用户管理
Virtual Desktop Service

NetApp
April 12, 2022

目录

用户管理

管理用户帐户

创建新用户

管理员可以通过单击 " 工作空间 ">" 用户和组 ">" 添加 / 导入 " 来添加用户

用户可以单独添加，也可以批量导入。

[宽度 = 25%]

在此阶段提供准确的电子邮件和移动电话号码，可大大改进稍后启用 MFA 的过程。

创建用户后，您可以单击其名称以查看其创建时间，连接状态（无论其当前是否已登录）以及特定设置等详细信息。

为现有 **AD** 用户激活虚拟桌面

如果用户已在 AD 中，您只需单击用户名称旁边的工具，然后启用其桌面即可激活用户的虚拟桌面。[宽度 = 50%]

仅限 Azure AD 域服务：要使登录正常工作，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可能需要长达 20 分钟，因此 Azure AD 中的密码更改通常需要 20 分钟才能反映在 AADDS 中，进而反映在 VDS 环境中。

删除用户帐户

编辑用户信息

在用户详细信息页面上，可以更改用户详细信息，例如用户名和联系人详细信息。电子邮件和电话值用于自助密码重置（ SSPR ）过程。

[]

编辑用户安全设置

- VDI User Enabled —一种 RDS 设置，启用后，此设置将构建一个专用的 VM 会话主机，并将此用户分配为唯一连接到该主机的用户。激活此复选框时，系统会提示 CCMS 管理员选择虚拟机映像，大小和存储类型。
  - AVD VDI 用户应在 AVD 页面上作为 VDI 主机池进行管理。
- Account Expiration Enabled —允许 CMS 管理员在最终用户帐户上设置到期日期。
- 下次登录时强制重置密码—提示最终用户在下次登录时更改密码。
- 多因素身份验证已启用—为最终用户启用 MFA ，并提示他们在下次登录时设置 MFA 。
- 已启用移动驱动器—当前 RDS 或 AVD 部署中不使用的一项原有功能。

- 已启用本地驱动器访问—允许最终用户从云环境访问其本地设备存储，包括复制 / 粘贴， USB 大容量存储和系统驱动器。
- 已启用按需唤醒—对于通过适用于 Windows 的顺时针客户端进行连接的 RDS 用户，启用此功能后，最终用户将有权在工作负载计划定义的正常工作时间以外进行连接时使用其环境。

已锁定帐户

默认情况下，五次失败的登录尝试将锁定用户帐户。除非启用了 _Enable Password 复杂性 _ ，否则用户帐户将在 30 分钟后解锁。启用密码复杂度后，帐户不会自动解锁。无论哪种情况， VDS 管理员都可以从 VDS 中的 " 用户 / 组 " 页面手动解锁用户帐户。

重置用户密码

重置用户密码。

注意：在重置 Azure AD 用户密码（或解除帐户锁定）时，重置可能会延迟长达 20 分钟，因为重置会通过 Azure AD 传播。

管理员访问

启用此选项后，最终用户将对其租户的管理门户具有有限的访问权限。常见用途包括为现场员工提供重置对等方密码的访问权限，分配应用程序或允许手动服务器唤醒访问。此处还设置了控制台哪些区域可以显示的权限。

注销用户

VDS 管理员可以从 VDS 中的 " 用户 / 组 " 页面注销已登录的用户。

应用程序

显示在此工作空间中部署的应用程序。此复选框会将应用程序配置为此特定用户。可在此处找到完整的应用程序管理文档。也可以从应用程序界面或安全组授予对应用程序的访问权限。

查看 / 终止用户进程

显示当前正在该用户会话中运行的进程。也可以从此界面结束进程。

管理数据权限

最终用户视角

虚拟桌面最终用户可以访问多个映射的驱动器。这些驱动器包括一个 FTPS 可访问的团队共享，一个公司文件共享及其主驱动器（用于其文档，桌面等）… 。所有这些映射的驱动器都会引用回存储服务（如 Azure NetApp Files ）或文件服务器 VM 上的中央存储层。

根据用户可能采用的配置，他们可能不会公开 H ： 或 F ： 驱动器，因此可能只会看到其桌面，文档等… 文件夹。此外， VDS 管理员有时会在部署时设置不同的驱动器号。[]

[]

管理权限

通过 VDS ，管理员可以编辑安全组和文件夹权限，所有这些都可从 VDS 门户中完成。

安全组

可以通过单击 " 组 " 部分下的 " 工作空间 ">" 租户名称 ">" 用户和组 ">" 来管理安全组

在本节中，您可以：

1. 创建新的安全组
2. 将用户添加 / 删除到组
3. 将应用程序分配给组
4. 启用 / 禁用对组的本地驱动器访问

[]

文件夹权限

可以通过单击 " 工作空间 ">" 租户名称 ">" 管理 " （在 " 文件夹 " 部分中）来管理文件夹权限。

在本节中，您可以：

1. 添加 / 删除文件夹
2. 为用户或组分配权限
3. 将权限自定义为只读，完全控制和无

[]

应用程序授权

概述

VDS 内置了强大的应用程序自动化和授权功能。通过此功能，用户可以在连接到同一会话主机时访问不同的应用程序。这是通过一些自定义 GPO 隐藏快捷方式以及自动化有选择地在用户桌面上放置快捷方式来实现的。

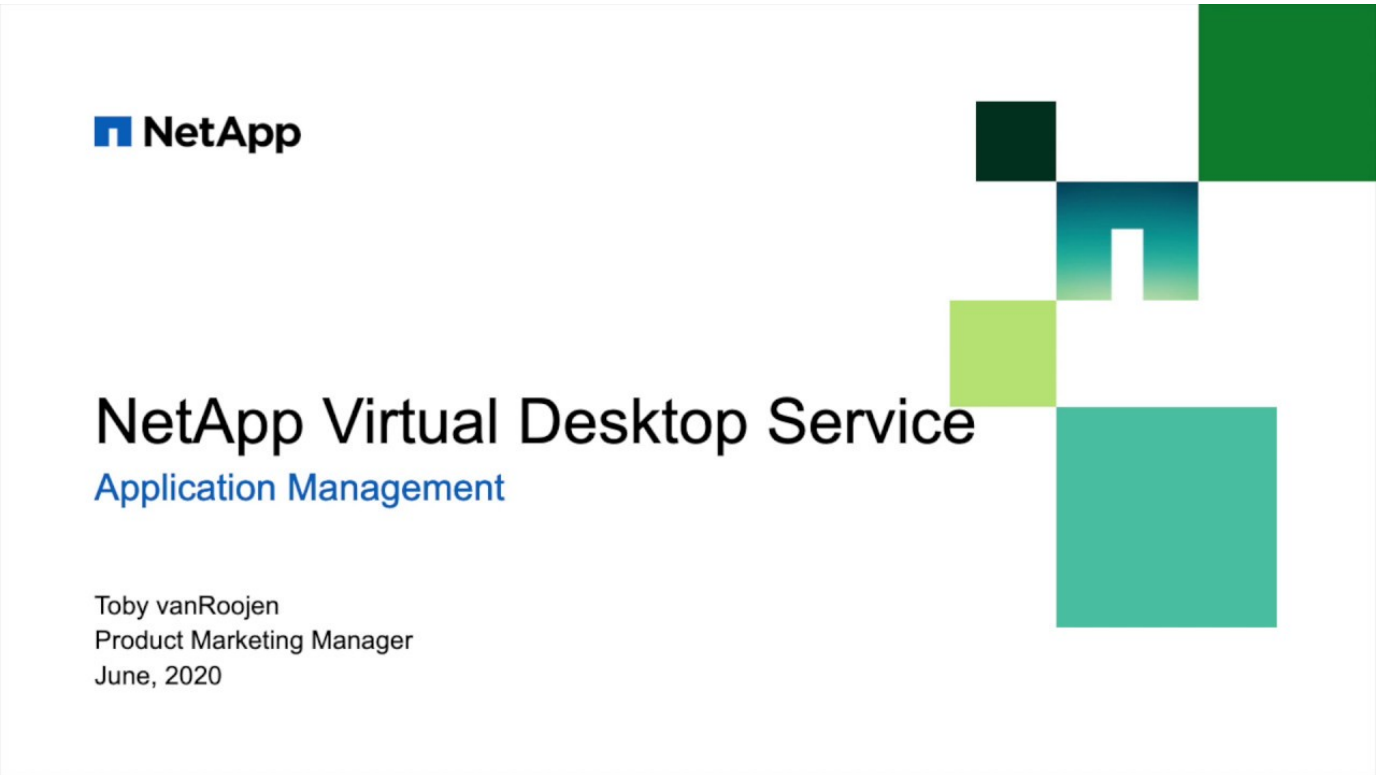
> 此工作流仅适用于适用场景 RDS 部署。有关 AVD 应用程序授权文档，请参见 "适用于 AVD 的应用程序授权工作流"

可以直接将应用程序分配给用户，也可以通过 VDS 中管理的安全组分配应用程序。

总体而言，应用程序配置过程遵循以下步骤。

1. 将应用程序添加到应用程序目录
2. 将应用程序添加到工作空间
3. 在所有会话主机上安装应用程序
4. 选择快捷方式路径
5. 将应用程序分配给用户和 / 或组

步骤 3 和 4 可以通过脚本化事件完全自动化，如下图所示



视频演练

将应用程序添加到应用程序目录

VDS 应用程序授权从应用程序目录开始，此列表列出了可部署到最终用户环境的所有应用程序。

要将应用程序添加到目录中，请按照以下步骤进行操作

1. 登录到 VDS https://manage.cloudworkspace.com 使用主管理员凭据。
2. 在右上角，单击用户名旁边的箭头图标，然后选择设置。
3. 单击应用程序目录选项卡。
4. 单击应用程序目录标题栏中的添加应用程序选项。
5. 要添加一组应用程序，请选择导入应用程序选项。
    a. 此时将显示一个对话框，其中提供了一个要下载的 Excel 模板，用于为应用程序列表创建正确的格式。
    b. 对于此评估， NetApp VDS 已创建了一个用于导入的应用程序列表示例，可在此处找到。
    c. 单击上传区域并选择应用程序模板文件，然后单击导入按钮。
6. 要添加单个应用程序，请选择添加应用程序按钮，此时将显示一个对话框。
    a. 输入应用程序的名称。
    b. 外部 ID 可用于输入内部跟踪标识符，例如产品 SKU 或计费跟踪代码（可选）。
    c. 如果要以订阅产品的形式报告应用程序，请选中订阅框（可选）。
    d. 如果产品未按版本（例如 Chrome ）安装，请选中不需要版本复选框。这样可以在安装 " 持续更新 " 产品时不跟踪其版本。

e. 相反，如果某个产品支持多个命名版本（例如： QuickBooks ），则需要选中此框，以便可以安装多个版本，并在可授权给和最终用户的应用程序列表中为每个可用版本设置 VDS 专用版本。

f. 如果不希望 VDS 为此产品配置桌面图标，请选中 " 无用户桌面图标 " 。这用于 SQL Server 等 " 后端 " 产品，因为最终用户没有可访问的应用程序。

g. " 应用程序必须关联 " 强制要求安装关联的应用程序。例如，客户端服务器应用程序可能还需要安装 SQL Server 或 MySQL 。

h. 选中需要许可证复选框表示 VDS 应先请求为该应用程序的安装上传许可证文件，然后再将该应用程序状态设置为活动状态。此步骤在 VDS 的 " 应用程序 " 详细信息页面上执行。

i. 对所有人可见—应用程序授权可以限制为多通道层次结构中的特定子合作伙伴。出于评估目的，请单击复选框，以便所有用户都可以在其可用应用程序列表中看到它。

将应用程序添加到工作空间

要开始部署过程，您需要将此应用程序添加到工作空间中。

要执行此操作，请执行以下步骤：

1. 单击 Workspaces
2. 向下滚动到应用程序
3. 单击添加。
4. 选中应用程序复选框，输入所需信息，单击添加应用程序，然后单击添加应用程序。

手动安装应用程序

将应用程序添加到工作空间后，您需要在所有会话主机上安装该应用程序。这可以手动完成，也可以自动完成。

要在会话主机上手动安装应用程序，请执行以下步骤

1. 导航到服务板。
2. 单击服务板任务。
3. 单击服务器名称以作为本地管理员进行连接。
4. 安装应用程序，确认此应用程序的快捷方式位于 " 开始 " 菜单路径中。
   a. 对于 Server 2016 和 Windows 10： C： \ProgramData\Microsoft\Windows\Start Menu" \Programs.
5. 返回到服务板任务，单击浏览，然后选择快捷方式或包含快捷方式的文件夹。
6. 无论您选择哪个选项，分配应用程序时最终用户桌面上都会显示的内容。
7. 当一个应用程序实际上是多个应用程序时，文件夹非常好。例如，可以更轻松地将 Microsoft Office 部署为文件夹，并将每个应用程序作为文件夹中的快捷方式。
8. 单击 Complete Installation 。
9. 如果需要，打开已创建图标添加服务板任务并确认已添加此图标。

将应用程序分配给用户

应用程序授权由 VDS 处理，应用程序可通过三种方式分配给用户

将应用程序分配给用户

1. 导航到用户详细信息页面。
2. 导航到应用程序部分。
3. 选中此用户所需的所有应用程序旁边的框。

将用户分配给应用程序

1. 导航到 " 工作空间详细信息 " 页面上的 " 应用程序 " 部分。
2. 单击应用程序的名称。
3. 选中应用程序用户旁边的框。

将应用程序和用户分配给用户组

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。

重置用户密码

重置用户密码步骤

1. 导航到 VDS 中的已用详细信息页面

   []

2. 找到 Password 部分，输入新的 PW 两次，然后单击

   []

   []

生效时间

- 对于在环境中的 VM 上运行 " 内部 " AD 的环境，密码更改应立即生效。
- 对于运行 Azure AD 域服务（ AADDS ）的环境，密码更改应大约需要 20 分钟才能生效。
- 可以在部署详细信息页面上确定 AD 类型：

  []

自助服务密码重置（ **SSRP** ）

在登录到 v5.2 （或更高版本）虚拟桌面部署时， NetApp VDS Windows 客户端和 NetApp VDS Web 客户端将提示输入错误密码的用户。如果用户已锁定其帐户，则此过程也会解锁用户的帐户。

注意：用户必须已输入手机号码或电子邮件地址，此过程才能正常运行。

以下项支持 SSPR：

- NetApp VDS 窗口客户端
- NetApp VDS Web 客户端

在这组说明中，您将介绍使用 SSPR 的过程，这是一种简单的方法，可使用户重置密码并解除帐户锁定。

NetApp VDS Windows 客户端

1. 以最终用户身份单击忘记密码链接以继续。

   []

2. 选择是通过手机还是电子邮件接收您的代码。

   []

3. 如果最终用户仅提供了其中一种联系方法，则只会显示这种方法。

   []

4. 完成此步骤后，系统将向用户显示一个代码字段，用户应在其中输入通过移动设备或收件箱收到的数值（具体取决于所选的数字）。输入该代码并输入新密码，然后单击重置继续。

   []

5. 用户将看到一条提示，告知其密码重置已成功完成—单击 " 完成 " 继续完成登录过程。

   > 如果您的部署使用的是 Azure Active Directory 域服务，则会有一个 Microsoft 定义的密码同步期限—每 20 分钟一次。同样，此操作由 Microsoft 控制，不能更改。考虑到这一点， VDS 显示用户应等待长达 20 分钟，以使其新密码生效。如果您的部署未使用 Azure Active Directory 域服务，用户将能够在几秒钟内重新登录。

   []

HTML5 门户

1. 如果用户在尝试通过 HTML5 登录时未能输入正确的密码，则现在将为他们提供一个重置密码的选项：

   []

2. 单击此选项以重置其密码后，系统将为其显示重置选项：

   []

3. ‘Request ' 按钮将生成的代码发送到选定选项（此处为用户的电子邮件）。此代码的有效期为 15 分钟。

   []

4. 现在，密码已重置！请务必记住， Windows Active Directory 通常需要一段时间才能传播更改内容，因此，如果新密码不能立即生效，只需等待几分钟，然后重试。这对于驻留在 Azure Active Directory 域服务部署中的用户尤其重要，在该部署中，密码重置可能需要长达 20 分钟才能传播。

   []

为用户启用自助服务密码重置（ **SSPR** ）

要使用自助服务密码重置（ SSPR ），管理员必须先输入最终用户的移动电话号码和 / 或电子邮件帐户。要为虚拟桌面用户输入移动电话号码和电子邮件地址，请使用以下两种方式，详细信息如下。

在这组说明中，您将介绍配置 SSPR 的过程，这是最终用户重置密码的一种简单方法。

通过 **VDS** 批量导入用户

首先导航到 " 工作空间 " 模块，然后导航到 " 用户和组 " ，然后单击 " 添加 / 导入 " 。

您可以在逐个创建用户时为其输入以下值：[]

或者，在批量导入用户下载并上传预先配置的 Excel XLSX 文件并填写此内容时，也可以包括这些内容：[]

通过 **VDS API** 提供数据

NetApp VDS API —具体来说就是此调用 https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser –提供更新此信息的功能。

正在更新现有用户电话

在 VDS 中的 User Detail Overview 页面上更新用户的电话号码。

[]

使用其他控制台

注意：您目前无法通过 Azure 控制台，合作伙伴中心或 Office 365 管理控制台为用户提供电话号码。

自定义 **SSPR** 发送地址

可以将 NetApp VDS 配置为发送自定义地址的确认电子邮件 *from* 。这是为我们的服务提供商合作伙伴提供的一项服务，这些合作伙伴希望其最终用户接收重置密码电子邮件，以便从其自己的自定义电子邮件域发送。

此自定义需要执行一些额外步骤来验证发送地址。要开始此过程，请与 VDS 支持部门一起创建一个支持案例，请求自定义 " 自助服务密码重置源地址 " 。请定义以下内容：

- 您的合作伙伴代码（可通过单击右上角下箭头菜单下的 _settings_ 来 找到此代码。请参见下面的屏幕截图）

  []

- 所需的 " 发件人 " 地址（必须有效）
- 此设置应应用于哪些客户端（或全部应用）

要创建支持案例，请发送电子邮件至： support@spotpc.netapp.com

收到此消息后， VDS 支持将使用我们的 SMTP 服务验证此地址并激活此设置。理想情况下，您可以更新源地址域上的公有 DNS 记录，以最大程度地提高电子邮件传送能力。

密码复杂度

可以配置 VDS 以强制实施密码复杂性。此设置位于云工作空间设置部分的工作空间详细信息页面上。

[]

[]

密码复杂度： **off**

策略	准则
最小密码长度	8 个字符
最长密码期限	110 天
最短密码期限	0 天
强制执行密码历史记录	记住 24 个密码
密码锁定	如果输入的条目不正确，则会自动锁定
锁定持续时间	30 分钟

密码复杂度：启用

策略	准则
最小密码长度	8 个字符不包含用户的帐户名称或用户全名中超过两个连续字符的部分字符包含以下四个类别中的三个字符： 英文大写字符（ A 到 Z ）英文小写字符（ a 到 z ）基本 10 位数（ 0 到 9 ）非字母字符（例如！， $ ， # ， % ）在更改或创建密码时会强制执行复杂度要求。
最长密码期限	110 天
最短密码期限	0 天
强制执行密码历史记录	记住 24 个密码
密码锁定	如果输入 5 个错误，则会自动锁定
锁定持续时间	保持锁定状态，直到管理员解锁为止

多因素身份验证（ **MFA** ）

概述

NetApp 虚拟桌面服务（ Virtual Desktop Service ， VDS ）包括基于 SMS/Email 的 MFA 服务，无需额外付费。此服务独立于任何其他服务（例如 Azure 条件访问），可用于确保管理员登录到 VDS 以及用户登录到虚拟桌面的安全。

MFA 基础知识

- VDS MFA 可以分配给管理员用户，单个最终用户或应用于所有最终用户
- VDS MFA 可以发送 SMS 或电子邮件通知

- VDS MFA 具有自助式初始设置和重置功能

指南范围

本指南将指导您完成 MFA 的设置以及最终用户体验图

本指南涵盖以下主题：

1. 为单个用户启用 MFA
2. 所有用户都需要 MFA
3. 为单个管理员启用 MFA
4. 最终用户初始设置

为单个用户启用 **MFA**

可以通过单击 _Multi-Factor Auth Enabled" 在用户详细信息页面上为单个用户启用 MFA

工作空间 > 工作空间名称 > 用户和组 > 用户名 > 多因素身份验证已启用 > 更新

此外，还可以将 MFA 分配给所有用户，如果设置为不变，则会选中此复选框，并在复选框标签上附加 _ （通过客户端设置） _ 。

所有用户都需要 **MFA**

可以通过单击为所有用户启用 _ 的 _MFA 在工作空间详细信息页面上的所有用户之间启用和强制实施 MFA

工作空间 > 工作空间名称 > 已启用所有用户的 MFA > 更新

为单个管理员启用 **MFA**

此外，访问 VDS 门户的管理员帐户还可以使用 MFA 。可以在管理员详细信息页面上为每个管理员启用此功能。管理员 > 管理员名称 > 需要多因素身份验证 > 更新

初始设置

启用 MFA 后，在首次登录时，系统将提示用户或管理员输入电子邮件地址或移动电话号码。他们将收到一个确认代码，用于输入并确认成功注册。