架构

Virtual Desktop Service

NetApp
March 15, 2022

目录

架构

正在重定向存储平台

概述

虚拟桌面服务部署技术支持多种存储选项，具体取决于底层基础架构，本指南介绍了如何在部署后进行更改。

虚拟桌面性能取决于各种关键资源，存储性能是主要变量之一。随着需求的变化和工作负载的变化，需要更改存储基础架构也是一项常见任务。在几乎所有情况下，这都涉及从文件服务器平台迁移到 NetApp 存储技术（例如 Azure NetApp Files ， Google 中的 NetApp Cloud Volumes Service 或 AWS 中的 NetApp Cloud Volumes ONTAP ），因为这些技术通常可为最终用户计算环境提供最佳性能。

创建新存储层

由于各种云和 HCI 基础架构提供商的潜在存储服务种类繁多，因此本指南假定已建立一个新的存储服务，并且 SMB 路径已知。

创建存储文件夹

1. 在新存储服务中，创建三个文件夹：
   - 数据
   - 主页
   - /Pro

     []
2. 设置文件夹权限
   a. 在文件夹属性上，选择 _Security ， > 高级 > 禁用继承 _

      []

   b. 调整其余设置，使其与部署自动化最初创建的原始存储层上的设置相匹配。

移动数据

可以通过多种方式移动目录，数据，文件和安全设置。以下 Robocopy 语法将实现必要的更改。需要根据您的环境更改路径。

```
robocopy c:\data\zucd \\uyy-1c37.deskapps.mobi\zucd-data /xd ~snapshot
/MIR /CopyAll /R:1 /W:1 /tee /log:C:\temp\roboitD.txt
```

在转换时重定向 **SMB** 路径

在转换时间结束后，一些更改会将所有存储功能重定向到整个 VDS 环境。

更新 **GPOs**

1. 需要使用新的共享路径更新用户 GPO （名为 *<company-code>-users* ）。选择 *User Configuration* > *Windows Settings* > *Preferences* > *Drive Maps*

   []

2. 右键单击 _H： _ ，选择属性 > 编辑 > 操作：替换 _ 并输入新路径

   []

3. 使用经典或混合 AD 更新在公司 OU 中的 ADUC 中定义的共享。这反映在 VDS 文件夹管理中。

   []

更新 **FSLogix** 配置文件路径

1. 在原始文件服务器和任何其他已配置的会话主机上打开 Regedit 。

   如果需要，也可以通过 GPO 策略进行设置。

2. 使用新值编辑 *VHD Locations_value* 。此路径应为新的 *SMB* 路径加上 *_pro/profilecontainers* ，如以下屏幕截图所示。

   []

更新主目录的文件夹重定向设置

1. 打开组策略管理，选择链接到 DC= 域， DC=mobi/ 云工作空间 / 云工作空间公司 /< 公司代码 >/< 公司代码 >-Desktop 用户的用户 GPO 。
2. 在用户配置 > 策略 > Windows 设置 > 文件夹重定向下编辑文件夹重定向路径。
3. 只需要更新桌面和文档，并且路径应与主卷的新 SMB 路径挂载点匹配。

   []

使用命令中心更新 **VDS SQL** 数据库

CMGR1 包含一个名为 Command Center 的帮助程序实用程序应用程序，该应用程序可以批量更新 VDS 数据库。

要进行最终数据库更新，请执行以下操作：

1. 连接到 CMGR1 ，导航并运行 CommandCenter.exe

   []

2. 导航到 *Operals* 选项卡，单击 *Load Data* 以填充公司代码下拉列表，选择公司代码并输入存储层的新存储路径，然后单击 *Execute Command* 。

   []

将存储平台重定向到 **Azure Files**

概述

虚拟桌面服务部署技术支持多种存储选项，具体取决于底层基础架构。本指南介绍如何在部署后更改 Azure Files 的使用。

前提条件

- 已安装并设置 AD Connect
- Azure 全局管理员帐户
- AZFilesHybrid PowerShell 模块 https://github.com/Azure-Samples/azure-files-samples/releases
- AZ PowerShell 模块
- ActiveDirectory PowerShell 模块

创建新的存储层

1. 使用全局管理员帐户登录到 Azure
2. 在与工作空间相同的位置和资源组中创建新的存储帐户

   []

3. 在存储帐户下创建数据，主目录和专业文件共享

   []

设置 **Active Directory**

1. 在云工作空间 > 云工作空间服务帐户 OU 下创建一个名为 `S存储帐户` 的新组织单位

   []

2. 启用 AD DS 身份验证（必须使用 PowerShell 完成） https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable

   a. DomainAccountType 应为 `ServiceLogonAccount`

   b. OraganizationalUniteDistinguishedName 是上一步创建的 OU 的可分辨名称（即`OU=Storage Account ， OU=Cloud Workspace Service Accounts ， OU=Cloud Workspace ， DC=TrainingKrisG ， DC=onmicrosoft ， DC=com` ）

设置共享的角色

1. 在 Azure 门户中，将 " `S存储文件数据 SMB 共享提升贡献者` " 角色提供给 CloudWorkspaceSVC 和 Level3 技术人员

   []

2. 将 " 存储文件数据 SMB 共享贡献者 " 角色分配给 "` < 公司代码 >-all users` " 组

   []

创建目录

1. 在每个共享（ data ， home ， pro ）中使用公司代码作为名称（在此示例中，公司代码为 "`Kift` " ）创建一个目录

   []

2. 在专业共享的 < 公司代码 > 目录中，创建 "`ProfileContainers` " 目录

   []

设置 **NTFS** 权限

1. 连接到共享
   a. 导航到 Azure 门户中存储帐户下的共享，单击三个点，然后单击连接

      []

   b. 选择 Active Directory 进行身份验证方法，然后单击代码右下角的复制到剪贴板图标

      []

   c. 使用 Level3 技术人员组的成员帐户登录到 CMGR1 服务器
   d. 在 PowerShell 中运行复制的代码以映射驱动器
   e. 对每个共享执行相同的操作，同时为每个共享选择不同的驱动器盘符
2. 禁用 < 公司代码 > 目录的继承
3. 系统和 AD 组客户端 DHPAccess 应具有对 < 公司代码 > 目录的完全控制权限
4. 域计算机应对专业共享中的 < 公司代码 > 目录以及中的 ProfileContainers 目录具有完全控制权限
5. 公司代码 >-all 用户 AD 组应具有对主目录和专业共享中 <companycode> 目录的 List folder/read data 权限
6. 对于数据共享中的目录， <companycode>-all users AD 组应具有以下特殊权限

   []

7. 公司代码 >-all users AD 组应对 ProfileContainers 目录具有修改权限

更新组策略对象

1. 更新位于 Cloud Workspace > Cloud Workspace 公司 > < 公司代码 > -Desktop 用户下的 GPO < 公司代码 > 用户
   a. 更改主驱动器映射以指向新的主共享

      []

   b. 更改文件夹重定向以指向桌面和文档的主共享

      []

[]

更新 **Active Directory** 用户和计算机中的共享

1. 对于传统或混合 AD ，需要将公司代码 OU 中的共享更新到新位置

   []

更新 **VDS** 中的数据 **/** 主目录 **/Pro** 路径

1. 使用 Level3 技术人员组中的帐户登录到 CMGR1 ，然后启动命令中心
2. 在命令下拉列表中，选择更改数据 / 主目录 /Pro 文件夹
3. 单击加载数据按钮，然后确保从下拉列表中选择了正确的公司代码
4. 输入数据，主位置和专业位置的新 patsh
5. 取消选中 Is Windows Server 复选框
6. 单击 Execute Command 按钮

   []

更新 **FSLogix** 配置文件路径

1. 打开会话主机上的临时注册表
2. 编辑 HKLM\SOFTWARE\FSLogix \Profiles\ 中的 VHDLocations 条目，使其成为新 ProfileContainers 目录的 UNC 路径

   []

配置备份

1. 建议为新共享设置和配置备份策略
2. 在同一资源组中创建新的恢复服务存储
3. 导航到存储，然后在 Getting Started 下选择 Backup
4. 选择 Azure 作为工作负载的运行位置，选择 Azure 文件共享作为要备份的内容，然后单击 Backukp
5. 选择用于创建共享的存储帐户
6. 添加要备份的共享
7. 根据需要编辑和创建备份策略

数据迁移注意事项

概述

迁移到任何类型的云解决方案时，迁移数据几乎是一项通用要求。虽然管理员负责将数据迁移到其虚拟桌面，但 NetApp 的经验是可以获得的，而且经验证，对于无数客户迁移来说， NetApp 的经验是非常宝贵的。虚拟桌面环境只是一个托管的 Windows 环境，因此可以采用任何所需的方法。

通常迁移的数据：

- 用户配置文件（桌面，文档，收藏夹等…）
- 文件服务器共享
- 数据共享（应用程序数据，数据库，备份缓存）

在虚拟桌面环境中，存储和组织数据的主要位置有两个：

- 用户（通常为 H： \）驱动器：这是对每个用户可见的映射驱动器。
  - 此路径将映射回 < 驱动器 >： \home\CustomerCode\user.name 路径
  - 每个用户都有自己的 H： \ 驱动器，无法查看其他用户
- 共享（通常为 I： \）驱动器：这是对所有用户可见的共享映射驱动器
  - 此路径将映射回 < 驱动器 >： \data\CustomerCode\ 路径
  - 所有用户均可访问此驱动器。其对所含文件夹 / 文件的访问级别在 VDS 的文件夹部分进行管理。

通用迁移过程

1. 将数据复制到云环境
2. 将数据移动到 H： \ 和 I： \ 驱动器的相应路径
3. 在虚拟桌面环境中分配适当的权限

FTPS 传输和注意事项

使用 **FTPS** 进行迁移

1. 如果在 CWA 部署过程中启用了 FTPS 服务器角色，请通过登录到 VDS ，导航到报告并运行组织的主客户端报告来收集 FTPS 凭据
2. 上传数据
3. 将数据移动到 H： \ 和 I： \ 驱动器的相应路径
4. 通过文件夹模块在虚拟桌面环境中分配适当的权限

通过 FTPS 传输数据时，任何中断都将阻止按预期传输数据。由于虚拟桌面服务管理的服务器每晚重新启动一次，因此标准的夜间传输策略可能会中断。要解决此问题，管理员可以启用迁移模式，以防止 VM 在 1 周内重新启动。

启用迁移模式非常简单—导航到组织，向下滚动到 Virtual Desktop Settings 部分并选中 Migration Mode 复选框，然后单击 Update 。

NetApp 建议管理员启用一个合规性设置，通过强化部署的网关等来帮助组织满足 PCI ， HIPAA 和 NIST 控制的要求。这样，如果启用了默认 FTP 服务器角色，则也不允许通过端口 21 接受默认的未加密传输。FileZilla 不允许使用 SFTP ，这意味着应使用 FTPS 通过端口 990 进行连接。

要启用此设置，请连接到 CMGR1 并导航到 CwVmAutomationService 程序，然后启用 PCI v3 合规性。

同步工具和注意事项

企业文件同步和共享通常称为 EFSS 或同步工具，在迁移数据时非常有用，因为该工具会捕获双方的更改，直到转换为止。Office 365 附带的 OneDrive 等工具可以帮助您同步文件服务器数据。如果 VDI 用户部署中的用户和虚拟机之间存在 1： 1 关系，则此功能也很有用，前提是用户不会尝试将共享内容同步到其 VDI 服务器，而共享数据只能部署一次（通常为 I： \） 推动整个企业使用。迁移 SQL 和类似数据（打开的文件）

常见的同步和 / 或迁移解决方案不会传输打开的文件，其中包括以下文件类型：

- 邮箱（ .ost ）文件
- QuickBooks 文件
- Microsoft Access 文件
- SQL 数据库

这意味着，如果整个文件的一个元素（例如，显示 1 个新电子邮件）或数据库（在应用程序的系统中输入 1 个新记录），则整个文件将与标准同步工具（例如， Dropbox ）不同。 会认为它是一个全新的文件，需要再次移动。如果需要，可以从第三方提供商购买专用工具。

处理这些迁移的另一种常见方法是，提供对第三方 VAR 的访问权限，第三方 VAR 通常简化了数据库的导入 / 导出。

运输驱动器

许多数据中心提供商不再提供硬盘驱动器，或者他们要求您遵循其特定的策略和程序。

Microsoft Azure 支持企业使用 Azure Data Box ，管理员可以通过与其 Microsoft 代表进行协调来利用它。

通配符 **SSL** 证书续订过程

创建证书签名请求（ **CSR** ）：

1. 连接到 CWMGR1
2. 从管理员工具打开 IIS 管理器
3. 选择 CMGR1 并打开服务器证书
4. 单击操作窗格中的创建证书请求

   []

5. 在请求证书向导中填写可分辨名称属性，然后单击下一步：
   a. 公用名：通配符的 FQDN - * 。 .domain.com
   b. 组织：贵公司的合法注册名称
   c. 组织单位： ‘IT ' 工作正常
   d. City ： 公司所在的城市
   e. 省 / 自治区 / 直辖市：公司所在的省 / 自治区 / 直辖市
   f. 国家 / 地区：公司所在的国家 / 地区

[]

6. 在加密服务提供程序属性页面上，验证是否显示以下内容，然后单击下一步：

   []

7. 指定文件名并浏览到要保存 CSR 的位置。如果不指定位置，则 CSR 将位于 C： \Windows\System32：

   []

8. 完成后，单击完成。您将使用此文本文件将订单提交给证书注册商
9. 请联系注册商支持部门为您的证书购买新的通配符 SSL： * .domain.com
10. 收到 SSL 证书后，将 SSL 证书 .cer 文件保存在 CMGR1 上的某个位置，然后按照以下步骤进行操作。

安装和配置 **CSR**：

1. 连接到 CWMGR1
2. 从管理员工具打开 IIS 管理器
3. ‘SCMGR1 并打开 " 服务器证书 "
4. 单击操作窗格中的完成证书请求

   []

5. 填写完整证书请求中的以下字段，然后单击确定：

   []

   a. 文件名：选择先前保存的 .cer 文件
   b. 友好名称： * 。 .domain.com
   c. 证书存储：选择 Web 托管或个人

正在分配 **SSL** 证书：

1. 验证是否未启用迁移模式。您可以在 VDS 中的 "Security Settings" 下的 "Workspace Overview" 页面上找到此信息。

   []

2. 连接到 CWMGR1
3. 从管理员工具打开 IIS 管理器
4. ‘SCMGR1 并打开 " 服务器证书 "
5. 单击操作窗格中的导出
6. 以 .pfx 格式导出证书
7. 创建密码。存储密码，因为将来需要导入或重新使用 .pfx 文件
8. 将 .pfx 文件保存到 C： \installs\RDPcert 目录

9. 单击确定并关闭 IIS 管理器

   []

10. 打开 DCConfig
11. 在通配符证书下，将证书路径更新为新的 .pfx 文件
12. 出现提示时，输入 .pfx 密码
13. 单击保存。

    []

14. 如果证书的有效期超过 30 天，则允许自动化在一周内的每天早晨操作任务期间应用新证书
15. 定期检查平台服务器以验证新证书是否已传播。验证并测试用户连接以确认。
    a. 在服务器上，转到管理工具
    b. 选择远程桌面服务 > 远程桌面网关管理器
    c. 右键单击网关服务器名称，然后选择属性。单击 SSL 证书选项卡以查看到期日期

       []

16. 定期检查运行连接代理角色的客户端 VM

    a. 转至服务器管理器 > 远程桌面服务
    b. 在部署概述下，选择任务下拉列表，然后选择编辑部署属性

       []

    c. 单击 Certificates ，选择 certificate ，然后单击 View Details 。此时将列出到期日期。

       []

    []

17. 如果不到 30 天，或者您希望立即推出新证书，请使用 TestVdcTools 强制更新。应在维护时段完成此操作，因为任何已登录用户的连接以及与 CMGR1 的连接都将断开。
    a. 转至 C： \Program Files\CloudWorkspace\TestVdcTools ，单击 Operations 选项卡，然后选择通配符 Cert-Install 命令
    b. 将服务器字段留空
    c. 选中强制复选框
    d. 单击 Execute Command
    e. 使用上述步骤验证证书传播

       []

AVD 拆卸指南

概述

本文介绍如何在保留 AVD 最终用户访问权限的同时删除 VDS 和 NetApp 控制。未来的管理将借助原生 Azure/Windows 管理工具进行。完成此过程后，建议您联系 support@spotpc.netapp.com ，以便 NetApp 能够清理我们的后端和计费系统。

初始状态

- AVD 部署
- HDDS1 是 FS Logix 文件共享
- TS1 是会话主机
- 用户已登录并在以下位置创建了 FS Logix 磁盘：

```
\\****TSD1\****-Pro$\ProfileContainers (**** = Unique Company Code)
```

删除顺时针代理服务

此 CW 代理会在环境中的每台计算机上运行。应在环境中的每个 VM 上使用以下命令卸载启动此过程的服务。可以跳过 CMGR1 ，因为大多数情况下，此 VM 将关闭并最终删除。理想情况下，此操作将通过脚本化自动化运行。以下视频显示了手动完成。

```
C:\Program files\CloudWorkspace\CwAgent\CwAgent.exe -u
```

删除顺时针代理服务视频

[] | *https://img.youtube.com/vi/l9ASmM5aap0/maxresdefault.jpg*

删除顺时针代理目录

上次卸载将删除启动 CW Agent 的服务，但文件仍保留。删除目录：

```
"C:\Program Files\CloudWorkspace"
```

删除 **CW Agent** 目录视频

[] | *https://img.youtube.com/vi/hMM_z4K2-iI/maxresdefault.jpg*

删除启动快捷方式

启动项目录包含两个快捷方式，用于访问上一步中删除的文件。为了避免最终用户出现错误消息，应删除这些文件。

```
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Pen.lnk"
"C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\StartUp\CwRemoteApps.lnk"
```

删除启动快捷方式视频

[] | *https://img.youtube.com/vi/U0YLZ3Qfu9w/maxresdefault.jpg*

取消链接 ‘Users ' 和 ‘公司 ' GPO

VDS 实施了三个 GPO 。我们建议取消其中两个链接并查看第三个的内容。

取消链接：

- AADDC 用户 > Cloud Workspace 公司
- ADDC 用户 > Cloud Workspace 用户

请查看

- AADDC 计算机 > Cloud Workspace 计算机

取消链接 ‘**Users** ' 和 ‘公司的 **GPO** 视频

[] | *https://img.youtube.com/vi/cb68ri3HKUw/maxresdefault.jpg*

关闭 **CMGR1**

应用 GPO 更改后，我们现在可以关闭 CMGR1 虚拟机。确认 AVD 功能是否继续后，可以永久删除此虚拟机。

在极少数情况下，如果正在运行另一个服务器角色（例如 DC ， FTP 服务器… ）。在这种情况下，可以禁用三种服务来禁用 CMGR1 上的 VDS 功能：

- 顺时针代理（请参见上文）
- 顺时针自动化服务
- CW VM 自动化

关闭 **CMGR1** 视频

[] | *https://img.youtube.com/vi/avk9HyliC_s/maxresdefault.jpg*

删除 **NetApp VDS** 服务帐户

可以删除 VDS 使用的 Azure AD 服务帐户。登录到 Azure 管理门户并删除用户：

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

可以保留其他用户帐户：

- 最终用户
- Azure 管理员
- .tech 域管理员

删除 **NetApp VDS** 服务帐户视频

[] | *https://img.youtube.com/vi/_VToVNp49cg/maxresdefault.jpg*

删除应用程序注册

部署 VDS 时会注册两个应用程序。可以删除这些内容：

- 云工作空间 API
- 云工作空间 AVD

删除应用程序注册视频

[] | *https://img.youtube.com/vi/iARz2nw1Oks/maxresdefault.jpg*

删除企业级应用程序

部署 VDS 时会部署两个企业级应用程序。可以删除这些内容：

- 云工作空间
- 云工作空间管理 API

删除企业应用程序视频

[] | *https://img.youtube.com/vi/3eQzTPdilWk/maxresdefault.jpg*

确认已停止 **CMGR1**

在测试最终用户是否仍可连接之前，请确认已停止 CMGR1 以进行实际测试。

确认 **CMGR1** 已停止视频

[] | *https://img.youtube.com/vi/Ux9nkDk5lU4/maxresdefault.jpg*

登录和最终用户

要确认成功，请以最终用户身份登录并保持确认功能不变。

登录和最终用户视频

[] | *https://img.youtube.com/vi/SuS-OTHJz7Y/maxresdefault.jpg*

Copyright Information

Trademark Information