使用 VDS 部署

Virtual Desktop Service

NetApp
February 16, 2022

目录

使用 VDS 部署

Azure 酒店

Azure 虚拟桌面

AVD 部署指南

概述

本指南将提供在 Azure 中使用 NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）创建 Azure 虚拟桌面（ AVD ）部署的分步说明。

本指南从以下位置开始： https://cwasetup.cloudworkspace.com/

本概念验证（ POC ）指南旨在帮助您在自己的测试 Azure 订阅中快速部署和配置 AVD 。本指南假设在一个全新的非生产 Azure Active Directory 租户中进行绿色现场部署。

生产部署，尤其是在现有 AD 或 Azure AD 环境中的部署非常常见，但本 POC 指南不会考虑此过程。复杂的 POC 和生产部署应由 NetApp VDS 销售 / 服务团队启动，而不是以自助式方式执行。

本 POC 文档将带您完成整个 AVD 部署，并简要介绍 VDS 平台中部署后配置的主要方面。完成后，您将拥有一个完全部署且功能正常的 AVD 环境，其中包括主机池，应用程序组和用户。您也可以选择配置自动应用程序交付，安全组，文件共享权限， Azure Cloud Backup 和智能成本优化。VDS 通过 GPO 部署一组最佳实践设置。此外，还提供了有关在 POC 不需要安全控制时如何选择禁用这些控制的说明，这与非受管本地设备环境类似。

AVD 基础知识

Azure 虚拟桌面是一种在云中运行的全面桌面和应用程序虚拟化服务。下面是一些关键特性和功能的快速列表：

- 平台服务，包括网关，代理，许可和登录，并作为 Microsoft 的一项服务提供。这样可以最大限度地减少需要托管和管理的基础架构。
- Azure Active Directory 可用作身份提供程序，从而可以对附加的 Azure 安全服务进行分层，例如有条件的访问。
- 用户体验 Microsoft 服务的单点登录体验。
- 用户会话通过专有的反向连接技术连接到会话主机。这意味着无需打开任何入站端口，而是由代理创建与 AVD 管理平面的出站连接，而 AVD 管理平面又连接到最终用户设备。
- 反向连接甚至允许虚拟机在不暴露于公有 Internet 的情况下运行，即使在保持远程连接的情况下也能实现隔离的工作负载。
- AVD 支持访问 Windows 10 多会话，从而提供 Windows 10 Enterprise 体验，并提高高密度用户会话的效率。
- FSLogix 配置文件容器化技术包括，可提高用户会话性能，存储效率并增强非持久性环境中的 Office 体验。
- AVD 支持完全桌面和 RemoteApp 访问。持久或非持久体验，以及专用和多会话体验。
- 企业可以通过 Windows 许可节省成本，因为 AVD 可以利用 "Windows 10 Enterprise E3" 来取代对 RDS CAL 的需求，并显著降低 Azure 中会话主机 VM 的每小时成本。

指南范围

本指南将从 Azure 和 VDS 管理员的角度引导您完成使用 NetApp VDS 技术部署 AVD 的过程。您可以为 Azure 租户和订阅提供零预配置，本指南可帮助您端到端设置 AVD

本指南包括以下步骤：

1. 确认 Azure 租户， Azure 订阅和 Azure 管理员帐户权限的前提条件
2. 收集所需的发现详细信息
3. 使用专门构建的适用于 Azure 的 VDS 设置向导构建 Azure 环境
4. 使用标准 Windows 10 EVD 映像创建第一个主机池
5. 将虚拟桌面分配给 Azure AD 用户
6. 将用户添加到默认应用程序组，以便为用户提供桌面环境。 （可选） 创建其他主机池以提供 RemoteApp 服务
7. 以最终用户身份通过客户端软件和 / 或 Web 客户端进行连接
8. 以本地和域管理员身份连接到平台和客户端服务
9. 也可以为 VDS 管理员和 AVD 最终用户启用 VDS 的多因素身份验证
10. 您也可以选择浏览整个应用程序授权工作流，包括填充应用程序库，应用程序安装自动化，用户和安全组屏蔽应用程序
11. 也可以按组创建和管理 Active Directory 安全组，文件夹权限和应用程序授权。
12. 也可以配置成本优化技术，包括工作负载计划和实时扩展
13. 也可以创建，更新和 SysPrep 虚拟机映像，以供将来部署时使用
14. 也可以配置 Azure Cloud Backup
15. 也可以禁用默认安全控制组策略

Azure 前提条件

VDS 使用原生 Azure 安全上下文部署 AVD 实例。在启动 VDS 设置向导之前，需要建立一些 Azure 前提条件。

在部署期间，通过对 Azure 租户中的现有管理员帐户进行身份验证，将服务帐户和权限授予 VDS 。

快速前提条件检查清单

- Azure 租户与 Azure AD 实例（可以是 Microsoft 365 实例）
- Azure 订阅
- Azure 虚拟机的可用 Azure 配额
- 具有全局管理员和订阅所有权角色的 Azure 管理员帐户

有关详细前提条件的文档，请参见 "本 PDF"

Azure AD 中的 **Azure** 管理员

此现有 Azure 管理员必须是目标租户中的 Azure AD 帐户。Windows Server AD 帐户可以使用 VDS 设置进行部署，但要设置与 Azure AD 的同步，还需要执行其他步骤（本指南不在适用范围内）

可以通过在 Azure 管理门户中的 "Users" （用户） >"All Users" （所有用户）下查找用户帐户来确认此情况。[]

全局管理员角色

必须在 Azure 租户中为 Azure 管理员分配全局管理员角色。

要检查您在 **Azure AD** 中的角色，请执行以下步骤：

1. 登录到 Azure 门户，网址为 https://portal.azure.com/
2. 搜索并选择 Azure Active Directory
3. 在右侧的下一个窗格中，单击管理部分中的用户选项
4. 单击要检查的管理员用户的名称
5. 单击目录角色。在最右侧窗格中，应列出全局管理员角色[]

如果此用户没有全局管理员角色，您可以执行以下步骤来添加它（请注意，登录帐户必须是全局管理员才能执行这些步骤）：

1. 从上述步骤 5 中的用户目录角色详细信息页面中，单击详细信息页面顶部的添加分配按钮。
2. 单击角色列表中的全局管理员。单击添加按钮。[]

Azure 订阅所有权

Azure 管理员还必须是要包含部署的订阅的订阅所有者。

要检查管理员是否为订阅所有者，请执行以下步骤：

1. 登录到 Azure 门户，网址为 https://portal.azure.com/
2. 搜索并选择订阅
3. 在右侧的下一个窗格中，单击订阅名称以查看订阅详细信息
4. 单击左边第二个窗格中的访问控制（ IAM ）菜单项
5. 单击角色分配选项卡。Azure 管理员应列在所有者部分中。[]

如果未列出 **Azure** 管理员，您可以按照以下步骤将帐户添加为订阅所有者：

1. 单击页面顶部的添加按钮，然后选择添加角色分配选项
2. 右侧将显示一个对话框。在角色下拉列表中选择 " 所有者 " ，然后开始在选择框中键入管理员的用户名。显示管理员的全名后，将其选中
3. 单击对话框底部的保存按钮[]

Azure 计算核心配额

CWA" 设置 " 向导和 VDS 门户将创建新的虚拟机，并且 Azure 订阅必须具有可用配额才能成功运行。

要检查配额，请执行以下步骤：

1. 导航到订阅模块，然后单击 " 使用量 + 配额 "
2. 在 " 提供程序 " 下拉列表中选择所有提供程序，然后在 " 提供程序 " 下拉列表中选择 Microsoft.Compute
3. 在 " 位置 " 下拉列表中选择目标区域

4. 此时应按虚拟机系列显示可用配额列表[]如果需要增加配额，请单击 Request Increase ，然后按照提示添加更多容量。对于初始部署，请特别请求增加 " 标准 DSv3 系列 vCPU" 的报价

收集发现详细信息

完成 CWA" 设置 " 向导后，需要回答几个问题。NetApp VDS 提供了一个链接的 PDF ，可用于在部署之前记录这些选择。项目包括：

项目	**Description**
VDS 管理员凭据	收集现有 VDS 管理员凭据（如果已有）。否则，将在部署期间创建新的管理员帐户。
Azure 区域	根据服务的性能和可用性确定目标 Azure 区域。这 "Microsoft 工具" 可以根据区域估算最终用户体验。
Active Directory 类型	VM 需要加入域，但无法直接加入 Azure AD 。VDS 部署可以构建新虚拟机或使用现有域控制器。
文件管理	性能在很大程度上取决于磁盘速度，尤其是与用户配置文件存储相关的速度。VDS 设置向导可以部署简单的文件服务器或配置 Azure NetApp Files （ ANF ）。对于几乎任何生产环境，建议使用 ANF ，但对于 POC ，文件服务器选项可提供足够的性能。可以在部署后修改存储选项，包括使用 Azure 中的现有存储资源。有关详细信息，请参见 ANF 定价：https://azure.microsoft.com/en-us/pricing/details/netapp/
虚拟网络范围	部署需要一个可路由的 /20 网络范围。您可以通过 VDS 设置向导定义此范围。此范围不应与 Azure 或内部环境中的任何现有 vNet 重叠（如果这两个网络将通过 VPN 或 ExpressRoute 进行连接），这一点非常重要。

VDS 设置部分

登录到 https://cwasetup.cloudworkspace.com/ 使用您的 Azure 管理员凭据，可在前提条件部分中找到。

IaaS 和平台

[]

Azure AD 域名

Azure AD 域名由选定租户继承。

位置

选择适当的 "Azure Region" 。这 "Microsoft 工具" 可以根据区域估算最终用户体验。

Active Directory 类型

可以使用一个 * 新虚拟机 * 来配置 VDS ，以使域控制器功能或设置利用现有域控制器。在本指南中，我们将选择新的 Windows Server Active Directory ，此操作将根据在此过程中所做的选择在订阅下创建一个或两个 VM 。

有关现有 AD 部署的详细文章，请参见 "此处"。

Active Directory domain name

输入一个 "* 域名 "* 。建议从上述位置镜像 Azure AD 域名。

文件管理

VDS 可以配置简单的文件服务器虚拟机，也可以设置和配置 Azure NetApp Files 。在生产环境中， Microsoft 建议为每个用户分配 30 GB 的空间，我们发现，要获得最佳性能，需要为每个用户分配 5-15 IOPS 。

在 POC （非生产环境）环境中，文件服务器是一种低成本且简单的部署选项，但是，即使是小型生产部署，Azure 受管磁盘的可用性能也可能会被 IOPS 消耗所覆盖。

例如， Azure 中的 4 TB 标准 SSD 磁盘最多支持 500 IOPS ，而每个用户最多只能支持 100 个用户，而每个用户只能支持 5 IOPS/ 用户。使用 ANF 高级版时，相同大小的存储设置可支持 16 ， 000 次 IOPS ，使 IOPS 增加 32 倍。

对于生产 AVD 部署， Microsoft 建议使用 Azure NetApp Files 。

Azure NetApp Files 需要提供给您要部署到的订阅 - 请联系您的 NetApp 客户代表或使用以下链接： https://aka.ms/azurenetappfiles

此外，您还必须将 NetApp 注册为订阅的提供商。可通过执行以下操作来实现此目的：

- 导航到 Azure 门户中的订阅
  - 单击资源提供程序
  - 筛选 NetApp
  - 选择提供程序，然后单击注册

RDS 许可证编号

NetApp VDS 可用于部署 RDS 和 / 或 AVD 环境。部署 AVD 时，此字段可以 * 保留为空 * 。

ThinPrint

NetApp VDS 可用于部署 RDS 和 / 或 AVD 环境。部署 AVD 时，此切换可以保持为 "Off" （关闭）状态（向左切换）。

通知电子邮件

VDS 将向提供的电子邮件 * 发送部署通知和持续运行状况报告。可以稍后更改。

VM 和网络

为了支持 VDS 环境，需要运行多种服务—这些服务统称为 " VDS 平台 " 。根据配置的不同，它们可能包括 CVMGR ，一个或两个 RDS 网关，一个或两个 HTML5 网关，一个 FTPS 服务器以及一个或两个 Active Directory VM 。

大多数 AVD 部署都利用单个虚拟机选项，因为 Microsoft 将 AVD 网关作为 PaaS 服务进行管理。

对于包含 RDS 使用情形的小型和简单环境，所有这些服务均可精简为 Single Virtual Machine 选项，以降低 VM

成本（可扩展性有限）。对于用户数超过 100 的 RDS 使用情形，建议使用多个虚拟机选项，以便于 RDS 和 / 或 HTML5 网关可扩展性[]

平台 **VM** 配置

NetApp VDS 可用于部署 RDS 和 / 或 AVD 环境。在部署 AVD 时，建议选择单个虚拟机。对于 RDS 部署，您需要部署和管理代理和网关等其他组件，在生产环境中，这些服务应在专用和冗余虚拟机上运行。对于 AVD ，所有这些服务均由 Azure 作为附带服务提供，因此，建议使用 "* 单个虚拟机 " 配置。

单个虚拟机

对于仅使用 AVD （而不是 RDS 或两者的组合）的部署，建议选择此选项。在单个虚拟机部署中，以下角色均托管在 Azure 中的单个虚拟机上：

- CW Manager
- HTML5 网关
- RDS 网关
- 远程应用程序
- FTPS 服务器（可选）
- 域控制器角色

在此配置中，建议的 RDS 使用情形的最大用户数为 100 个用户。在此配置中，负载平衡 RS/HTML5 网关不是一个选项，这限制了冗余和未来扩展的选项。同样，此限制不适用于 AVD 部署，因为 Microsoft 将网关作为 PaaS 服务进行管理。

如果此环境是为多租户设计的，则不支持单个虚拟机配置— AVD 或 AD Connect 也不支持。

多个虚拟机

将 VDS 平台拆分为多个虚拟机时， Azure 中的专用 VM 会托管以下角色：

- 远程桌面网关

  VDS 设置可用于部署和配置一个或两个 RDS 网关。这些网关会将 RDS 用户会话从开放式 Internet 中继到部署中的会话主机 VM 。RDS 网关具有一项重要功能，可保护 RDS 免受来自开放式互联网的直接攻击，并对环境中 / 之外的所有 RDS 流量进行加密。选择两个远程桌面网关后， VDS 安装程序会部署 2 个 VM 并对其进行配置，以便对传入的 RDS 用户会话进行负载平衡。

- HTML5 网关

  VDS 设置可用于部署和配置一个或两个 HTML5 网关。这些网关托管 VDS 和基于 Web 的 VDS 客户端（ H5 门户）中的 *Connect to Server* 功能使用的 HTML5 服务。选择两个 HTML5 门户后， VDS 安装程序会部署 2 个 VM 并对其进行配置，以便对传入的 HTML5 用户会话进行负载平衡。

  如果使用多个服务器选项（即使用户仅通过已安装的 VDS 客户端进行连接），强烈建议至少使用一个 HTML5 网关从 VDS 启用 *Connect to Server* 功能。

- 网关可扩展性注意事项

对于 RDS 使用情形，可以使用其他网关 VM 横向扩展环境的最大大小，每个 RDS 或 HTML5 网关大约支持 500 个用户。稍后，只需极少的 NetApp 专业服务协助，即可添加其他网关

如果此环境是为多租户设计的，则需要选择多个虚拟机。

时区

虽然最终用户的体验将反映其本地时区，但需要选择默认时区。选择要从其中执行环境的 "* 主管理 " 的时区。

虚拟网络范围

最佳做法是，根据虚拟机的用途将其隔离到不同的子网。首先，定义网络范围并添加一个 /20 范围。

VDS 设置会检测到一个范围，并建议一个范围，该范围应证明是成功的。根据最佳实践，子网 IP 地址必须属于专用 IP 地址范围。

这些范围包括：

- 192.168.0.0 到 192.168.255.255
- 172.16.0.0 到 172.31.255.255
- 10.0.0.0 到 10.255.255.255

如果需要，请查看并调整，然后单击验证以确定以下每项的子网：

- 租户：这是会话主机服务器和数据库服务器将驻留在的范围
- 服务：这是 Azure NetApp Files 等 PaaS 服务将驻留在的范围
- 平台：这是平台服务器将驻留在的范围
- 目录：这是 AD 服务器将驻留在的范围

请查看

在最后一页，您可以查看自己的选择。完成此审核后，单击验证按钮。VDS 安装程序将查看所有条目，并验证是否可以使用提供的信息继续部署。此验证可能需要 2 到 10 分钟。要跟踪进度，您可以单击日志标识（右上角）以查看验证活动。

验证完成后，绿色的配置按钮将代替验证按钮。单击配置以启动部署的配置过程。

Status

根据 Azure 工作负载和您所做的选择，配置过程需要 2 到 4 小时。您可以通过单击状态页面来跟踪日志中的进度，也可以等待显示部署过程已完成的电子邮件。部署可构建支持 VDS 和远程桌面或 AVD 实施所需的虚拟机和 Azure 组件。其中包括一个虚拟机，该虚拟机既可以充当远程桌面会话主机，也可以充当文件服务器。在 AVD 实施中，此虚拟机将仅充当文件服务器。

安装和配置 **AD Connect**

成功安装后，需要立即在域控制器上安装和配置 AD Connect 。在单平台 VM 设置中， CMGR1 计算机是 DC 。AD 中的用户需要在 Azure AD 和本地域之间同步。

要安装和配置 **AD Connect** ，请执行以下步骤：

1. 以域管理员身份连接到域控制器。
    a. 从 Azure 密钥存储获取凭据（请参见 "此处提供密钥存储说明"）
2. 安装 AD Connect ，使用域管理员（具有企业管理员角色权限）和 Azure AD 全局管理员登录

激活 **AVD** 服务

部署完成后，下一步是启用 AVD 功能。AVD 支持过程要求 Azure 管理员执行多个步骤来注册其 Azure AD 域并订阅使用 Azure AVD 服务进行访问。同样， Microsoft 要求 VDS 为 Azure 中的自动化应用程序请求相同的权限。以下步骤将指导您完成此过程。

创建 **AVD** 主机池

最终用户对 AVD 虚拟机的访问由主机池进行管理，主机池包含虚拟机，应用程序组又包含用户和用户访问类型。

构建第一个主机池

1. 单击 AVD 主机池部分标题右侧的添加按钮。[]
2. 输入主机池的名称和问题描述。
3. 选择主机池类型
    a. "** 池化 " 表示多个用户将访问安装了相同应用程序的同一个虚拟机池。
    b. "* 个人 "* 可创建一个主机池，为用户分配自己的会话主机 VM 。
4. 选择负载平衡器类型
    a. 在池中的第二个虚拟机上启动之前， "Depth First" （深度优先）将使第一个共享虚拟机填充到最大用户数
    b. "* 宽度优先 "* 将以轮循方式将用户分布到池中的所有虚拟机
5. 选择一个 Azure 虚拟机模板以在此池中创建虚拟机。虽然 VDS 会显示订阅中提供的所有模板，但我们建议选择最新的 Windows 10 多用户内部版本，以获得最佳体验。当前版本为 Windows-10-20h1-EVD 。（也可以使用配置收集功能创建黄金映像，以便从自定义虚拟机映像构建主机）
6. 选择 Azure 计算机大小。出于评估目的， NetApp 建议使用 D 系列（适用于多用户的标准计算机类型）或 E 系列（适用于负载较重的多用户情形的增强型内存配置）。如果您要尝试不同的系列和大小，可以稍后在 VDS 中更改计算机大小
7. 从下拉列表中为虚拟机的受管磁盘实例选择兼容的存储类型
8. 选择要在主机池创建过程中创建的虚拟机数量。您可以稍后将虚拟机添加到池中，但 VDS 会构建您请求的虚拟机数量，并在创建主机池后将其添加到该主机池中
9. 单击添加主机池按钮以启动创建过程。您可以在 AVD 页面上跟踪进度，也可以在 "Tasks" 部分的 "Deployments/Deployment name" 页面上查看进程日志的详细信息
10. 创建主机池后，它将显示在 AVD 页面上的主机池列表中。单击主机池的名称可查看其详细信息页面，其中包括其虚拟机，应用程序组和活动用户的列表

VDS 中的 AVD 主机是使用一个禁止用户会话连接的设置创建的。按照设计，这允许在接受用户连接之前进行自定义。可以通过编辑会话主机的设置来更改此设置。 []

为用户启用 **VDS** 桌面

如上所述， VDS 会创建在部署期间支持最终用户工作空间所需的所有要素。部署完成后，下一步是为要引入 AVD 环境的每个用户启用工作空间访问。此步骤将创建配置文件配置和最终用户数据层访问，这是虚拟桌面的默认设置。VDS 会重新使用此配置将 Azure AD 最终用户链接到 AVD 应用程序池。

要为最终用户启用工作空间，请执行以下步骤：

1. 登录到 VDS https://manage.cloudworkspace.com 使用您在配置期间创建的 VDS 主管理员帐户。如果您不记得帐户信息，请联系 NetApp VDS 以获取检索信息的帮助
2. 单击工作空间菜单项，然后单击配置期间自动创建的工作空间的名称
3. 单击用户和组选项卡[]
4. 对于要启用的每个用户，滚动用户名，然后单击齿轮图标
5. 选择 " 启用云工作空间 " 选项[]
6. 完成支持过程大约需要 30 到 90 秒。请注意，用户状态将从 "Pending" 更改为 "Available"

> 激活 Azure AD 域服务会在 Azure 中创建一个受管域，创建的每个 AVD 虚拟机都将加入该域。要使传统登录到虚拟机正常工作，必须同步 Azure AD 用户的密码哈希，以支持 NTLM 和 Kerberos 身份验证。完成此任务的最简单方法是在 Office.com 或 Azure 门户中更改用户密码，这将强制执行密码哈希同步。域服务服务器的同步周期最长可能需要 20 分钟。

启用用户会话

默认情况下，会话主机无法接受用户连接。此设置通常称为 " 耗电模式 " ，因为它可以在生产环境中用于阻止新的用户会话，从而允许主机最终删除所有用户会话。如果主机允许新的用户会话，则此操作通常称为将会话主机置于 " 轮换 " 状态。

在生产环境中，在耗电模式下启动新主机是有意义的，因为在主机准备好处理生产工作负载之前，通常需要完成一些配置任务。

在测试和评估中，您可以立即使主机退出耗电模式，以启用用户连接并确认功能是否正常。要在会话主机上启用用户会话，请执行以下步骤：

1. 导航到工作空间页面的 AVD 部分。
2. 单击 "AVD 主机池 " 下的主机池名称。[]
3. 单击会话主机的名称并选中允许新会话复选框，然后单击更新会话主机。对需要置于轮换状态的所有主机重复上述步骤。[]
4. 对于每个主行项目， AVD 主页上也会显示当前的统计信息 " 允许新会话 " 。

默认应用程序组

请注意，默认情况下，在创建主机池的过程中会创建桌面应用程序组。通过此组，可以对所有组成员进行交互式桌面访问。要向组添加成员，请执行以下操作：

1. 单击应用程序组的名称[]
2. 单击显示添加的用户数的链接[]
3. 选中要添加到应用程序组的用户名称旁边的框，以选择这些用户

4. 单击选择用户按钮
5. 单击更新应用程序组按钮

创建其他 **AVD** 应用程序组

可以将其他应用程序组添加到主机池中。这些应用程序组将使用 RemoteApp 将特定应用程序从主机池虚拟机发布到应用程序组用户。

> AVD 仅允许在同一主机池中为最终用户分配桌面应用程序组类型或 RemoteApp 应用程序组类型，但不允许同时分配这两者，因此请确保相应地隔离用户。如果用户需要访问桌面和流式应用程序，则需要第二个主机池来托管此应用程序。

要创建新的应用程序组，请执行以下操作：

1. 单击应用程序组部分标题中的添加按钮[]
2. 输入应用程序组的名称和问题描述
3. 单击添加用户链接，选择要添加到组的用户。单击每个用户名称旁边的复选框以选择每个用户，然后单击选择用户按钮[]
4. 单击添加 RemoteApps 链接将应用程序添加到此应用程序组。AVD 会通过扫描虚拟机上安装的应用程序列表自动生成可能的应用程序列表。单击应用程序名称旁边的复选框以选择应用程序，然后单击选择 RemoteApps 按钮。[]
5. 单击添加应用程序组按钮以创建应用程序组

最终用户 **AVD** 访问

最终用户可以使用 Web Client 或在各种平台上安装的客户端访问 AVD 环境

- Web 客户端： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- Web Client 登录 URL： http://aka.ms/AVDweb
- Windows 客户端： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Android 客户端： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- macOS 客户端： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- IOS 客户端： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- IGEL 瘦客户端： https://www.igel.com/igel-solution-family/windows-virtual-desktop/

使用最终用户用户用户名和密码登录。请注意，远程应用程序和桌面连接（ RADC ），远程桌面连接（ mstsc ）以及适用于 Windows 的 CloudWorksapce 客户端应用程序当前不支持登录到 AVD 实例。

监控用户登录

主机池详细信息页面还会在活动用户登录到 AVD 会话时显示其列表。

管理连接选项

VDS 管理员可以通过多种方式连接到环境中的虚拟机。

连接到服务器

在整个门户中， VDS 管理员将找到 " 连接到服务器 " 选项。默认情况下，此功能通过动态生成本地管理员凭据并将其注入 Web 客户端连接来将管理员连接到虚拟机。管理员无需知道（也不会向其提供）凭据即可进行连接。

可以按管理员禁用此默认行为，如下一节所述。

.tech/3 级管理员帐户

在 CWA 设置过程中，会创建一个 "Level II" 管理员帐户。用户名的格式为 username.tech@domain.xyz

这些帐户通常称为 ".tech" 帐户，名为域级管理员帐户。VDS 管理员可以在连接到 CMGR1 （平台）服务器时使用其 .tech 帐户，也可以在连接到环境中的所有其他虚拟机时使用。

要禁用自动本地管理员登录功能并强制使用级别 III 帐户，请更改此设置。导航到 VDS > 管理员 > 管理员名称 > 选中 " 已启用技术帐户 " 。 选中此框后， VDS 管理员不会以本地管理员身份自动登录到虚拟机，而是会提示输入其 .tech 凭据。

这些凭据以及其他相关凭据会自动存储在 _Azure 密钥存储库 _ 中，并可从 Azure 管理门户访问，网址为 https://portal.azure.com/。

可选的部署后操作

多因素身份验证（ **MFA** ）

NetApp VDS 免费提供 SMS/Email MFA 。此功能可用于保护 VDS 管理员帐户和 / 或最终用户帐户的安全。"MFA 文章"

应用程序授权工作流

VDS 提供了一种机制，可从称为应用程序目录的预定义应用程序列表中为最终用户分配对应用程序的访问权限。此应用程序目录涵盖所有受管部署。

> 自动部署的 TSD1 服务器必须保持原样，以支持应用程序授权。具体而言，请勿对此虚拟机运行 " 转换为数据 " 功能。

应用程序管理在本文中进行了详细介绍： ""

Azure AD 安全组

VDS 包括创建，填充和删除由 Azure AD 安全组支持的用户组的功能。这些组可以像任何其他安全组一样在 VDS 外部使用。在 VDS 中，可以使用这些组分配文件夹权限和应用程序授权。

创建用户组

在工作空间中的 " 用户和组 " 选项卡上创建用户组。

按组分配文件夹权限

可以将查看和编辑公司共享中的文件夹的权限分配给用户或组。

""

按组分配应用程序

除了将应用程序单独分配给用户之外，还可以将应用程序配置给组。

1. 导航到用户和组详细信息。[]
2. 添加新组或编辑现有组。[]
3. 将用户和应用程序分配给组。[]

配置成本优化选项

工作空间管理还扩展到管理支持 AVD 实施的 Azure 资源。VDS 允许您配置工作负载计划和实时扩展，以便根据最终用户活动打开和关闭 Azure 虚拟机。这些功能可以将 Azure 资源利用率和支出与最终用户的实际使用模式进行匹配。此外，如果您配置了概念验证 AVD 实施，则可以从 VDS 界面转换整个部署。

工作负载计划

工作负载计划是一项功能，可使管理员为要运行的 Workspace 虚拟机创建一个设置的计划，以支持最终用户会话。当一周中的特定日期达到计划时间段结束时， VDS 会停止 / 取消分配 Azure 中的虚拟机，从而停止每小时收费。

启用工作负载计划：

1. 登录到 VDS https://manage.cloudworkspace.com 使用您的 VDS 凭据。
2. 单击 Workspace 菜单项，然后单击列表中的 Workspace 名称。 []
3. 单击工作负载计划选项卡。 []
4. 单击工作负载计划标题中的管理链接。 []
5. 从状态下拉列表中选择默认状态：始终打开（默认），始终关闭或已计划。
6. 如果选择已计划，则计划选项包括：
    a. 每天按分配的间隔运行。此选项会将一周中所有七天的计划设置为相同的开始时间和结束时间。 []
    b. 按指定间隔运行指定天数。此选项仅会将一周中选定日期的计划设置为相同的开始时间和结束时间。如果未选择一周中的某些天，则发生原因 VDS 将在这些天内不会打开虚拟机。 []
    c. 以不同的时间间隔和天数运行。此选项会将每个选定日期的计划设置为不同的开始时间和结束时间。 []
    d. 设置完计划后，单击 Update schedule 按钮。 []

实时扩展

实时扩展会根据并发用户负载自动打开和关闭共享主机池中的虚拟机。当每个服务器填满时，会打开一个额外的服务器，以便在主机池负载平衡器发送用户会话请求时，该服务器可以随时运行。要有效使用实时扩展，请选择 " 深度优先 " 作为负载平衡器类型。

启用实时扩展：

1. 登录到 VDS https://manage.cloudworkspace.com 使用您的 VDS 凭据。
2. 单击 Workspace 菜单项，然后单击列表中的 Workspace 名称。 []
3. 单击工作负载计划选项卡。 []

4. 单击实时扩展部分中的已启用单选按钮。 []
5. 单击每个服务器的最大用户数，然后输入最大数量。根据虚拟机大小，此数字通常介于 4 到 20 之间。 []
6. 可选—单击 Additional Poweredon Servers Enabled ，然后输入要用于主机池的多个其他服务器。此设置除了激活正在填充的服务器之外，还会激活指定数量的服务器，以便为在同一时间窗口中登录的大型用户组提供缓冲区。 []

实时扩展当前适用场景所有共享资源池。在不久的将来，每个池都将具有独立的实时扩展选项。

关闭整个部署

如果您计划仅在非生产环境下零星使用评估部署，则可以在不使用此部署中的所有虚拟机时将其关闭。

要打开或关闭部署（即关闭部署中的虚拟机），请按照以下步骤操作：

1. 登录到 VDS https://manage.cloudworkspace.com 使用您的 VDS 凭据。
2. 单击部署菜单项。 []将光标滚动到目标部署所在的行上，以显示配置齿轮图标。 []
3. 单击齿轮，然后选择停止。 []
4. 要重新启动或启动，请按照步骤 1-3 进行操作，然后选择启动。 []

停止或启动部署中的所有虚拟机可能需要几分钟的时间。

创建和管理 **VM** 映像

VDS 包含用于创建和管理虚拟机映像以供将来部署的功能。要访问此功能，请导航到： VDS > 部署 > 部署名称 > 配置集合。下面介绍了 "VDI 映像收集 " 功能： ""

配置 **Azure Cloud Backup Service**

VDS 可以本机配置和管理 Azure Cloud Backup ，这是一种用于备份虚拟机的 Azure PaaS 服务。可以按类型或主机池将备份策略分配给单个计算机或一组计算机。有关详细信息，请参见： ""

选择应用程序管理 / 策略模式

默认情况下， VDS 会实施许多组策略对象（ GPO ）来锁定最终用户工作空间。这些策略会阻止访问两个核心数据层位置（例如 C ： \），并阻止以最终用户身份执行应用程序安装。

此评估旨在演示 Window 虚拟桌面的功能，因此您可以选择删除 GPO ，以便实施一个 " 基本工作空间 " ，该工作空间提供与物理工作空间相同的功能和访问权限。要执行此操作，请按照 " 基本工作空间 " 选项中的步骤进行操作。

您还可以选择使用完整的虚拟桌面管理功能集来实施 " 受控工作空间 " 。这些步骤包括为最终用户应用程序授权创建和管理应用程序目录，以及使用管理员级别权限管理对应用程序和数据文件夹的访问。按照 " 受控工作空间 " 一节中的步骤在 AVD 主机池上实施此类工作空间。

受控 **AVD** 工作空间（默认策略）

VDS 部署的默认模式是使用受控工作空间。策略将自动应用。此模式要求 VDS 管理员安装应用程序，然后通过会话桌面上的快捷方式为最终用户授予对该应用程序的访问权限。同样，通过创建映射的共享文件夹并设置权限以仅查看这些映射的驱动器号，而不是标准启动和 / 或数据驱动器，可以为最终用户分配对数据文件夹的访问权

限。要管理此环境，请按照以下步骤安装应用程序并提供最终用户访问权限。

还原到基本 **AVD** 工作空间

要创建基本工作空间，需要禁用默认创建的默认 GPO 策略。

要执行此操作，请执行以下一次性过程：

1. 登录到 VDS https://manage.cloudworkspace.com 使用主管理员凭据。
2. 单击左侧的部署菜单项。 []
3. 单击部署的名称。 []
4. 在 Platform Servers 部分（右中页面）下，滚动到 CMGR1 行的右侧，直到出现相应的齿轮为止。 []
5. 单击相应设备，然后选择 Connect 。 []
6. 输入您在配置期间创建的 "Tech" 凭据，以便使用 HTML5 访问登录到 CMGR1 服务器。 []
7. 单击开始（ Windows ）菜单，然后选择 Windows 管理工具。 []
8. 单击组策略管理图标。 []
9. 单击左窗格列表中的 AADDC 用户项。 []
10. 右键单击右窗格列表中的 " 云工作空间用户 " 策略，然后取消选择 " 已启用链接 " 选项。单击确定确认此操作。 [] []
11. 从菜单中选择操作，组策略更新，然后确认要在这些计算机上强制更新策略。 []
12. 重复步骤 9 和 10 ，但选择 "AADDC 用户 " 和 " 云工作空间公司 " 作为策略以禁用此链接。完成此步骤后，您无需强制更新组策略。 [] []
13. 关闭组策略管理编辑器和管理工具窗口，然后注销。 []这些步骤将为最终用户提供一个基本的工作空间环境。要进行确认，请以最终用户帐户之一的身份登录—会话环境不应具有任何受控的工作空间限制，例如隐藏的 " 开始 " 菜单，锁定对 C ： \ 驱动器的访问以及隐藏的 " 控制面板 " 。

> 在部署期间创建的 .tech 帐户可以完全访问在独立于 VDS 的文件夹上安装应用程序和更改安全性。但是，如果您希望 Azure AD 域中的最终用户具有类似的完全访问权限，则应将其添加到每个虚拟机上的本地管理员组。

AVD 部署指南—现有 **AD** 补充

概述

VDS 安装程序可以将新部署连接到现有 AD 结构。本说明详细介绍了该选项。本文不是独立的，而是详细说明了中所述的新 AD 选项的替代方案 "AVD 部署指南"

Active Directory 类型

下一节定义了 VDS 部署的 Active Directory 部署类型。在本指南中，我们将选择现有的 Windows Server Active Directory ，它将利用已存在的 AD 结构。

现有 **AD** 网络

VDS 设置将显示 vNets 列表，这些 vNets 可能表示现有 AD 结构与 Azure AD 之间的连接。您选择的 vNet 应具有已在 Azure 中配置的 Azure 托管 DC 。此外， vNet 还会将自定义 DNS 设置指向 Azure 托管的 DC 。

[]

现有 **Active Directory** 域名

输入要使用的现有域名。注意：您不希望使用 Azure 门户中 Active Directory 模块下的域，因为它可能会出现发生原因 DNS 问题。这方面的主要示例是，用户将无法从其桌面内部访问该网站（例如 <yourdomain>.com ）。

现有 **AD** 用户名和密码

可以通过三种方式提供必要的凭据，以便使用现有 AD 结构进行部署。

1. 提供 Active Directory 域管理员用户名和密码

   这是最简单的方法—提供域管理员凭据，以便于部署。

   此帐户可以一次性创建，并在部署过程完成后删除。

2. 创建帐户匹配所需权限

   此方法需要客户管理员在此处手动创建权限结构，然后在此处输入 CloudWorkspaceSVC 帐户的凭据并继续操作。

3. 手动部署过程

   请联系 NetApp VDS 支持部门，以获得有关使用权限最低的帐户主体配置 AD 访问的帮助。

后续步骤

本文介绍了部署到现有 AD 环境中的独特步骤。完成这些步骤后，您可以返回到标准部署指南 "此处"。

VDS 组件和权限

AVD 和 **VDS** 安全实体和服务

Azure Virtual Desktop （ AVD ）需要 Azure AD 和本地 Active Directory 中的安全帐户和组件来执行自动化操作。NetApp 的虚拟桌面服务（ Virtual Desktop Service ， VDS ）可在部署过程中创建组件和安全设置，以使管理员能够控制 AVD 环境。本文档介绍了这两种环境中的相关 VDS 帐户，组件和安全设置。

部署自动化流程的组件和权限主要与最终部署的环境的组件不同。因此，本文分为两个主要部分：部署自动化部分和已部署环境部分。

[宽度 = 75%]

AVD 部署自动化组件和权限

VDS 部署利用多个 Azure 和 NetApp 组件以及安全权限来实施部署和工作空间。

VDS 部署服务

企业级应用程序

VDS 利用租户 Azure AD 域中的企业级应用程序和应用程序注册。企业应用程序是从 Azure AD 实例安全上下文中调用 Azure Resource Manager ， Azure 图形和（如果使用 AVD 秋季版本） AVD API 端点的管道，并使用授予关联服务主体的委派角色和权限。根据租户通过 VDS 获得的 AVD 服务的初始化状态，可以创建应用程序注册。

为了能够创建和管理这些 VM ， VDS 会在 Azure 订阅中创建多个支持组件：

云工作空间

这是企业级应用程序管理员最初授予的许可，并在 VDS 设置向导的部署过程中使用。

在 VDS 设置过程中， Cloud Workspace Enterprise 应用程序会请求一组特定的权限。这些权限包括：

- 以登录用户身份访问目录（已委派）
- 读写目录数据（已委派）
- 登录并读取用户配置文件（已委派）
- 对用户进行签名（已委派）
- 查看用户的基本配置文件（已委派）
- 以组织用户身份访问 Azure 服务管理（已委派）

云工作空间 **API**

处理 Azure PaaS 功能的常规管理调用。Azure PaaS 功能的示例包括 Azure Compute ， Azure Backup ， Azure Files 等。此服务主体要求在初始部署期间拥有目标 Azure 订阅的所有者权限，并要求为持续管理提供贡献者权限（注： 使用 Azure Files 需要订阅所有者权限才能为 Azure 文件对象设置每个用户的权限。

在 VDS 设置过程中， Cloud Workspace API Enterprise 应用程序会请求一组特定的权限。这些权限包括：

- 订阅贡献者（如果使用 Azure 文件，则为订阅所有者）
- Azure AD 图形
  - 读取和写入所有应用程序（应用程序）
  - 管理此应用程序创建或拥有的应用程序（应用程序）
  - 读写设备（应用程序）
  - 以登录用户身份访问目录（已委派）
  - 读取目录数据（应用程序）
  - 读取目录数据（已委派）
  - 读写目录数据（应用程序）
  - 读写目录数据（已委派）
  - 读取和写入域（应用程序）
  - 读取所有组（已委派）
  - 读取和写入所有组（已委派）

- 读取所有隐藏的成员资格（应用程序）
- 读取隐藏的成员资格（已委派）
- 登录并读取用户配置文件（已委派）
- 读取所有用户的完整配置文件（已委派）
- 读取所有用户的基本配置文件（已委派）

- Azure 服务管理
  - 以组织用户身份访问 Azure 服务管理（已委派）

NetApp VDS

NetApp VDS 组件可通过 VDS 控制平面来自动部署和配置 AVD 角色，服务和资源。

自定义角色

创建自动化贡献者角色的目的是，通过特权最少的方法来促进部署。此角色允许 CMGR1 虚拟机访问 Azure 自动化帐户。

自动化帐户

自动化帐户会在部署期间创建，并且是配置过程中所需的组件。Automation 帐户包含变量，凭据，模块和所需状态配置，并引用密钥存储。

所需状态配置

这是用于构建 CMGR1 配置的方法。配置文件会下载到虚拟机中，并通过虚拟机上的本地 Configuration Manager 应用。配置要素的示例包括：

- 安装 Windows 功能
- 正在安装软件
- 正在应用软件配置
- 确保应用正确的权限集
- 应用 Let 的加密证书
- 确保 DNS 记录正确无误
- 确保已将 CMGR1 加入此域

模块：

- ActiveDirectoryDsc ： 部署和配置 Active Directory 所需的状态配置资源。通过这些资源，您可以配置新域，子域和高可用性域控制器，建立跨域信任并管理用户，组和 OU 。
- AZ 帐户： Microsoft 提供的一个模块，用于管理 Azure 模块的凭据和通用配置元素
- AZ-Automation ： Microsoft 为 Azure Automation 命令集提供了一个模块
- Az.Compute:A Microsoft 为 Azure 计算命令小程序提供了模块
- AZ-KeyVault ： Microsoft 为 Azure Key Vault 命令集提供的模块

- AZ 资源： Microsoft 为 Azure Resource Manager 命令集提供的模块
- cChoca ： 使用 chocolatey 下载和安装软件包所需的状态配置资源
- cjAz ： 此 NetApp 创建的模块可为 Azure 自动化模块提供自动化工具
- cjAzACS ： 此 NetApp 创建的模块包含在用户环境中运行的环境自动化功能和 PowerShell 进程。
- cjAzBuild ： 此 NetApp 创建的模块包含在系统环境中运行的构建和维护自动化以及 PowerShell 流程。
- cNtfsAccessControl ： NTFS 访问控制管理所需的状态配置资源
- ComputerManagementDsc ： 所需的状态配置资源，用于执行计算机管理任务，例如加入域和计划任务，以及配置虚拟内存，事件日志，时区和电源设置等项。
- cUserRightsAssignment ： 允许管理用户权限（例如登录权限和特权）的所需状态配置资源
- NetworkingDsc ： 网络所需的状态配置资源
- xCertificate ： 用于简化 Windows Server 上证书管理的所需状态配置资源。
- xDnsServer ： 用于配置和管理 Windows Server DNS 服务器的所需状态配置资源
- xNetworking ： 与网络连接相关的所需状态配置资源。
- "xRemoteDesktopAdmin"：此模块利用一个存储库，其中包含在本地或远程计算机上配置远程桌面设置和 Windows 防火墙所需的状态配置资源。
- xRemoteDesktopSessionHost ： 所需的状态配置资源（ xRDSessionDeployment ， xRDSessionCollection ， xRDSessionCollectionConfiguration 和 xRDRemoteApp ），用于创建和配置远程桌面会话主机（ RDSH ）实例
- xSmbShare ： 配置和管理 SMB 共享所需的状态配置资源
- xSystemSecurity ： 用于管理 UAC 和 IE Esc 的所需状态配置资源

> Azure Virtual Desktop 还会安装 Azure 组件，包括适用于 Azure Virtual Desktop 和 Azure Virtual Desktop Client ， AVD 租户， AVD 主机池， AVD 应用程序组和 AVD 注册虚拟机的企业级应用程序和应用程序注册。虽然 VDS Automation 组件负责管理这些组件，但 AVD 会控制其默认配置和属性集，因此，有关详细信息，请参见 AVD 文档。

混合 **AD** 组件

为了便于与现有的公有云中运行的现有 AD 进行集成，现有 AD 环境还需要其他组件和权限。

域控制器

现有域控制器可通过 AD Connect 和 / 或站点到站点 VPN （或 Azure ExpressRoute ）集成到 AVD 部署中。

AD Connect

为了便于通过 AVD PaaS 服务成功进行用户身份验证，可以使用 AD 连接将域控制器与 Azure AD 同步。

安全组

VDS 使用名为 CW-Infrastructure 的 Active Directory 安全组来提供自动执行域加入和 GPO 策略附件等与 Active Directory 相关的任务所需的权限。

服务帐户

VDS 使用名为 CloudworkspaceSVC 的 Active Directory 服务帐户，该帐户用作 VDS Windows 服务和 IIS 应用程序服务的标识。此帐户为非交互式帐户（不允许 RDP 登录），是 CW-Infrastructure 帐户的主要成员

VPN 或 **ExpressRoute**

可以使用站点到站点 VPN 或 Azure ExpressRoute 直接将 Azure VM 加入现有域。这是一种可选配置，可在项目要求需要时使用。

本地 **AD** 权限委派

NetApp 提供了一种可简化混合 AD 流程的可选工具。如果使用 NetApp 的可选工具， IT 必须：

- 在服务器操作系统上运行，而不是在工作站操作系统上运行
- 在加入域或作为域控制器的服务器上运行
- 在运行此工具的服务器（如果未在域控制器上运行）和域控制器上安装 PowerShell 5.0 或更高版本
- 由具有域管理员权限的用户运行，或者由具有本地管理员权限并能够提供域管理员凭据的用户运行（用于 RunA ）

无论是手动创建还是通过 NetApp 的工具应用，所需权限均为：

- CW-Infrastructure 组
  - Cloud Workspace Infrastructure （ * CW-Infrastructure* ）安全组被授予对 Cloud Workspace OU 级别和所有后代对象的完全控制权限
  - <deployment code>.cloudworkworkspace .app DNS Zone — CW-Infrastructure 组授予 Create儿童， Delete儿童， ListChildren's， ReadProperty， DeleteTree， ExtendedRight， Delete， GenericWrite
  - DNS 服务器— CW-Infrastructure Group 授予 ReadProperty 和 GenericExecute 权限
  - 已创建 VM 的本地管理员访问（ CMGR1 ， AVD 会话 VM ）（通过受管 AVD 系统上的组策略完成）
- CW-CVMGRAccess 组此组为所有模板，单个服务器，新的原生 Active Directory 模板利用内置的组服务器操作员远程桌面用户和网络配置操作员向 CMGR1 提供本地管理权限。

AVD 环境组件和权限

部署自动化流程完成后，持续使用和管理部署和工作空间需要一组不同的组件和权限，如下所述。上述的许多组件和权限仍然相关，但本节重点介绍了如何定义已部署的的结构。

VDS 部署和工作空间的组件可以分为多个逻辑类别：

- 最终用户客户端
- VDS 控制面板组件
- Microsoft Azure AVD-PaaS 组件
- VDS 平台组件
- Azure 租户中的 VDS 工作空间组件
- 混合 AD 组件

最终用户客户端

用户可以连接到其 AVD 桌面和 / 或各种端点类型。Microsoft 已发布适用于 Windows ， macOS ， Android 和 iOS 的客户端应用程序。此外，还可以使用 Web 客户端进行无客户端访问。

有些 Linux 瘦客户端供应商已经发布了适用于 AVD 的端点客户端。这些信息在中列出 https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

VDS 控制面板组件

VDS REST API

VDS 基于完整记录的 REST API 构建，因此 Web 应用程序中的所有可用操作也可通过 API 来执行。API 文档如下所示： https://api.cloudworkspace.com/5.4/swagger/ui/index#

VDS Web 应用程序

VDS 管理员可以通过 VDS Web 应用程序与 ADS 应用程序进行交互。此 Web 门户位于： https://manage.cloudworkspace.com

控制平面数据库

VDS 数据和设置存储在 NetApp 托管和管理的控制平面 SQL 数据库中。

VDS 通信

Azure 租户组件

VDS 部署自动化会创建一个 Azure 资源组来包含其他 AVD 组件，包括 VM ，网络子网，网络安全组以及 Azure 文件容器或 Azure NetApp Files 容量池。注意—默认情况下为单个资源组，但如果需要， VDS 可通过工具在其他资源组中创建资源。

Microsoft Azure AVD-PaaS 组件

AVD REST API

Microsoft AVD 可通过 API 进行管理。VDS 广泛利用这些 API 来自动化和管理 AVD 环境。文档位于： https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

会话代理

代理将确定为用户授权的资源，并编排用户与网关的连接。

Azure 诊断

Azure 诊断专为支持 AVD 部署而构建。

AVD Web 客户端

Microsoft 提供了一个 Web 客户端，用户无需在本地安装客户端即可连接到其 AVD 资源。

会话网关

本地安装的 RD 客户端连接到网关，以便安全地与 AVD 环境进行通信。

VDS 平台组件

CMGR1

CMWGR1 是每个部署的 VDS 控制 VM 。默认情况下，它会在目标 Azure 订阅中创建为 Windows 2019 Server VM 。有关安装在 CMGR1 上的 VDS 和第三方组件的列表，请参见 " 本地部署 " 一节。

AVD 要求 AVD VM 加入 Active Directory 域。为了便于执行此过程并提供用于管理 VDS 环境的自动化工具，上述的 CMGR1 VM 上安装了多个组件，并向 AD 实例添加了多个组件。这些组件包括：

- * Windows 服务 * — VDS 使用 Windows 服务在部署中执行自动化和管理操作：
  - * 连续运行自动化服务 * 是在每个 AVD 部署中部署在 CMGR1 上的一项 Windows 服务，用于在环境中执行许多面向用户的自动化任务。此服务在 * CloudWorkspaceSVc* AD 帐户下运行。
  - * 四路虚拟机自动化服务 * 是在每个 AVD 部署中部署在 CMGR1 上的一项 Windows 服务，用于执行虚拟机管理功能。此服务在 * CloudWorkspaceSVc* AD 帐户下运行。
  - **CW Agent Service** 是一种 Windows 服务，部署在 VDS 管理下的每个虚拟机上，包括 CMGR1 。此服务在虚拟机上的 * 本地系统 * 环境下运行。
  - * 在每个 AVD 部署中， WCMGR1 上安装了一个基于 IIS 应用程序池的侦听器。此操作将处理来自全局控制平台的入站请求，并在 * CloudWorkspaceSVC/ AD 帐户下运行。
- * SQL Server 2017 Express* — VDS 在 CMGR1 VM 上创建一个 SQL Server Express 实例，用于管理自动化组件生成的元数据。
- * 互联网信息服务（ Internet Information Services ， IIS ） * —在 CMGR1 上启用了 IIS 以托管 CWManagerX 和 CWApps IIS 应用程序（仅当启用了 RDS RemoteApp 功能时）。VDS 需要使用 IIS 7.5 或更高版本。
- * HTML5 Portal （可选） * — VDS 安装了 Spark 网关服务，以便在部署中和从 VDS Web 应用程序对 VM 进行 HTML5 访问。这是一个基于 Java 的应用程序，如果不需要使用此访问方法，可以禁用并删除此应用程序。
- * RD 网关（可选） * — VDS 使 CMGR1 上的 RD 网关角色能够为基于 RDS 收集的资源池提供 RDP 访问。如果仅需要 AVD 反向连接访问，则可以禁用 / 卸载此角色。
- * RD Web （可选） * — VDS 启用 RD Web 角色并创建 CWApps IIS Web 应用程序。如果只需要 AVD 访问，则可以禁用此角色。
- * DC Config* —一种 Windows 应用程序，用于执行部署和 VDS 站点专用配置以及高级配置任务。
- * 测试 VDC 工具 * —一种 Windows 应用程序，支持直接执行虚拟机任务和客户端级别配置更改，在极少数情况下需要修改 API 或 Web 应用程序任务以进行故障排除。
- * 我们来加密通配符证书（可选） * —由 VDS 创建和管理—所有需要通过 TLS 传输 HTTPS 流量的虚拟机每晚都使用证书进行更新。续订也通过自动任务来处理（证书为 90 天，因此不久将开始续订）。如果需要，客户可以提供自己的通配符证书。VDS 还需要多个 Active Directory 组件来支持自动化任务。设计目的是利用最少数量的 AD 组件和权限添加，同时仍支持环境的自动化管理。这些组件包括：
- * 云工作空间组织单位（ OU ） * —此组织单位将充当所需子组件的主 AD 容器。CW-Infrastructure 和客户端 DHP 访问组的权限将在此级别及其子组件进行设置。有关在此 OU 中创建的子 OU ，请参见附录 A 。
- * 云工作空间基础架构组（ CW-Infrastructure ） * 是在本地 AD 中创建的一个安全组，用于将所需的委派权限分配给 VDS 服务帐户（ * CloudWorkspaceSVC* ）

- * 客户端 DHP 访问组（ ClientDHPAccess ） * 是在本地 AD 中创建的一个安全组，可通过 VDS 控制公司共享数据，用户主目录数据和配置文件数据所在的位置。
- * CloudWorkspaceSVC/ 服务帐户（ Cloud Workspace Infrastructure Group 成员）
- 部署代码 >.cloudworkworkspace .app 域 * 的 * DNS 分区（此域管理会话主机 VM 的自动创建 DNS 名称）—由 Deploy 配置创建。
- 链接到云工作空间组织单位的各个子 OU 的 * NetApp 专用 GPO * 。这些 GPO 包括：
  - * 云工作空间 GPO （链接到云工作空间 OU ） * —定义 CW-Infrastructure 组成员的访问协议和方法。此外，还会将该组添加到 AVD 会话主机上的本地管理员组。
  - * 云工作空间防火墙 GPO * （链接到专用客户服务器，远程桌面和暂存 OU ）—创建一个策略，用于确保与平台服务器的会话主机连接并将其隔离。
  - * 云工作空间 RDS* （专用客户服务器，远程桌面和暂存 OU ）—会话质量，可靠性和断开连接超时限制的策略集限制。对于 RDS 会话，定义了 TS 许可服务器值。
  - * 云工作空间公司 * （默认情况下不链接）—可选的 GPO ，用于通过阻止访问管理工具和区域来 " 锁定 " 用户会话 / 工作空间。可以通过链接 / 启用来提供受限活动工作空间。

可以根据请求提供默认组策略设置配置。

VDS 工作空间组件

数据层

Azure NetApp Files

如果您在 VDS 设置中选择 Azure NetApp Files 作为数据层选项，则会创建 Azure NetApp Files 容量池和关联的卷。卷托管用户配置文件（通过 FSLogix 容器），用户个人文件夹和企业数据共享文件夹的共享归档存储。

Azure 文件

如果您在 CWS 设置中选择 Azure 文件作为数据层选项，则会创建 Azure 文件共享及其关联的 Azure 存储帐户。Azure 文件共享托管用户配置文件（通过 FSLogix 容器），用户个人文件夹和企业数据共享文件夹的共享归档存储。

具有受管磁盘的文件服务器

如果您在 VDS 设置中选择文件服务器作为数据层选项，则会使用受管磁盘创建 Windows Server VM 。文件服务器托管用户配置文件（通过 FSLogix 容器），用户个人文件夹和企业数据共享文件夹的共享归档存储。

Azure 网络

Azure 虚拟网络

VDS 创建 Azure 虚拟网络并支持子网。VDS 要求为 CMGR1 ， AVD 主机和 Azure 域控制器使用单独的子网，并在子网之间建立对等关系。请注意， AD 控制器子网通常已存在，因此 VDS 部署的子网需要与现有子网建立对等关系。

网络安全组

系统会创建一个网络安全组来控制对 CMGR1 虚拟机的访问。

- 租户：包含用于会话主机和数据 VM 的 IP 地址
- 服务：包含供 PaaS 服务（例如 Azure NetApp Files ）使用的 IP 地址
- 平台：包含用作 NetApp 平台 VM （ CMGR1 和任何网关服务器）的 IP 地址
- 目录：包含用作 Active Directory VM 的 IP 地址

Azure AD

VDS 自动化和流程编排会将虚拟机部署到目标 Active Directory 实例中，然后将这些虚拟机加入指定的主机池。AVD 虚拟机在计算机级别由 AD 结构（组织单位，组策略，本地计算机管理员权限等）和 AVD 结构中的成员资格（主机池，工作空间应用程序组成员资格）进行管理，这些结构由 Azure AD 实体和权限管理。VDS 通过使用 VDS Enterprise 应用程序 /Azure 服务主体执行 AVD 操作以及使用本地 AD 服务帐户（ CloudWorkspaceSVC ）执行本地 AD 和本地计算机操作来处理此 " 双重控制 " 环境。

创建 AVD 虚拟机并将其添加到 AVD 主机池的具体步骤包括：

- 从 Azure 创建虚拟机模板对与 AVD 关联的 Azure 订阅可见（使用 Azure 服务主体权限）
- 使用 VDS 部署期间指定的 Azure vNet 检查 / 配置新虚拟机的 DNS 地址（需要本地 AD 权限（所有权限均委派给上述 CW-Infrastructure ）使用标准 VDS 命名方案 * _ ｛ companycode ｝ TS ｛ sequencenumber ｝ _* 设置虚拟机名称。示例： XYZTS3 。（需要本地 AD 权限（置于我们在内部创建的 OU 结构中）（远程桌面 / 公司代码 / 共享）（与上述权限 / 组问题描述相同）
- 将虚拟机放置在指定的 Active Directory 组织单位（ AD ）中（需要向 OU 结构委派权限（在上述手动过程中指定））
- 使用新计算机名称 /IP 地址更新内部 AD DNS 目录（需要本地 AD 权限）
- 将新虚拟机加入本地 AD 域（需要本地 AD 权限）
- 使用新的服务器信息更新 VDS 本地数据库（不需要其他权限）
- 将 VM 加入指定的 AVD 主机池（需要 AVD 服务主体权限）
- 将 chocolatey 组件安装到新虚拟机（需要为 * CloudWorkspaceSVS* 帐户提供本地计算机管理权限）
- 为 AVD 实例安装 FSLogix 组件（需要对本地 AD 中的 AVD OU 具有本地计算机管理权限）
- 更新 AD Windows 防火墙 GPO 以允许流量传输到新虚拟机（需要为与 AVD OU 及其关联虚拟机关联的策略创建 / 修改 AD GPO 。需要在本地 AD 的 AVD OU 上创建 / 修改 AD GPO 策略。如果不通过 VDS 管理 VM ，则可以在安装后关闭。）
- 在新虚拟机上设置 " 允许新连接 " 标志（需要 Azure 服务主体权限）

将 **VM** 加入 **Azure AD**

Azure 租户中的虚拟机需要加入域，但 VM 无法直接加入 Azure AD 。因此， VDS 会在 VDS 平台中部署域控制器角色，然后使用 AD Connect 将该 DC 与 Azure AD 同步。其他配置选项包括使用 Azure AD 域服务（ AADDS ），使用 AD Connect 同步到混合 DC （内部或其他位置的 VM ），或者通过站点到站点 VPN 或 Azure ExpressRoute 将 VM 直接加入到混合 DC 。

AVD 主机池

主机池是 Azure Virtual Desktop 环境中一个或多个相同虚拟机（ VM ）的集合。每个主机池可以包含一个应用程序组，用户可以像在物理桌面上一样与该应用程序组进行交互。

会话主机

在任何主机池中，都是一个或多个相同的虚拟机。这些连接到此主机池的用户会话由 AVD 负载平衡器服务进行负载平衡。

应用程序组

默认情况下， *Desktop Users* 应用程序组会在部署时创建。此应用程序组中的所有用户均可获得完整的 Windows 桌面体验。此外，还可以创建应用程序组来提供流式应用程序服务。

日志分析工作空间

此时将创建日志分析工作空间，用于存储部署和 DSC 进程以及其他服务的日志。此功能可以在部署后删除，但不建议这样做，因为它可以启用其他功能。默认情况下，日志保留 30 天，不会产生任何保留费用。

可用性集

在部署过程中设置了可用性集，以便在故障域之间隔离共享 VM （共享 AVD 主机池， RDS 资源池）。如果需要，可以在部署后删除此选项，但会禁用为共享 VM 提供额外容错的选项。

Azure 恢复存储

恢复服务存储是由 VDS Automation 在部署期间创建的。默认情况下，此功能当前处于激活状态，因为在部署过程中， Azure Backup 会应用于 CMGR1 。如果需要，可以停用并删除此设置，但如果在环境中启用了 Azure Backup ，则会重新创建此设置。

Azure 密钥存储

Azure 密钥存储在部署过程中创建，用于存储 Azure 自动化帐户在部署期间使用的证书， API 密钥和凭据。

附录 **A —**默认云工作空间组织单位结构

- 云工作空间
  - 云工作空间公司
  - 云工作空间服务器
    - 专用客户服务器
    - 基础架构
- CWMGR 服务器
- 网关服务器
- FTP 服务器
- 模板 VM
  - 远程桌面

- 暂存
  - 云工作空间服务帐户
- 客户端服务帐户
- 基础架构服务帐户
  - Cloud Workspace 技术用户
- 组
- 技术 3 技术人员

AVD 和 VDS v5.4 前提条件

AVD 和 VDS 要求和说明

本文档介绍使用 NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）部署 Azure 虚拟桌面（ AVD ）所需的要素。" 快速检查清单 " 简要列出了确保高效部署所需的组件和部署前步骤。本指南的其余部分将根据所做的配置选择详细介绍每个元素。

快速检查清单

Azure 要求

- Azure AD 租户
- Microsoft 365 许可以支持 AVD
- Azure 订阅
- Azure 虚拟机的可用 Azure 配额
- 具有全局管理员和订阅所有权角色的 Azure 管理员帐户
- 域管理员帐户，具有 AD Connect 设置的 " 企业管理员 " 角色

部署前信息

- 确定用户总数
- 确定 Azure 区域
- 确定 Active Directory 类型
- 确定存储类型
- 确定会话主机 VM 映像或要求
- 评估现有 Azure 和内部网络配置

VDS 部署详细要求

最终用户连接要求

以下远程桌面客户端支持 **Azure** 虚拟桌面：

- Windows 桌面

- Web
- macOS
- iOS
- IGEL 思考客户端（ Linux ）
- Android （预览）

Azure 虚拟桌面不支持 RemoteApp and Desktop Connection （ RADC ）客户端或远程桌面连接（ MSTSC ）客户端。

Azure 虚拟桌面当前不支持从 Windows 应用商店使用远程桌面客户端。未来版本将添加对此客户端的支持。

- 远程桌面客户端必须能够访问以下 URL： *

Address	出站 **TCP** 端口	目的	客户端
* .AVD.microsoft.com	443.	服务流量	全部
* .servicebus.windows.net 443 故障排除数据	全部	go.microsoft.com	443.
Microsoft FWLinks	全部	也称为 .ms	443.
Microsoft URL 缩写	全部	docs.microsoft.com	443.
文档。	全部	privacy.microsoft.com	443.
隐私声明	全部	query.prod.cms.rt.microsoft.com	443.

打开这些 URL 对于获得可靠的客户端体验至关重要。不支持阻止对这些 URL 的访问，并会影响服务功能。这些 URL 仅对应于客户端站点和资源，不包括 Azure Active Directory 等其他服务的 URL 。

VDS 设置向导的起点

VDS 设置向导可以处理成功部署 AVD 所需的许多前提条件设置。设置向导（""）创建或使用以下组件。

Azure 租户

- 必填： * Azure 租户和 Azure Active Directory

Azure 中的 AVD 激活是一种租户范围的设置。VDS 支持每个租户运行一个 AVD 实例。

Azure 订阅

- 必填： * Azure 订阅（请记下要使用的订阅 ID ）

所有已部署的 Azure 资源应设置在一个专用订阅中。这样可以更轻松地跟踪 AVD 的成本，并简化部署过程。注意：不支持 Azure 免费试用，因为它们没有足够的抵免额来部署功能正常的 AVD 部署。

Azure 核心配额

为要使用的 VM 系列提供足够的配额—特别是在初始平台部署中， DS v3 系列至少有 10 个核心（只能使用 2 个核心，但每个初始部署可能都有 10 个核心）。

Azure 管理员帐户

- 必填： * 一个 Azure 全局管理员帐户。

VDS 设置向导会请求 Azure 管理员向 VDS 服务主体授予委派的权限，并安装 VDS Azure Enterprise 应用程序。管理员必须分配以下 Azure 角色：

- 租户的全局管理员
- 订阅中的所有者角色

VM 映像

- 必填： * 支持多会话 Windows 10 的 Azure 映像。

Azure Marketplace 提供其基本 Windows 10 映像的最新版本，所有 Azure 订阅均可自动访问这些映像。如果您要使用其他映像或自定义映像，希望 VDS 团队提供有关创建或修改其他映像的建议，或者对 Azure 映像有一些一般性问题，请告知我们，我们可以安排对话。

Active Directory

AVD 要求用户身份属于 Azure AD ，并且 VM 加入与同一 Azure AD 实例同步的 Active Directory 域。VM 不能直接连接到 Azure AD 实例，因此需要配置域控制器并与 Azure AD 同步。

支持的选项包括：

- 在订阅中自动构建 Active Directory 实例。AD 实例通常由 VDS 在 VDS 控制虚拟机（ CMGR1 ）上为使用此选项的 Azure 虚拟桌面部署创建。在设置过程中，必须设置并配置 AD Connect 以与 Azure AD 同步。

  []

- 集成到可通过 Azure 订阅（通常通过 Azure VPN 或 Express Route ）访问的现有 Active Directory 域中，并使用 AD Connect 或第三方产品将其用户列表同步到 Azure AD 。

  []

存储层

在 AVD 中，存储策略的设计目的是， AVD 会话 VM 上不会驻留任何永久性用户 / 公司数据。用户配置文件，用户文件和文件夹以及公司 / 应用程序数据的永久性数据托管在独立数据层上托管的一个或多个数据卷上。

FSLogix 是一种配置文件容器化技术，可通过在会话初始化时将用户配置文件容器（ VHD 或 VHDX 格式）挂载到会话主机来解决许多用户配置文件问题（如数据无序增长和登录速度较慢）。

由于采用这种架构，需要具备数据存储功能。此功能必须能够处理每天早晨 / 下午当大部分用户同时登录 / 注销时所需的数据传输。即使规模适中的环境也可能需要大量数据传输。数据存储层的磁盘性能是最终用户性能的主要变量之一，必须特别注意适当调整此存储的性能大小，而不仅仅是存储容量。通常，存储层的大小应支持每个用户 5-15 IOPS 。

VDS 设置向导支持以下配置：

- 设置和配置 Azure NetApp Files （ ANF ）（建议）。_ANF 标准服务级别最多支持 150 个用户，而建议使用 150-500 个用户的环境。 ANF 高级版。对于 500 多个用户，建议使用 ANF 超高级版。 _

  []

- 设置和配置文件服务器虚拟机

  []

网络

- 必填： * 所有现有网络子网的清单，包括通过 Azure Express Route 或 VPN 对 Azure 订阅可见的任何子网。此部署需要避免子网重叠。

通过 VDS 设置向导，您可以在计划内与现有网络集成时定义所需或必须避免的网络范围。

在部署期间确定用户的 IP 范围。根据 Azure 最佳实践，仅支持专用范围内的 IP 地址。

支持的选项包括以下，但默认为 **/20** 范围：

- 192.168.0.0 到 192.168.255.255
- 172.16.0.0 到 172.31.255.255
- 10.0.0.0 到 10.255.255.255

CMGR1

VDS 的某些独特功能，例如，节省成本的工作负载计划和实时扩展功能需要在租户和订阅中具有管理功能。因此，在 VDS 设置向导自动化过程中会部署一个名为 CMGR1 的管理 VM 。除了 VDS 自动化任务之外，此 VM 还在 SQL 快速数据库，本地日志文件和一个名为 DCConfig 的高级配置实用程序中保存 VDS 配置。

根据在 **VDS** 设置向导中所做的选择，此虚拟机可用于托管其他功能，包括：

- RDS 网关（仅用于 RDS 部署）
- HTML 5 网关（仅用于 RDS 部署）
- RDS 许可证服务器（仅用于 RDS 部署）
- 域控制器（如果选择）

部署向导中的决策树

在初始部署过程中，我们会回答一系列问题，以自定义新环境的设置。下面概述了要做出的主要决策。

Azure 区域

确定要托管 AVD 虚拟机的 Azure 区域。请注意， Azure NetApp Files 和某些 VM 系列（例如支持 GPU 的 VM ）都定义了 Azure 区域支持列表，而 AVD 则在大多数地区可用。

- 此链接可用于标识 "按区域划分的 Azure 产品可用性"

Active Directory 类型

确定要使用的 Active Directory 类型：

- 现有内部 Active Directory
- 请参见 "AVD VDS 组件和权限" 文档，介绍 Azure 和本地 Active Directory 环境中所需的权限和组件
- 基于 Azure 订阅的新 Active Directory 实例
- Azure Active Directory 域服务

数据存储

确定用户配置文件，单个文件和企业共享的数据放置位置。选项包括：

- Azure NetApp Files
- Azure 文件
- 传统文件服务器（采用受管磁盘的 Azure VM ）

现有组件的 **NetApp VDS** 部署要求

使用现有 **Active Directory** 域控制器部署 **NetApp VDS**

此配置类型可扩展现有 Active Directory 域以支持 AVD 实例。在这种情况下， VDS 会将一组有限的组件部署到域中，以支持 AVD 组件的自动配置和管理任务。

此配置需要：

- 一种现有 Active Directory 域控制器，可由 Azure vNet 上的 VM 访问，通常通过 Azure VPN 或 Express Route 或已在 Azure 中创建的域控制器进行访问。
- 添加了 AVD 主机池和数据卷加入域时的 VDS 管理所需的 VDS 组件和权限。AVD VDS 组件和权限指南定义了所需的组件和权限，部署过程要求具有域权限的域用户运行将创建所需元素的脚本。
- 请注意，默认情况下， VDS 部署会为 VDS 创建的 VM 创建一个 vNet 。vNet 可以与现有 Azure 网络 VNets 建立对等关系，也可以将 CMGR1 VM 移至已预先定义了所需子网的现有 vNet 。

凭据和域准备工具

管理员必须在部署过程的某个时刻提供域管理员凭据。可以稍后创建，使用和删除临时域管理员凭据（部署过程完成后）。或者，在构建前提条件方面需要帮助的客户也可以使用域准备工具。

使用现有文件系统部署 **NetApp VDS**

VDS 创建的 Windows 共享允许从 AVD 会话 VM 访问用户配置文件，个人文件夹和企业数据。默认情况下， VDS 将部署文件服务器或 Azure NetApp 文件选项，但如果您有现有文件存储组件，则 VDS 可以在 VDS 部署完成后将共享指向该组件。

使用和现有存储组件的要求：

- 此组件必须支持 SMB v3
- 组件必须与 AVD 会话主机加入同一 Active Directory 域
- 该组件必须能够公开一个 UNC 路径以供 VDS 配置使用—所有三个共享都可以使用一个路径，或者可以为每

个共享指定单独的路径。请注意， VDS 将为这些共享设置用户级别权限，因此请参阅 VDS AVD 组件和权限文档，以确保已为 VDS 自动化服务授予适当的权限。

使用现有 **Azure AD** 域服务部署 **NetApp VDS**

此配置需要通过一个过程来确定现有 Azure Active Directory 域服务实例的属性。请联系您的客户经理以申请此类部署。NetApp VDS 部署与现有 AVD 部署此配置类型假定已存在所需的 Azure vNet ， Active Directory 和 AVD 组件。VDS 部署的执行方式与 " 使用现有 AD 部署 NetApp VDS " 配置相同，但增加了以下要求：

- 需要为 Azure 中的 VDS 企业应用程序授予 AVD 租户的 RD 所有者角色
- 需要使用 VDS Web App 中的 VDS 导入功能将 AVD 主机池和 AVD 主机池 VM 导入到 VDS 中此过程会收集 AVD 主机池和会话 VM 元数据并将其存储在 VDS 中，以便这些元素可通过 VDS 进行管理
- 需要使用 CRA 工具将 AVD 用户数据导入到 VDS 用户部分中。此过程会将有关每个用户的元数据插入 VDS 控制平面，以便 VDS 可以管理其 AVD 应用程序组成员资格和会话信息

附录 **A**： **VDS** 控制面板 **URL** 和 **IP** 地址

Azure 订阅中的 VDS 组件可与 VDS 全局控制平面组件进行通信，例如 VDS Web 应用程序和 VDS API 端点。要进行访问，需要在端口 443 上安全列出以下基本 URI 地址，以便进行双向访问：

""

https://cjdownload3.file.core.windows.net/media

如果您的访问控制设备只能按 IP 地址安全列出，则应将以下 IP 地址列表列入安全列表。请注意， VDS 使用 Azure Traffic Manager 服务，因此此列表可能会随时间而变化：

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.22723.99.136.91 40.119.157 40.78.132.166 40.78.40.129.17 122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.11.21.208.132.132.172.1320.21.208.1721.138.172.138.172.138.1720.21.208.138.1720.21.138.132.138.1720.21.202.138.138.138.138.138.213.620.1.238.138.138.138.138.138.138.138.138.138.217.21.208.138.138.138.138.138.217.21.208.138.138.138.138.17

附录 **B**： **Microsoft AVD** 要求

此 Microsoft AVD 要求部分汇总了 Microsoft 的 AVD 要求。要了解完整且最新的 AVD 要求，请访问：

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Azure 虚拟桌面会话主机许可

Azure Virtual Desktop 支持以下操作系统，因此请确保根据您计划部署的桌面和应用程序为用户提供适当的许可证：

OS	所需许可证
Windows 10 Enterprise 多会话或 Windows 10 Enterprise	Microsoft 365 e3 ， e5 ， a3 ， a5 ， Business Premium Windows e3 ， e5 ， a3 ， a5
Windows 7 Enterprise	Microsoft 365 e3 ， e5 ， a3 ， a5 ， Business Premium Windows e3 ， e5 ， a3 ， a5
Windows Server 2012 R2 ， 2016 ， 2019	具有软件保证的 RDS 客户端访问许可证（ CAL ）

AVD 计算机的 **URL** 访问

您为 Azure Virtual Desktop 创建的 Azure 虚拟机必须能够访问以下 URL：

Address	出站 **TCP** 端口	目的	服务标签
* .AVD.microsoft.com	443.	服务流量	Windows 虚拟桌面
mrsglobalsteus2prod.blob.core.windows.net	443.	代理和 SXS 堆栈更新	AzureCloud
* .core.windows.net	443.	代理流量	AzureCloud
* .servicebus.windows.net	443.	代理流量	AzureCloud
prod.warmpath.msftcloudes.com	443.	代理流量	AzureCloud
catalogartifact.azureedge.net	443.	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows 激活	互联网
AVDportalstorageblob.blob.core.windows.net	443.	Azure 门户支持	AzureCloud

下表列出了 Azure 虚拟机可以访问的可选 URL：

Address	出站 **TCP** 端口	目的	服务标签
* .microsoftonline.com	443.	对 MS Online Services 进行身份验证	无
* .events.data.microsoft.com	443.	遥测服务	无
www.msftconnecttest.com	443.	检测操作系统是否已连接到 Internet	无
* .prod.do.dsp.mp.microsoft.com	443.	Windows 更新	无
login.windows.net	443.	登录到 MS Online Services ， Office 365	无
* 。 sfx.ms	443.	OneDrive 客户端软件的更新	无
* .digicert.com	443.	证书撤消检查	无

最佳性能因素

要获得最佳性能，请确保您的网络满足以下要求：

- 从客户端网络到已部署主机池的 Azure 区域的往返（ RTT ）延迟应小于 150 毫秒。
- 当托管桌面和应用程序的 VM 连接到管理服务时，网络流量可能会超出国家 / 地区边界。

- 为了优化网络性能，我们建议会话主机的 VM 与管理服务位于同一 Azure 区域。

支持的虚拟机操作系统映像

Azure Virtual Desktop 支持以下 x64 操作系统映像：

- Windows 10 Enterprise 多会话，版本 1809 或更高版本
- Windows 10 Enterprise ，版本 1809 或更高版本
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure 虚拟桌面不支持 x86 （ 32 位）， Windows 10 Enterprise N 或 Windows 10 Enterprise KN 操作系统映像。由于扇区大小限制， Windows 7 也不支持托管 Azure 存储上托管的任何基于 VHD 或 VHDX 的配置文件解决方案。

可用的自动化和部署选项取决于您选择的操作系统和版本，如下表所示：

操作系统	**Azure** 映像库	手动部署 **VM**	与支撑模板集成	在 **Azure Marketplace** 上配置主机池
Windows 10 多会话版本 1903	是的。	是的。	是的。	是的。
Windows 10 多会话，版本 1809	是的。	是的。	否	否
Windows 10 Enterprise 版本 1903	是的。	是的。	是的。	是的。
Windows 10 Enterprise ，版本 1809	是的。	是的。	否	否
Windows 7 Enterprise	是的。	是的。	否	否
Windows Server 2019	是的。	是的。	否	否
Windows Server 2016	是的。	是的。	是的。	是的。
Windows Server 2012 R2	是的。	是的。	否	否

AVD 和 **VDS v6.0** 的前提条件

AVD 和 **VDS** 要求和说明

本文档介绍使用 NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）部署 Azure 虚拟桌面（ AVD ）所需的要素。" 快速检查清单 " 简要列出了确保高效部署所需的组件和部署前步骤。本指南的其余部分将根据所做的配置选择详细介绍每个元素。

快速检查清单

Azure 要求

- Azure AD 租户
- Microsoft 365 许可以支持 AVD

- Azure 订阅
- Azure 虚拟机的可用 Azure 配额
- 具有全局管理员和订阅所有权角色的 Azure 管理员帐户
- 域管理员帐户，具有 AD Connect 设置的 " 企业管理员 " 角色

部署前信息

- 确定用户总数
- 确定 Azure 区域
- 确定 Active Directory 类型
- 确定存储类型
- 确定会话主机 VM 映像或要求
- 评估现有 Azure 和内部网络配置

VDS 部署详细要求

最终用户连接要求

以下远程桌面客户端支持 **Azure** 虚拟桌面：

- Windows 桌面
- Web
- macOS
- iOS
- IGEL 思考客户端（ Linux ）
- Android （预览）

Azure 虚拟桌面不支持 RemoteApp and Desktop Connection （ RADC ）客户端或远程桌面连接（ MSTSC ）客户端。

Azure 虚拟桌面当前不支持从 Windows 应用商店使用远程桌面客户端。未来版本将添加对此客户端的支持。

- 远程桌面客户端必须能够访问以下 URL： *

Address	出站 TCP 端口	目的	客户端
* .wvd.microsoft.com	443.	服务流量	全部
* .servicebus.windows.net	443.	对数据进行故障排除	全部
go.microsoft.com	443.	Microsoft FWLinks	全部
也称为 .ms	443.	Microsoft URL 缩写	全部
docs.microsoft.com	443.	文档。	全部

Address	出站 TCP 端口	目的	客户端
privacy.microsoft.com	443.	隐私声明	全部
query.prod.cms.rt.microsoft.com	443.	客户端更新	Windows 桌面

打开这些 URL 对于获得可靠的客户端体验至关重要。不支持阻止对这些 URL 的访问，并会影响服务功能。这些 URL 仅对应于客户端站点和资源，不包括 Azure Active Directory 等其他服务的 URL 。

VDS 设置向导的起点

VDS 设置向导可以处理成功部署 AVD 所需的许多前提条件设置。设置向导（""）创建或使用以下组件。

Azure 租户

- 必填： * Azure 租户和 Azure Active Directory

Azure 中的 AVD 激活是一种租户范围的设置。VDS 支持每个租户运行一个 AVD 实例。

Azure 订阅

- 必填： * Azure 订阅（请记下要使用的订阅 ID ）

所有已部署的 Azure 资源应设置在一个专用订阅中。这样可以更轻松地跟踪 AVD 的成本，并简化部署过程。注意：不支持 Azure 免费试用，因为它们没有足够的抵免额来部署功能正常的 AVD 部署。

Azure 核心配额

为要使用的 VM 系列提供足够的配额—特别是在初始平台部署中， DS v3 系列至少有 10 个核心（只能使用 2 个核心，但每个初始部署可能都有 10 个核心）。

Azure 管理员帐户

- 必填： * 一个 Azure 全局管理员帐户。

VDS 设置向导会请求 Azure 管理员向 VDS 服务主体授予委派的权限，并安装 VDS Azure Enterprise 应用程序。管理员必须分配以下 Azure 角色：

- 租户的全局管理员
- 订阅中的所有者角色

VM 映像

- 必填： * 支持多会话 Windows 10 的 Azure 映像。

Azure Marketplace 提供其基本 Windows 10 映像的最新版本，所有 Azure 订阅均可自动访问这些映像。如果您要使用其他映像或自定义映像，希望 VDS 团队提供有关创建或修改其他映像的建议，或者对 Azure 映像有一些一般性问题，请告知我们，我们可以安排对话。

Active Directory

AVD 要求用户身份属于 Azure AD ，并且 VM 加入与同一 Azure AD 实例同步的 Active Directory 域。VM 不能直接连接到 Azure AD 实例，因此需要配置域控制器并与 Azure AD 同步。

支持的选项包括：

- 在订阅中自动构建 Active Directory 实例。AD 实例通常由 VDS 在 VDS 控制虚拟机（ CMGR1 ）上为使用此选项的 Azure 虚拟桌面部署创建。在设置过程中，必须设置并配置 AD Connect 以与 Azure AD 同步。

  []

- 集成到可通过 Azure 订阅（通常通过 Azure VPN 或 Express Route ）访问的现有 Active Directory 域中，并使用 AD Connect 或第三方产品将其用户列表同步到 Azure AD 。

  []

存储层

在 AVD 中，存储策略的设计目的是， AVD 会话 VM 上不会驻留任何永久性用户 / 公司数据。用户配置文件，用户文件和文件夹以及公司 / 应用程序数据的永久性数据托管在独立数据层上托管的一个或多个数据卷上。

FSLogix 是一种配置文件容器化技术，可通过在会话初始化时将用户配置文件容器（ VHD 或 VHDX 格式）挂载到会话主机来解决许多用户配置文件问题（如数据无序增长和登录速度较慢）。

由于采用这种架构，需要具备数据存储功能。此功能必须能够处理每天早晨 / 下午当大部分用户同时登录 / 注销时所需的数据传输。即使规模适中的环境也可能需要大量数据传输。数据存储层的磁盘性能是最终用户性能的主要变量之一，必须特别注意适当调整此存储的性能大小，而不仅仅是存储容量。通常，存储层的大小应支持每个用户 5-15 IOPS 。

VDS 设置向导支持以下配置：

- 设置和配置 Azure NetApp Files （ ANF ）（建议）。_ANF 标准服务级别最多支持 150 个用户，而建议使用 150-500 个用户的环境。 ANF 高级版。对于 500 多个用户，建议使用 ANF 超高级版。 _

  []

- 设置和配置文件服务器虚拟机

  []

网络

- 必填： * 所有现有网络子网的清单，包括通过 Azure Express Route 或 VPN 对 Azure 订阅可见的任何子网。此部署需要避免子网重叠。

通过 VDS 设置向导，您可以在计划内与现有网络集成时定义所需或必须避免的网络范围。

在部署期间确定用户的 IP 范围。根据 Azure 最佳实践，仅支持专用范围内的 IP 地址。

支持的选项包括以下，但默认为 **/20** 范围：

- 192.168.0.0 到 192.168.255.255
- 172.16.0.0 到 172.31.255.255

- 10.0.0.0 到 10.255.255.255

CMGR1

VDS 的某些独特功能，例如，节省成本的工作负载计划和实时扩展功能需要在租户和订阅中具有管理功能。因此，在 VDS 设置向导自动化过程中会部署一个名为 CMGR1 的管理 VM 。除了 VDS 自动化任务之外，此 VM 还在 SQL 快速数据库，本地日志文件和一个名为 DCConfig 的高级配置实用程序中保存 VDS 配置。

根据在 **VDS** 设置向导中所做的选择，此虚拟机可用于托管其他功能，包括：

- RDS 网关（仅用于 RDS 部署）
- HTML 5 网关（仅用于 RDS 部署）
- RDS 许可证服务器（仅用于 RDS 部署）
- 域控制器（如果选择）

部署向导中的决策树

在初始部署过程中，我们会回答一系列问题，以自定义新环境的设置。下面概述了要做出的主要决策。

Azure 区域

确定要托管 AVD 虚拟机的 Azure 区域。请注意， Azure NetApp Files 和某些 VM 系列（例如支持 GPU 的 VM ）都定义了 Azure 区域支持列表，而 AVD 则在大多数地区可用。

- 此链接可用于标识 "按区域划分的 Azure 产品可用性"

Active Directory 类型

确定要使用的 Active Directory 类型：

- 现有内部 Active Directory
- 请参见 "AVD VDS 组件和权限" 文档，介绍 Azure 和本地 Active Directory 环境中所需的权限和组件
- 基于 Azure 订阅的新 Active Directory 实例
- Azure Active Directory 域服务

数据存储

确定用户配置文件，单个文件和企业共享的数据放置位置。选项包括：

- Azure NetApp Files
- Azure 文件
- 传统文件服务器（采用受管磁盘的 Azure VM ）

现有组件的 **NetApp VDS** 部署要求

使用现有 **Active Directory** 域控制器部署 **NetApp VDS**

此配置类型可扩展现有 Active Directory 域以支持 AVD 实例。在这种情况下， VDS 会将一组有限的组件部署到域中，以支持 AVD 组件的自动配置和管理任务。

此配置需要：

- 一种现有 Active Directory 域控制器，可由 Azure vNet 上的 VM 访问，通常通过 Azure VPN 或 Express Route 或已在 Azure 中创建的域控制器进行访问。
- 添加了 AVD 主机池和数据卷加入域时的 VDS 管理所需的 VDS 组件和权限。AVD VDS 组件和权限指南定义了所需的组件和权限，部署过程要求具有域权限的域用户运行将创建所需元素的脚本。
- 请注意，默认情况下， VDS 部署会为 VDS 创建的 VM 创建一个 vNet 。vNet 可以与现有 Azure 网络 VNets 建立对等关系，也可以将 CMGR1 VM 移至已预先定义了所需子网的现有 vNet 。

凭据和域准备工具

管理员必须在部署过程的某个时刻提供域管理员凭据。可以稍后创建，使用和删除临时域管理员凭据（部署过程完成后）。或者，在构建前提条件方面需要帮助的客户也可以使用域准备工具。

使用现有文件系统部署 **NetApp VDS**

VDS 创建的 Windows 共享允许从 AVD 会话 VM 访问用户配置文件，个人文件夹和企业数据。默认情况下，VDS 将部署文件服务器或 Azure NetApp 文件选项，但如果您有现有文件存储组件，则 VDS 可以在 VDS 部署完成后将共享指向该组件。

使用和现有存储组件的要求：

- 此组件必须支持 SMB v3
- 组件必须与 AVD 会话主机加入同一 Active Directory 域
- 该组件必须能够公开一个 UNC 路径以供 VDS 配置使用—所有三个共享都可以使用一个路径，或者可以为每个共享指定单独的路径。请注意， VDS 将为这些共享设置用户级别权限，因此请参阅 VDS AVD 组件和权限文档，以确保已为 VDS 自动化服务授予适当的权限。

使用现有 **Azure AD** 域服务部署 **NetApp VDS**

此配置需要通过一个过程来确定现有 Azure Active Directory 域服务实例的属性。请联系您的客户经理以申请此类部署。NetApp VDS 部署与现有 AVD 部署此配置类型假定已存在所需的 Azure vNet ， Active Directory 和 AVD 组件。VDS 部署的执行方式与 " 使用现有 AD 部署 NetApp VDS " 配置相同，但增加了以下要求：

- 需要为 Azure 中的 VDS 企业应用程序授予 AVD 租户的 RD 所有者角色
- 需要使用 VDS Web App 中的 VDS 导入功能将 AVD 主机池和 AVD 主机池 VM 导入到 VDS 中此过程会收集 AVD 主机池和会话 VM 元数据并将其存储在 VDS 中，以便这些元素可通过 VDS 进行管理
- 需要使用 CRA 工具将 AVD 用户数据导入到 VDS 用户部分中。此过程会将有关每个用户的元数据插入 VDS 控制平面，以便 VDS 可以管理其 AVD 应用程序组成员资格和会话信息

附录 **A**： **VDS** 控制面板 **URL** 和 **IP** 地址

Azure 订阅中的 VDS 组件可与 VDS 全局控制平面组件进行通信，例如 VDS Web 应用程序和 VDS API 端点。要进行访问，需要在端口 443 上安全列出以下基本 URI 地址，以便进行双向访问：

""

https://cjdownload3.file.core.windows.net/media

如果您的访问控制设备只能按 IP 地址安全列出，则应将以下 IP 地址列表列入安全列表。请注意， VDS 使用 Azure Traffic Manager 服务，因此此列表可能会随时间而变化：

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.22723.99.136.91 40.119.157 40.78.132.166 40.78.40.129.17 122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.11.21.208.132.132.172.1320.21.208.1721.138.172.138.172.138.1720.21.208.138.1720.21.138.132.138.1720.21.202.138.138.138.138.138.213.620.1.238.138.138.138.138.138.138.138.138.138.217.21.208.138.138.138.138.138.217.21.208.138.138.138.138.17

附录 B： Microsoft AVD 要求

此 Microsoft AVD 要求部分汇总了 Microsoft 的 AVD 要求。要了解完整且最新的 AVD 要求，请访问：

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Azure 虚拟桌面会话主机许可

Azure Virtual Desktop 支持以下操作系统，因此请确保根据您计划部署的桌面和应用程序为用户提供适当的许可证：

os	所需许可证
Windows 10 Enterprise 多会话或 Windows 10 Enterprise	Microsoft 365 e3， e5， a3， a5， Business Premium Windows e3， e5， a3， a5
Windows 7 Enterprise	Microsoft 365 e3， e5， a3， a5， Business Premium Windows e3， e5， a3， a5
Windows Server 2012 R2， 2016， 2019	具有软件保证的 RDS 客户端访问许可证（ CAL ）

AVD 计算机的 URL 访问

您为 Azure Virtual Desktop 创建的 Azure 虚拟机必须能够访问以下 URL：

Address	出站 TCP 端口	目的	服务标签
* .AVD.microsoft.com	443.	服务流量	Windows 虚拟桌面
mrsglobalsteus2prod.blob.core.windows.net	443.	代理和 SXS 堆栈更新	AzureCloud
* .core.windows.net	443.	代理流量	AzureCloud
* .servicebus.windows.net	443.	代理流量	AzureCloud
prod.warmpath.msftcloudes.com	443.	代理流量	AzureCloud
catalogartifact.azureedge.net	443.	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows 激活	互联网
AVDportalstorageblob.blob.core.windows.net	443.	Azure 门户支持	AzureCloud

下表列出了 Azure 虚拟机可以访问的可选 URL：

Address	出站 TCP 端口	目的	服务标签
* .microsoftonline.com	443.	对 MS Online Services 进行身份验证	无
* .events.data.microsoft.com	443.	遥测服务	无
www.msftconnecttest.com	443.	检测操作系统是否已连接到 Internet	无
* .prod.do.dsp.mp.microsoft.com	443.	Windows 更新	无
login.windows.net	443.	登录到 MS Online Services ， Office 365	无
* 。 sfx.ms	443.	OneDrive 客户端软件的更新	无
* .digicert.com	443.	证书撤消检查	无

最佳性能因素

要获得最佳性能，请确保您的网络满足以下要求：

- 从客户端网络到已部署主机池的 Azure 区域的往返（ RTT ）延迟应小于 150 毫秒。
- 当托管桌面和应用程序的 VM 连接到管理服务时，网络流量可能会超出国家 / 地区边界。
- 为了优化网络性能，我们建议会话主机的 VM 与管理服务位于同一 Azure 区域。

支持的虚拟机操作系统映像

Azure Virtual Desktop 支持以下 x64 操作系统映像：

- Windows 10 Enterprise 多会话，版本 1809 或更高版本
- Windows 10 Enterprise ，版本 1809 或更高版本
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure 虚拟桌面不支持 x86 （ 32 位）， Windows 10 Enterprise N 或 Windows 10 Enterprise KN 操作系统映像。由于扇区大小限制， Windows 7 也不支持托管 Azure 存储上托管的任何基于 VHD 或 VHDX 的配置文件解决方案。

可用的自动化和部署选项取决于您选择的操作系统和版本，如下表所示：

操作系统	**Azure** 映像库	手动部署 **VM**	与支撑模板集成	在 **Azure Marketplace** 上配置主机池
Windows 10 多会话版本 1903	是的。	是的。	是的。	是的。
Windows 10 多会话，版本 1809	是的。	是的。	否	否
Windows 10 Enterprise 版本 1903	是的。	是的。	是的。	是的。
Windows 10 Enterprise ，版本 1809	是的。	是的。	否	否
Windows 7 Enterprise	是的。	是的。	否	否
Windows Server 2019	是的。	是的。	否	否
Windows Server 2016	是的。	是的。	是的。	是的。
Windows Server 2012 R2	是的。	是的。	否	否

Google

适用于 **Google Cloud** 的 **RDS** 部署指南（ **GCP** ）

概述

本指南将提供在 Google Cloud 中使用 NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）创建远程桌面服务（ Remote Desktop Service ， RDS ）部署的分步说明。

本概念验证（ POC ）指南旨在帮助您在自己的测试 GCP 项目中快速部署和配置 RDS 。

生产部署，尤其是在现有 AD 环境中的部署非常常见，但本 POC 指南不会考虑这一过程。复杂的 POC 和生产部署应由 NetApp VDS 销售 / 服务团队启动，而不是以自助式方式执行。

本 POC 文档将带您完成整个 RDS 部署，并简要介绍 VDS 平台中部署后配置的主要方面。完成后，您将拥有一个完全部署且功能完备的 RDS 环境，其中包括会话主机，应用程序和用户。您也可以选择配置自动应用程序交付，安全组，文件共享权限， Cloud Backup 和智能成本优化。VDS 通过 GPO 部署一组最佳实践设置。此外，还提供了有关在 POC 不需要安全控制时如何选择禁用这些控制的说明，这与非受管本地设备环境类似。

部署架构

[宽度 = 75%]

RDS 基础知识

VDS 部署一个功能完备的 RDS 环境，从零开始提供所有必要的支持服务。此功能可以包括：

- RDS 网关服务器
- Web 客户端访问服务器
- 域控制器服务器
- RDS 许可服务
- ThinPrint 许可服务

- FileZilla FTPS 服务器服务

指南范围

本指南将从 GCP 和 VDS 管理员的角度引导您完成使用 NetApp VDS 技术部署 RDS 的过程。您将 GCP 项目的预配置为零，本指南可帮助您端到端设置 RDS

创建服务帐户

1. 在 GCP 中，导航到（或搜索） *IAM & Admin > Service Accounts*

   []

2. 单击 ++ create service account_

   []

3. 输入唯一的服务帐户名称，然后单击 *cre* 。记下此服务帐户的电子邮件地址，此地址将在后续步骤中使用。

   []

4. 选择服务帐户的 *owner* 角色，然后单击 _Continue"

   []

5. 下一页无需进行任何更改（ *Grant users access to this service account* （ *optional* ） _ ），请单击 *_don*

   []

6. 从 *Service accounts* 页面中，单击操作菜单并选择 *Create key*

   []

7. 选择 *P12* ，然后单击 *cre*

   []

8. 下载 .p12 文件并将其保存到您的计算机中。保持 *private key password* 不变。

   []

   []

启用 **Google** 计算 **API**

1. 在 GCP 中，导航到（或搜索） *APIs & Services > Library*

   []

2. 在 GCP API 库中，导航到（或搜索） *Compute Engine API* ，然后单击 *enable*

   []

创建新的 **VDS** 部署

1. 在 VDS 中，导航到 *deployments_*然后 单击 _+ *New Deployment*

   []

2. 输入部署的名称

   []

3. 选择 *Google Cloud Platform*

   []

基础架构平台

1. 输入 *Project ID* 和 OAuth 电子邮件地址。上传本指南前面介绍的 .p12 文件，然后为此部署选择适当的分区。单击 *Test* 以确认条目正确无误且已设置适当的权限。

   OAuth 电子邮件是本指南前面创建的服务帐户的地址。

   []

2. 确认后，单击 _Continue"

   []

—帐户

本地 **VM** 帐户

1. 提供本地管理员帐户的密码。记录此密码以供日后使用。
2. 提供 SQL SA 帐户的密码。记录此密码以供日后使用。

密码复杂度要求至少包含 8 个字符，其中包含以下 4 种字符类型中的 3 种：大写，小写，数字，特殊字符

SMTP 帐户

VDS 可以通过自定义 SMTP 设置发送电子邮件通知，也可以通过选择 *Automatic* 使用内置 SMTP 服务。

1. 输入在 VDS 发送电子邮件通知时用作 *from* 地址的电子邮件地址。*no-reply@* < 您的域 >*.com* 是一种通用格式。
2. 输入成功报告应发送到的电子邮件地址。
3. 输入应定向失败报告的电子邮件地址。

[]

3 级技术人员

3 级技术人员帐户（也称为_.tech accounts_ ）是 VDS 管理员在 VDS 环境中对 VM 执行管理任务时可以使用的域级帐户。可以在此步骤和 / 或更高版本中创建其他帐户。

1. 输入 3 级管理员帐户的用户名和密码。".tech" 将附加到您输入的用户名中，以帮助区分最终用户和技术帐户。记录这些凭据以供日后使用。

   最佳实践是为所有应具有环境域级凭据的 VDS 管理员定义命名帐户。没有此类帐户的 VDS 管理员仍可通过 VDS 中内置的 *Connect to server* 功能进行 VM 级别的管理员访问。

   []

域

Active Directory

输入所需的 AD 域名。

公有域

外部访问通过 SSL 证书进行保护。您可以使用自己的域和自管理 SSL 证书对其进行自定义。或者，如果选择 *Automatic* ，则 VDS 可以管理 SSL 证书，包括自动 90 天刷新证书。在使用自动时，每个部署都使用一个唯一的子域 *cloudworkspace .app* 。

[]

虚拟机

对于 RDS 部署，需要在平台服务器上安装所需的组件，例如域控制器， RDS 代理和 RDS 网关。在生产环境中，这些服务应在专用和冗余虚拟机上运行。对于概念验证部署，可以使用一个 VM 来托管所有这些服务。

平台 **VM** 配置

单个虚拟机

这是 POC 部署的建议选择。在单个虚拟机部署中，以下角色均托管在单个虚拟机上：

- CW Manager
- HTML5 网关
- RDS 网关
- 远程应用程序
- FTPS 服务器（可选）
- 域控制器

在此配置中，建议的 RDS 使用情形的最大用户数为 100 个用户。在此配置中，负载平衡 RS/HTML5 网关不是一个选项，这限制了冗余和未来扩展的选项。

如果此环境是为多租户设计的，则不支持单个虚拟机配置。

多个服务器

将 VDS 平台拆分为多个虚拟机时，以下角色托管在专用 VM 上：

- 远程桌面网关

  VDS 设置可用于部署和配置一个或两个 RDS 网关。这些网关会将 RDS 用户会话从开放式 Internet 中继到部署中的会话主机 VM 。RDS 网关具有一项重要功能，可保护 RDS 免受来自开放式互联网的直接攻击，并对环境中 / 之外的所有 RDS 流量进行加密。选择两个远程桌面网关后， VDS 安装程序会部署 2 个 VM 并对其进行配置，以便对传入的 RDS 用户会话进行负载平衡。

- HTML5 网关

  VDS 设置可用于部署和配置一个或两个 HTML5 网关。这些网关托管 VDS 和基于 Web 的 VDS 客户端（ H5 门户）中的 *Connect to Server* 功能使用的 HTML5 服务。选择两个 HTML5 门户后， VDS 安装程序会部署 2 个 VM 并对其进行配置，以便对传入的 HTML5 用户会话进行负载平衡。

  

  如果使用多个服务器选项（即使用户仅通过已安装的 VDS 客户端进行连接），强烈建议至少使用一个 HTML5 网关从 VDS 启用 *Connect to Server* 功能。

- 网关可扩展性注意事项

  对于 RDS 使用情形，可以使用其他网关 VM 横向扩展环境的最大大小，每个 RDS 或 HTML5 网关大约支持 500 个用户。稍后，只需极少的 NetApp 专业服务协助，即可添加其他网关

如果此环境是为多租户设计的，则需要选择 *Multiple servers* 。

服务角色

- Cwmgr1.

  此 VM 是 NetApp VDS 管理 VM 。它运行 SQL Express 数据库，帮助程序实用程序和其他管理服务。在 *single server* 部署中，此 VM 也可以托管其他服务，但在 *multiple server* 配置中，这些服务会移动到不同的 VM 。

- CWPortal1 （ 2 ）

  第一个 HTML5 网关名为 *cbportal1* ，第二个网关名为 *cbport2* 。可以在部署时创建一个或两个。部署后可以添加更多服务器以增加容量（每个服务器~500 个连接）。

- CWRDSGateway1 （ 2 ）

  第一个 RDS 网关名为 *CWRDSGateway1* ，第二个名为 *CWRDSGateway2* 。可以在部署时创建一个或两个。部署后可以添加更多服务器以增加容量（每个服务器~500 个连接）。

- 远程应用程序

  App Service 是一个专用于托管 RemotApp 应用程序的集合，但使用 RDS 网关及其 RDWeb 角色来路由最终用户会话请求并托管 RDWeb 应用程序订阅列表。没有为此服务角色部署 VM 专用 VM 。

- 域控制器

在部署时，可以自动构建和配置一个或两个域控制器，以便与 VDS 配合使用。

[]

操作系统

选择要为平台服务器部署的所需服务器操作系统。

时区

选择所需时区。此时将配置平台服务器，日志文件将反映此时区。无论此设置如何，最终用户会话仍将反映其自己的时区。

其他服务

FTP

VDS 可以选择安装和配置 FileZilla 来运行 FTPS 服务器，以便将数据移入和移出环境。此技术是一种较旧的技术，建议使用更现代的数据传输方法（如 Google Drive ）。

[]

网络

最佳做法是，根据虚拟机的用途将其隔离到不同的子网。

定义网络范围并添加 /20 范围。

VDS 设置会检测到一个范围，并建议一个范围，该范围应证明是成功的。根据最佳实践，子网 IP 地址必须属于专用 IP 地址范围。

这些范围包括：

- 192.168.0.0 到 192.168.255.255
- 172.16.0.0 到 172.31.255.255
- 10.0.0.0 到 10.255.255.255

如果需要，请查看并调整，然后单击验证以确定以下每项的子网：

- 租户：这是会话主机服务器和数据库服务器所在的范围
- 服务：这是 Cloud Volumes Service 等 PaaS 服务所在的范围
- 平台：这是平台服务器所在的范围
- 目录：这是 AD 服务器所在的范围

[]

许可

SPLA 编号

输入您的 SPLA 编号，以便 VDS 可以配置 RDS 许可服务，以便于进行 SPLA RDS CAL 报告。可以为 POC 部署输入一个临时数字（例如 12345 ），但在试用期（~120 天）后， RDS 会话将停止连接。

SPLA 产品

输入通过 SPLA 获得许可的任何 Office 产品的 MAK 许可证代码，以便在 VDS 报告中简化 SPLA 报告。

ThinPrint

选择安装随附的 ThinPrint 许可服务器和许可证，以简化最终用户打印机重定向。

[]

审核和配置

完成所有步骤后，请查看所做的选择，然后验证并配置环境。[]

后续步骤

现在，部署自动化过程将使用您在整个部署向导中选择的选项部署一个新的 RDS 环境。

部署完成后，您将收到多封电子邮件。完成后，您将有一个环境为您的第一个工作空间做好准备。工作空间将包含支持最终用户所需的会话主机和数据服务器。一旦部署自动化在 1-2 小时内完成，请返回本指南以执行后续步骤。

创建新的配置集合

配置集合是 VDS 中的一项功能，可用于创建，自定义和 SysPrep VM 映像。进入工作场所部署后，我们需要一个要部署的映像，以下步骤将指导您创建 VM 映像。

按照以下步骤创建基本映像以进行部署：

1. 导航到 *deployments> Provisioning Collections* ，然后单击 *Add*

   []

2. 输入名称和问题描述。选择 *Type* ： *Shared* 。

   > 您可以选择共享或 VDI 。共享将支持一个会话服务器以及一个业务服务器（可选），用于数据库等应用程序。VDI 是一个虚拟机映像，专用于单个用户。

3. 单击 *Add* 以定义要构建的服务器映像的类型。

   []

4. 选择 TSData 作为 *server role* ，相应的 VM 映像（此处为 Server 2016 ）以及所需的存储类型。单击 *Add Server*

   []

5. 也可以选择要安装在此映像上的应用程序。

a. 可用应用程序列表将从应用程序库中填充，您可以单击右上角 *Settings* > *App Catalog* 页面下的 admin name 菜单来访问该应用程序。

[]

6. 单击 *Add Collection* ，然后等待虚拟机构建完成。VDS 将构建一个可以访问和自定义的 VM 。
7. 虚拟机构建完成后，请连接到服务器并进行所需的更改。

a. 状态显示 _Collection Validation 后，单击收集名称。

[]

b. 然后，单击 *server template name*

[]

c. 最后，单击 *Connect to Server* 按钮以进行连接，并使用本地管理员凭据自动登录到虚拟机。

[]

[]

8. 完成所有自定义设置后，单击 *Validate Collection* ，以便 VDS 可以对映像进行系统准备并最终确定。完成后， VM 将被删除，并且映像可通过 VDS 部署向导进行部署。

[]5.

创建新工作空间

工作空间是指支持一组用户的会话主机和数据服务器的集合。一个部署可以包含一个工作空间（单租户）或多个工作空间（多租户）。

工作空间用于定义特定组的 RDS 服务器集合。在此示例中，我们将部署一个集合来演示虚拟桌面功能。但是，可以将此模型扩展到多个工作空间 /RDS 集合，以支持同一 Active Directory 域空间中的不同组和不同位置。此外，管理员还可以限制工作空间 / 集合之间的访问权限，以支持需要对应用程序和数据进行有限访问的使用情形。

客户端和设置

1. 在 NetApp VDS 中，导航到 *Workspaces* ，然后单击 _+ New Workspace _

[]

2. 单击 *Add* 以创建新客户端。客户端详细信息通常表示公司信息或特定位置 / 部门的信息。

[]

a. 输入公司详细信息并选择要将此工作空间部署到的部署。

b. * 数据驱动器： * 定义要用于公司共享映射驱动器的驱动器号。

c. * 用户主驱动器： * 定义要用于个人映射驱动器的驱动器盘符。

d. * 其他设置 *

可以在部署时和 / 或在部署后选择以下设置。

i. _Enable Remote App： _ 远程应用程序将应用程序呈现为流式应用程序，而不是（或除此之外）呈现完整的远程桌面会话。

ii. _Enable App Blocker： _ VDS 包含应用程序部署和授权功能，默认情况下，系统将向最终用户显示 / 隐藏应用程序。启用应用程序锁将通过 GPO 安全列表强制应用程序访问。

iii. _ 启用工作空间用户数据存储： _ 确定最终用户是否需要在其虚拟桌面中拥有数据存储访问权限。对于 RDS 部署，应始终选中此设置，以便为用户配置文件启用数据访问。

iv. _Disable Printer Access： _ VDS 可能会阻止对本地打印机的访问。

v. _permit Access to Task Manager： _ VDS 可以在 Windows 中启用 / 禁用最终用户对任务管理器的访问。

vi. _Require complex User Password： _ Require complex passwords 用于启用原生 Windows Server 复杂密码规则。它还会禁用锁定用户帐户的延迟自动解锁。因此，启用后，如果最终用户在多次密码尝试失败的情况下锁定其帐户，则需要管理员干预。

vii. _ 为所有用户启用 MFA： _ VDS 包括一个免费电子邮件 /SMS MFA 服务，可用于保护最终用户和 / 或 VDS 管理员帐户访问的安全。要启用此功能，此工作空间中的所有最终用户都需要通过 MFA 进行身份验证才能访问其桌面和 / 或应用程序。

选择应用程序

选择本指南前面创建的 Windows 操作系统版本和配置集合。

此时可以添加其他应用程序，但对于此 POC ，我们将在部署后处理应用程序授权问题。

[]

添加用户

可以通过选择现有 AD 安全组或单个用户来添加用户。在本 POC 指南中，我们将添加部署后的用户。

[]

审核和配置

在最后一页上，查看所选选项，然后单击 *provision* 开始自动构建 RDS 资源。

[]

在部署过程中，系统会创建日志，并可在 "Deployment details" 页面底部附近的 *Task History* 下访问这些日志。可通过导航到 _VDS > 部署 > 部署名称 _ 来访问

后续步骤

现在，工作场所自动化流程将使用您在整个部署向导中选择的选项部署新的 RDS 资源。

完成后，您将按照几个常见工作流自定义典型的 RDS 部署。

- "添加用户"
- "最终用户访问"

- "应用程序授权"
- "成本优化"

Google Compute Platform （ GCP ）和 VDS 前提条件

GCP 和 VDS 要求和说明

本文档介绍使用 NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）部署远程桌面服务（ Remote Desktop Services ， RDS ）所需的要素。" 快速检查清单 " 简要列出了确保高效部署所需的组件和部署前步骤。本指南的其余部分将根据所做的配置选择详细介绍每个元素。

[宽度 = 75%]

快速检查清单

GCP 要求

- GCP 租户
- GCP 项目
- 分配了所有者角色的服务帐户

部署前信息

- 确定用户总数
- 确定 GCP 区域和分区
- 确定 Active Directory 类型
- 确定存储类型
- 确定会话主机 VM 映像或要求
- 评估现有的 GCP 和内部网络配置

VDS 部署详细要求

最终用户连接要求

以下远程桌面客户端支持 **GCP** 中的 **RDS**：

- "适用于 Windows 的 NetApp VDS 客户端"
  - NetApp VDS Client for Windows 出站 URL 安全列表要求
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app
  - 增强功能：
    - VDS 按需唤醒

        - ThinPrint 客户端和鼠标
        - 自助式密码重置
        - 自动服务器和网关地址协商
        - 全面的桌面和流式应用程序支持
        - 可用的自定义品牌
        - 用于自动部署和配置的安装程序交换机
        - 内置故障排除工具
- "NetApp VDS Web 客户端"
- "Microsoft RD 客户端"
    - Windows
    - macOS
    - ISO
    - Android
- 第三方软件和 / 或瘦客户端
    - 要求：支持 RD 网关配置

存储层

在由 VDS 部署的 RDS 中，存储策略的设计目的是，在 AVD 会话 VM 上不会驻留任何永久性用户 / 公司数据。用户配置文件，用户文件和文件夹以及公司 / 应用程序数据的永久性数据托管在独立数据层上托管的一个或多个数据卷上。

FSLogix 是一种配置文件容器化技术，可通过在会话初始化时将用户配置文件容器（ VHD 或 VHDX 格式）挂载到会话主机来解决许多用户配置文件问题（如数据无序增长和登录速度较慢）。

由于采用这种架构，需要具备数据存储功能。此功能必须能够处理每天早晨 / 下午当大部分用户同时登录 / 注销时所需的数据传输。即使规模适中的环境也可能需要大量数据传输。数据存储层的磁盘性能是最终用户性能的主要变量之一，必须特别注意适当调整此存储的性能大小，而不仅仅是存储容量。通常，存储层的大小应支持每个用户 5-15 IOPS 。

网络

- 必需： * 所有现有网络子网的清单，包括通过 VPN 对 GCP 项目可见的任何子网。此部署需要避免子网重叠。

通过 VDS 设置向导，您可以在计划内与现有网络集成时定义所需或必须避免的网络范围。

在部署期间确定用户的 IP 范围。根据最佳实践，仅支持专用范围内的 IP 地址。

支持的选项包括以下，但默认为 **/20** 范围：

- 192.168.0.0 到 192.168.255.255
- 172.16.0.0 到 172.31.255.255
- 10.0.0.0 到 10.255.255.255

CMGR1

VDS 的某些独特功能，例如，节省成本的工作负载计划和实时扩展功能需要在组织和项目中具有管理功能。因此，在 VDS 设置向导自动化过程中会部署一个名为 CMGR1 的管理 VM 。除了 VDS 自动化任务之外，此 VM 还在 SQL 快速数据库，本地日志文件和一个名为 DCConfig 的高级配置实用程序中保存 VDS 配置。

根据在 **VDS** 设置向导中所做的选择，此虚拟机可用于托管其他功能，包括：

- RDS 网关
- 一个 HTML 5 网关
- RDS 许可证服务器
- 域控制器

部署向导中的决策树

在初始部署过程中，我们会回答一系列问题，以自定义新环境的设置。下面概述了要做出的主要决策。

GCP 区域

确定要托管 VDS 虚拟机的 GCP 区域。请注意，应根据与最终用户和可用服务之间的距离选择区域。

数据存储

确定用户配置文件，单个文件和企业共享的数据放置位置。选项包括：

- 适用于 GCP 的 Cloud Volumes Service
- 传统文件服务器

现有组件的 NetApp VDS 部署要求

使用现有 Active Directory 域控制器部署 NetApp VDS

此配置类型可扩展现有 Active Directory 域以支持 RDS 实例。在这种情况下， VDS 会将一组有限的组件部署到域中，以支持 RDS 组件的自动配置和管理任务。

此配置需要：

- 一种现有 Active Directory 域控制器，可由 GCP VPC 网络上的 VM 访问，通常通过 VPN 或在 GCP 中创建的域控制器访问。
- 添加了加入域时对 RDS 主机和数据卷进行 VDS 管理所需的 VDS 组件和权限。部署过程需要具有域权限的域用户运行脚本，以创建所需的元素。
- 请注意，默认情况下， VDS 部署会为 VDS 创建的 VM 创建 VPC 网络。VPC 网络可以与现有 VPC 网络建立对等关系，也可以将 CMGR1 VM 移至已预先定义了所需子网的现有 VPC 网络。

凭据和域准备工具

管理员必须在部署过程的某个时刻提供域管理员凭据。可以稍后创建，使用和删除临时域管理员凭据（部署过程完成后）。或者，在构建前提条件方面需要帮助的客户也可以使用域准备工具。

使用现有文件系统部署 **NetApp VDS**

VDS 创建的 Windows 共享允许从 RDS 会话主机访问用户配置文件，个人文件夹和企业数据。默认情况下，VDS 将部署文件服务器，但如果您有现有文件存储组件，则 VDS 可以在 VDS 部署完成后将共享指向该组件。

使用和现有存储组件的要求：

- 此组件必须支持 SMB v3
- 此组件必须与 RDS 会话主机加入同一 Active Directory 域
- 该组件必须能够公开一个 UNC 路径以供 VDS 配置使用—所有三个共享都可以使用一个路径，或者可以为每个共享指定单独的路径。请注意， VDS 将为这些共享设置用户级别权限，请确保已为 VDS 自动化服务授予相应的权限。

附录 **A**： **VDS** 控制面板 **URL** 和 **IP** 地址

GCP 项目中的 VDS 组件与 Azure 中托管的 VDS 全局控制平面组件进行通信，包括 VDS Web 应用程序和 VDS API 端点。要进行访问，需要在端口 443 上安全列出以下基本 URI 地址，以便进行双向访问：

""

如果您的访问控制设备只能按 IP 地址安全列出，则应将以下 IP 地址列表列入安全列表。请注意， VDS 使用具有冗余公有 IP 地址的负载平衡器，因此此列表可能会随时间而变化：

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.22723.99.136.91 40.119.157 40.78.132.166 40.78.40.129.17 122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.11.21.208.132.132.172.1320.21.208.1721.138.172.138.172.138.1720.21.208.138.1720.21.138.132.138.1720.21.202.138.138.138.138.138.213.620.1.238.138.138.138.138.138.138.138.138.138.217.21.208.138.138.138.138.138.217.21.208.138.138.138.138.17

最佳性能因素

要获得最佳性能，请确保您的网络满足以下要求：

- 从客户端网络到已部署会话主机的 GCP 区域的往返（ RTT ）延迟应小于 150 毫秒。
- 当托管桌面和应用程序的 VM 连接到管理服务时，网络流量可能会超出国家 / 地区边界。
- 为了优化网络性能，我们建议会话主机的 VM 与管理服务位于同一区域。

支持的虚拟机操作系统映像

由 VDS 部署的 RDS 会话主机支持以下 x64 操作系统映像：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2