每个内部部署邮箱，可能需要购买 EOP 许可证。有关详细信息，请与您的 Microsoft 经销商联系。

当集中邮件传输被禁用(默认配置)时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 chris@contoso.com 和 david@contoso.com。Chris 的邮箱位于内部部署组织中的 Exchange 2007 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 contoso.com 电子邮件地址，并且 contoso.com 的 MX 记录指向 EOP，所以邮件会传递到 EOP。
3. EOP 将两个收件人的邮件都路由到 Exchange Online。
4. Exchange Online 对邮件进行病毒扫描并对每个收件人执行查找。通过查找，确定 Chris 的邮箱位于内部部署组织中，而 David 的邮箱位于 Exchange Online 组织中。
5. Exchange Online 将邮件拆分为两个副本。将邮件的一个副本传递到 David 的邮箱。
6. 将第二个副本从 Exchange Online 发送回 EOP。
7. EOP 发送邮件到内部部署组织中的 Exchange 2013 客户端访问服务器。
8. Exchange 2013 客户端访问服务器通过在 Exchange 2013 服务器和 Exchange 2007 服务器之间配置的路由组连接器将邮件发送到 Exchange 2007 邮件服务器。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

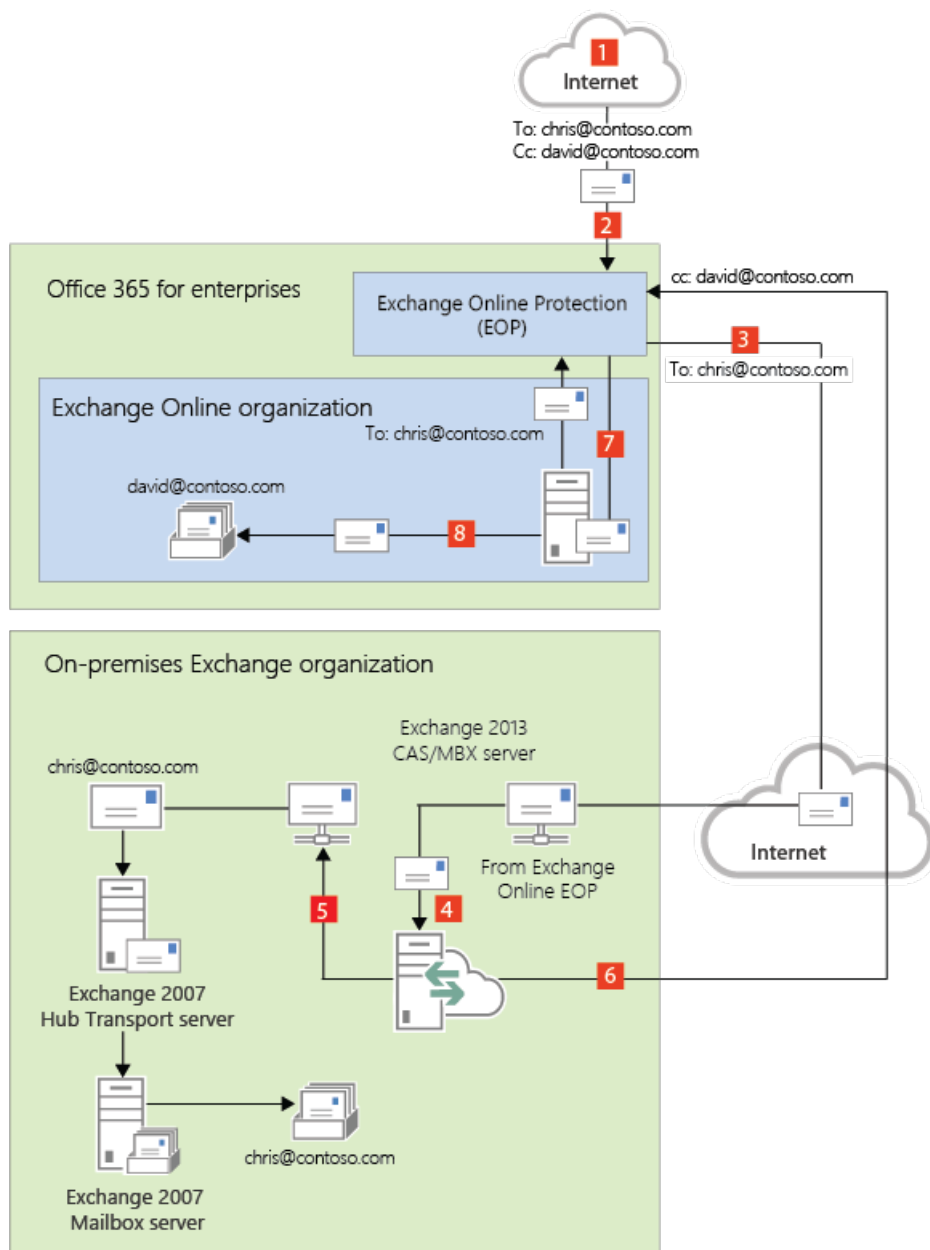
通过 **Exchange Online** 组织为内部部署组织和 **Exchange Online** 组织路由邮件，同时禁用集中邮件传输（默认配置）



当集中邮件传输被启用时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 `chris@contoso.com` 和 `david@contoso.com`。Chris 的邮箱位于内部部署组织中的 Exchange 2007 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 `contoso.com` 电子邮件地址，并且 `contoso.com` 的 MX 记录指向 EOP，所以邮件会传递到 EOP 并扫描病毒。
3. 由于启用了集中邮件传输，EOP 会将这两个收件人的邮件路由到内部部署 Exchange 2013 客户端访问服务器。
4. Exchange 2013 服务器为每个收件人执行查找。通过查找，确定 Chris 的邮箱位于内部部署组织中，而 David 的邮箱位于 Exchange Online 组织中。
5. Exchange 2013 服务器将邮件拆分为两个副本。邮件的一个副本被发送给 Chris 在内部部署 Exchange 2007 邮箱服务器中的邮箱。
6. 第二个副本从 Exchange 2013 服务器发送回 EOP。
7. EOP 将邮件发送到 Exchange Online。
8. Exchange 将邮件发送到 David 的邮箱。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

通过 Exchange Online 组织为内部部署组织和 Exchange Online 组织路由邮件，同时启用集中邮件传输



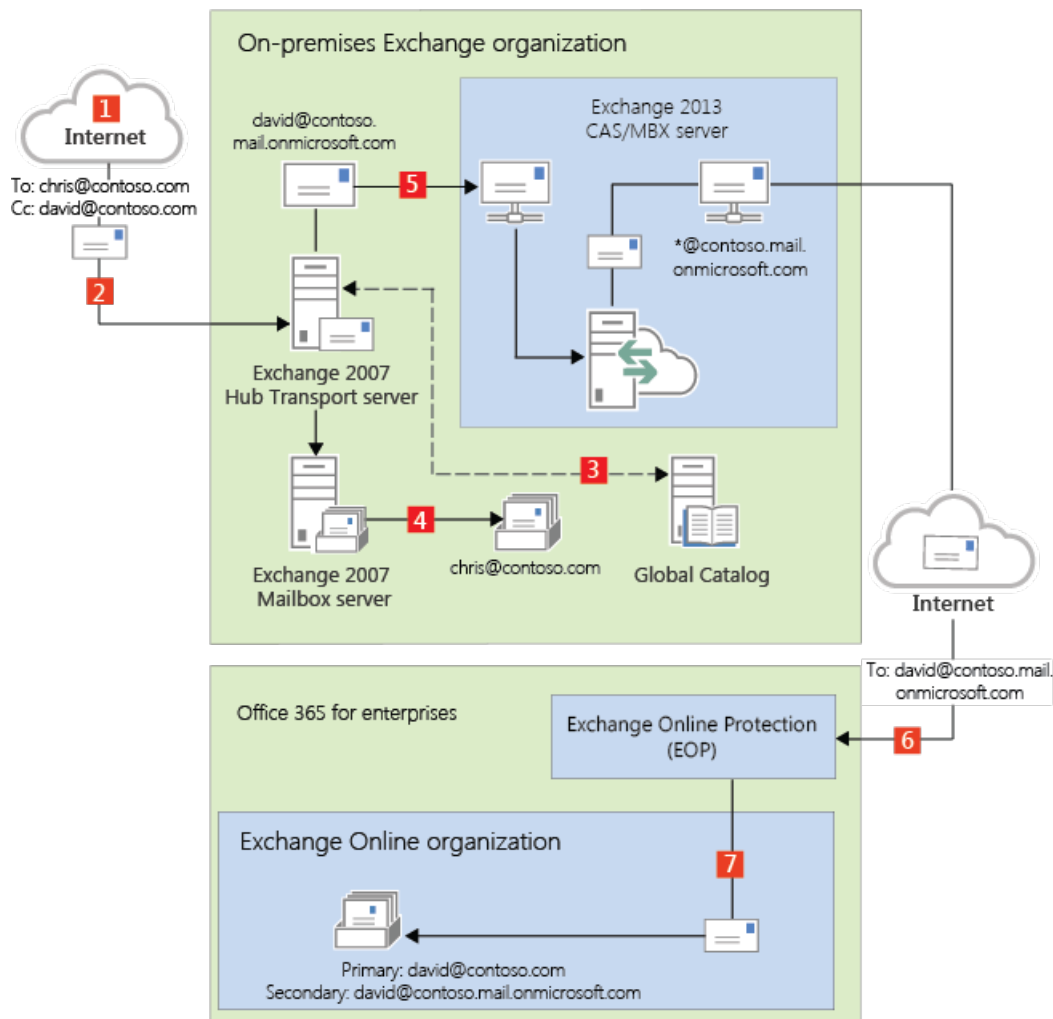
通过内部部署组织路由入站 Internet 邮件

以下步骤和图表举例说明了在决定保持指向您的内部部署组织的 MX 记录的情况下，混合部署中将出现的入站 Internet 邮件路径。

1. 入站邮件从 Internet 发件人发送给收件人 `chris@contoso.com` 和 `david@contoso.com`。Chris 的邮箱位于内部部署组织中的 Exchange 2007 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 `contoso.com` 电子邮件地址，并且 `contoso.com` 的 MX 记录指向内部部署组织，所以邮件会传递到 Exchange 2007 集线器传输服务器。
3. Exchange 2007 邮箱服务器使用内部部署全局编录服务器对每个收件人执行查找。通过全局编录查找，该服务器可确定 Chris 的邮箱位于 Exchange 2007 邮箱服务器上，而 David 的邮箱在 Exchange Online 组织中，并具有混合路由地址 `david@contoso.mail.onmicrosoft.com`。
4. Exchange 2007 邮箱服务器将邮件拆分为两个副本。将邮件的一个副本传递到 Chris 的邮箱。
5. 邮件的第二个副本通过在 Exchange 2013 服务器与 Exchange 2007 服务器之间配置的路由组连接器发送。
6. Exchange 2013 邮箱服务器通过配置为使用 TLS 的发送连接器将邮件发送到 EOP。EOP 接收传送给 Exchange Online 组织的邮件。

7. EOP 将邮件发送到 Exchange Online 组织, 在该组织中对邮件进行病毒和基于内容的垃圾邮件的扫描并将其传递到 David 的邮箱。在此示例中, 客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

通过内部部署组织为内部部署组织和 Exchange Online 组织路由邮件



发送到 Internet 的出站邮件

除了选择如何对发送给组织中的收件人的进站邮件进行路由之外, 还可以选择如何对从 Exchange Online 收件人发送的出站邮件进行路由。运行“混合配置”向导时, 可以选择两个选项之一:

- **不启用集中邮件传输:** 默认情况下, 在“混合配置”向导中选择此选项可将从 Exchange Online 组织发送的出站邮件直接路由到 Internet。如果无需将任何内部部署合规性策略或其他处理规则应用于从 Exchange Online 组织中的收件人发送的邮件, 请使用此选项。
- **启用集中邮件传输:** 选择此选项可通过内部部署组织路由从 Exchange Online 组织发送的出站邮件。除了向同一个 Exchange Online 组织中的其他收件人发送的邮件之外, 从 Exchange Online 组织中的收件人发送的所有出站邮件都会通过内部部署组织发送。这使您可以将合规性规则应用于这些邮件以及必须应用于所有收件人(无论这些收件人是处于 Exchange Online 组织中还是处于内部部署组织中)的任何其他过程或要求。

NOTE

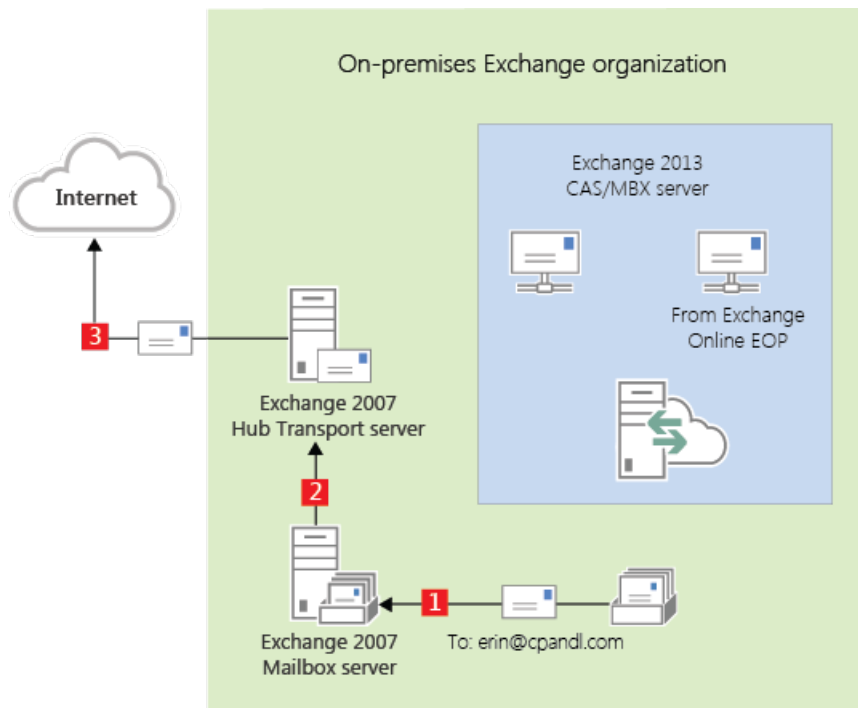
仅对具有与符合性相关的特定传输需求的组织推荐使用集中式邮件传输。我们建议典型的 Exchange 组织不要启用集中式邮件传输。

从内部部署收件人发送的邮件会始终使用 DNS 直接发送到 Internet 收件人(无论在“混合配置”向导中选择了以上哪个选项)。

以下步骤和图表说明从内部部署收件人发送的邮件的出站邮件路径。

1. 在内部部署 Exchange 2007 邮箱服务器上拥有一个邮箱的 Chris 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange 2007 邮箱服务器将邮件发送到 Exchange 2007 集线器传输服务器。
3. Exchange 2007 集线器传输服务器查找 cpandl.com 的 MX 记录，然后将邮件发送到位于 Internet 上的 cpandl.com 邮件服务器。

从内部部署发件人发送给 Internet 收件人的邮件



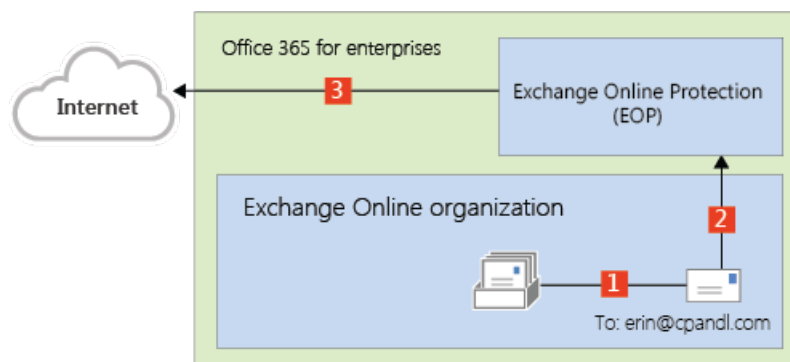
阅读下面与您计划将从 Exchange Online 组织中收件人发送的邮件路由到 Internet 收件人的方式相匹配的章节。

使用 DNS (集中式邮件传输已禁用) 传递来自 Exchange Online 的 Internet 邮件。

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 Exchange Online EOP 服务。
3. EOP 会在 MX 记录中查找 cpandl.com，并将邮件发送给位于 Internet 上的 cpandl.com 邮件服务器。

来自 Exchange Online 发件人的邮件将直接路由到 Internet，同时禁用集中邮件传输（默认配置）

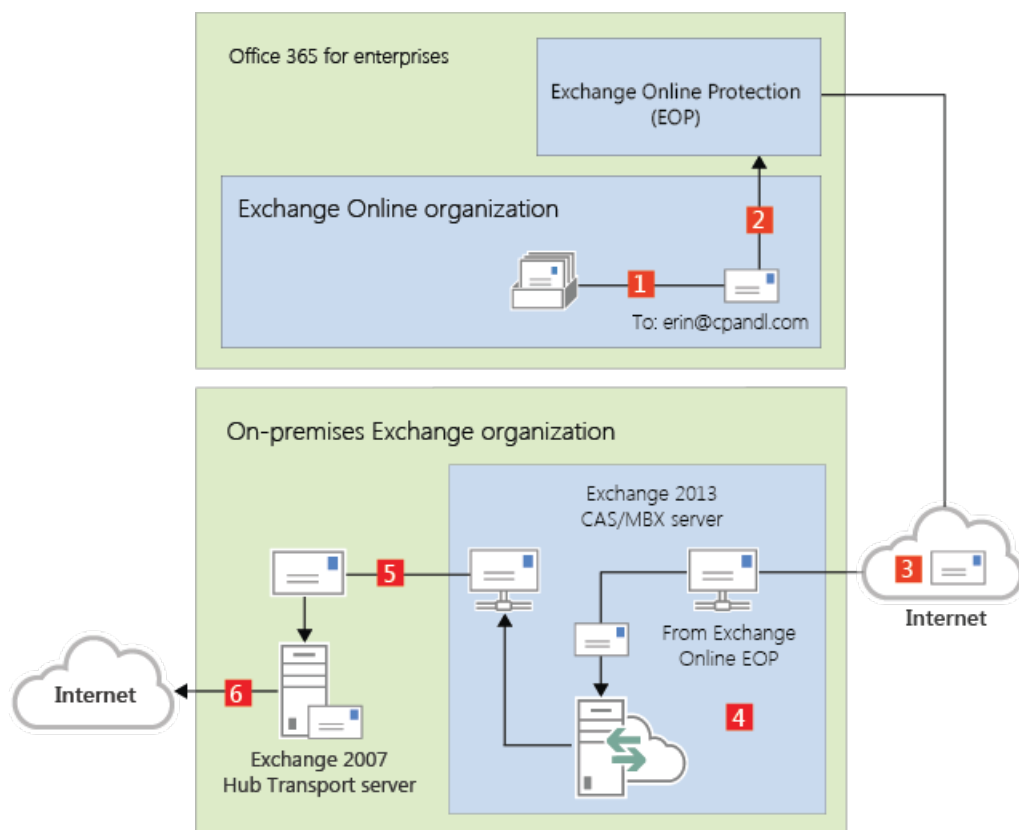


通过本地组织路由来自 Exchange Online 的 Internet 邮件(集中式邮件传输已启用)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 EOP。
3. EOP 配置为将所有 Internet 出站邮件发送给内部部署服务器，因此邮件会路由到 Exchange 2013 客户端访问服务器。邮件使用 TLS 发送。
4. Exchange 2013 客户端访问服务器对 David 的邮件执行遵从性、防病毒以及管理员配置的任何其他过程。
5. Exchange 2013 客户端访问服务器将邮件转发到 Exchange 2007 集线器传输服务器。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。
6. Exchange 2007 集线器传输服务器查找 cpandl.com 的 MX 记录，然后将邮件发送到位于 Internet 上的 cpandl.com 邮件服务器。

通过内部部署组织路由的来自 Exchange Online 发件人的邮件(启用集中邮件传输)



Exchange 2013 和 Exchange 2010 的混合部署

2019/6/5 •

随着 Microsoft Exchange Server 2013 引入混合配置向导的最新改进和体系结构更改，配置和管理基于 Exchange 2013 的与 Exchange 2010 混合的部署变得更加简单。无论是要将 Exchange 2010 内部部署与 Exchange Online 组织连接以实现长期共存，还是要作为云迁移策略的一部分，了解混合部署概念都十分重要。

选择以下一个主题开始并了解详细信息：

[Exchange 2013/Exchange 2010 混合部署中的服务器角色](#)

[Exchange 2013/Exchange 2010 混合部署中的混合管理](#)

[Exchange 2013/Exchange 2010 混合部署中的边缘传输服务器](#)

[Exchange 2013/Exchange 2010 混合部署中的传输选项](#)

[Exchange 2013/Exchange 2010 混合部署中的传输路由](#)

Exchange 2013/Exchange 2010 混合部署中的服务器角色

2019/6/5 •

在 Exchange 2010 组织中配置混合部署时, 我们强烈建议至少有一个 Exchange 2013 服务器, 其中包含现有 Exchange 2010 组织中的客户端访问和邮箱服务器角色。Exchange 2013 客户端访问服务器和邮箱服务器协调现有的 Exchange 2010 本地组织和 Exchange Online 组织之间的通信。此通信包括本地组织与 Exchange Online 组织之间的邮件传输和消息功能。

我们强烈建议在本地组织中安装多个 Exchange 2013 服务器, 以帮助提高混合部署功能的可靠性和可用性。

混合部署中的服务器角色

下面是混合部署中的 Exchange 2013 服务器角色的快速概述:

- **客户端访问服务器角色:** Exchange 2013 客户端访问服务器角色继续提供许多与贵组织中的 Exchange 2010 客户端访问服务器通常一起提供的功能, 其中包含支持混合的一些附加功能。Exchange 2010 的部署和共存。客户端访问服务器还处理从 Exchange Online 组织发送到本地组织的安全邮件, 以及处理混合部署中的传输规则、日记策略和到邮箱服务器的邮件传递。在客户端访问服务器上配置了专门的接收连接器以支持安全混合邮件传输。所有客户端连接(包括 Outlook 客户端访问、Outlook Web App 和 Outlook Anywhere)都通过客户端访问服务器角色进行。内部部署组织与 Exchange Online 组织之间的组织关系功能(如忙/闲共享)也由客户端访问服务器角色处理。

有关详细信息, 请参阅[客户端访问服务](#)。

- **邮箱服务器角色:** Exchange 2013 邮箱服务器角色处理从内部部署组织发送到 Exchange Online 组织的安全邮件邮件。尽管不典型, 但它也可以托管本地收件人邮箱并与通过本地客户端访问服务器代理的 Exchange Online 组织通信。在邮箱服务器角色上默认配置了专门的发送连接器以支持安全混合邮件传输。

有关详细信息, 请参阅[Mailbox Server](#)。

根据所需的混合部署配置, Exchange 2013 服务器需要安装一个或两个服务器角色:

- **单一 exchange server:** 如果选择在内部部署组织中安装一台 Exchange 服务器, 则需要在单台服务器上同时安装客户端访问和邮箱服务器角色。
- **多个 exchange 服务器:** 如果选择在内部部署组织中安装多个 exchange 服务器, 则可以在内部部署组织中的不同服务器上安装服务器角色。例如, 可以安装一个安装了邮箱和客户端访问服务器角色的 Exchange 2013 服务器, 同时也再安装一个仅安装了客户端访问服务器角色的 Exchange 服务器。但是, 最佳实践及推荐的服务器配置是在内部部署组织中部署的“每个”Exchange 2013 服务器上同时安装客户端访问和邮箱服务器。

有关 Exchange 容量规则的详细信息, 请参阅[了解容量规划中的多个服务器角色配置](#)。

混合部署中的 Exchange 服务器功能

Exchange 服务器为混合部署中的内部部署组织提供了几个重要功能:

- **联合:** exchange 2013 和 exchange 2010 服务器使您能够为内部部署组织创建与 Microsoft 联合网关的联合身份验证信任。Microsoft 联合网关是 Microsoft 提供的一项基于云的免费服务, 该服务可充当内部部署组织与 Office 365 租户组织之间的信任代理。联合身份验证是关于在内部部署组织与 Exchange Online 组织之间创建组织关系的要求。

有关详细信息, 请参阅[Understanding Federation](#)。

- **组织关系:** 通过使用客户端访问服务器角色的 Exchange 2013 服务器, 可以在内部部署组织和 Exchange Online 组织之间创建组织关系关系。混合部署中的许多其他服务 (包括日历忙/闲信息共享、邮件跟踪以及内部部署组织与 Exchange Online 组织之间的邮箱移动) 需要组织关系。

有关详细信息, 请参阅 [Understanding Federated Sharing](#)。

- **邮件传输:** 具有客户端访问和邮箱服务器角色的 Exchange 2013 服务器负责混合部署中的邮件传输。通过使用发送和接收连接器, 这些服务器可用作传入外部邮件的连接终结点, 并提供到 Internet 和 Exchange Online 组织的出站邮件传递。

有关详细信息, 请参阅 [Exchange 2013/Exchange 2010 混合部署中的传输选项](#)。

- **邮件传输安全性:** 具有客户端访问和邮箱服务器角色的 Exchange 2013 服务器通过使用 Exchange 中的域安全功能, 可帮助保护内部部署组织与 Exchange Online 组织之间的邮件通信安全。可以通过将相互传输层安全性身份验证和加密用于邮件通信, 来增强安全。

有关详细信息, 请参阅[了解域安全性](#)。

- **Outlook Web App:** 具有客户端访问服务器角色的 Exchange 2013 服务器支持将单个 URL 终结点配置为与内部部署和 Exchange Online 邮箱的外部连接。对于内部部署邮箱, 客户端访问服务器被配置为响应 Outlook Web App 请求。对于 Exchange Online 组织邮箱, 客户端访问服务器被配置为自动显示到 Exchange Online 组织上的 Outlook Web App 终结点的链接。

有关详细信息, 请参阅[web 上的 Outlook](#)。

Exchange 服务器拓扑

如果添加额外的 Exchange 2013 服务器来支持混合部署, 则 Exchange 服务器的部署将与其他任何 Exchange 服务器部署到现有 Exchange 2010 组织的方式非常相似。为混合部署配置现有的本地 Exchange 2010 组织不需要任何特殊的 Exchange 服务器拓扑。但是必须在 Exchange 2010 服务器上安装 Exchange 2010 Service Pack 3 (SP3) 和 Exchange 2013 累积更新 1 (CU1) 或更高版本以启用 Office 365 的兼容性和完全混合功能。

下表简要描述配置了混合部署后的服务更改。

服务	混合部署之前	混合部署之后	说明
邮件传输(入站和出站)	Exchange 2010 客户端访问服务器	Office 365 包含 Exchange 2013 客户端访问服务器或 Exchange Online Protection (EOP)	域的 MX(邮件交换器)记录可以保留不变, 或者更新为指向 EOP。
Outlook Web App 公用 URL	Exchange 2010 客户端访问服务器	Exchange 2013 客户端访问服务器	Exchange 2013 客户端访问服务器将本地邮箱的 Outlook Web App 请求代理到 Exchange 2010 客户端访问服务器。Outlook Web App Online 上托管的邮箱的 Exchange 请求随指向 Exchange Online Outlook Web App URL 的链接一起提供。

Exchange 服务器软件

Exchange 2013 CU1 或更高版本通过混合配置向导启用混合部署功能。在安装额外的 Exchange 2013 服务器时, 可使用任何 Exchange 2013 CU1 或更高版本介质。

有关如何下载 Exchange Server 的最新版本的信息, 请参阅[Exchange 更新](#)。

IMPORTANT

在配置混合部署时, 您需要为您的混合服务器授予许可证。现在, HCW 可以在不转到单独的网站或呼叫 Microsoft 支持的情况下, 检测并许可指定的本地 Exchange 2010、Exchange 2013 或 Exchange 2016 混合服务器, 以供免费使用。您可以在[此处](#)访问 HCW。请注意, Exchange 2019 混合服务器不提供免费 Exchange Server 许可证。

Exchange 2013/Exchange 2010 混合部署中的混合管理

2019/6/5 •

在 Exchange 2010 内部部署组织中安装运行 Microsoft Exchange Server 2013 的服务器时，会自动在服务器上安装 Exchange 2013 管理工具。您将使用以下工具来配置和管理内部部署 Exchange 和 Exchange Online 组织的混合功能：

- **Exchange 管理中心:** EAC 是一种基于 web 的管理 2013 控制台，它易于使用，并针对内部部署、在线或混合 Exchange 部署进行了优化。EAC 补充了用于管理 Exchange Server 2010 的 Exchange 管理控制台 (EMC) 和 Exchange 控制面板 (ECP) 界面。
- **Exchange 命令行管理程序:** exchange 命令行管理程序是基于 Windows PowerShell 的命令行界面。

Exchange 管理中心

EAC 允许您同时在内部部署 Exchange 服务器和 Exchange Online 组织上执行许多部署任务和最常见的日常管理任务。默认情况下，它将在每个 Exchange 2013 服务器上安装。此外，由于它是基于 Web 的管理控制台，您还可以使用网络中的其他计算机的 Web 浏览器或通过使用 ECP 虚拟目录 URL 访问它。

IMPORTANT

如果想要使用邮箱位于 Exchange 2010 邮箱服务器中的帐户(例如域管理员帐户)访问 EAC，则必须在浏览器中使用以下地址访问 EAC: > `https://<FQDN of Exchange 2013 Client Access server>/ECP? ExchClientVer=15`

您可以通过选择 Office 365 跨界导航选项卡来访问 EAC 中的 Exchange Online 组织。跨界导航允许您在 Exchange Online 和内部部署 Exchange 组织之间轻松切换。如果您已经配置混合部署，选择 Office 365 选项卡将允许您管理 Exchange Online 组织和收件人对象。如果您没有 Exchange Online 组织，选择 Office 365 链接会将您转到 Office 365 注册页面。

有关 EAC 的详细信息，请参阅 [Exchange Administration Center](#)。

Exchange 命令行管理程序

Exchange 命令行管理程序可以执行 EAC 执行的任何任务，以及只能在 Exchange 命令行管理程序中执行的某些其他任务。Exchange 命令行管理程序是安装 Exchange 2013 管理工具时安装在计算机上的 Windows PowerShell 脚本和 cmdlet 的集合。只有在使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，才会加载这些脚本和 cmdlet。如果你直接打开 Windows PowerShell，则不会加载 Exchange 脚本和 cmdlet，并且你将无法管理内部部署组织。

NOTE

你可以创建到本地内部部署组织的手动 Windows PowerShell 连接，方式与手动连接到以下 Exchange Online 组织类似。但是，强烈建议你使用 Exchange 命令行管理程序图标来打开 Exchange 命令行管理程序，以管理内部部署 Exchange 服务器。

当你在安装了管理工具的计算机上使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序时，可以管理内部部署组织。但是，在使用此图标打开 Exchange 命令行管理程序时不能管理 Exchange Online 组织。这是因为使用 Exchange 命令行管理程序图标打开 Exchange 命令行管理程序会自动连接到本地 Exchange 服务器。

如果要使用 Windows PowerShell 管理 Exchange Online 组织，必须直接打开 Windows PowerShell，而不要通过

Exchange 命令行管理程序图标打开。打开 Windows PowerShell 后，你便可以手动指定要连接的位置。当你创建手动连接时，可在 Office 365 租户组织中指定一个管理员帐户，然后运行命令以创建连接。建立该连接后，你即可使用有权运行的 Exchange cmdlet。有关更多信息，请参阅[使用 Windows PowerShell](#)。

如果你不熟悉 Exchange 命令行管理程序，请查看 [Exchange Management Shell](#)，以了解有关 Exchange 命令行管理程序的工作方式的基本信息、命令语法及更多内容。

Exchange 2013/Exchange 2010 混合部署中的边缘传输服务器

2019/6/5 •

使用 Microsoft Exchange 部署的边缘传输服务器部署在组织的内部部署外围网络中。它们是未加入域的计算机，可处理面向 Internet 的邮件流，并充当内部网络中的 Exchange 服务器的 SMTP 中继和智能主机。

对于想要使用边缘传输服务器的 Exchange 2013 组织，提供部署 Exchange Server 2013 边缘传输服务器或运行 Exchange 2010 Service Pack 3 (SP3) 的 Exchange 2010 边缘传输服务器的选项。如果您不想将内部 Exchange 2013 客户端访问或邮箱服务器直接暴露给 Internet，请使用边缘传输服务器。

可在以下位置了解 Exchange 2013 边缘传输服务器角色的详细信息：[Overview of the Edge Transport Server Role](#)。

有关 Exchange 2010 边缘传输服务器的详细信息，请参阅[边缘传输服务器角色概述](#)。

基于 Exchange 2013 的混合部署组织中的边缘传输服务器

在内部部署与混合部署中的 Exchange Online 组织之间路由的邮件要求 Microsoft Exchange Online Protection (EOP) 服务代表 Exchange Online 直接连接到运行 Exchange 2013 或 Exchange 2010 SP3 的边缘传输服务器。

IMPORTANT

如果您在其他位置具有其他 Exchange 2010 边缘传输服务器，但是这些服务器不处理混合传输，那么这些服务器无需升级到 Exchange 2010 SP3。然而，如果希望 EOP 在未来连接至混合传输的其他边缘传输服务器，那么这些服务器必须使用 Exchange 2010 SP3 升级或升级到 Exchange 2013 边缘传输服务器。

向混合部署添加边缘传输服务器

当配置混合部署时，在内部部署组织中部署边缘传输服务器是可选项。当配置混合部署时，混合配置向导允许您选择一个或多个客户端访问和邮箱服务器用于混合邮箱传输，或选择一个或多个内部部署边缘传输服务器处理 Exchange Online 组织的混合邮件传输。

在将边缘传输服务器添加到混合部署时，混合配置向导将代表内部 Exchange 2013 客户端访问和邮箱服务器与 EOP 进行通信。边缘传输服务器作为内部部署邮箱服务器和 EOP 之间的中继，用于从内部部署组织到 Exchange Online 的出站邮件。边缘传输服务器还作为内部部署客户端访问服务器之间的中继，用于从 Exchange Online 组织到内部部署组织的入站邮件。所有以前由客户端访问服务器处理的连接安全性由边缘传输服务器处理。收件人查找、合规性策略和其他邮件检查继续由客户端访问服务器处理。

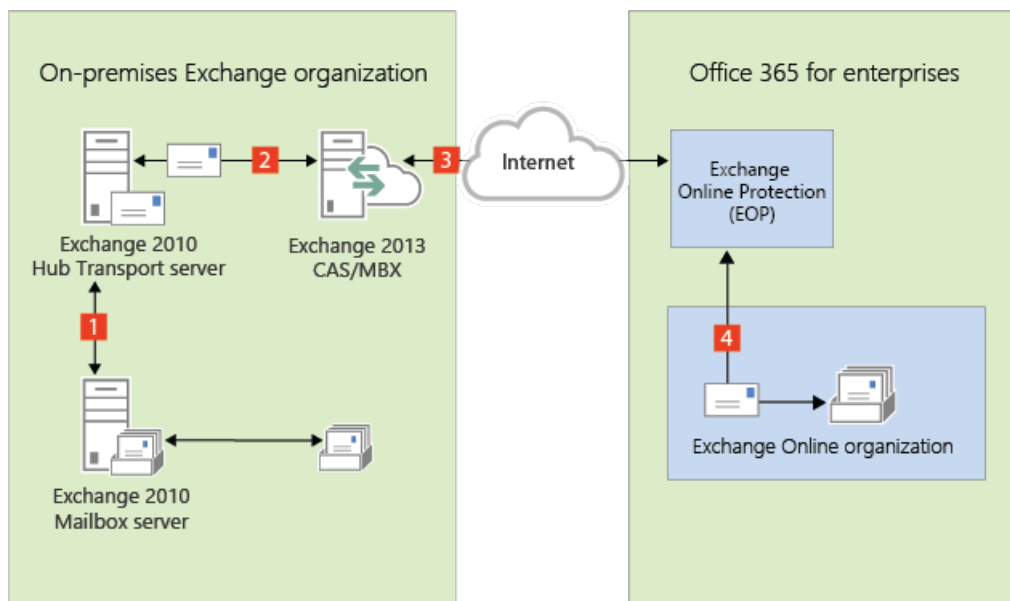
不使用边缘传输服务器的邮件流

以下过程与图表描述了在无边缘传输服务器部署时，内部部署组织与 Exchange Online 之间的邮件的路径：

1. 从内部部署组织到 Exchange Online 组织中收件人的出站邮件将从 Exchange 2010 邮箱服务器中的邮箱发送到 Exchange 2010 集线器传输服务器。
2. Exchange 2010 集线器传输服务器将邮件发送到 Exchange 2013 邮箱服务器。
3. Exchange 2013 邮箱服务器将邮件直接发送至 Exchange Online EOP 公司。
4. EOP 将邮件传送给 Exchange Online 组织。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

从 Exchange Online 组织发送到内部部署组织中的收件人的邮件将遵循相反的路由。

未部署边缘传输服务器的混合部署中的邮件流



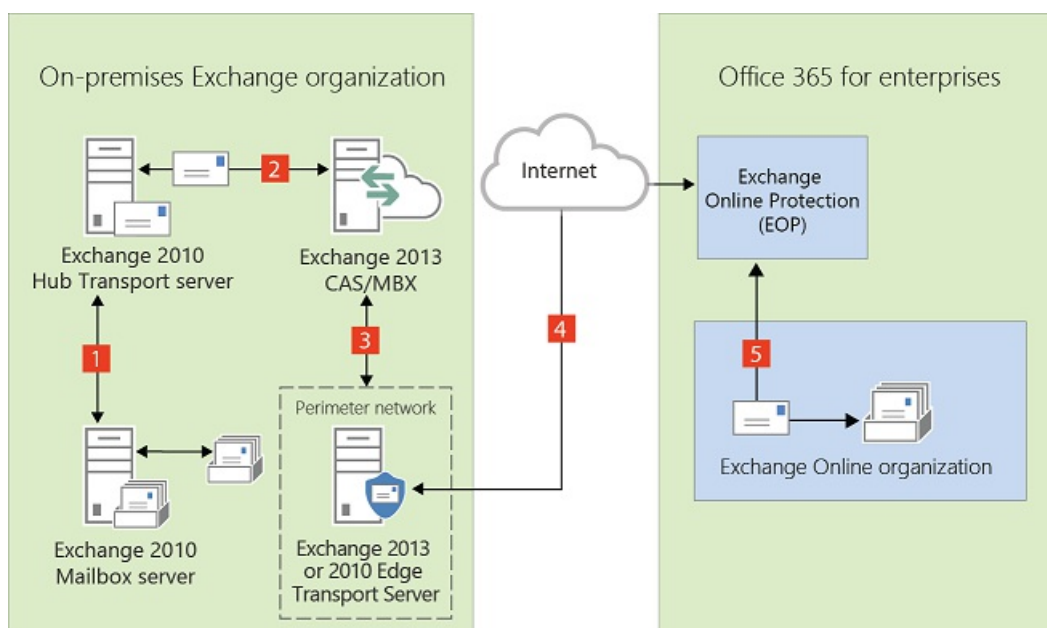
使用边缘传输服务器的邮件流

以下流程介绍了在部署边缘传输服务器后，邮件在内部部署组织与 Exchange Online 之间采用的路径。从内部部署组织到 Exchange Online 组织中收件人的邮件是从 Exchange 2010 邮箱服务器发送的：

1. 从内部部署组织到 Exchange Online 组织中收件人的出站邮件将从 Exchange 2010 邮箱服务器中的邮箱发送到 Exchange 2010 集线器传输服务器。
2. Exchange 2010 集线器传输服务器将邮件发送到 Exchange 2013 邮箱服务器。
3. Exchange 2013 邮箱服务器将邮件发送至 Exchange 2013 或 Exchange 2010 SP3 边缘传输服务器。
4. 边缘传输服务器将邮件发送到 Exchange Online EOP 公司。
5. EOP 将邮件传送给 Exchange Online 组织。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

从 Exchange Online 组织发送到内部部署组织中的收件人的邮件将遵循相反的路由。

部署了 Exchange 2013 或 2010 SP3 边缘传输服务器的混合部署中的邮件流



Exchange 2013/Exchange 2010 混合部署中的传输选项

2019/6/5 •

在混合部署中，可以具有既驻留在本地 Exchange 组织中也驻留在 Exchange Online 组织中的邮箱。为了使这两个单独组织对用户及在他们之间交换的邮件表现为一个合并的组织，关键组件是混合传输。通过混合传输，在任一组织中的收件人之间发送的邮件会经过身份验证、加密并使用传输层安全性 (TLS) 传输，并且向 Exchange 组件 (如传输规则、日记和反垃圾邮件策略) 显示为“内部”。混合传输是由 Exchange 2013 中的混合配置向导自动配置的。

为了在混合配置向导中使用混合传输配置，接受来自 Microsoft Exchange Online Protection (EOP) (用于处理 Exchange Online 组织的传输) 的连接的本地的 SMTP 终结点必须是 Exchange 2013 客户端访问服务器、Exchange 2013 边缘传输服务器或 Exchange Server 2010 SP3 边缘传输服务器。

IMPORTANT

本地 Exchange 2013 客户端访问服务器或 Exchange 2013/Exchange 2010 SP3 边缘传输服务器与 EOP 之间可以没有任何其他 SMTP 主机或服务。当邮件经过非 Exchange 2013 服务器、预 Exchange 2010 SP3 服务器或 SMTP 主机时，会删除添加到邮件中用于启用混合传输功能的信息。如果在组织中部署了 Exchange 2010 SP2 边缘传输服务器，并且要将这些服务器用于混合传输，则它们必须升级到 Exchange 2010 SP3。

从外部 Internet 发件人发送到两个组织中的收件人的入站邮件会采用通用入站路由。从组织发送到外部 Internet 收件人的出站邮件可以采用通用出站路由，也可以通过独立的路由发送。

在计划和配置混合部署时需要选择如何路由入站和出站邮件。发送到和发送自内部部署和 Exchange Online 组织中收件人的入站和出站邮件采用的路由取决于以下因素：

- 您是否希望通过 Microsoft Office 365 和 EOP 或内部部署组织路由内部部署和 Exchange Online 邮箱的入站 Internet 邮件？

可以选择通过内部部署组织或通过 EOP 和 Exchange Online 组织为两个组织路由入站 Internet 邮件。两个组织入站邮件的路由取决于是否在混合部署中启用了集中邮件传输。

- 是要通过内部部署组织 (集中邮件传输) 路由来自 Exchange Online 组织的出站邮件到外部收件人，还是要将其直接路由到 Internet？

作为集中邮件传输，可以先通过内部部署组织路由来自 Exchange Online 组织中邮箱的所有邮件，然后再将这些邮件传递到 Internet。此方法用于合规性方案，在这类方案中，发送到和发送自 Internet 的所有邮件都必须由内部部署服务器进行处理。或者，可以配置 Exchange Online 以将外部收件人的邮件直接传递到 Internet。

NOTE

仅对具有与符合性相关的特定传输需求的组织推荐使用集中式邮件传输。我们建议典型的 Exchange 组织不要启用集中式邮件传输。

- 是否要在内部部署组织中部署边缘传输服务器？

如果您不想将加入域的内部 Exchange 2013 服务器直接向 Internet 公开，则可在外围网络中部署 Exchange 2013 边缘传输服务器或 Exchange 2010 SP3 边缘传输服务器。有关向混合部署添加边缘传输服务器的详细信息，请参阅 [Exchange 2013/Exchange 2010 混合部署中的边缘传输服务器](#)。

无论如何路由发送到和发送自 Internet 的邮件，在内部部署与 Exchange Online 组织之间发送的所有邮件都使用安全传输进行发送。有关详细信息，请参阅本主题后面的[受信任通信](#)。

有关这些选项如何影响您的组织中的邮件路由的详细信息，请参阅[Exchange 2013/Exchange 2010 混合部署中的传输路由](#)。

混合部署中的 Exchange Online Protection

EOP 是 Microsoft 提供的联机服务，由许多公司用于保护其内部部署组织免受病毒、垃圾邮件、欺诈邮件和策略违规的危害。在 Office 365 中，EOP 用于保护 Exchange Online 组织免受相同威胁的危害。在注册 Office 365 时，会自动创建与您的 Exchange Online 组织关联的 EOP 公司。

EOP 公司包含一些邮件传输设置，可以为 Exchange Online 组织配置这些设置。可以指定哪些 SMTP 域必须来自特定 IP 地址，需要 TLS 和安全套接字层 (SSL) 证书，可以绕过合规性策略，等等。EOP 是 Exchange Online 组织的前门。所有邮件(无论其来源如何)都必须先经过 EOP，然后才能到达 Exchange Online 组织中的邮箱。而且，从 Exchange Online 组织发送的所有邮件都必须先经过 EOP，然后才能到达 Internet。

在使用混合配置向导配置混合部署时，会在内部部署组织以及为 Exchange Online 组织设置的 EOP 公司中自动配置所有传输设置。混合配置向导会在此 EOP 公司中配置所有入站和出站连接器及其他设置，以保护在内部部署与 Exchange Online 组织之间发送的邮件并将邮件路由到正确目标。如果要为 Exchange Online 组织配置自定义传输设置，则也会在此 EOP 公司中配置这些设置。

受信任通信

为了帮助保护内部部署和 Exchange Online 组织中的收件人，并帮助确保不会截获和读取组织之间发送的邮件，内部部署组织与 EOP 之间的传输会配置为使用强制 TLS。TLS 传输使用受信任第三方证书颁发机构 (CA) 提供的安全套接字层 (SSL) 证书。EOP 与 Exchange Online 组织之间的邮件也使用 TLS。

当使用强制 TLS 传输时，发送和接收服务器会检查在其他服务器上配置的证书。对证书配置的使用者名称或使用替代名称 (SAN) 之一，必须与管理员在其他服务器上显式指定的 FQDN 匹配。例如，如果 EOP 配置为接受并保护从 mail.contoso.com FQDN 发送的邮件，则发送内部部署客户端访问或边缘传输服务器必须具有在主题名称或 SAN 中包含 mail.contoso.com 的 SSL 证书。如果不满足此要求，则 EOP 会拒绝连接。

NOTE

使用的 FQDN 无需与收件人的电子邮件域名匹配。唯一要求在于证书主题名称或 SAN 中的 FQDN 必须与接收或发送服务器配置为接受的 FQDN 匹配。

除了使用 TLS 以外，还可将组织之间的邮件作为“内部”邮件处理。此方法使邮件可以绕过反垃圾邮件设置和其他服务。

有关 SSL 证书和域安全性的详细信息，请参阅 [混合部署的证书要求](#) 和 [了解 TLS 证书](#)。

Exchange 2013/Exchange 2010 混合部署中的传输路由

2019/6/5 •

本主题讨论来自 Internet 的进站邮件和发送到 Internet 的出站邮件的路由选项。

IMPORTANT

不要在处理或修改 SMTP 通信的内部部署 Exchange 服务器和 Office 365 之间放置任何服务器、服务或设备。内部部署 Exchange 组织和 Office 365 之间的安全邮件流取决于组织之间发送的邮件中包含的信息。支持允许 TCP 端口 25 上的 SMTP 通信通过而无需修改的防火墙。如果服务器、服务或设备处理内部部署 Exchange 组织和 Office 365 之间发送的邮件，此信息将被删除。如果发生这种情况，该邮件将不再被视为组织内部邮件，并且将会对其应用反垃圾邮件筛选、传输和日记规则以及可能不适用于它的其他策略。

NOTE

本主题中的示例不包括将边缘传输服务器添加到混合部署中。邮件在内部部署组织、Exchange Online 组织与 Internet 之间采用的路由不会随着添加边缘传输服务器而更改。只有内部部署组织中的路由会更改。有关向混合部署添加边缘传输服务器的详细信息，请参阅 [Exchange 2013/Exchange 2010 混合部署中的边缘传输服务器](#)。

来自 Internet 的进站邮件

作为计划和配置混合部署的一部分，需要决定是否想要通过 Exchange Online 或本地组织路由来自 Internet 发件人的所有邮件。所有来自 Internet 发件人的邮件最初会传递到所选的组织，然后根据收件人邮箱所在的位置路由。是否选择通过 Exchange Online 或本地组织路由邮件取决于各种因素，包括是否想要对发送到两种组织的所有邮件应用合规性策略以及每个组织中的邮箱数等。

本地和 Exchange Online 组织中发送到收件人的路径取决于在混合部署中决定如何配置 MX 记录。首选方法是配置 MX 记录，使其指向 Office 365 中的 Exchange Online Protection (EOP)，因为该配置提供最准确的垃圾邮件筛选。混合邮件配置向导不配置本地或 Exchange Online 组织的进站 Internet 邮件的路由。如果想要更改进站 Internet 邮件传递的方式，则必须手动配置 MX 记录。

- **如果您将 MX 记录更改为指向 Office 365 中的 Exchange Online Protection 服务：**这是混合部署的推荐配置。所有发送到任一组织中的任何收件人的邮件都将首先通过 Exchange Online 组织路由。发往位于本地组织中的收件人的邮件会首先通过 Exchange Online 组织路由，随后传递到本地组织中的收件人。如果您的 Exchange Online 组织中的收件人数量比本地组织中的多，并且如果您希望邮件被 EOP 筛选，则推荐该路由。Exchange Online Protection 需要该配置选项，以提供对垃圾邮件的扫描和阻止。
- **如果您决定将 MX 记录保留为您的内部部署组织：**则所有发送到任一组织中的任何收件人的邮件都将首先通过您的内部部署组织进行路由。发往位于 Exchange Online 中的收件人的邮件会首先通过本地组织进行路由，随后传递到 Exchange Online 中的收件人。对于具有合规性策略（该策略要求日记解决方案检查发送到和发送至组织的邮件）的组织，此路由可能很有帮助。如果选取了该选项，则 Exchange Online Protection 将不能有效地扫描垃圾邮件。

有关详细信息，请参阅 [Mail flow best practices for Exchange Online and Office 365 \(Overview\)](#)。

阅读下面与您计划将从 Internet 收件人发送的邮件路由到内部部署和 Exchange Online 收件人的方式相匹配的章节。

通过 Exchange Online 组织路由入站 Internet 邮件

以下步骤和图表举例说明了在指向 MX 记录到 Office 365 组织中的 EOP 服务的情况下，混合部署中出现的入站邮件路径。邮件路径因是否选择启用集中邮件传输而异。

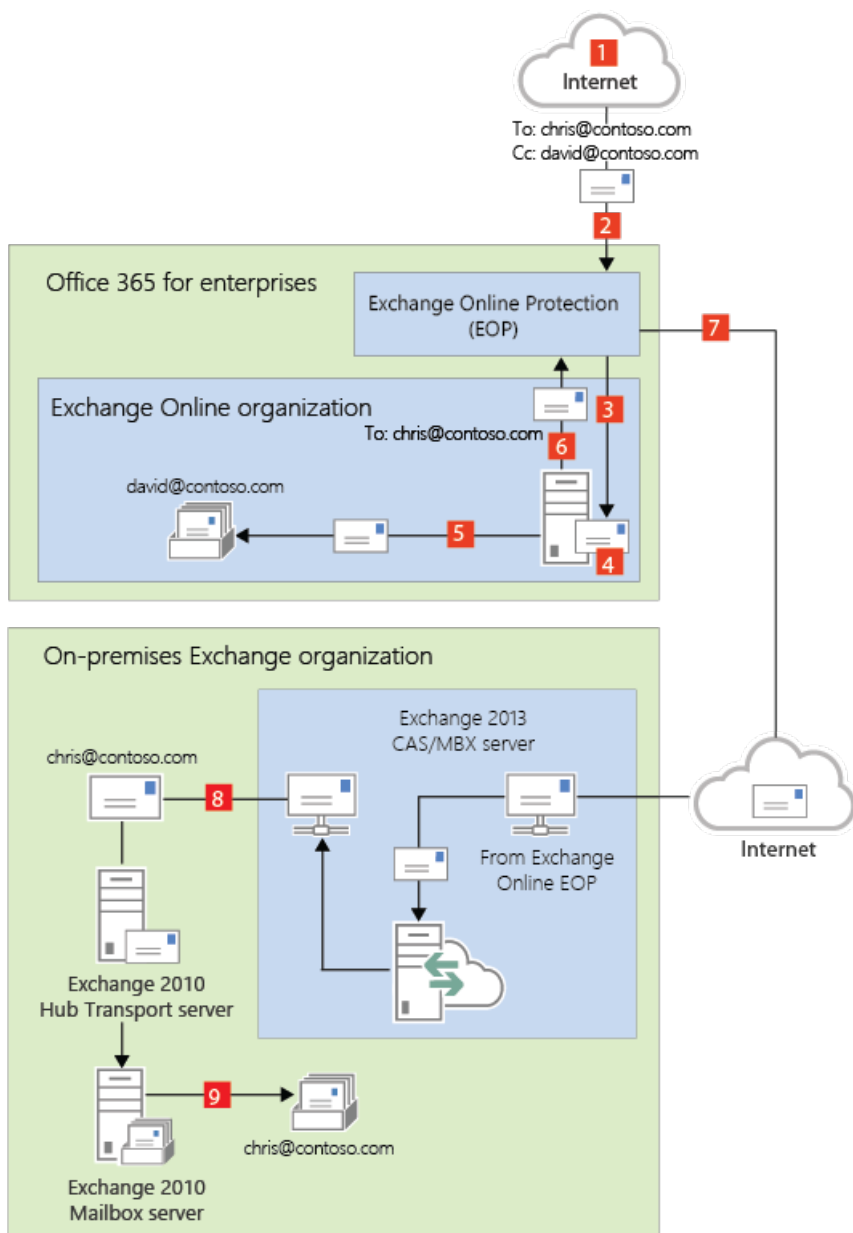
IMPORTANT

对于接收首先传递到 EOP 然后通过 Exchange Online 组织进行路由的邮件的每个内部部署邮箱，可能需要购买 EOP 许可证。有关详细信息，请与您的 Microsoft 经销商联系。

当集中邮件传输被禁用(默认配置)时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 chris@contoso.com 和 david@contoso.com。Chris 的邮箱位于内部部署组织中的 Exchange 2010 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 contoso.com 电子邮件地址，并且 contoso.com 的 MX 记录指向 EOP，所以邮件会传递到 EOP。
3. EOP 将两个收件人的邮件都路由到 Exchange Online。
4. Exchange Online 对邮件进行病毒扫描并对每个收件人执行查找。通过查找，确定 Chris 的邮箱位于内部部署组织中，而 David 的邮箱位于 Exchange Online 组织中。
5. Exchange Online 将邮件拆分为两个副本。将邮件的一个副本传递到 David 的邮箱。
6. 将第二个副本从 Exchange Online 发送回 EOP。
7. EOP 发送邮件到内部部署组织中的 Exchange 2013 客户端访问服务器。
8. Exchange 2013 客户端访问服务器通过在 Exchange 2013 服务器和 Exchange 2010 集线器传输服务器之间配置的路由组连接器发送邮件。
9. Exchange 2010 邮箱服务器接收邮件并传递到 Chris 的邮箱。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

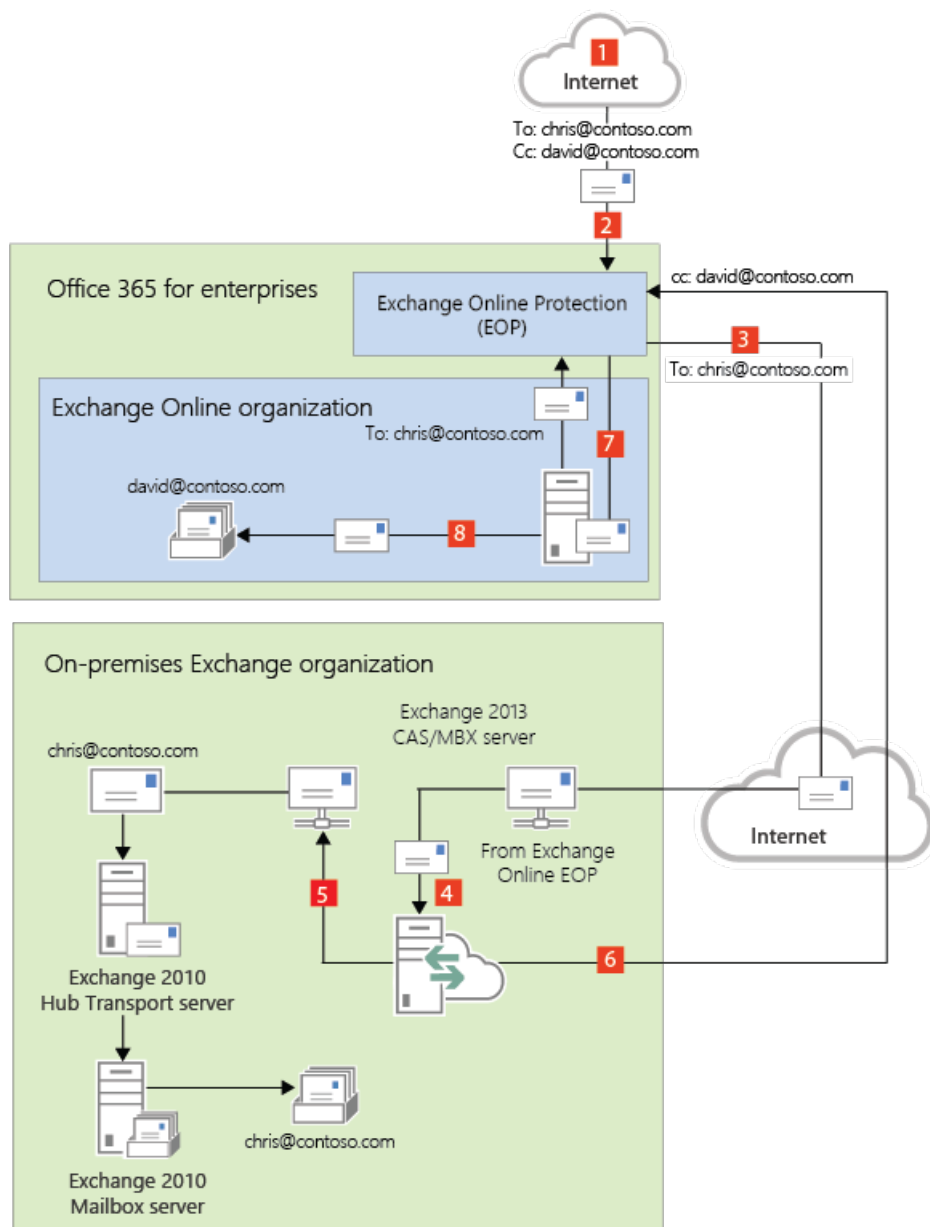
通过 **Exchange Online** 组织为内部部署组织和 **Exchange Online** 组织路由邮件，同时禁用集中邮件传输（默认配置）



当集中邮件传输被启用时，混合部署中的入站 Internet 邮件按以下路由：

1. 入站邮件从 Internet 发件人发送给收件人 chris@contoso.com 和 david@contoso.com。Chris 的邮箱位于内部部署组织中的 Exchange 2010 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 contoso.com 电子邮件地址，并且 contoso.com 的 MX 记录指向 EOP，所以邮件会传递到 EOP 并扫描病毒。
3. 由于启用了集中邮件传输，EOP 会将这两个收件人的邮件路由到内部部署 Exchange 2013 客户端访问服务器。
4. Exchange 2013 服务器为每个收件人执行查找。通过查找，确定 Chris 的邮箱位于内部部署组织中，而 David 的邮箱位于 Exchange Online 组织中。
5. Exchange 2013 服务器将邮件拆分为两个副本。邮件的一个副本被发送给 Chris 在内部部署 Exchange 2010 邮箱服务器中的邮箱。
6. 第二个副本从 Exchange 2013 服务器发送回 EOP。
7. EOP 将邮件发送到 Exchange Online。
8. Exchange 将邮件发送到 David 的邮箱。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

通过 Exchange Online 组织为内部部署组织和 Exchange Online 组织路由邮件，同时启用集中邮件传输



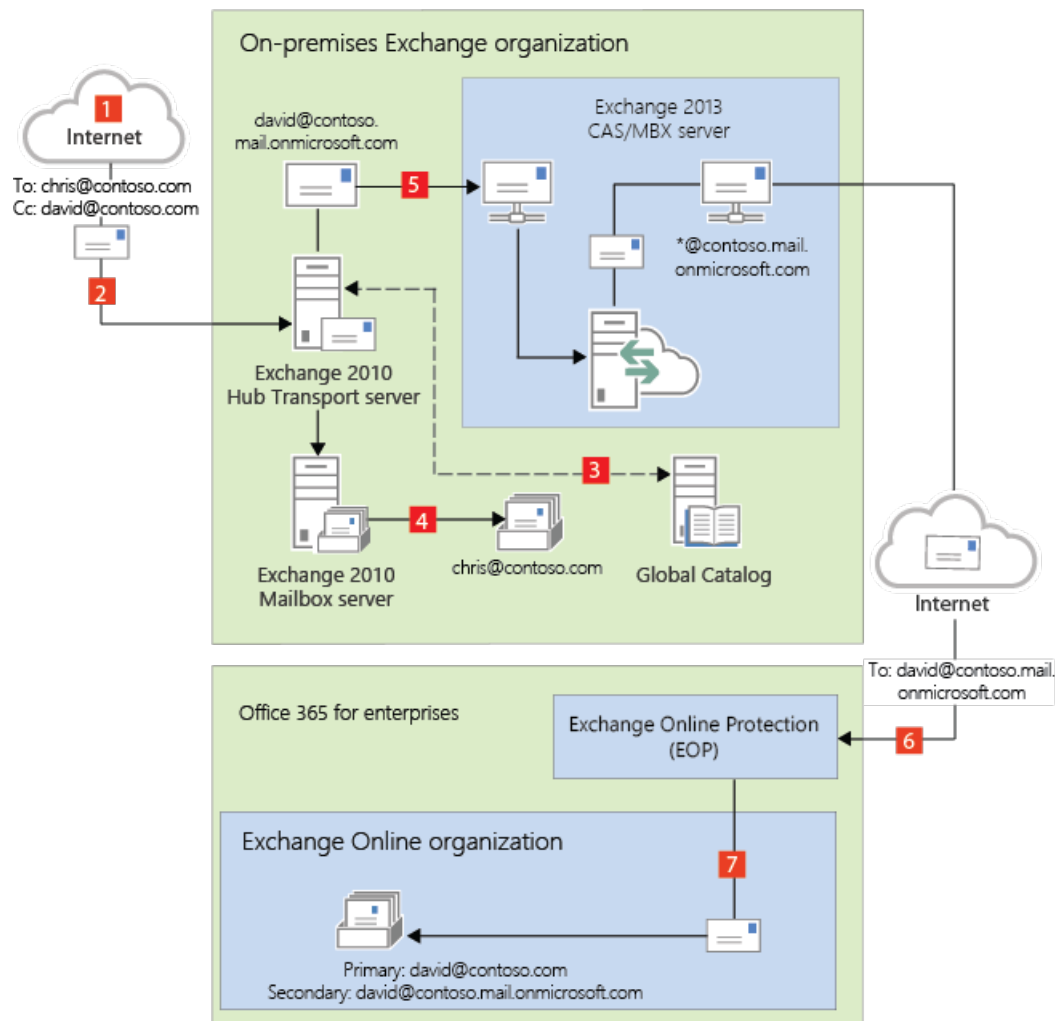
通过内部部署组织路由入站 Internet 邮件

以下步骤和图表举例说明了在决定保持指向您的内部部署组织的 MX 记录的情况下，混合部署中将出现的入站 Internet 邮件路径。

1. 入站邮件从 Internet 发件人发送给收件人 chris@contoso.com 和 david@contoso.com。Chris 的邮箱位于内部部署组织中的 Exchange 2010 邮箱服务器上。David 的邮箱位于 Exchange Online 中。
2. 因为这两个收件人都有 contoso.com 电子邮件地址，并且 contoso.com 的 MX 记录指向内部部署组织，所以邮件会传递到 Exchange 2010 集线器传输服务器。
3. Exchange 2010 邮箱服务器使用内部部署全局编录服务器对每个收件人执行查找。通过全局编录查找，该服务器可确定 Chris 的邮箱位于 Exchange 2010 邮箱服务器上，而 David 的邮箱在 Exchange Online 组织中，并具有混合路由地址 david@contoso.mail.onmicrosoft.com。
4. Exchange 2010 邮箱服务器将邮件拆分为两个副本。将邮件的一个副本传递到 Chris 的邮箱。
5. 邮件的第二个副本通过在 Exchange 2013 服务器与 Exchange 2010 服务器之间配置的路由组连接器发送。
6. Exchange 2013 邮箱服务器通过配置为使用 TLS 的发送连接器将邮件发送到 EOP。EOP 接收传送给 Exchange Online 组织的邮件。
7. EOP 将邮件发送到 Exchange Online 组织，在该组织中对邮件进行病毒和基于内容的垃圾邮件的扫描并将

其传递到 David 的邮箱。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。

通过内部部署组织为内部部署组织和 Exchange Online 组织路由邮件



发送到 Internet 的出站邮件

除了选择如何对发送给组织中的收件人的进站邮件进行路由之外，还可以选择如何对从 Exchange Online 收件人发送的出站邮件进行路由。运行“混合配置”向导时，可以选择两个选项之一：

- **不启用集中邮件传输：**默认情况下，在“混合配置”向导中选择此选项可将从 Exchange Online 组织发送的出站邮件直接路由到 Internet。如果无需将任何内部部署合规性策略或其他处理规则应用于从 Exchange Online 组织中的收件人发送的邮件，请使用此选项。
- **启用集中邮件传输：**选择此选项可通过内部部署组织路由从 Exchange Online 组织发送的出站邮件。除了向同一个 Exchange Online 组织中的其他收件人发送的邮件之外，从 Exchange Online 组织中的收件人发送的所有出站邮件都会通过内部部署组织发送。这使您可以将合规性规则应用于这些邮件以及必须应用于所有收件人（无论这些收件人是处于 Exchange Online 组织中还是处于内部部署组织中）的任何其他过程或要求。

NOTE

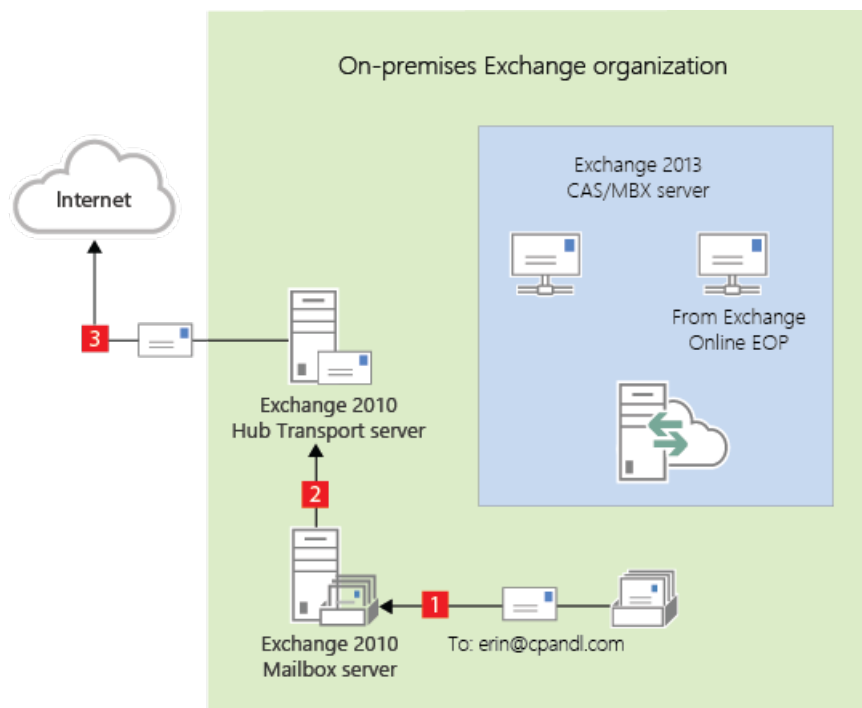
仅对具有与符合性相关的特定传输需求的组织推荐使用集中式邮件传输。我们建议典型的 Exchange 组织不要启用集中式邮件传输。

从内部部署收件人发送的邮件会始终使用 DNS 直接发送到 Internet 收件人（无论在“混合配置”向导中选择了以上哪个选项）。

以下步骤和图表说明从内部部署收件人发送的邮件的出站邮件路径。

1. 在内部部署 Exchange 2010 邮箱服务器上拥有一个邮箱的 Chris 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange 2010 邮箱服务器将邮件发送到 Exchange 2010 集线器传输服务器。
3. Exchange 2010 集线器传输服务器查找 cpandl.com 的 MX 记录, 然后将邮件发送到位于 Internet 上的 cpandl.com 邮件服务器。

从内部部署发件人发送给 Internet 收件人的邮件



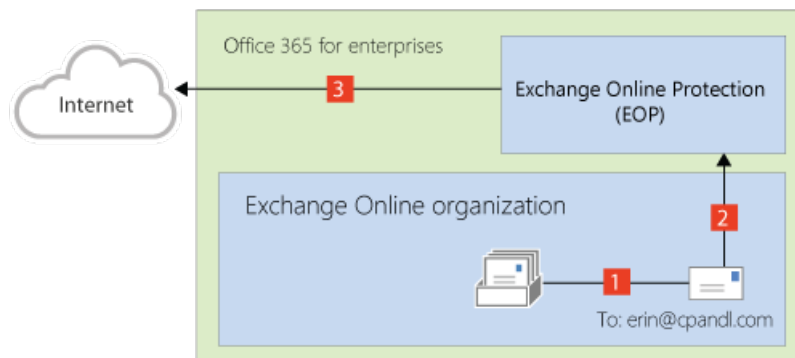
阅读下面与您计划将从 Exchange Online 组织中收件人发送的邮件路由到 Internet 收件人的方式相匹配的章节。

使用 DNS (集中式邮件传输已禁用) 传递来自 Exchange Online 的 Internet 邮件。

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 Exchange Online EOP 服务。
3. EOP 会在 MX 记录中查找 cpandl.com, 并将邮件发送给位于 Internet 上的 cpandl.com 邮件服务器。

来自 Exchange Online 发件人的邮件将直接路由到 Internet, 同时禁用集中邮件传输 (默认配置)



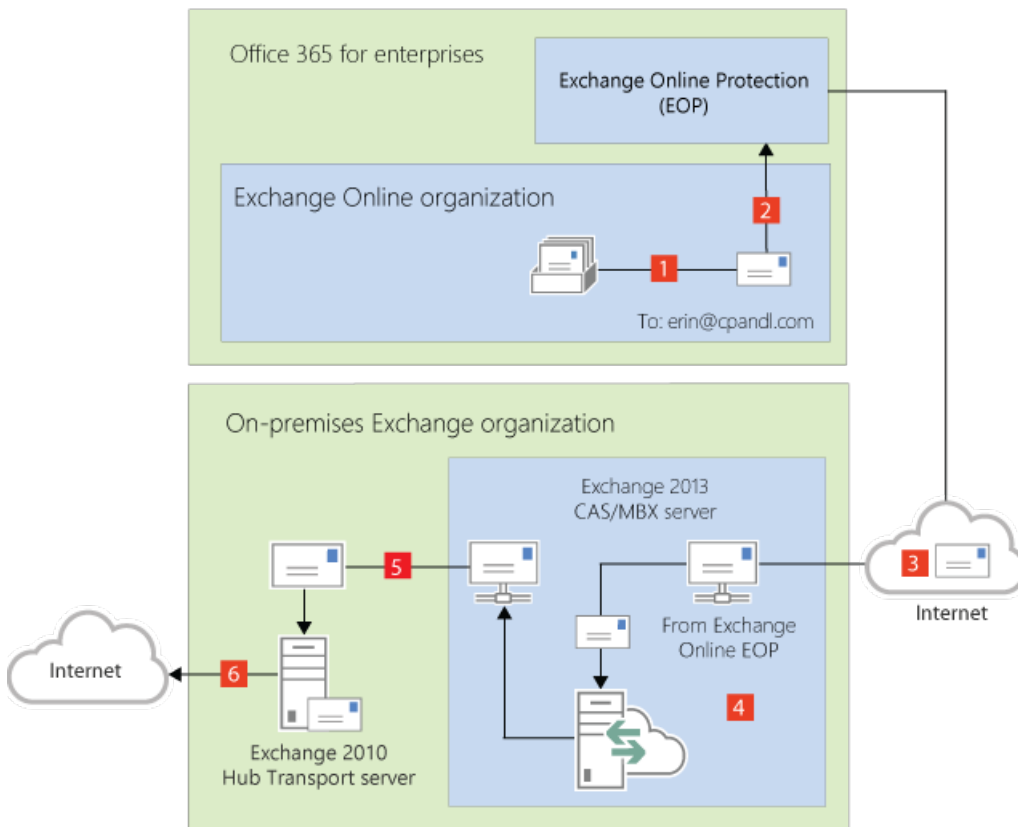
通过本地组织路由来自 Exchange Online 的 Internet 邮件 (集中式邮件传输已启用)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online

recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. 在内部部署 Exchange Online 组织中拥有一个邮箱的 David 将一封邮件发送给外部 Internet 收件人 erin@cpandl.com。
2. Exchange Online 对邮件进行病毒扫描并将邮件发送给 EOP。
3. EOP 配置为将所有 Internet 出站邮件发送给内部部署服务器，因此邮件会路由到 Exchange 2013 客户端访问服务器。邮件使用 TLS 发送。
4. Exchange 2013 客户端访问服务器对 David 的邮件执行遵从性、防病毒以及管理员配置的任何其他过程。
5. Exchange 2013 客户端访问服务器将邮件转发到 Exchange 2010 集线器传输服务器。在此示例中，客户端访问和邮箱服务器角色安装在同一 Exchange 2013 服务器上。
6. Exchange 2010 集线器传输服务器查找 cpandl.com 的 MX 记录，然后将邮件发送到位于 Internet 上的 cpandl.com 邮件服务器。

通过内部部署组织路由的来自 **Exchange Online** 发件人的邮件(启用集中邮件传输)



关于 Exchange 文档

2019/6/5 •

您现在阅读的本文档由概念主题和过程主题集合而成，按照主题或 Microsoft Exchange 使用的技术进行组织。从左侧窗格中的目录、其他帮助主题的链接、搜索结果或自定义收藏夹主题列表可以直接访问每一个主题。

其他与 Exchange 文档相关的信息位于[第三方版权声明](#)。

能获取 Exchange 文档的地方

[面向 IT 专业人员的 Exchange Server TechCenter](#) 是深入了解 Microsoft Exchange 技术信息的主要“关卡”。通过 Microsoft TechNet 站点上的 TechCenter，可以访问 Exchange 库和 Exchange 团队博客。

如果你是 Exchange 混合部署或 Exchange Online 部署的管理员，还可能希望访问[面向 IT 专业人员的 Office 365 TechCenter](#)。

[Exchange 库](#)包含最新的帮助文档。此类文档经过 Exchange 产品团队的审阅和审核，并会在有新的信息、问题和疑难解答提示时随时进行补充。

[Exchange 团队博客](#)包含 Exchange 团队撰写的技术文章，以及产品公告和更新。通过此博客，你可以与 Exchange 团队进行积极交互。我们会阅读你提出的反馈和意见，并予以回复。

其他资源

除文档之外，是否还需要查找其他文档？请查看这些其他 Exchange 资源：

- [Exchange Server 下载](#) 在此页上可下载 Service Pack、外接程序、工具和试用软件，从而优化你的 Exchange 组织。
- [Exchange Server 论坛](#) 在此论坛上可与用户和 Exchange 团队成员讨论 Exchange。
- [面向开发者的 Exchange Server](#) 在此页上可查看 Exchange 开发者文档。
- [Microsoft Exchange Server 支持](#) 在此页上可获取多个 Exchange 版本的支持资源。
- [面向残障人士的辅助功能](#) 本主题提供有助于使残障人士更容易使用 Microsoft Exchange 的功能、产品和服务的有关重要信息。

面向残障人士的辅助功能

2019/6/5 •

Microsoft 努力使每个用户更容易使用其产品和服务。下列各节提供使残障人士更容易使用 Microsoft Exchange 的功能、产品和服务的有关信息：

- [Exchange 的辅助功能](#)
- [Exchange 的辅助功能帮助](#)
- [Microsoft 提供的辅助产品和服务](#)

Exchange 的辅助功能

以下功能有助于残障人士更容易使用 Microsoft Exchange：

- [Exchange 2013 中的键盘快捷方式预览](#)
- [Outlook Web App 中的键盘快捷方式](#)

此外，Windows 中的某些辅助功能和实用程序也可能对 Exchange 用户中的残障人士有用。使用 Exchange 命令行管理程序时，还可以通过 Windows PowerShell 大小和颜色的变化提供辅助功能选项。有关 Windows PowerShell 辅助功能选项的详细信息，请参阅 [Windows PowerShell 2.0 ISE 中的辅助功能](#)。

Exchange 的辅助功能帮助

Microsoft Exchange 帮助中的每个图示（包括屏幕快照、图表、流程图和其他图示）均有关联的替换文字。查看图示有困难的用户可以将光标停留在图示上，以阅读替换文字。替换文字说明图中所示的内容。

Microsoft 提供的辅助产品和服务

下列各节提供使残障人士更容易使用 Microsoft Windows 的功能、产品和服务的有关信息。

NOTE

本节中的信息只适用于在美国获得 Microsoft 产品使用许可的用户。如果从美国以外获得此产品，请访问 [Microsoft 辅助功能网站](#) 获取 Microsoft 支持服务部门的电话号码和地址列表。可以与分支机构联系，了解本节中所述的产品和服务类型在你所在的地区是否可用。可以在 Microsoft 产品中的辅助功能网站上详细了解 Microsoft 产品中包括的辅助功能。

Windows 的辅助功能

Windows 操作系统包含许多内置的辅助功能，可以帮助键入和使用鼠标有困难的用户、失明或低视力的用户或者失聪或听力不好的用户。这些功能在安装操作系统期间安装。有关这些功能的详细信息，请参阅 Windows 中的帮助以及 [Microsoft 辅助功能](#)。

- **免费的分步教程：**Microsoft 提供一系列分步教程，提供有关调整计算机上的辅助功能选项和设置的详细过程。此信息以并排格式呈现，以便您可以了解如何使用鼠标、键盘或组合使用这两者。

若要查找 Microsoft 产品的分步指南，请参阅 [Microsoft 辅助功能](#)。

- **适用于 Windows 的辅助技术产品：**提供多种辅助技术产品，使计算机更易于为残障人士使用。可以在 Microsoft Accessibility (Microsoft 辅助功能) 上搜索 Windows 上运行的辅助技术产品目录。

如果您使用辅助技术，请确保在升级软件或硬件之前与辅助技术供应商联系以检查可能的兼容性问题。

替代格式的文档

如果你阅读或处理打印材料有困难，可以获取更容易使用的格式的许多 Microsoft 产品文档。可以在 [Microsoft 辅助功能](#) 上获取可访问的产品文档索引。

此外，还可以从 Learning Ally 获取其他 Microsoft 出版物。Learning Ally 将这些文档分发给已注册其分发服务的合格成员。有关 Microsoft Press 出版的 Microsoft 产品文档和书籍的信息，请与 Learning Ally 联系。

Learning Ally

20 Roszel Road

Princeton, NJ 08540

美国以内拨打的电话号码:(800) 221-4792

网站:[Learning Ally](#)

针对听力损伤人士的客户服务

如果您是失聪人士或有听力障碍的人士，可通过文本电话 (TTY/TDD) 服务访问 Microsoft 产品和服务：

- 要获得客户服务，请在周一至周五（节假日除外）的太平洋时间 6:30 A.M. 和 5:30 P.M. 之间通过 (800) 892-5234 与 Microsoft 销售信息中心联系。
- 要获得美国境内的技术帮助，请在周一至周五（节假日除外）的太平洋时间 6:00 A.M. 和 6:00 P.M. 之间通过 (800) 892-5234 与 Microsoft 产品支持服务部门联系。在加拿大，请在周一至周五（节假日除外）的东部时间 8:00 A.M. 和 8:00 P.M. 之间拨打 (905) 568-9641。

Microsoft 支持服务受使用服务时执行的价格、条款和条件的约束。有关详细信息，请参阅 [Microsoft 支持](#)。

详细信息

有关计算机的辅助技术如何改善残障人士的生活的详细信息，请参阅 [Microsoft 辅助功能](#)。

第三方版权声明

2019/6/5 •

Outside In HTML Export © 1991, 2011 Oracle

支持的平台 - Outside In HTML Export:

Windows (32 位):

Windows 2000

Windows Server 2003

Windows Vista

Windows Server 2008

Windows XP

Windows 7

Windows Itanium (64 位):

Windows .NET Server 2003 Enterprise Edition (适用于 Itanium)

Windows (64 位):

Windows 2003 x 64 数据中心

Windows 2003 x 64 Enterprise

Windows 2003 x 64 Standard Windows Server

Windows Server 2008

Windows Server 2008 R2

Windows 7

组织配置传输属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 可以将下列主题中列出的属性从内部部署 exchange 组织复制到 Exchange Online。

[Active Sync 设备访问规则](#)

[可用同步邮箱策略](#)

[Active Sync 组织设置](#)

[地址列表](#)

[Dlp 策略](#)

[恶意软件筛选器策略](#)

[移动设备邮箱策略](#)

[组织配置](#)

[OWA 邮箱策略](#)

[策略提示配置](#)

[保留策略](#)

[保留策略标记](#)

可用同步设备访问规则属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 将从内部部署 exchange 组织中将 "ActiveSync 设备访问规则" 的以下属性复制到 Exchange Online。

NEW-ACTIVESYNCDEVICEACCESSRULE	可在
AccessLevel	Exchange 2010、2013、2016
特征	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
QueryString	Exchange 2010、2013、2016

Active Sync 邮箱策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, Active Sync 邮箱策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

NEW-ACTIVESYNMAILBOXPOLICY	可在
AllowApplePushNotifications	Exchange 2013、2016
AllowBluetooth	Exchange 2010、2013、2016
AllowBrowser	Exchange 2010、2013、2016
AllowCamera	Exchange 2010、2013、2016
AllowConsumerEmail	Exchange 2010、2013、2016
AllowDesktopSync	Exchange 2010、2013、2016
AllowExternalDeviceManagement	Exchange 2010、2013、2016
AllowHTMLEmail	Exchange 2010、2013、2016
AllowInternetSharing	Exchange 2010、2013、2016
AllowIrDA	Exchange 2010、2013、2016
AllowMobileOTAUpdate	Exchange 2010、2013、2016
AllowNonProvisionableDevices	Exchange 2010、2013、2016
AllowPOPIMAPEmail	Exchange 2010、2013、2016
AllowRemoteDesktop	Exchange 2010、2013、2016
AllowSimpleDevicePassword	Exchange 2010、2013、2016
AllowSMIMEEncryptionAlgorithmNegotiation	Exchange 2010、2013、2016
AllowSMIMESoftCerts	Exchange 2010、2013、2016
AllowStorageCard	Exchange 2010、2013、2016
AllowTextMessaging	Exchange 2010、2013、2016
AllowUnsignedApplications	Exchange 2010、2013、2016
AllowUnsignedInstallationPackages	Exchange 2010、2013、2016

NEW-ACTIVESYNCMAILBOXPOLICY	可在
AllowWiFi	Exchange 2010、2013、2016
AlphanumericDevicePasswordRequired	Exchange 2010、2013、2016
ApprovedApplicationList	Exchange 2010、2013、2016
AttachmentsEnabled	Exchange 2010、2013、2016
DeviceEncryptionEnabled	Exchange 2010、2013、2016
DevicePasswordEnabled	Exchange 2010、2013、2016
DevicePasswordExpiration	Exchange 2010、2013、2016
DevicePasswordHistory	Exchange 2010、2013、2016
DevicePolicyRefreshInterval	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
IrmEnabled	Exchange 2010、2013、2016
IsDefault	Exchange 2013、2016
IsDefaultPolicy	Exchange 2010、2013、2016
MaxAttachmentSize	Exchange 2010、2013、2016
MaxCalendarAgeFilter	Exchange 2010、2013、2016
MaxDevicePasswordFailedAttempts	Exchange 2010、2013、2016
MaxEmailAgeFilter	Exchange 2010、2013、2016
MaxEmailBodyTruncationSize	Exchange 2010、2013、2016
MaxEmailHTMLBodyTruncationSize	Exchange 2010、2013、2016
MaxInactivityTimeDeviceLock	Exchange 2010、2013、2016
MinDevicePasswordComplexCharacters	Exchange 2010、2013、2016
MinDevicePasswordLength	Exchange 2010、2013、2016
名称	Exchange 2010、2013、2016
PasswordRecoveryEnabled	Exchange 2010、2013、2016
RequireDeviceEncryption	Exchange 2010、2013、2016

NEW-ACTIVESYNCMailboxPolicy	可在
RequireEncryptedSMIMEMessages	Exchange 2010、2013、2016
RequireEncryptionSMIMEAlgorithm	Exchange 2010、2013、2016
RequireManualSyncWhenRoaming	Exchange 2010、2013、2016
RequireSignedSMIMEAlgorithm	Exchange 2010、2013、2016
RequireSignedSMIMEMessages	Exchange 2010、2013、2016
RequireStorageCardEncryption	Exchange 2010、2013、2016
UnapprovedInROMApplicationList	Exchange 2010、2013、2016
UNCAccessEnabled	Exchange 2010、2013、2016
WSSAccessEnabled	Exchange 2010、2013、2016

ActiveSync 组织设置属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 将从内部部署 exchange 组织中将 "ActiveSync 组织" 设置的以下属性复制到 Exchange Online。

GET-ACTIVESYNCCONFIGURATIONSETTINGS	可在
Guid	Exchange 2010、2013、2016
DefaultAccessLevel	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
OtaNotificationMailInsert	Exchange 2010、2013、2016
UserMailInsert	Exchange 2010、2013、2016

地址列表属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 地址列表的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

ADDRESSLIST	可在
条件公司	Exchange 2010、2013、2016
ConditionalCustomAttribute1	Exchange 2010、2013、2016
ConditionalCustomAttribute10	Exchange 2010、2013、2016
ConditionalCustomAttribute11	Exchange 2010、2013、2016
ConditionalCustomAttribute12	Exchange 2010、2013、2016
ConditionalCustomAttribute13	Exchange 2010、2013、2016
ConditionalCustomAttribute14	Exchange 2010、2013、2016
ConditionalCustomAttribute15	Exchange 2010、2013、2016
ConditionalCustomAttribute2	Exchange 2010、2013、2016
ConditionalCustomAttribute3	Exchange 2010、2013、2016
ConditionalCustomAttribute4	Exchange 2010、2013、2016
ConditionalCustomAttribute5	Exchange 2010、2013、2016
ConditionalCustomAttribute6	Exchange 2010、2013、2016
ConditionalCustomAttribute7	Exchange 2010、2013、2016
ConditionalCustomAttribute8	Exchange 2010、2013、2016
ConditionalCustomAttribute9	Exchange 2010、2013、2016
ConditionalDepartment	Exchange 2010、2013、2016
ConditionalStateOrProvince	Exchange 2010、2013、2016
Container	Exchange 2010、2013、2016
DisplayName	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016

ADDRESSLIST	可在
IncludedRecipients	Exchange 2010、2013、2016
名称	Exchange 2010、2013、2016
RecipientFilter	Exchange 2010、2013、2016

Dlp 策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, Dlp 策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

DLPPOLICY	可在
说明	Exchange 2013、2016
标识	Exchange 2013、2016
模式	Exchange 2013、2016
名称	Exchange 2013、2016
状态	Exchange 2013、2016

恶意软件筛选器策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 恶意软件筛选器策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

GET-MALWAREFILTERPOLICY	可在
操作	Exchange 2013、2016
AdminDisplayName	Exchange 2013、2016
CustomAlertText	Exchange 2013、2016
CustomExternalBody	Exchange 2013、2016
CustomExternalSubject	Exchange 2013、2016
CustomFromAddress	Exchange 2013、2016
CustomFromName	Exchange 2013、2016
CustomInternalBody	Exchange 2013、2016
CustomInternalSubject	Exchange 2013、2016
CustomNotifications	Exchange 2013、2016
EnableExternalSenderAdminNotifications	Exchange 2013、2016
EnableExternalSenderNotifications	Exchange 2013、2016
EnableInternalSenderAdminNotifications	Exchange 2013、2016
EnableInternalSenderNotifications	Exchange 2013、2016
ExternalSenderAdminAddress	Exchange 2013、2016
标识	Exchange 2013、2016
InternalSenderAdminAddress	Exchange 2013、2016
名称	Exchange 2013、2016

移动设备邮箱策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 移动设备邮箱策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

NEW-MOBILEDEVICEMAILBOXPOLICY	可在
AllowBluetooth	Exchange 2010、2013、2016
AllowBrowser	Exchange 2010、2013、2016
AllowCamera	Exchange 2010、2013、2016
AllowConsumerEmail	Exchange 2010、2013、2016
AllowDesktopSync	Exchange 2010、2013、2016
AllowExternalDeviceManagement	Exchange 2010、2013、2016
AllowHTMLEmail	Exchange 2010、2013、2016
AllowInternetSharing	Exchange 2010、2013、2016
AllowIrrDA	Exchange 2010、2013、2016
AllowMobileOTAUpdate	Exchange 2010、2013、2016
AllowNonProvisionableDevices	Exchange 2010、2013、2016
AllowPOPIMAPEmail	Exchange 2010、2013、2016
AllowRemoteDesktop	Exchange 2010、2013、2016
AllowSimplePassword	Exchange 2010、2013、2016
AllowSMIMEEncryptionAlgorithmNegotiation	Exchange 2010、2013、2016
AllowSMIMESoftCerts	Exchange 2010、2013、2016
AllowStorageCard	Exchange 2010、2013、2016
AllowTextMessaging	Exchange 2010、2013、2016
AllowUnsignedApplications	Exchange 2010、2013、2016
AllowUnsignedInstallationPackages	Exchange 2010、2013、2016
AllowWiFi	Exchange 2010、2013、2016

NEW-MOBILEDEVICEEMAILBOXPOLICY	可在
AlphanumericPasswordRequired	Exchange 2010、2013、2016
ApprovedApplicationList	Exchange 2010、2013、2016
AttachmentsEnabled	Exchange 2010、2013、2016
DeviceEncryptionEnabled	Exchange 2010、2013、2016
DevicePolicyRefreshInterval	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
IrmEnabled	Exchange 2010、2013、2016
IsDefault	Exchange 2010、2013、2016
MaxAttachmentSize	Exchange 2010、2013、2016
MaxCalendarAgeFilter	Exchange 2010、2013、2016
MaxEmailAgeFilter	Exchange 2010、2013、2016
MaxEmailBodyTruncationSize	Exchange 2010、2013、2016
MaxEmailHTMLBodyTruncationSize	Exchange 2010、2013、2016
MaxInactivityTimeLock	Exchange 2010、2013、2016
MaxPasswordFailedAttempts	Exchange 2010、2013、2016
MinPasswordComplexCharacters	Exchange 2010、2013、2016
MinPasswordLength	Exchange 2010、2013、2016
名称	Exchange 2010、2013、2016
PasswordEnabled	Exchange 2010、2013、2016
PasswordExpiration	Exchange 2010、2013、2016
PasswordHistory	Exchange 2010、2013、2016
PasswordRecoveryEnabled	Exchange 2010、2013、2016
RequireDeviceEncryption	Exchange 2010、2013、2016
RequireEncryptedSMIMEMessages	Exchange 2010、2013、2016
RequireEncryptionSMIMEAlgorithm	Exchange 2010、2013、2016

NEW-MOBILEDEVICEMAILBOXPOLICY	可在
RequireManualSyncWhenRoaming	Exchange 2010、2013、2016
RequireSignedSMIMEAlgorithm	Exchange 2010、2013、2016
RequireSignedSMIMEMessages	Exchange 2010、2013、2016
RequireStorageCardEncryption	Exchange 2010、2013、2016
UnapprovedInROMApplicationList	Exchange 2010、2013、2016
UNCAccessEnabled	Exchange 2010、2013、2016
WSSAccessEnabled	Exchange 2010、2013、2016

组织配置

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 组织配置的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

SET-ORGANIZATIONCONFIG	可在
ActivityBasedAuthenticationTimeoutEnabled	Exchange 2010、2013、2016
ActivityBasedAuthenticationTimeoutInterval	Exchange 2010、2013、2016
ActivityBasedAuthenticationTimeoutWithSingleSignOnEnabled	Exchange 2010、2013、2016
AppsForOfficeEnabled	Exchange 2013、2016
AsyncSendEnabled	Exchange 2016
BookingsEnabled	Exchange 2016
ByteEncoderTypeFor7BitCharsets	Exchange 2010、2013、2016
ConnectorsActionableMessagesEnabled	Exchange 2016
ConnectorsEnabled	Exchange 2016
DefaultPublicFolderAgeLimit	Exchange 2013、2016
DefaultPublicFolderDeletedItemRetention	Exchange 2013、2016
DefaultPublicFolderIssueWarningQuota	Exchange 2013、2016
DefaultPublicFolderMaxItemSize	Exchange 2013、2016
DefaultPublicFolderMovedItemRetention	Exchange 2013、2016
DefaultPublicFolderProhibitPostQuota	Exchange 2013、2016
DirectReportsGroupAutoCreationEnabled	Exchange 2016
DistributionGroupDefaultOU	Exchange 2010、2013、2016
DistributionGroupNameBlockedWordsList	Exchange 2010、2013、2016
DistributionGroupNamingPolicy	Exchange 2010、2013、2016
ElcProcessingDisabled	Exchange 2016
EndUserDLUpgradeFlowsDisabled	Exchange 2016

SET-ORGANIZATIONCONFIG	可在
EwsAllowEntourage	Exchange 2010、2013、2016
EwsAllowList	Exchange 2010、2013、2016
EwsAllowMacOutlook	Exchange 2010、2013、2016
EwsAllowOutlook	Exchange 2010、2013、2016
EwsApplicationAccessPolicy	Exchange 2010、2013、2016
EwsBlockList	Exchange 2010、2013、2016
EwsEnabled	Exchange 2010、2013、2016
ExchangeNotificationEnabled	Exchange 2010、2013、2016
ExchangeNotificationRecipients	Exchange 2010、2013、2016
FocusedInboxOn	Exchange 2016
HierarchicalAddressBookRoot	Exchange 2010、2013、2016
IPListBlocked	Exchange 2016
IsAgendaMailEnabled	Exchange 2016
LeanPopoutEnabled	Exchange 2016
LinkPreviewEnabled	Exchange 2016
MailTipsAllTipsEnabled	Exchange 2010、2013、2016
MailTipsExternalRecipientsTipsEnabled	Exchange 2010、2013、2016
MailTipsGroupMetricsEnabled	Exchange 2010、2013、2016
MailTipsLargeAudienceThreshold	Exchange 2010、2013、2016
MailTipsMailboxSourcedTipsEnabled	Exchange 2010、2013、2016
OAuth2ClientProfileEnabled	Exchange 2013、2016
PerTenantSwitchToESTSEnabled	Exchange 2016
PreferredInternetCodePageForShiftJis	Exchange 2010、2013、2016
PublicComputersDetectionEnabled	Exchange 2013、2016
PublicFoldersEnabled	Exchange 2013、2016

SET-ORGANIZATIONCONFIG	可在
ReadTrackingEnabled	Exchange 2010、2013、2016
RefreshSessionEnabled	Exchange 2016
RemotePublicFolderMailboxes	Exchange 2013、2016
RequiredCharsetCoverage	Exchange 2010、2013、2016
SiteMailboxCreationURL	Exchange 2013、2016
SmtpActionableMessagesEnabled	Exchange 2016
UnblockUnsafeSenderPromptEnabled	Exchange 2016

OWA 邮箱策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, OWA 邮箱策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

SET-OWAMAILBOXPOLICY	可在
ActionForUnknownFileAndMIMETypes	Exchange 2010、2013、2016
ActiveSyncIntegrationEnabled	Exchange 2010、2013、2016
AllAddressListsEnabled	Exchange 2010、2013、2016
AllowCopyContactsToDeviceAddressBook	Exchange 2013、2016
AllowedFileTypes	Exchange 2010、2013、2016
AllowedMimeTypes	Exchange 2010、2013、2016
AllowOfflineOn	Exchange 2013、2016
BlockedFileTypes	Exchange 2010、2013、2016
BlockedMimeTypes	Exchange 2010、2013、2016
CalendarEnabled	Exchange 2010、2013、2016
ClassicAttachmentsEnabled	Exchange 2016
ContactsEnabled	Exchange 2010、2013、2016
DefaultTheme	Exchange 2010、2013、2016
DelegateAccessEnabled	Exchange 2010、2013、2016
DirectFileAccessOnPrivateComputersEnabled	Exchange 2010、2013、2016
DirectFileAccessOnPublicComputersEnabled	Exchange 2010、2013、2016
DisplayPhotosEnabled	Exchange 2013、2016
ExplicitLogonEnabled	Exchange 2010、2013、2016
ForceSaveAttachmentFilteringEnabled	Exchange 2010、2013、2016
ForceSaveFileTypes	Exchange 2010、2013、2016
ForceSaveMimeTypes	Exchange 2010、2013、2016

SET-OWAMAILBOXPOLICY	可在
ForceWacViewingFirstOnPrivateComputers	Exchange 2013、2016
ForceWacViewingFirstOnPublicComputers	Exchange 2013、2016
GlobalAddressListEnabled	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
InstantMessagingEnabled	Exchange 2010、2013、2016
InstantMessagingType	Exchange 2010、2013、2016
IRMEnabled	Exchange 2010、2013、2016
IsDefault	Exchange 2013、2016
JournalEnabled	Exchange 2010、2013、2016
LogonAndErrorLanguage	Exchange 2010、2013、2016
名称	Exchange 2010、2013、2016
NotesEnabled	Exchange 2010、2013、2016
OrganizationEnabled	Exchange 2010、2013、2016
OutboundCharset	Exchange 2010、2013、2016
OWALightEnabled	Exchange 2010、2013、2016
RecoverDeletedItemsEnabled	Exchange 2010、2013、2016
ReferenceAttachmentsEnabled	Exchange 2016
RemindersAndNotificationsEnabled	Exchange 2010、2013、2016
ReportJunkEmailEnabled	Exchange 2013、2016
RulesEnabled	Exchange 2010、2013、2016
SaveAttachmentsToCloudEnabled	Exchange 2016
SearchFoldersEnabled	Exchange 2010、2013、2016
SetPhotoEnabled	Exchange 2013、2016
SetPhotoURL	Exchange 2013、2016
SignaturesEnabled	Exchange 2010、2013、2016

SET-OWAMAILBOXPOLICY	可在
SpellCheckerEnabled	Exchange 2010、2013、2016
TasksEnabled	Exchange 2010、2013、2016
TextMessagingEnabled	Exchange 2010、2013、2016
ThemeSelectionEnabled	Exchange 2010、2013、2016
UMIntegrationEnabled	Exchange 2010、2013、2016
UseGB18030	Exchange 2010、2013、2016
UseISO885915	Exchange 2010、2013、2016
WacEditingEnabled	Exchange 2016
WacExternalServicesEnabled	Exchange 2013、2016
WacOMEXEnabled	Exchange 2013、2016
WacViewingOnPrivateComputersEnabled	Exchange 2013、2016
WacViewingOnPublicComputersEnabled	Exchange 2013、2016
WebPartsFrameOptionsType	Exchange 2013、2016

策略提示配置属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 策略提示配置的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

POLICYTIPCONFIG	可在
标识	Exchange 2013、2016
名称	Exchange 2013、2016
值	Exchange 2013、2016

保留策略标记属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 保留策略标记的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

GET-RETENTIONPOLICYTAG	可在
AgeLimitForRetention	Exchange 2010、2013、2016
Comment	Exchange 2010、2013、2016
标识	Exchange 2010、2013、2016
LegacyManagedFolder	Exchange 2010、2013、2016
LocalizedComment	Exchange 2010、2013、2016
LocalizedRetentionPolicyTagName	Exchange 2010、2013、2016
MessageClass	Exchange 2010、2013、2016
MustDisplayCommentEnabled	Exchange 2010、2013、2016
名称	Exchange 2010、2013、2016
RetentionAction	Exchange 2010、2013、2016
RetentionEnabled	Exchange 2010、2013、2016
RetentionId	Exchange 2010、2013、2016
SystemTag	Exchange 2010、2013、2016
类型	Exchange 2010、2013、2016
IsDefaultAutoGroupPolicyTag	Exchange 2013、2016
IsDefaultModeratedRecipientsPolicyTag	Exchange 2013、2016

保留策略属性

2019/6/5 •

当在 "混合配置" 向导中选择 "组织配置转移" 选项时, 保留策略的以下属性将从内部部署 exchange 组织复制到 Exchange Online。

保留策略	可在
标识	Exchange 2010、2013、2016
IsDefault	Exchange 2013、2016
IsDefaultArbitrationMailbox	Exchange 2013、2016
名称	Exchange 2010、2013、2016
RetentionId	Exchange 2010、2013、2016
RetentionPolicyTagLinks	Exchange 2010、2013、2016