

使用 Azure Recovery Services 实现数据安全

2019 年 1 月

Bespın Global

目录

一、Microsoft Azure Backup 介绍.....	3
二、使用 Recovery Services 备份 Azure VM.....	6
三、使用 Recovery Services 恢复 Azure VM.....	15

一、Microsoft Azure Backup 介绍

在所有企业中，我们所熟知的 IT 的最重要资产并不是机房里机架上的服务器、存储、交换机、路由器等硬件设备，而是存储了多年的企业大量的业务数据。因此，在涉及到保护企业业务数据时，IT 管理员时常需要完全备份或者增量备份企业所有数据。传统的，企业可能需要购买大量的存储设备以便存储数据，但是在云计算出现之后，这样的情况彻底发生了转变，基于云的备份解决方案能够提供可靠、廉价且可扩展的解决方案，其资本投入为零，可将运营费用降到最低。

Azure Backup 是基于 Azure 的服务，可用于 Backup（或保护）和还原 Microsoft 云端数据。Azure Backup 取代了现有的本地或异地 Backup 解决方案，并且是可靠、安全、高性价比的基于云的解决方案。Azure Backup 提供多个组件，可将其下载并部署到适当的计算机、服务器或云中。可根据要保护的内容选择部署的组件或代理。无论是保护本地数据还是云端数据，所有 Azure Backup 组件均可用于将数据备份到 Azure Backup 保管库中。

在中国，通过中国东部（上海）和中国北部（北京）两个数据中心为用户的数据保驾护航。Azure Backup 与 Windows Server 和 System Center 平台一同帮助您将业务数据以自动化的方式备份到公有云上。例如，您可以配置 Azure Backup 来将文件和数据从本地 Windows Server 系统备份到 Microsoft Azure 云中。您可以使用 Azure 恢复代理为注册的服务器指定备份计划，并且如果出现阻碍您访问物理服务器的问题时，您也可以在另外的服务器上恢复云中的文件和文件夹。如果您企业部署了 System Center Data Protection Manager (DPM)，您还可以结合使用 SCDPM 和 Microsoft Azure 备份服务来保护数据。例如，您无需再将主要 DPM 服务器备份到磁盘或本地的辅助 DPM 服务器，从 SCDPM2012SP1 开始，您可以使用 Azure Backup 将 DPM 服务器和这些服务器保护的数据备份到云中。

为何使用 Azure Backup?

传统的备份解决方案已演变成将云视为类似于磁盘/磁带的终结点或静态存储目标。该方法很简单，但用途有限，不能充分利用基础云平台，由此变成了一种效率低的昂贵解决方案。其他解决方案也很昂贵，因为你最终会为错误的存储类型或不需要的存储投资。其他解决方案的效率通常不高，因为它们不会提供所需的存储类型/存储量，或者管理任务需要耗费太多时间。与此相反，Azure Backup 具有以下主要优势：

自动存储管理 - 混合环境常常需要异类存储（部分在本地，部分在云）。通过 Azure Backup，使用本地存储设备时无需付费。Azure Backup 会自动分配和管理备份存储，且采用即用即付模型。即用即付是指只需为所用的存储付费。

无限缩放 - Azure Backup 利用 Azure 云的基础功能和无限缩放功能实现高可用性 - 无需维护或监视开销。可设置警报来获取相关事件信息，但无需担忧云数据的高可用性。

多个存储选项 - 高可用性的一个方面是存储复制。Azure Backup 提供两种类型的复制：本地冗余存储和异地冗余存储。根据需要选择 Backup 存储选项：

- 本地冗余存储 (LRS) 将同一区域的配对数据中心内的数据复制三次（创建三个数据副本）。LRS 是一个低成本选项，可在本地硬件故障时保护数据。
- 异地冗余存储 (GRS) 将数据复制到源数据主位置数英里之外的次要区域中。GRS 的成本比 LRS 的高，但 GRS 可让数据更为持久，即使出现区域性中断也是如此。

无限制的数据传输 - Azure Backup 不会限制传输的入站或出站数据量。Azure Backup 也不会对传输的数据收费。但如果使用 Azure 导入/导出服务来导入大量数据，则入站数据将产生相关费用。有关此费用的详细信息，请参阅 Azure Backup 中的脱机 Backup 工作流。出站数据是指还原操作期间从 Backup 保管库传输的数据。

数据加密 - 该服务允许在公有云中安全地传输和存储数据。加密通行短语存储在本地, 绝不会传输或存储到 Azure 中。如有必要还原任何数据, 只需具有加密通行短语或密码即可。

应用程序一致的 Backup - 无论是 Backup 文件服务器、虚拟机还是 SQL 数据库, 都需要知道恢复点具有还原 Backup 副本所需的全部数据。Azure Backup 提供了应用程序一致的 Backup, 确保了还原数据时无需额外的修补程序。还原应用程序一致的数据可减少还原时间, 使得可快速恢复到运行状态。

长期保留 - 可使用 Azure 实现短期和长期保留, 无需将 Backup 副本从磁盘转到磁带中, 也无需将磁带移到异地位置。Azure 不会限制 Backup 或恢复服务保管库中数据的保留时间长度。可以根据需要设置数据在保管库中的保留时间。Azure Backup 的限制为每个受保护实例仅限 9999 个恢复点。

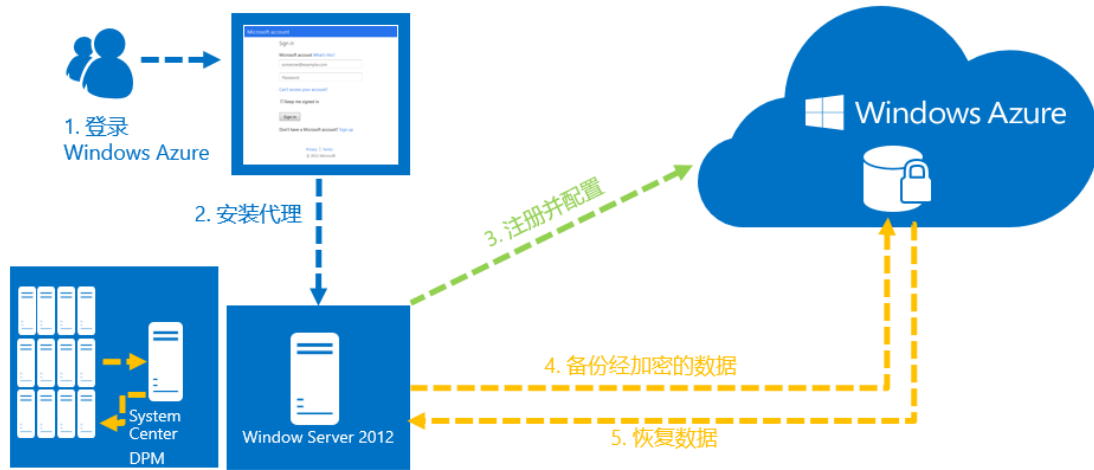
应使用哪些 Azure Backup 组件?

如果不确定哪个 Azure Backup 组件适合你的企业需求, 下表列出了每个组件可保护的内容。Azure 门户提供了一个内置向导, 可引导你选择要下载和部署的组件。该向导是恢复服务保管库创建的一部分, 可引导你完成相关步骤来选择 Backup 目标和选择要保护的数据或应用程序。

组件	优点	限制	受保护内容	Backup 存储的位置
Azure Backup(MARS) 代理	<ul style="list-style-type: none"> ● 将文本和文件夹 Backup 到物理或虚拟 Windows OS (VM 可以在本地或在 Azure 中) ● 无需单独的 Backup 服务器 	<ul style="list-style-type: none"> ● 每天 Backup 三次 ● 不感知应用程序; 仅支持文件、文件夹和卷级别的还原, ● 不支持 Linux 	文件、文件夹	Azure BackupBackup 保管库
System Center DPM	<ul style="list-style-type: none"> ● 应用程序感知快照 (VSS) ● 在 Backup 时间上完全灵活 ● 恢复粒度 (全部) ● 可使用 Azure Backup 保管库 ● Hyper-V 和 VMware VM 对 Linux 的支持 	无法 Backup Oracle 工作负荷	<ul style="list-style-type: none"> ● 文件、 ● 文件夹、 ● 卷、 ● VM、 ● 应用程序、 ● 工作负荷 	<ul style="list-style-type: none"> ● Azure Backup 保管库 ● 本地附加磁盘 ● 磁带 (仅限本地)

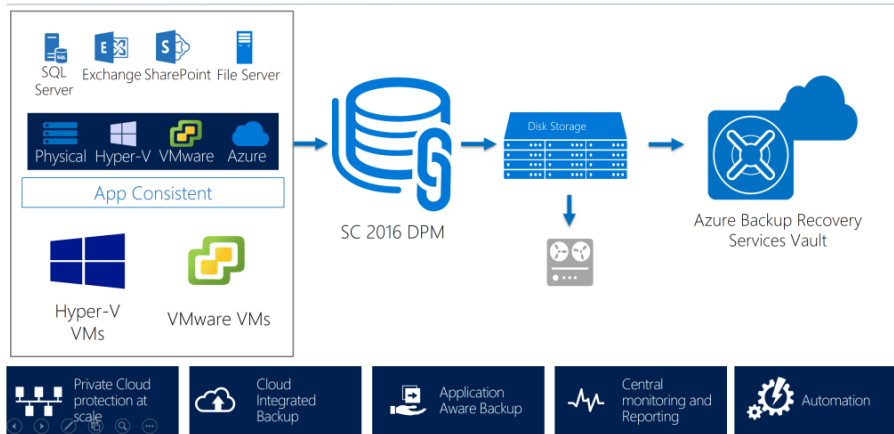
	<ul style="list-style-type: none"> ● 使用 DPM 2012 R2 Backup 和还原 VMware VM 			
Azure Backup Server	<ul style="list-style-type: none"> ● 应用感知快照 (VSS) ● 在 Backup 时间上完全灵活 ● 恢复粒度 (全部) ● 可使用 Azure Backup 保管库 ● Hyper-V 和 VMware VM 对 Linux 的支持 ● Backup 和还原 VMware VM ● 不需要 System Center 许可证 	<ul style="list-style-type: none"> ● 无法 Backup Oracle 工作负荷。 ● 始终需要实时 Azure 订阅 ● 不支持磁带 Backup 	<ul style="list-style-type: none"> ● 文件、 ● 文件夹、 ● 卷、 ● VM、 ● 应用程序、 ● 工作负荷 	<ul style="list-style-type: none"> ● Azure Backup 保管库 ● 本地附加磁盘
Azure IaaS VM Backup	<ul style="list-style-type: none"> ● 针对 Windows/Linux 的本地 Backup ● 无需安装特定代理 ● 无需使用 Backup 基础结构进行结构级 Backup 	<ul style="list-style-type: none"> ● 每天 Backup VM 一次 ● 仅在磁盘级还原 VM ● 无法本地 Backup 	<ul style="list-style-type: none"> ● 仅在磁盘级还原 VM ● 所有磁盘 (使用 PowerShell) 	<ul style="list-style-type: none"> ● Azure Backup 保管库

下图是使用 Microsoft Azure Backup 备份企业内部数据的过程。



System Center DPM 如下

System Center DPM Overview

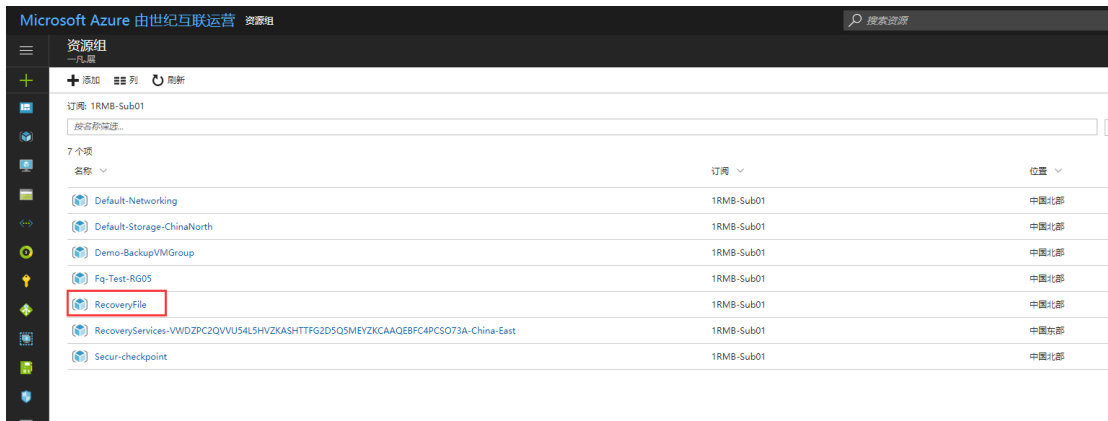


二、使用 Recovery Services 备份 Azure VM

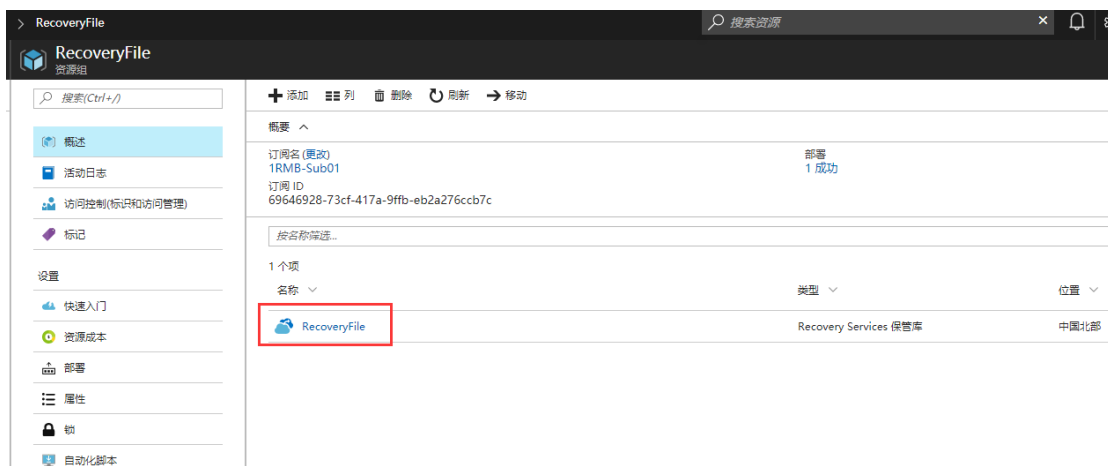
登陆 Azure China 门户网站: <https://portal.azure.cn>

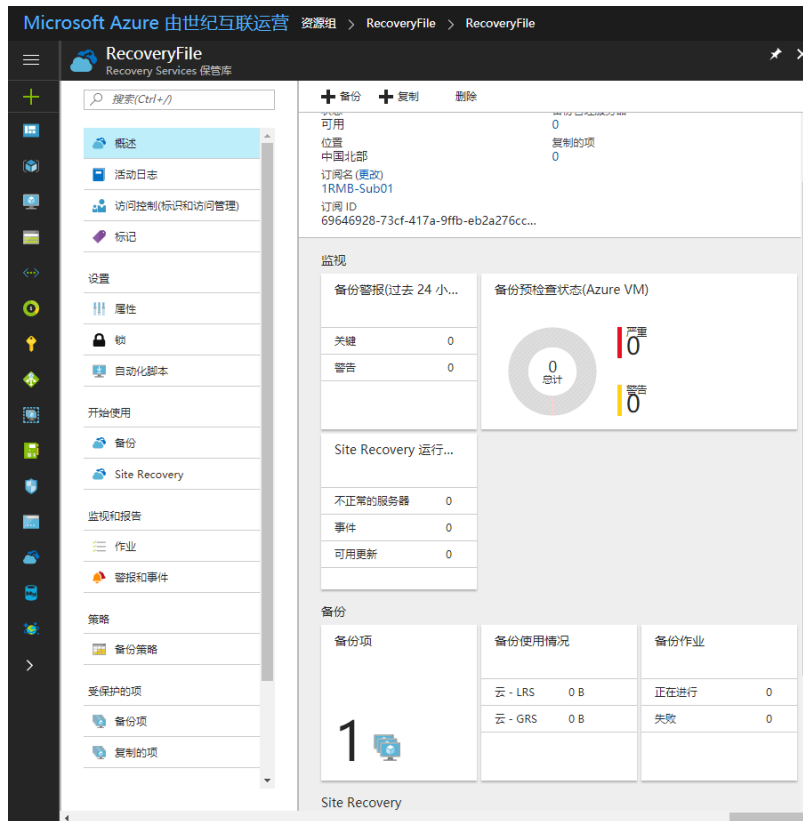


Azure 仪表盘页面，点击“资源组”，选择之前创建的 Recovery Services 保管库



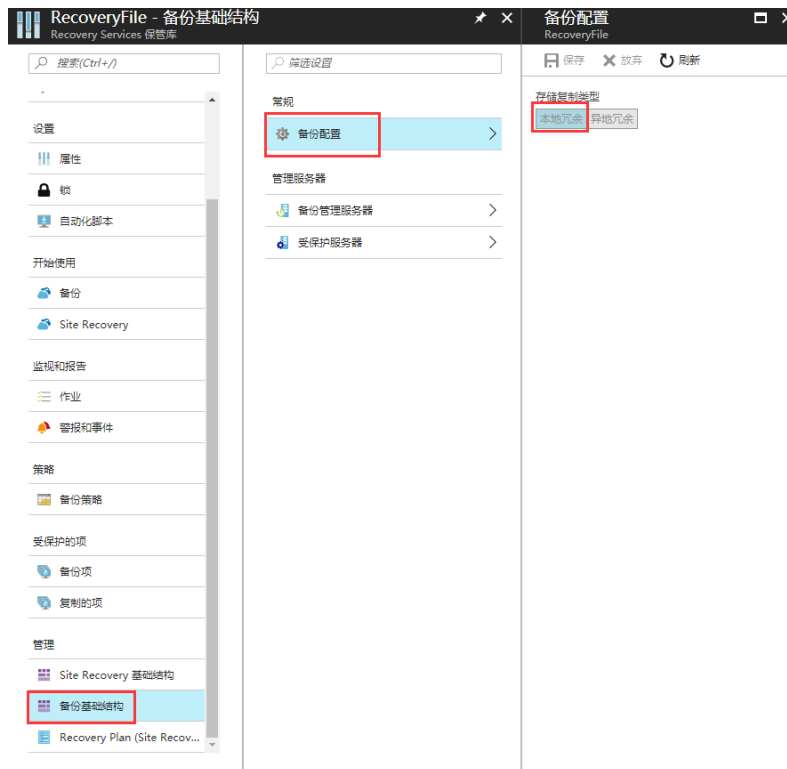
单击“RecoveryFile”选择保管库时，“设置”边栏选项卡（顶部有保管库的名称）和保管库详细信息边栏选项卡会打开。





在新保管库的“设置”边栏选项卡中，使用垂直滚动条向下滚动到“管理”部分，然后单击“备份基础结构”。此时会打开“备份基础结构”边栏选项卡。

在“备份基础结构”边栏选项卡中，单击“备份配置”打开“备份配置”边栏选项卡



默认情况下，保管库具有异地冗余存储。如果使用 Azure 作为主要备份存储终结点，请继续使用“异地冗余”。如果不使用 Azure 作为主要的备份存储终结点，则请选择“本地冗余”。

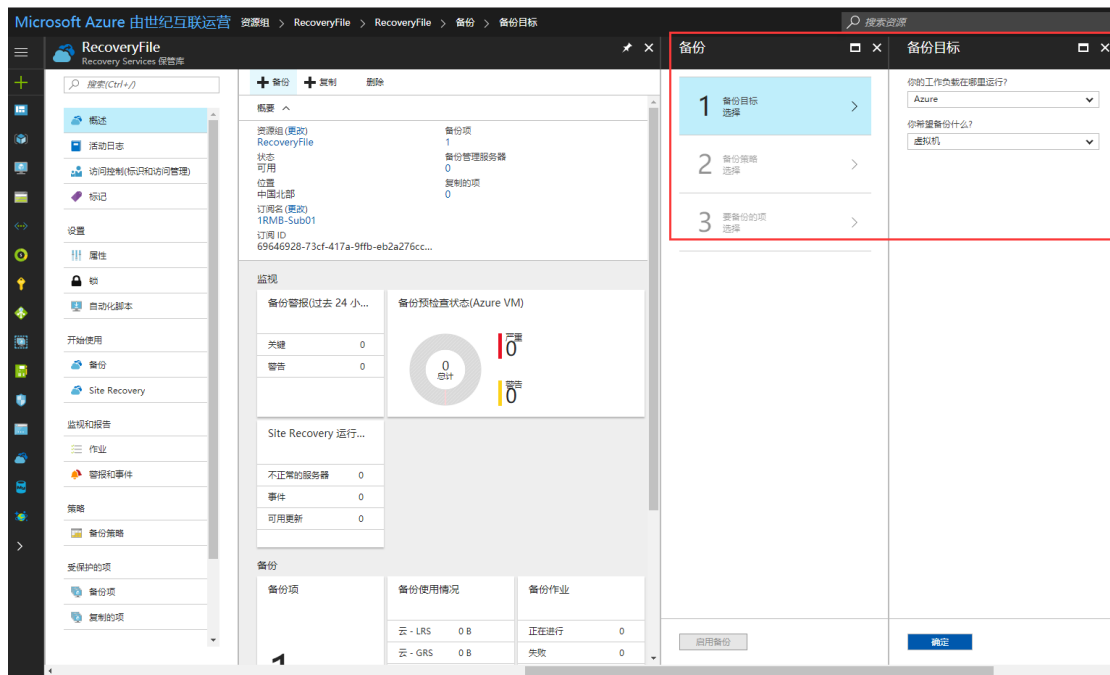
余”，减少 Azure 存储费用。

在向保管库注册 VM 前，请先执行发现过程，以确保能够识别任何添加到订阅中的新虚拟机。该过程将在 Azure 上查询订阅中的虚拟机列表和其他信息，例如云服务名称、区域等。在 Azure 门户中，方案是指要放入恢复服务保管库中的项。策略是有关恢复点创建频率和时间的计划。策略还包含恢复点的保留范围。

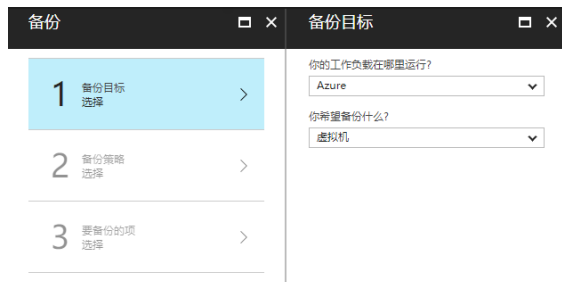
在保管库仪表板菜单中，单击“备份”打开“备份”边栏选项卡



此时会打开“备份”和“备份目标”边栏选项卡

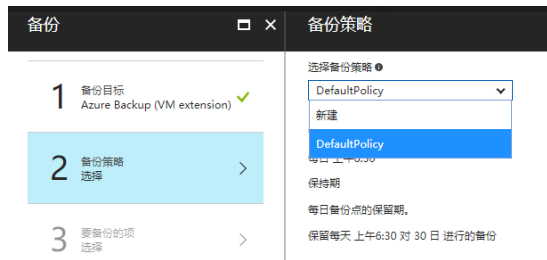


在“备份目标”边栏选项卡上，从“工作负载的运行位置”下拉菜单中选择 Azure。从“希望备份的内容”下拉列表中选择虚拟机，然后单击“确定”。

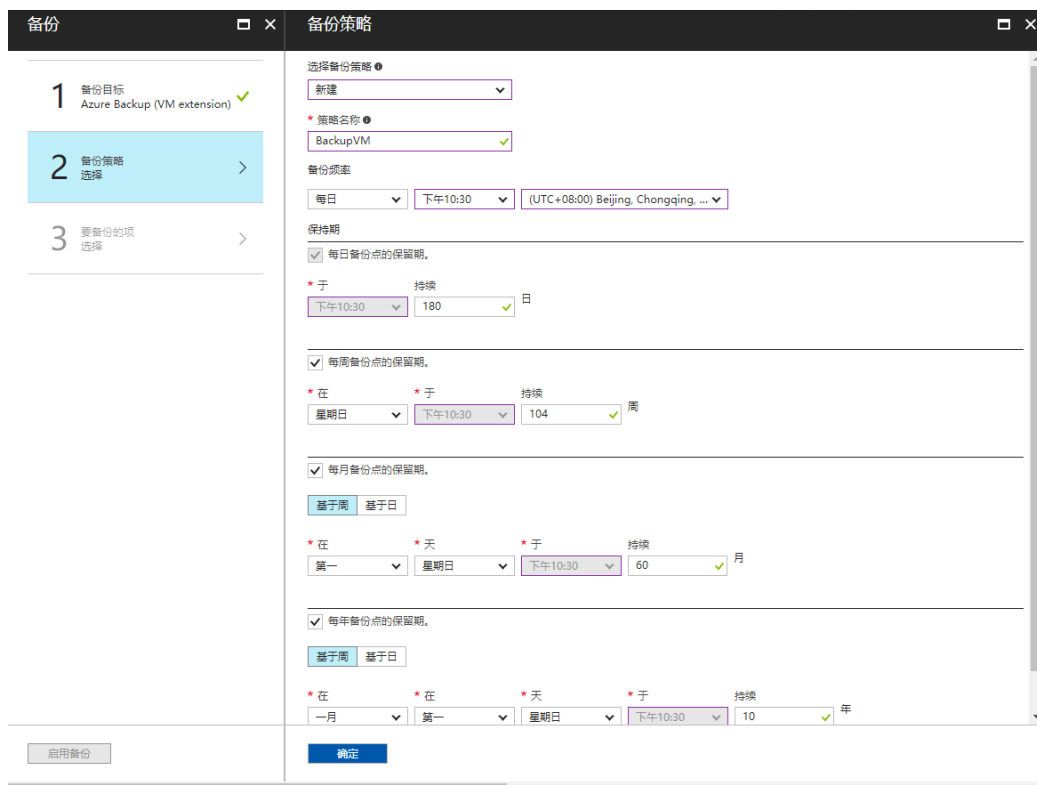


这些操作将向保管库注册 VM 扩展。随即关闭“备份目标”边栏选项卡，然后打开“备份策略”边栏选项卡。

在“备份策略”边栏选项卡中，选择要应用到保管库的备份策略。

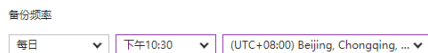


默认策略的详细信息将在下拉菜单下列出。如果要创建策略，请从下拉菜单中选择“新建”。这里选择新建。备份策略定义由数据快照创建时间和这些快照的保留时间长度构成的矩阵。定义 VM 的备份策略时，可以一天一次地触发备份作业。创建新策略时，该策略将应用到保管库。

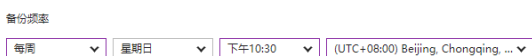


数据快照可按“每日”或“每周”的间隔来创建。使用“备份频率”下拉菜单来选择要“每日”还是“每周”创建数据快照。

如果选择“每日”间隔，可使用突出显示的控件来选择要在一天中的什么时间创建快照。若要更改小时，请取消选择该小时值，然后选择新的小时值。

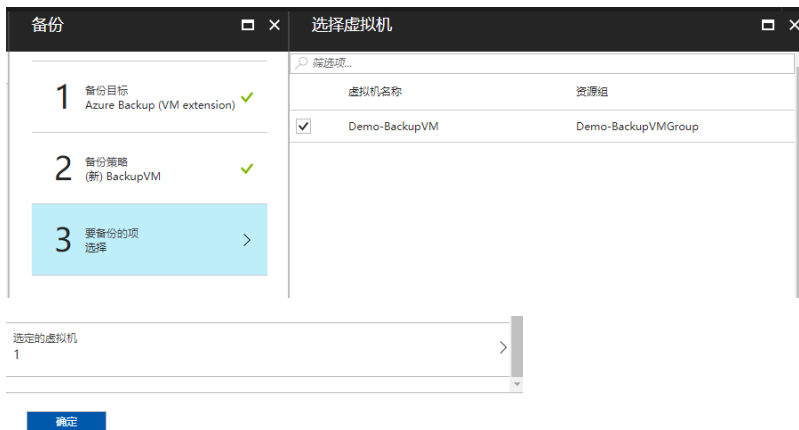


如果选择“每周”间隔，可使用突出显示的控件来选择要在哪个星期日期，以及该日期的什么时间创建快照。在日期菜单中选择一个或多个日期。在小时菜单中选择某个小时。若要更改小时，请取消选择选定的小时值，然后选择新的小时值。

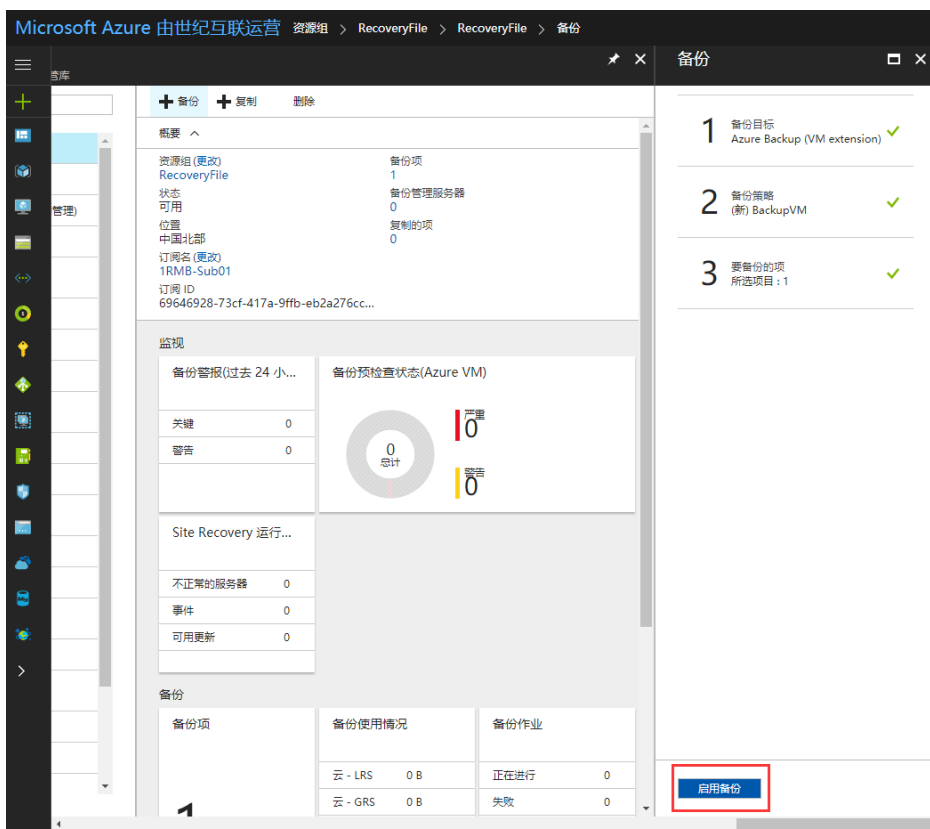


单击“确定”，将备份策略与保管库关联。

在“选择虚拟机”边栏选项卡中，选择要与指定策略关联的虚拟机，然后单击“确定”。



现在已定义保管库的所有设置，接下来将在“备份”边栏选项卡中，单击“启用备份”将策略部署到保管库和 VM。部署备份策略不会创建虚拟机的初始恢复点。



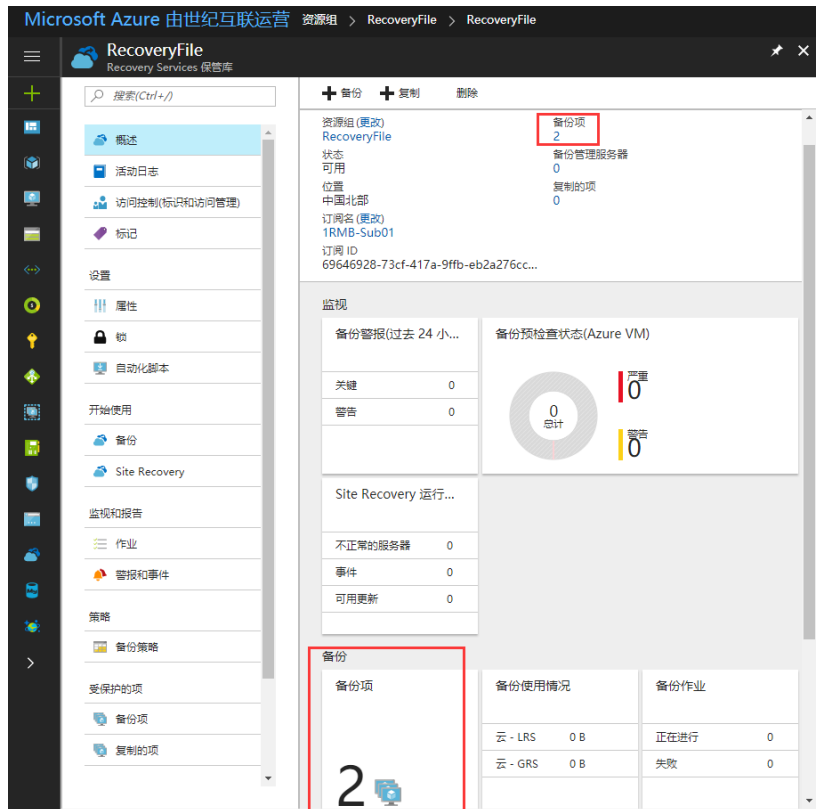
初始备份

在虚拟机上部署备份策略后，并不意味着已备份好数据。默认情况下，第一个计划的备份（在备份策略中定义）是初始备份。在执行初始备份之前，“备份作业”边栏选项卡上的

“上次备份状态”显示为“警告(等待初始备份)”。



在保管库仪表板上，单击“备份项”下的数字，或单击“备份项”磁贴



“备份项”边栏选项卡随即打开。



在“备份项”列表中，单击省略号“...”以打开上下文菜单。



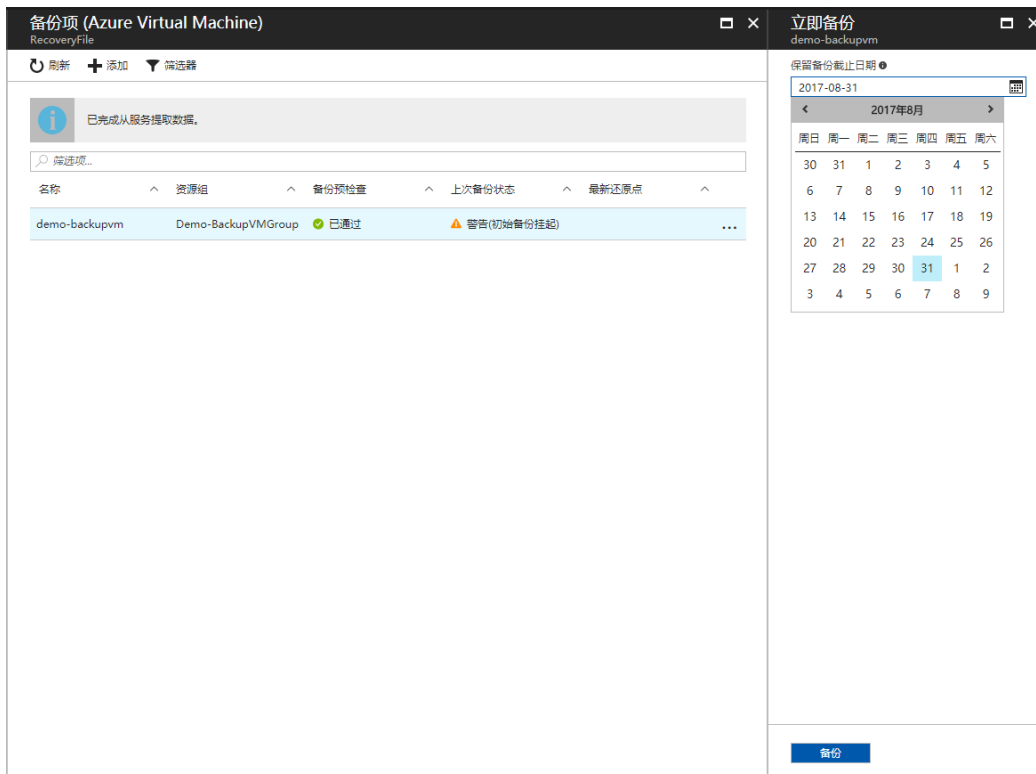
上下文菜单随即打开，在上下文菜单上，单击“立即备份”



“立即备份”边栏选项卡随即打开



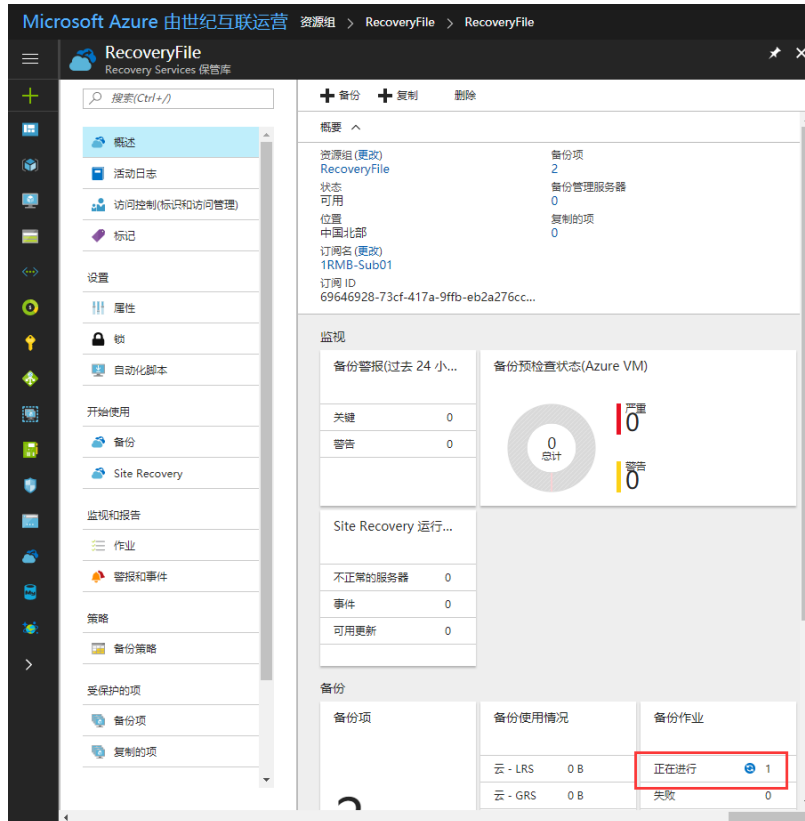
在“立即备份”边栏选项卡上，单击日历图标，使用日历控件选择保留此恢复点的最后一天，然后单击“备份”。



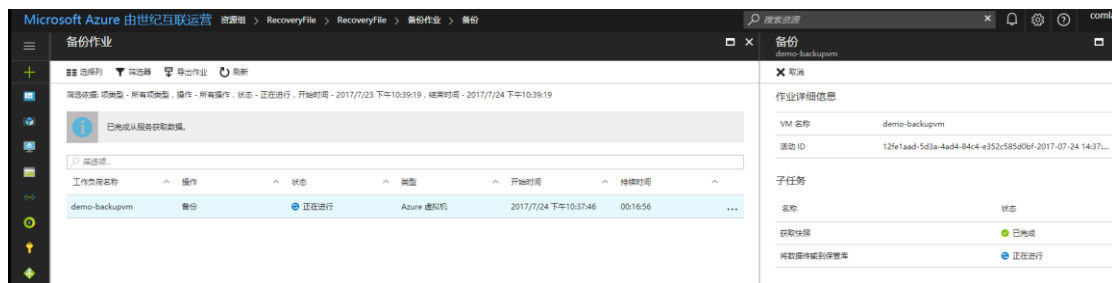
部署通知会告知你备份作业已触发，并且你可以在“备份作业”页面上监视作业的进度。创建初始备份可能需要一些时间，具体取决于 VM 的大小。



若要查看或跟踪初始备份的状态，请在保管仪表板的“备份作业”磁贴上，单击“正在进行”。



“备份作业”边栏选项卡随即打开



在“备份作业”边栏选项卡中，可以看到所有作业的状态。请查看 VM 的备份作业仍在进行中，还是已完成。完成备份作业后，状态将变为“已完成”。



注意：在执行备份操作的过程中，Azure 备份服务将向每个 VM 中的备份扩展发出一条命令，刷新所有写入并取得一致快照。

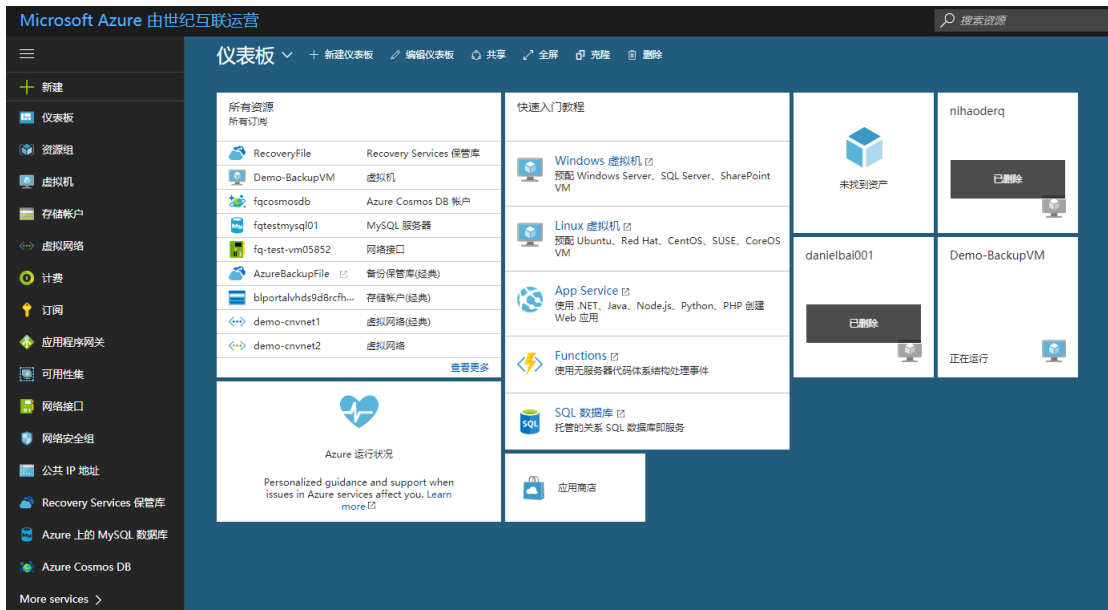
关于使用 Azure Backup 备份 Azure VM，还需要注意：

- 不支持备份超过 16 个数据磁盘的虚拟机。
- 不支持备份带 4TB 磁盘的虚拟机。
- 不支持备份使用保留 IP 地址且未定义终结点的虚拟机。
- 不支持备份仅使用 BEK 加密的 VM。不支持备份使用 LUKS 加密 Linux VM。
- 不支持备份装有 Docker 扩展的 Linux 虚拟机。
- 备份数据不包括连接到 VM 的网络挂载驱动器。
- 不支持在恢复过程中替换现有虚拟机。如果在 VM 存在时尝试还原 VM，还原操作将会失败。
- 不支持跨区域备份和还原。
- 可以在 Azure 的所有公共区域中备份虚拟机（请参阅支持区域的清单）。在创建保管库期间，如果你要寻找的区域目前不受支持，则不会在下拉列表中显示它。
- 仅支持通过 PowerShell 还原属于多 DC 配置的域控制器(DC) VM。
- 仅支持通过 PowerShell 还原采用以下特殊网络配置的虚拟机。还原操作完成后，在 UI 中使用还原工作流创建的 VM 将不采用这些网络配置。采用负载均衡器配置的虚拟机（内部和外部）、使用多个保留 IP 地址的虚拟机、使用多个网络适配器的虚拟机

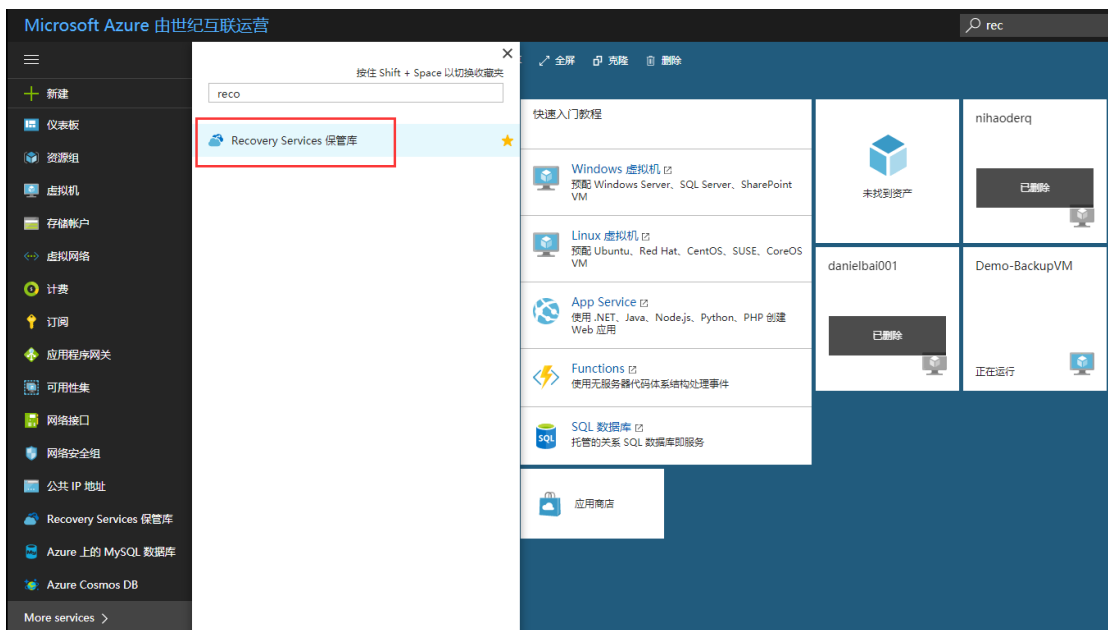
三、使用 Recovery Services 恢复 Azure VM

Azure VM 已经完成了备份，但是不小心删除了一台重要服务器，那么这个时候需要使用恢复技术，将之前备份的 Azure 恢复出来以便最大化减小业务宕机时间。本节将为大家演示如何在 Azure 中恢复 VM，并在之前的恢复点下数据不丢失。

登陆 Azure 门户网站：<https://portal.azure.cn>



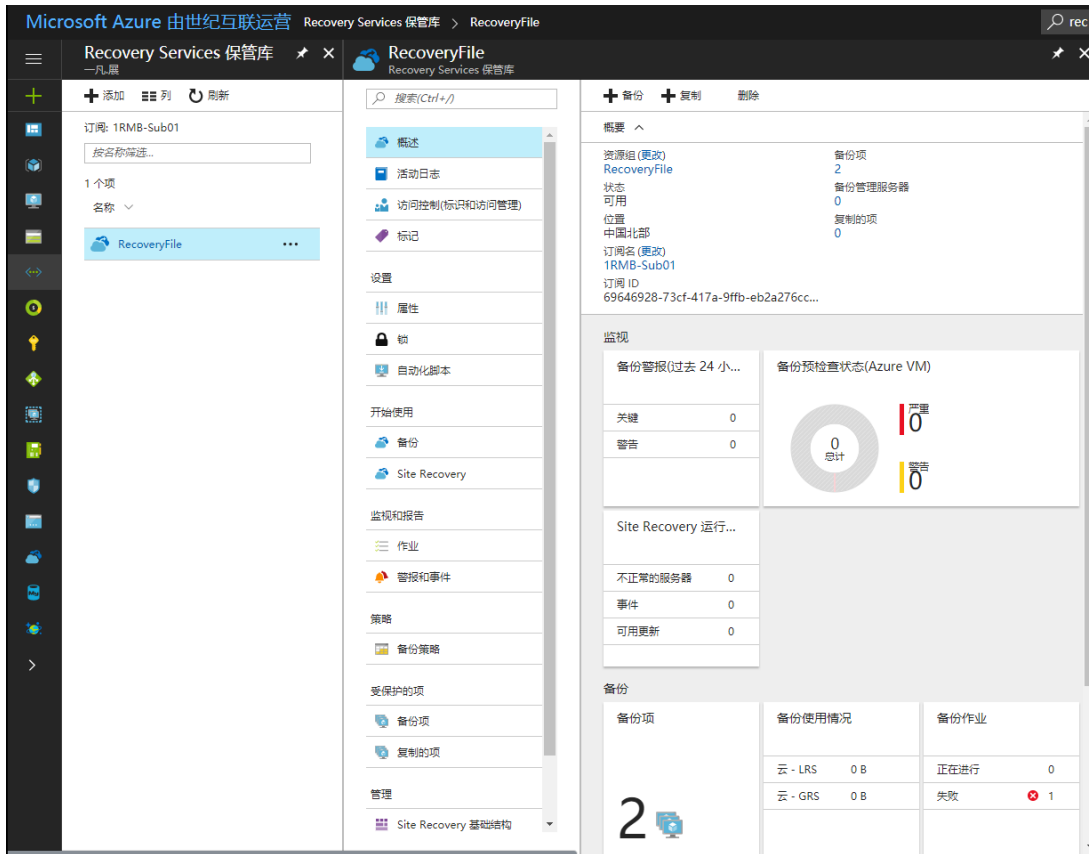
在 Azure 菜单中，单击“浏览”，然后在服务列表中键入“恢复服务”。服务列表会根据键入的内容调整。出现“恢复服务保管库”时，请选择它。



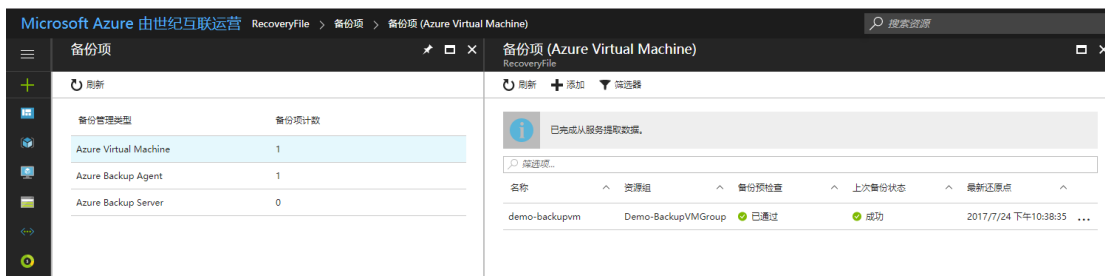
随后将显示订阅中保管库的列表



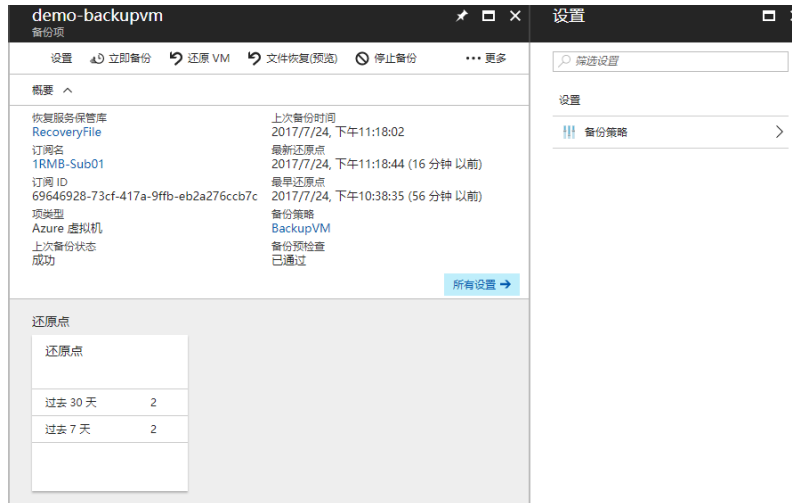
从列表中选择与要还原的 VM 关联的保管库。当你单击该保管库时，其仪表板将会打开



在“备份项”磁贴上，单击“Azure 虚拟机”，以显示与保管库关联的 VM



从列表中选择 一个 VM 以打开仪表板。在 VM 仪表板中，默认会打开包含“还原点”磁贴的“监视”区域



在 VM 仪表板菜单中，单击“还原”

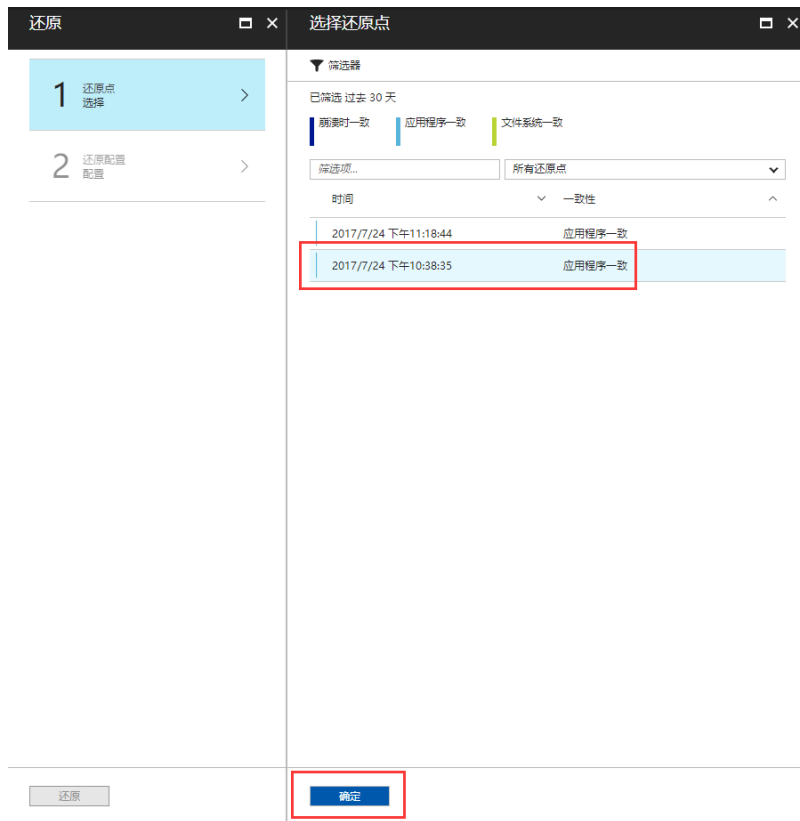


在“还原”边栏选项卡中，单击“还原点”，打开“选择还原点”边栏选项卡



默认情况下，对话框会显示过去 30 天的所有还原点。使用“筛选器”可更改显示的还原点的时间范围。默认情况下，将显示所有一致性还原点。修改“所有还原点”筛选器，以选择特定的还原点一致性。在 Azure 中“还原点一致性”，主要有崩溃一致还原点，应用程序一致还原点，文件系统一致还原点，所有还原点。

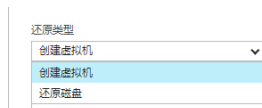
选择一个还原点并单击“确定”。



“还原”边栏选项卡将显示已设置还原点。



设置还原点后，“还原”边栏选项卡中会自动打开“还原配置”，在 Azure 中，还原类型有两种：创建虚拟机、还原磁盘



从还原点创建新的 VM

选择“创建虚拟机”，需要在“还原配置”边栏选项卡中，输入或选择以下每个字段的值

- 虚拟机名称 - 提供 VM 的名称。此名称对于资源组（适用于 Resource Manager 部署型 VM）或云服务（适用于经典 VM）必须是唯一的。如果虚拟机已存在于订阅中，则不能替换该虚拟机。

- 资源组 - 使用现有资源组，或创建新组。如果要还原经典 VM，请使用此字段来指定新云服务的名称。创建新资源组/云服务时，该名称必须全局唯一。通常，云服务名称与面向公众的 URL 相关联 - 例如: [cloudservice].cloudapp.net。如果你尝试使用已用的云资源组/云服务名称，Azure 将为资源组/云服务分配与 VM 相同的名称。Azure 将显示不与任何地缘组关联的资源组/云服务和 VM。
- 虚拟网络 - 创建 VM 时，请选择虚拟网络(VNET)。该字段提供与订阅关联的所有 VNET。VM 的资源组显示在括号中。
- 子网 - 如果 VNET 包含子网，则默认情况下会选择第一个子网 如果有其他子网，请选择所需的子网。
- 存储帐户 - 此菜单列出与恢复服务保管库位于相同位置的存储帐户。不支持区域冗余的存储帐户。如果没有与恢复服务保管库位于同一位置的存储帐户，必须在开始还原操作之前创建一个存储帐户。存储帐户的复制类型在括号中注明。



在“还原配置”边栏选项卡中，单击“确定”完成还原配置。在“还原”边栏选项卡中，单击“还原”以触发还原操作。

demo-backupvm

备份项

设置 立即备份 还原 VM 文件恢复(预览) 停止备份 更多

概要

恢复服务保管库: RecoveryFile
 订购名: 1RMB-Sub01
 订购 ID: 69646928-73cf-417a-9ffb-eb2a276ccb7c
 项类型: Azure 虚拟机
 上次备份状态: 成功

上次备份时间: 2017/7/24, 下午11:18:02
 最新还原点: 2017/7/24, 下午11:18:44 (16 分钟 以前)
 最早还原点: 2017/7/24, 下午10:38:35 (56 分钟 以前)

备份策略: BackupVM
 备份预检查: 已通过

[所有设置](#)

还原点

还原点	数量
过去 30 天	2
过去 7 天	2

还原

- 1 还原点
2017/7/24 下午10:38:35 ✓
- 2 还原配置
已配置 ✓

还原

通知

消除: 信息 已完成 全部

正在触发 demo-backupvm 的还原 正在运行
 正在进行触发还原。

查看恢复状态

Microsoft Azure 由世纪互联运营 备份作业 > 还原

筛选: 选择列 筛选器 导出作业 刷新

筛选依据: 项类型, 所有项类型, 操作, 所有操作, 状态, 所有状态 - 2017/7/23 下午11:43:49, 结束时间 - 2017/7/24 下午11:43:49

已成功从服务器获取数据。

工作项名称	操作	状态	类型	开始时间	持续时间
demo-backupvm	还原	正在运行	Azure 虚拟机	2017/7/24 下午11:42:58	00:00:51
demo-backupvm	备份	已完成	Azure 虚拟机	2017/7/24 下午11:18:02	00:15:12
demo-backupvm	备份	失败	Azure 虚拟机	2017/7/24 下午10:42:20	00:12:03
demo-backupvm	备份	已完成	Azure 虚拟机	2017/7/24 下午10:37:46	00:25:13
demo-backupvm	配置备份	已完成	Azure 虚拟机	2017/7/24 下午10:29:36	00:01:24
demo-backupvm	还原	已完成	文件和文件夹	2017/7/24 下午10:00:20	00:00:40
demo-backupvm	还原	已完成	文件和文件夹	2017/7/24 下午9:44:30	00:05:02
demo-backupvm	备份	已完成	文件和文件夹	2017/7/24 下午9:30:47	00:00:41

还原 demo-backupvm

取消

作业详细信息

作业类型: 将 VM 恢复到备用位置

源 VM 名称: demo-backupvm

目标 VM 名称: DEMO-RecoveryVM

目标 VNet 名称: Group Demo-BackupVMGroup Demo-BackupVMGroup-net

目标存储帐户名称: demobackupvmgroup185

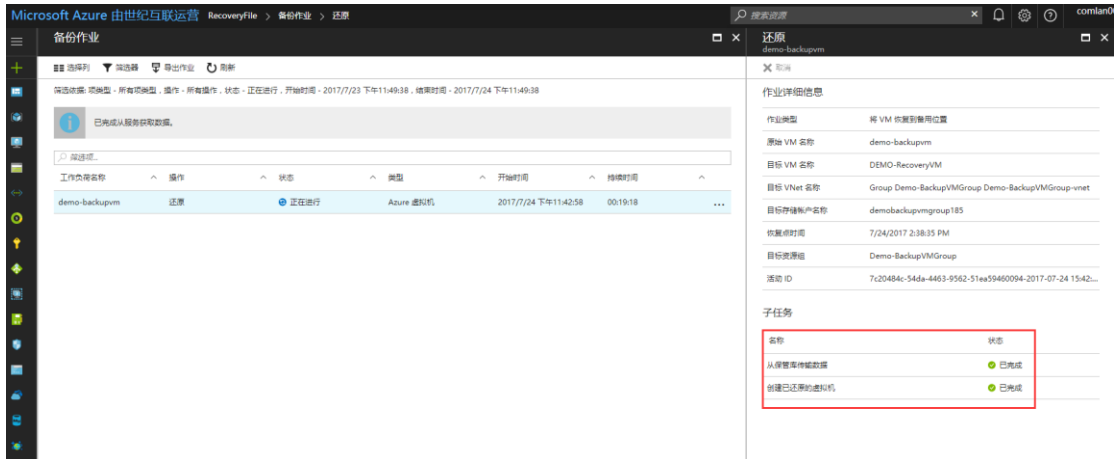
恢复点时间: 7/24/2017 2:38:35 PM

目标资源组: Demo-BackupVMGroup

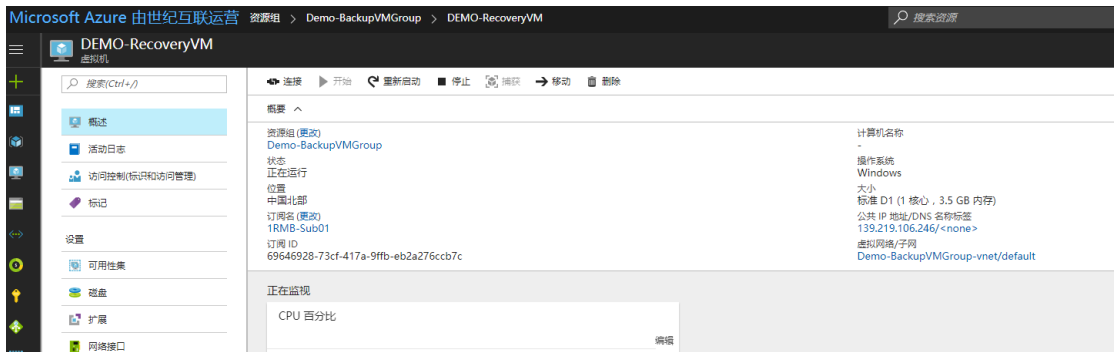
项 ID: 7c20484c-54da-4463-9562-51ea59460094-2017-07-24 15:42...

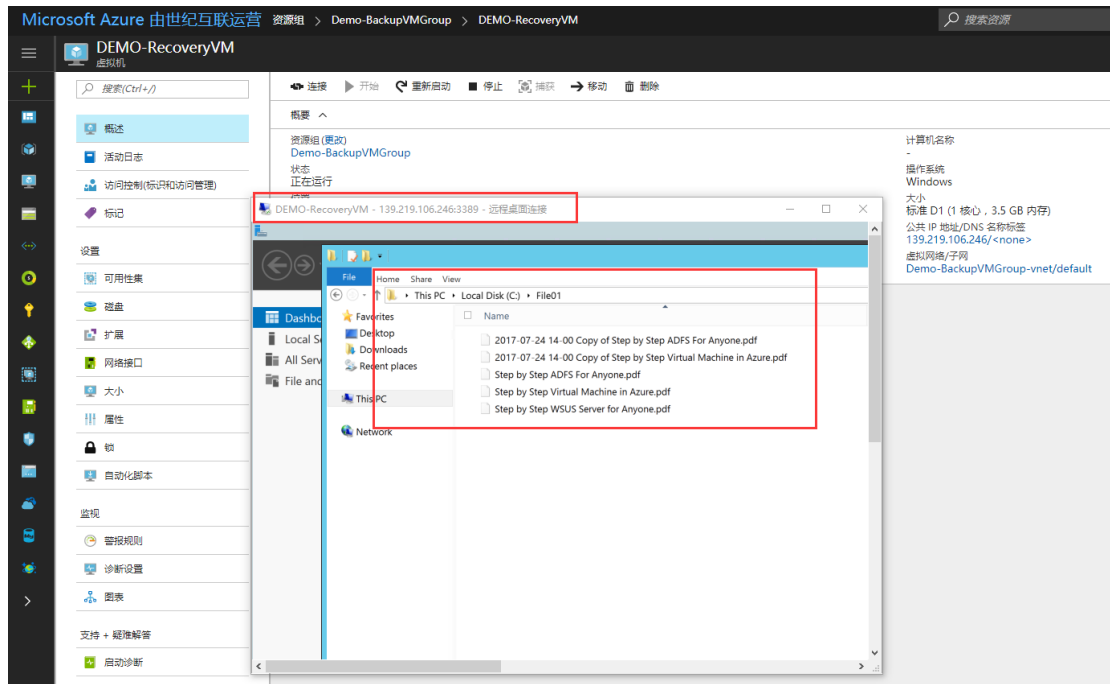
子任务

名称	状态
从保管库检索数据	正在运行
创建已还原的虚拟机	未开始



资源组“Demo-BackupVMGroup”下查看恢复的 VM



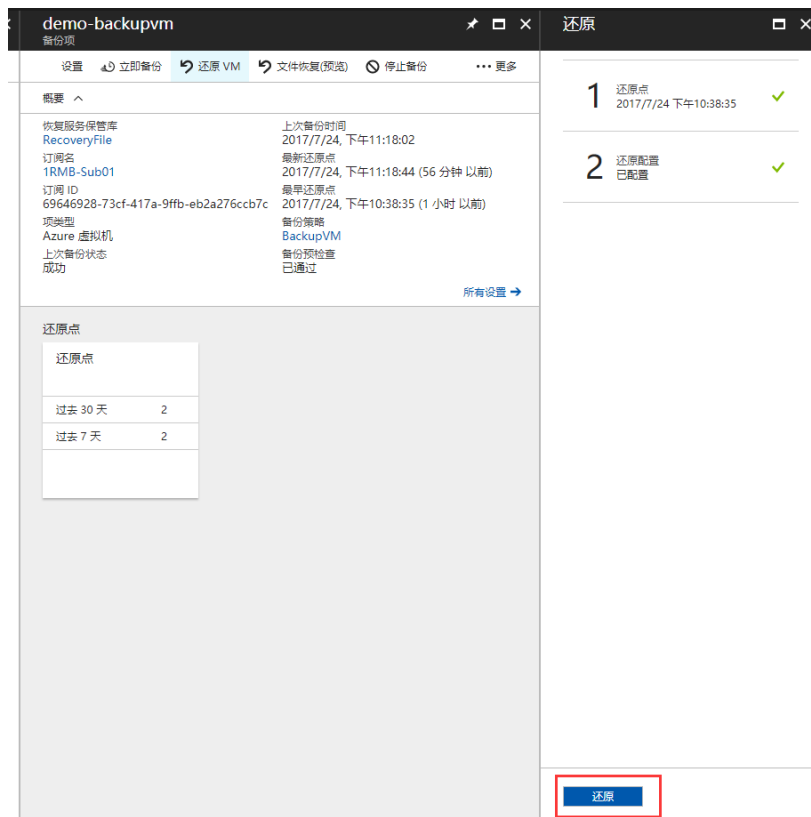


还原备份磁盘

如果要自定义从备份磁盘而不是还原配置边栏选项卡显示的磁盘中创建的虚拟机，请选择“还原磁盘”作为“还原类型”的值。如果选择此选项，需要提供备份中磁盘要复制到的存储帐户。选择存储帐户时，可选择与恢复服务保管库共享相同位置的帐户。不支持区域冗余的存储帐户。如果没有与恢复服务保管库位于同一位置的存储帐户，必须在开始还原操作之前创建一个存储帐户。存储帐户的复制类型在括号中注明。

在“还原配置”边栏选项卡中，单击“确定”完成还原配置。在“还原”边栏选项卡中，单击“还原”以触发还原操作。





还原后的注意事项

- 如果使用基于 cloud-init 的 Linux 分发 (如 Ubuntu)，出于安全原因，还原后将阻止密码。请在还原的 VM 上使用 VMAccess 扩展重置密码。建议在这些分发上使用 SSH 密钥以避免还原后重置密码。
- 将会安装存在于备份配置期间的扩展，但不会启用这些扩展。如果发现任何问题，请重新安装扩展。
- 如果备份的 VM 具有静态 IP，则还原的 VM 将具有动态 IP 以避免在创建还原的 VM 时发生冲突。
- 还原的 VM 将不会设置可用性集。使用已还原的磁盘从 PowerShell 或模板创建 VM 时，建议使用还原磁盘选项和添加可用性集。