系统管理
Virtual Desktop Service

NetApp
April 12, 2022

目录

系统管理

创建域管理员（ " 级别 **3"** ）帐户

概述

有时， VDS 管理员需要域级凭据来管理环境。在 VDS 中，这些帐户称为 "3 级 " 或 ".tech" 帐户。

这些说明说明说明了如何使用适当的权限创建这些帐户。

Windows Server 域控制器

在运行内部托管域控制器（或通过 VPN/Express 路由链接到 Azure 的本地 DC ）时，可以直接在 Active Directory Manager 中管理 .tech 帐户。

1. 使用域管理员（ .tech ）帐户连接到域控制器（ CMGR1 ， DC01 或现有 VM ）。
2. 创建新用户（如果需要）。
3. 将此用户添加到 "Level3 技术人员 " 安全组

   [management.System Administration.create domain admin account 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

a. 如果缺少 "Level3 技术人员 " 安全组，请创建该组并使其成为 "CW-Infrastructure" 安全组的成员。

[management.System Administration.create domain admin account 0fc27] |

Management.System_Administration.create_domain_admin_account-0fc27.png

建议在用户名末尾添加 ".tech" ，以帮助从最终用户帐户中划分管理员帐户。

Azure AD 域服务

如果在 Azure AD 域服务中运行或在 Azure AD 中管理用户，则可以在 Azure 管理门户中以普通 Azure AD 用户的身份管理这些帐户（即密码更改）。

可以创建新帐户，将其添加到这些角色后，应为其提供所需的权限：

1. AAD DC 管理员
2. 客户端 HPAccess
3. 目录中的全局管理员。

建议在用户名末尾添加 ".tech" ，以帮助从最终用户帐户中划分管理员帐户。

[]

为第三方提供临时访问权限

概述

在迁移到任何云解决方案时，通常会提供对第三方的访问权限。

VDS 管理员通常会选择不向这些第三方授予与其所拥有的相同访问级别，而是遵循 " 最不需要 " 的安全访问策略。

要为第三方设置管理员访问权限，请登录到 VDS 并导航到组织模块，单击组织并单击用户和组。

接下来，为第三方创建一个新的用户帐户，向下滚动，直到看到 Admin Access 部分，然后选中相应框以启用管理员权限。

[]

然后， VDS Admin 将显示 Admin Access 设置屏幕。无需更改用户的名称，登录名或密码—如果要强制实施多因素身份验证并选择要授予的访问级别，只需添加电话号码和 / 或电子邮件即可。

对于 VAR 或 ISV 等数据库管理员， *Servers* 通常是唯一需要的访问模块。

[]

保存后，最终用户可以使用其标准 Virtual Desktop 用户凭据登录到 VDS 来访问自我管理功能。

新创建的用户登录时，他们只会看到您为其分配的模块。他们可以选择组织，向下滚动到 Servers 部分并连接到您告诉他们的服务器名称（例如， <XYZ>D1 ，其中 XYZ 是您的公司代码， D1 表示服务器是数据服务器。在以下示例中，我们会指示他们连接到 TSD1 服务器以执行分配。

[]

配置备份计划

概述

VDS 能够在包括 Azure 在内的某些基础架构提供商中配置和管理原生备份服务。

Azure 酒店

在 Azure 中， VDS 可以使用原生自动配置备份 "Azure Cloud Backup" 使用本地冗余存储（ LRS ）。如果需要，可以在 Azure 管理门户中配置地区冗余存储（ GRS ）。

- 可以为每种服务器类型定义单个备份策略（含默认建议）。此外，可以在 VDS UI 中为各个计算机分配独立于其服务器类型的计划，可以通过在 Workspace 页面上单击 Server name （服务器名称）导航到 Server Detail 视图来应用此设置（请参见以下视频：设置单个备份策略）
  - 数据
    - 备份，包括 7 个每日备份， 5 个每周备份和 2 个每月备份。根据业务需求延长保留期限。
    - 专用数据服务器以及应用程序和数据库的附加 VPS VM 都是如此。
  - 基础架构
    - CMGR1 —每天备份 7 个，每周 5 个，每月 2 个。
    - RDS 网关—每周备份一次，每周保留 4 个。
    - HTML5 网关—每周备份一次，每周保留 4 个。
  - poweruser （也称为 VDI 用户）
    - 请勿备份虚拟机，因为数据应存储在 D1 或 TSD1 服务器上。
    - 请注意，某些应用程序确实会在本地存储数据，如果是这种情况，应特别注意事项。
    - 如果虚拟机发生故障，可以通过克隆另一个虚拟机来构建新的虚拟机。如果只有一个 VDI VM （或一个唯一的 VM 内部版本），则建议对其进行备份，以便不需要完全重建该 VM 。
    - 如果需要，可以通过在 Azure 管理门户中手动配置一个 VM 来直接备份，从而最大限度地降低成本，而不是备份所有 VDI 服务器。
  - TS
    - 请勿备份虚拟机，因为数据应存储在 D1 或 TSD1 服务器上。
    - 请注意，某些应用程序确实会在本地存储数据，如果是这种情况，应特别注意事项。
    - 如果虚拟机发生故障，可以通过克隆另一个虚拟机来构建新的虚拟机。如果只有一个 TS VM ，则建议对其进行备份，以便不需要完全重建该 VM 。
    - 如果需要，可以通过在 Azure 管理门户中手动配置一个 VM 来直接备份，从而最大程度地降低成本，而不是备份所有 TS 服务器。
  - TSData
    - 备份，包括 7 个每日备份， 5 个每周备份和 2 个每月备份。根据业务需求延长保留期限。
- 可以将策略设置为每天或每周进行备份， Azure 不支持更频繁的计划。
- 对于每日计划，输入备份的首选时间。对于每周计划，输入备份的首选日期和时间。注意：将时间设置为恰好 12： 00 AM 可以在 Azure 备份中处理发生原因问题，因此建议上午 12： 01 。

- 定义应保留的每日，每周，每月和每年备份数。

设置部署默认值

[]

要为整个部署设置 **Azure** 备份，请执行以下步骤：

1. 导航到部署详细信息页面，选择备份默认值
2. 从下拉菜单中选择服务器类型。服务器类型包括：

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to
them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

   - 这将定义整个部署的总体备份设置。如果需要，可以稍后在特定于服务器的级别覆盖和设置这些设置。
3. 单击设置轮，然后单击显示的编辑弹出窗口。
4. 选择以下备份设置：

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. 最后，单击创建（或编辑）计划以将这些设置放置到位。

设置单个备份策略

要应用服务器专用的集成备份设置，请导航到 **Workspace** 详细信息页面。

1. 向下滚动到 Servers 部分，然后单击服务器的名称
2. 单击添加计划
3. 根据需要应用备份设置，然后单击创建计划

从备份还原

要还原给定虚拟机的备份，请首先导航到该 **Workspace** 详细信息页面。

1. 向下滚动到 Servers 部分，然后单击服务器的名称
2. 向下滚动到备份部分，然后单击滚轮展开选项，然后选择任一项
3. 还原到服务器或还原到磁盘（从备份连接驱动器，以便可以将数据从备份复制到虚拟机的现有版本）。
4. 从这一点开始继续还原，就像在任何其他还原情形中一样。

成本取决于您要维护的计划，完全由 Azure 备份成本决定。有关虚拟机的备份定价，请参见 Azure 成本计算器： https://azure.microsoft.com/en-us/pricing/calculator/

克隆虚拟机

概述

虚拟桌面服务（ Virtual Desktop Service ， VDS ）可以克隆现有虚拟机（ VM ）。此功能旨在随着定义的用户数增加或更多服务器添加到可用资源池而自动提高服务器单元数可用性。

管理员可以通过两种方式在 VDS 中使用克隆：

1. 按需自动从现有客户端服务器创建新服务器
2. 主动自动创建新的客户端服务器，以便根据合作伙伴定义和控制的规则自动扩展资源

克隆以添加其他共享服务器

克隆是现有虚拟机的副本。克隆功能可以节省时间并帮助管理员进行扩展，因为安装子操作系统和应用程序可能非常耗时。通过克隆，您可以通过一个安装和配置过程创建多个虚拟机副本。这通常如下所示：

1. 将所有所需的应用程序和设置安装到 TS 或 TSD 服务器上
2. 导航到： " 工作空间 ">" 服务器部分 ">" 源服务器的齿轮图标 "> 单击 " 克隆 "
3. 允许克隆进程运行（通常为 45-90 分钟）
4. 最后一步激活克隆的服务器，将其放入 RDS 池中以接受新连接。克隆的服务器在克隆后可能需要单独配置，因此 VDS 会等待管理员手动将服务器置于轮换状态。

根据需要重复多次。[]

为了增加共享会话主机环境中用户的容量，克隆会话主机是一个简单的过程，只需执行几个步骤即可。

1. 选择要克隆的会话主机，确认当前没有任何用户登录到该计算机。
2. 在 VDS 中，导航到目标客户端的 Workspace 。滚动到服务器部分，单击齿轮图标并选择克隆。此过程需要很长时间，并会使源计算机脱机。预计完成时间将超过 30 分钟。

   [] []

3. 此过程将关闭服务器，将服务器克隆到另一个映像，并将该映像按系统运行后再运行到客户的下一个 TS-# 。此服务器在服务器列表中显示为 *Type=Staged* 和 _Status=激 活要求 _ 。

   []

4. 登录到服务器并验证服务器是否已准备好投入生产。

   []

5. 准备好后，单击激活将服务器添加到会话主机池中，以开始接受用户连接。

   []

VDS 克隆过程定义

在任何克隆服务器操作下的 VDS > 部署 > 任务历史记录中详细介绍了分步过程。此过程包含 20 多个步骤，这些步骤从访问虚拟机管理程序开始克隆过程，到激活克隆的服务器结束。克隆过程包括以下关键步骤：

- 配置 DNS 并设置服务器名称
- 分配 StaticIP
- 添加到域
- 更新 Active Directory
- 更新 VDS 数据库（ CMGR1 上的 SQL 实例）
- 为克隆创建防火墙规则

除了任务历史记录之外，还可以在每个合作伙伴的虚拟桌面部署中的 CwVmAutomationService 日志中查看任何克隆过程的详细步骤。查看这些日志文件会记录下来 "此处"。

自动创建新服务器

此 VDS 功能旨在随着定义的用户数量的增长自动提高服务器单元数量的可用性。

配对节点通过 VDS 定义和管理（""） > 客户端 > 概述– VM 资源 > 自动扩展。合作伙伴可以通过多个控件来启用 / 禁用自动扩展以及为每个客户端创建自定义规则，例如：数量 / 用户 / 服务器，每个用户额外的 RAM 以及每个 CPU 的用户数量。

上述假设已为整个虚拟桌面部署启用自动克隆。例如，要停止所有自动克隆，请使用 DCConfig ，在高级窗口中取消选中服务器创建 → 自动克隆已启用。

自动克隆过程何时运行?

如果将每日维护配置为运行，则会运行自动克隆过程。默认值为午夜，但可以编辑此值。日常维护的一部分是为每个资源池运行 " 更改资源 " 线程。更改资源线程根据池配置的用户数（可自定义；每个服务器可以是 10 ， 21 ， 30 等用户）确定所需的共享服务器数量。

按需自动创建新服务器

通过此 VDS 功能，可以自动将其他服务器 " 按需 " 克隆到可用资源池。

VDS 管理员登录到 VDS ，然后在组织或工作空间模块下找到特定客户端并打开概述选项卡。" 服务器 " 图块列出了所有服务器（ TSD1 ， TS1 ， D1 等）。要克隆任何单个服务器，只需单击服务器名称最右侧的代码并选择克隆选项即可。

通常，此过程需要大约一个小时。但是，持续时间取决于虚拟机的大小以及底层虚拟机管理程序的可用资源。请注意，要克隆的服务器需要重新启动，因此合作伙伴通常会在非工作时间或计划的维护时段执行。

克隆 TSData 服务器时，其中一个步骤是删除 c： \Home ， c： \Data 和 c： \Pro 文件夹，使其不是任何重复文件。在这种情况下，克隆进程失败，删除这些文件时出现问题。此错误不明确。通常，这意味着克隆事件失败，因为存在打开的文件或进程。下次尝试，请禁用任何 AV （因为这可能会解释此错误）。

自动增加磁盘空间功能

概述

NetApp 认识到需要为管理员提供一种简单的方法，以确保用户始终有空间访问和保存文档。这样还可以确保 VM 有足够的可用空间来成功完成备份，从而支持并支持管理员及其灾难恢复和业务连续性计划。考虑到这一点，我们构建了一项功能，可在驱动器空间不足时自动将所使用的受管磁盘扩展到下一层。

默认情况下，此设置会应用于 Azure 中的所有新 VDS 部署，以确保所有部署都在默认情况下保护用户和租户的备份。

管理员可以通过导航到 " 部署 " 选项卡，然后选择一个部署，然后从该选项卡连接到其 CMGR1 服务器来验证此功能是否到位。接下来，打开桌面上的 DCConfig 快捷方式，单击高级并向下滚动到底部。

[]

管理员可以在 DCConfig 的 " 高级 " 部分中更改在移至下一层受管磁盘之前所需的可用空间量（以 GB 为单位）或驱动器的可用空间百分比。

[]

一些实用的应用示例：

- 如果要确保驱动器上至少有 50 GB 的可用空间，请将 MinFreeSpaceGB 设置为 50
- 如果要确保至少有 15% 的驱动器可用，请将 MinFreeSpacePercent 设置为 10 到 15 。

此操作将在服务器时区的午夜执行。

在 **Azure** 密钥存储中访问 **VDS** 凭据

概述

CWASetup 5.4 与以前的 Azure 部署方法不同。简化了配置和验证过程，以减少开始部署所需的信息量。其中许多删除的提示都适用于凭据或帐户，例如本地 VM 管理员， SMTP 帐户，技术帐户， SQL SA 等。这些帐户现在会自动生成并存储在 Azure 密钥存储库中。默认情况下，访问这些自动生成的帐户需要执行下述附加步骤。

- 找到 " 密钥存储 " 资源并单击它：

  [宽度 = 75%]

- 在 ‘S' 下，单击 ‘S' 日期 ' 。此时将显示一条消息，指出您未授权查看：

  [宽度 = 75%]

- 添加 ‘Access Policy ' 以授予 Azure AD 帐户（如全局管理员或系统管理员）对以下敏感密钥的访问权限：

  [宽度 = 75%]

- 本示例使用了全局管理员。选择主体后，单击 ‘Select ' ，然后单击 ‘Add ' ：

  [宽度 = 75%]

- ‘SSave ' ：

  [宽度 = 75%]

- 已成功添加访问策略：

  [宽度 = 75%]

- 重新访问 ‘S" 记录 " 以验证帐户现在是否有权访问部署帐户：

  [宽度 = 75%]

- 例如，如果您需要域管理员凭据才能登录到 CMGR1 并更新组策略，请通过单击每个条目检查 cjDomainAdministratorName 和 cjDomainAdministratorPassword 下的字符串：

  [宽度 = 75%]

  [宽度 = 75%]

- 显示或复制此值：

  [宽度 = 75%]

应用监控和防病毒

概述

虚拟桌面服务（ Virtual Desktop Service ， VDS ）管理员负责监控其平台基础架构（至少包含 CMGR1 ）以及所有其他基础架构和虚拟机（ VM ）。在大多数情况下，管理员直接与数据中心 /IaaS 提供商一起安排基础架构（虚拟机管理程序 /SAN ）监控。管理员负责监控终端服务器和数据服务器，通常是部署首选的远程管理和监控（ RMM ）解决方案。

防病毒是管理员的责任（对于平台基础架构和终端 / 数据服务器 VM ）。为了简化此过程，默认情况下，适用于 Azure 服务器的 VDS 会应用 Windows Defender" 。

在安装第三方解决方案时，请确保不要包含防火墙或任何可能会干扰 VDS 自动化的其他组件。

更具体地说，如果默认情况下设置了非常具体的防病毒策略，则在由虚拟桌面服务管理的服务器上安装这些防病毒代理时，可能会产生负面影响。

我们的总体指导原则是，虽然 VDS 平台自动化通常不受防病毒或防恶意软件产品的影响，但最佳做法是在所有平台服务器（ CMGR1 ， R5275Gateways ， FTP 等）上为以下过程添加例外 / 除外情形：

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

此外，我们建议在客户端服务器上安全列出以下进程：

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

添加和移动映射的驱动器

概述

默认情况下，有三个共享文件夹会公开给最终用户会话。这些文件夹位于定义的存储层上。这可以位于文件服务器（ TSD1 或 D1 ）上，也可以位于存储服务上，例如 Azure 文件， Azure NetApp Files ， NetApp CVO 和 NetApp CVS 。

为了便于明确起见，本文将使用公司代码为 "NECA " 的示例客户。 此示例假设已部署一个名为 NECATSD1 的 TDS1 服务器。我们将完成将文件夹移动到另一个 VM （名为 NECAD1 ）的过程。可以使用此策略在同一台计算机上的分区之间移动，也可以移动到另一台计算机，如以下示例… 所示

文件夹起始位置：

- 数据： NECATSD1\C： \data\NECA\ （ TSD1 意味着它是第一个终端服务器，也充当数据服务器）
- FTP： NECATSD1\C： \ftp\NECA\
- 主页： NECATSD1\C： \HOME\NECA\

文件夹结束位置：

- 数据： NECAD1\G： \data\NECA\ （ D1 表示它是第一个数据服务器）
- FTP ：相同的过程适用，无需将其描述为 3 倍
- 主页：相同的过程适用，无需将其描述为 3 倍

在 **NECAD1** 上为 **G：** 添加磁盘

1. 要将共享文件夹放在 E： 驱动器上，我们需要通过虚拟机管理程序（例如 Azure 管理门户），然后对其进行初始化和格式化

   []

2. 将现有文件夹（ NECATSD1 ， C： \）路径复制到新位置（ NECAD1 ， G： \）
3. 将文件夹从原始位置复制到新位置。

   []

从原始文件夹共享（ **NECATSD1** ， **C：** **\data\NECA** ）收集信息

1. 使用与原始位置中的文件夹完全相同的路径共享新文件夹。
2. 打开新的 NECAD1 G： \data\ 文件夹，您将在本示例中看到一个名为公司代码 "NECA " 的文件夹。

   []

3. 请注意原始文件夹共享的安全权限：

   []

4. 这是典型设置，但如果需要保留现有自定义设置，则复制原始设置非常重要。应从新文件夹共享中删除所有其他用户 / 组权限
   - system： 允许所有权限
   - LocalClientDHPAccess （在本地计算机上）： 允许的所有权限
   - ClientDHPAccess （在域上）： 允许的所有权限
   - NECA-ALL 用户（在域上）： 允许除 " 完全控制 " 以外的所有权限

将共享路径和安全权限复制到新共享文件夹

1. 返回到新位置（ NECAD1 ， G： \data\NECA ），并使用相同的网络路径（不包括计算机）共享 NECA 文件夹，在我们的示例中为 "NECA-data$"

   []

2. 为确保用户安全，请添加所有用户，并将其权限设置为匹配。

   []

3. 删除可能已存在的任何其他用户 / 组权限。

   []

编辑组策略（仅当文件夹移动到新计算机时）

1. 接下来，您将在组策略管理编辑器中编辑驱动器映射。对于 Azure AD 域服务，映射位于：

```
“Cloud Workspace Users > User Configuration > Preferences > Windows
Settings> Drive Maps”
```

[]

2. 更新组策略后，下次每个用户连接时，他们将看到映射的驱动器，这些驱动器会指向新位置。
3. 此时，您可以删除 NECATSD1 C： \ 上的原始文件夹。

故障排除

如果最终用户看到映射的驱动器带有红色 X ，请右键单击该驱动器并选择 "disconnect （断开连接） " 。注销并重新登录驱动器将正确存在。[]

Copyright Information

Trademark Information