

第 7 章

高可用性和灾难恢复概览

(Overview of high availability and disaster recovery)

目录:

单元概述 (Module Overview)	1
定义可用性级别 (Defining levels of availability)	2
使用 Hyper-V 虚拟机规划高可用性和灾难恢复解决方案(Planning high availability and disaster recovery solutions with Hyper-V virtual machines)	10
实验: 规划和实现高可用性和灾难恢复解决方案 (Planning and implementing a high availability and disaster recovery solution)	19
使用 Windows Server Backup 进行备份和还原 (Backing up and restoring by using Windows Server Backup)	23
Windows Server 2016 高可用性和故障转移群集 (High availability with failover clustering in Windows Server 2016)	26
单元复习和作业 (Module Review and Takeaways)	31

单元概述 (Module Overview)

IT 解决方案是大多数组织中的关键业务工具。关键服务的短暂中断往往会导致 IT 部门声名不佳，并且可能导致销售损失或企业声誉受损。提供高可用性对于希望为其用户提供连续服务的任何组织都很重要。故障转移群集是 Windows Server 2016 中的主要技术之一，可为各种应用程序和服务提供高可用性。在本单元中，您将了解故障转移群集，故障转移群集组件和实施技术。

定期备份 Windows Server 数据是您常规 Windows Server 管理的一个重要组成部分。数据备份使您能够在数据丢失，损坏或出于测试目的的情况下，在以后恢复数据。备份 Windows Server 2016 是一个相对简单的任务，但是备份硬件，备份窗口持续时间和恢复约束等因素决定了备份策略。服务级别协议 (SLA) 在确定备份方案中起着重要作用。例如，如果您的 Windows 服务器的 SLA 指定操作系统服务在灾难期间不能停机超过一小时，则必须设计备份策略以执行此目标。

本单元介绍 Windows Server 2016 中内置的高可用性技术以及影响高可用性解决方案的一些外部因素。此外，该单元描述了用于在 Windows Server 2016 中保护数据的备份和还原技术。

目标 (Objectives)

完成本单元后，您将能够：

- 定义可用性级别。
- 使用 Hyper-V 虚拟机规划高可用性和灾难恢复解决方案。
- 使用 Windows Server Backup 备份和还原数据。
- 在 Windows Server 2016 中使用故障转移群集定义高可用性。

第 1 课

定义可用性级别 (Defining levels of availability)

高可用性有助于确保 Windows Server 操作系统可以在单个服务器或甚至多个服务器发生故障时生存。当应用程序需要高可用性时，您必须考虑的不仅仅是应用程序组件。应用程序所依赖的所有基础架构和服务也必须高度可用。在规划高可用性时，请考虑以下附加组件。

例如，组织可能部署多个服务器运行提供高可用性的适当的应用程序。但是，如果将所有服务器连接到单个网络交换机，则网络交换机将会是单点故障。如果交换机不可操作，则没有客户端计算机可以连接到任何服务器，这使得解决方案不是高可用的。

课程目标 (Lesson Objectives)

完成本课后，您将能够：

- 描述高可用性。
- 描述连续可用性。
- 描述业务连续性。
- 创建灾难恢复计划。
- 描述网络的高可用性。
- 描述存储的高可用性。
- 描述高可用性计算机或硬件功能。

什么是高可用性 (What is high availability?)

IT 解决方案的高可用性 (high availability) 描述了需要冗余的组件和技术，以便解决方案在任何解决方案组件发生故障的情况下继续工作。设计解决方案的 IT 顾问必须确保解决方案无单点故障，这意味着无论哪个解决方案组件发生故障，解决方案都能继续工作，并且为用户提供数据和服务。

数据中心技术架构 (Data center infrastructure)

存储服务器的房间必须有足够的电源和冷却能力，并且该容量也必须高度可用。您可以通过确保在电力公司出现故障时提供备用电源（例如电池或发电机），从而实现电力高度可用。通过使用具有足够容量的多个冷却单元，可以使冷却容量高度可用，以在一个单元出现故障时保持数据中心冷却。在灾难性故障的情况下，您可以使用备用数据中心位置。

应用程序的所有部分及其依赖的基础设施必须高度可用：

- 数据中心基础设施
- 服务器硬件
- 存储
- 网络基础设施
- 互联网
- 网络服务

服务器硬件 (Server hardware)

为了使服务器硬件具有高可用性，必须有冗余组件 (redundant components)。冗余组件可以包括电源，网络适配器，处理器和存储器。纠错码 (Error-correction code ， ECC) 存储器有助于解决轻微的内存错误。

存储（Storage）

要使存储在单个服务器上高度可用，您可以使用独立磁盘冗余阵列（RAID）。RAID 使用奇偶校验信息（parity information），以确保服务器可以承受至少一个硬盘驱动器的丢失，而不会丢失任何数据。如果有多个服务器可用，您可以在服务器之间复制数据。这使得数据能够承受整个服务器的丢失，而不仅仅是硬盘驱动器。

网络基础架构（Network infrastructure）

要使局域网（LAN）高度可用，必须引入冗余组件。在 LAN 内，这通常意味着冗余交换机。即使是中等价位的交换机也包括冗余配置。要使任何单个计算机的网络连接能够容错，必须在计算机上配置冗余网络接口卡。这是大多数中级和高级服务器的标准功能。广域网（WAN）的高可用性通常是 WAN 服务提供商的责任。但是，如果您使用专用链路用于 WAN，则可以通过 WAN 创建冗余路径。

英特网连接性（Internet connectivity）

对于高可用性 Internet 访问，您必须具有冗余的 Internet 连接。理想情况下，您应该使用两个不同的 Internet 服务提供商（ISP）和两种不同的物理连接方法。例如，一个 ISP 可以是基于陆地的，而另一个 ISP 是无线的。如果使用这些方法，影响一个 ISP 的问题不太可能影响另一个。许多防火墙和路由器能够使用一个连接用于 Internet 连接，如果主服务失败，则可以故障切换到另一个连接。对于传入电子邮件，您必须使用多个邮件交换（MX）资源记录，其中一个记录指向每个 ISP 分配的 IP 地址。

网络服务（Network services）

Active Directory 域服务（Active Directory Domain Services，AD DS）和域名系统（Domain Name System，DNS）服务是必须高度可用以支持组织中的基础设施服务的两种服务。要使 AD DS 服务器具有高可用性，您应该具有多个域控制器（domain controller）和全局编录服务器（global catalog server）。根据位置的大小，多个域控制器和全局目录服务器可以驻留在单个位置。要使内部 DNS 服务器具有高可用性，您必须具有多个 DNS 服务器，并在它们之间同步 DNS 信息。默认情况下，AD DS 的 DNS 区域将在林中的所有 DNS 服务器之间进行集成和复制。

什么是连续可用性（What is continuous availability?）

连续可用性（continuous availability）依赖技术和流程，确保 IT 解决方案在故障情况和计划维护停机的情况下继续工作。由于维护程序，高可用性与硬件升级或更新操作系统而导致的计划不可用性相比，持续可用性意味着解决方案应在计划停机期间继续工作。

要为您的组织提供持续可用性，您应该制定策略以实现连续可用性，方法是收集以下数据：

- 业务影响分析（business impact analysis）。业务影响分析决定了组织的关键业务流程及其中断或故障可能导致的潜在损害或损失。
- 风险分析（risk analysis）。风险分析识别风险及其发生概率。风险分析还可以识别单个故障点，例如组织的磁盘驱动器，网络交换机，存储或电源。

有一系列策略可用于实现持续可用性。每个策略是针对不同的应用程序。持续可用性在服务器维护任务期间提供对数据和服务的访问，因此客户端不会中断。因此，组织中的每个管理员（例如 Exchange 管理员，SQL Server 管理员和 SharePoint 管理员）都必须通过使用维护和更新服务器和应用程序而不影响用户体验来规划连续可用性策略。

提供连续可用性：

- 执行业务影响分析
- 执行风险分析
- 执行应用程序特定分析
- 为不同应用程序创建不同的连续可用性策略

海量视频题库 <http://www.it-ebooks.com> QQ:5565462



注意：持续可用性需要完全连续性的供应策略，并且通常具有高成本。因此需要针对影响和风险很大的关键业务应用实施持续可用性。

什么是业务连续性(What is business continuity?)

通常情况下，需要在定制业务规划的初始阶段就着手分析业务连续性(business continuity)。业务规划要求根据组织的结构而有所不同。

以下是您的业务连续性计划应考虑的几个需求：

- IT 系统（包括硬件和软件）的 SLA。
- 恢复人员的联系信息和技术背景。
- 辅助站点，您可以从中访问关键业务功能的关键应用程序和应用程序数据。
- 临时解决方案（workaround solutions.）
- 您的应用程序允许的最长停机时间。

业务连续性规划的要求应包括：

- IT 系统的 SLA
- 指定的恢复人员的联系信息和技术背景
- 一个辅助站点
- 临时解决方案
- 应用程序允许的最大中断

创建一个完整的需求列表不仅需要 IT 员工，还要包括业务经理和其他高层决策者。业务经理应该了解风险，并应了解任何故障如何影响业务。业务经理还需要确定哪些应用程序对其业务至关重要，并且可能决定必须采取哪些恢复时间来帮助定义适当的备份和恢复策略。



注意：组织根据其业务基础架构和目标有不同的要求。业务连续性规划的要求不应该是静态的。相反，你应该定期评估和更新它们，通常情况下建议每隔几个月重新评估你的计划

要计划实施业务连续性的策略，应从以下各项收集数据：

- 业务影响分析。业务影响分析决定了组织的关键业务流程及其中断或故障可能导致的潜在损害或损失。
- 风险分析。风险分析识别可能的风险及其概率。此外，风险分析可识别单个故障点，例如组织的磁盘驱动器，网络交换机，存储或电源。

业务连续性策略因组织而异，基于业务需求。组织用于实现业务连续性战略的技术可以包括：

- 网络负载平衡（NLB）。
- 物理机或虚拟机上的故障转移群集。
- 应用感知的高可用性（Application-aware high availability）。
- 常规数据备份。
- 在线备份。
- 虚拟机备份。

具有关键业务 IT 基础架构的组织可能实施包括不同技术的完全连续性，高成本策略。例如，为了保护业务关键数据，一些组织可以使用 NLB 为 Web 服务器提供高可用性，使用故障转移群集为运行 Microsoft SQL Server 的服务器提供高可用性，并对磁带，磁盘和云备份服务执行数据备份，例如 Microsoft Azure Backup。此外，组织可能部署灾难恢复中心，它复制来自总部数据中心的数据，提供站点恢复能力。

其他组织可能决定部署低成本策略，在潜在影响最小或风险可接受的情况下提供保护。例如，组织可能仅执行关键数据的备份，承担服务器可能几个小时甚至一天不可用的风险。

创建灾难恢复规划 (Creating a disaster recovery plan)

为了确保您的组织从故障或灾难情形中恢复，您应该创建一个灾难恢复计划，以便以易于遵循的方式记录所有恢复过程。此外，灾难恢复计划应确保您和您的组织的人员准确地知道在发生故障后要执行的步骤。

制定恢复计划 (Developing a recovery plan)

在制定恢复计划时，请问自己以下问题：

- 应该在哪里找到恢复的数据？
- 何时应该进行恢复？
- 应该恢复哪些数据？

- 制定恢复计划包括：
 - 执行风险分析
 - 定义应恢复哪些数据
 - 定义应恢复数据的位置
 - 定义何时恢复数据
- 恢复计划应定期测试
- 恢复计划应定期评估

选择恢复那些数据 (Selecting what data to recover)

在大多数情况下，您将恢复已备份的所有内容。在某些情况下，您可能选择仅执行部分恢复以满足业务连续性目标，从而为以后的点完全恢复。这是值得考虑的，特别是如果完全恢复需要很长时间，而部分恢复可以让您的用户在短时间内恢复工作。

选择数据恢复位置 (Choosing a data-recovery location)

如果您的组织具有可替换的硬件（例如更换硬盘驱动器或整个服务器机箱），则选择恢复位置不那么复杂。

随着虚拟化的增长，当您需要执行完整的服务器恢复时，越来越不需要等待特定的硬件可用。可以对 Hyper-V 主机执行临时恢复，并使其能够虚拟地托管恢复的服务器，直到更换硬件到达时为止。这为您提供了从虚拟机迁移到物理服务器的时间。

确认何时恢复数据 (Determining when to recover data)

如果发生故障，而且您的组织与硬件供应商没有关于 24 小时更换组件的协议，则必须等待组件到达。这可能会影响您的 RTO（recovery time objective）。或者，您可以执行部分恢复到备用位置。例如，如果远程分支机构文件服务器失败，并且更换组件到达之前将是 72 小时，则可以选择临时在另一个文件服务器上托管文件共享。或者，如果您对共享文件使用 DFS，则可以在站点上创建新的副本，在原始文件服务器恢复运行后将其删除。

测试恢复计划 (Testing the recovery plan)

应该仔细规划和创建恢复计划，因为它们包括在组织中恢复关键业务和关键任务解决方案所需的每一个步骤。但是，必须测试恢复计划，以确保恢复步骤有效且成功。未能测试恢复计划可能会导致恢复过程失败。例如，在创建恢复计划期间，管理员忘记了在服务器上安装驱动程序步骤，导致服务器无法在操作系统安装过程中发现存储阵列。此外，恢复过程中的任何延迟都将延长恢复关键业务系统所需的时间，从而可能导致业务损失或其他类型的组织损失。

评估恢复计划 (Evaluating the recovery plan)

每个组织中的 IT 基础架构都是动态的。这意味着组织每年都会部署新的解决方案，网络设备，购买新的服务器和停用旧的服务器和设备。恢复计划必须跟随组织 IT 基础架构的变化。如果不进行更新，则恢复计划可能会过时，并且不与组织中的服务器和应用程序的当前配置相对应。例如，组织已使用新版本更新其备份软件，该版本的备份和恢复步骤略有不同。在恢复过程中，备份操作员遵循恢复计划步骤，并停止

恢复过程，因为备份软件上的接口与恢复计划中的指令不匹配。因此，恢复过程中存在延迟，这可能导致组织的其他类型的丢失。

服务级别协议 (Service Level Agreement -SLA)

SLA 文档描述了部门，组织或服务提供商的职责和具体目标。具体来说，IT SLA 描述了 IT 部门或 IT 服务提供商在组织的关键 IT 解决方案和数据的可用性，性能和保护方面的职责。此外，SLA 通常指定提供程序在故障后必须恢复服务的速度。

一些组织具有正式的 SLA，而其他组织则有一般性的准则。通常，IT 部门的绩效是根据 SLA 阐述的目标来衡量的。这些度量是 IT 部门绩效评估的一部分，可以影响预算和薪水等项目。SLA 对托管服务和云服务提供商的计费结构至关重要。在其他类型的组织中，SLA 提供较不正式的指南。成功的 SLA 必须是现实和可实现的。

SLA 可能包括以下元素：

- 运维时间 (hours of operation)。运维时间定义了用户可以使用的数据和服务的时间，以及由于系统维护而导致的计划停机时间。
- 服务可用性 (service availability)。服务可用性是指用户可获得数据和服务的时间 (通常为一个日历年) 的百分比。例如，每年 99.9% 的服务可用性意味着数据和服务每年的计划外停机时间不得超过 0.1%，或者每天 24 小时不超过 8.75 小时。但是，组织还应定义维护窗口，这些维护窗口表示系统因维护过程 (如硬件升级或部署软件更新) 而脱机的计划时间。
- 恢复点目标 (RPO)。恢复点目标对由于失败而丢失的数据设置了限制。RPO 是合同确定的时间。例如，如果组织将 RPO 设置为 6 小时，则有必要每 6 小时执行一次备份，或者每隔 6 小时在不同位置创建一个复制副本。如果发生故障，组织将使用最近的备份，这不会超过 6 小时。
- 您可以配置备份软件以每小时执行备份，并提供 60 分钟的理论恢复点目标。这意味着如果在上次备份后 60 分钟内发生任何数据丢失，您将无法恢复在该小时内创建的新数据。在备份之前创建的所有其他数据将使用备份介质进行恢复。计算 RPO 时，请考虑执行备份所需的时间。例如，假设执行备份需要 15 分钟，并且每小时备份一次。如果在备份过程中发生故障，您最好的 RPO 将为 1 小时 15 分钟。现实的 RPO 必须平衡您所需的恢复时间与您的网络基础设施的现实。当备份需要 3 个小时来完成时，您不应该针对两个小时的 RPO。
- RPO 也取决于您使用的备份软件技术。例如，当您使用 Windows Server Backup 中的快照功能或使用卷影复制服务 (Volume Shadow Copy , VSS) 的其他备份软件时，您将备份到备份开始的时间。
- 恢复时间目标 (RTO)。RTO 是从故障中恢复所需的时间量。RTO 根据故障类型而变化。关键服务器上的主板丢失具有与关键服务器上的磁盘丢失不同的 RTO，因为主板更换比磁盘更换显著更长。
- 保留目标 (retention objectives)。保留目标测量存储备份数据的时间长度。例如，您可能需要从上个月快速恢复数据，但必须以某种形式存储数据几年。您同意在 SLA 中恢复数据的速度取决于数据的年龄。您应该考虑数据可恢复的速度或者是否必须从存档中恢复。
- 系统性能。系统性能是一个重要的 SLA 组件，虽然它通常不直接与灾难恢复相关。SLA 包括的应用程序应该可用，并且应该对用户的请求具有可接受的响应时间。如果系统性能较低，则可能无法满足业务需求。

高可用性网络 (Highly available networking)

应该分析和计划网络的高可用性, 以满足组织对高可用性和业务连续性的业务需求。网络管理员应该评估网络可能不可用的每个场景, 并提出一个解决方案, 以消除网络组件中的单点故障。

规划网络中的高可用性应包括:

- 网络适配器。某些应用程序安装了多个网络适配器, 以实现高可用性和改进的网络带宽。如果其中一个网络适配器停止工作, 其他网络适配器仍然有效。但是, 您应该验证应用程序供应商推荐的最佳实践。例如, 一些应用程序不支持多个网络适配器, 而其他应用程序使用不同的技术提供高可用性, 并建议每个主机只有一个网络适配器。此外, 如果在虚拟机上配置网络, 根据安装的应用程序, 将应用不同的建议。
- 多路径 I/O (Multipath I/O- MPIO) 软件。在高可用性 IT 环境中, 如果应用程序支持, 您可以部署具有多个主机总线适配器的节点。Windows Server 通过使用 MPIO 软件支持此方案。使用多个主机适配器实现 MPIO 可为您提供存储设备的备用路径。这提供了最高级别的冗余和可用性。对于 Windows Server 2016, 您的多路径解决方案必须基于 MPIO。您的硬件供应商通常为您的硬件提供 MPIO 设备特定的模块 (DSM), 但 Windows Server 2016 在操作系统中包括一个或多个 DSM。
- 局域网 (LAN)。您可以将 LAN 中的组织的计算机与网络交换机, 路由器和无线接入点连接起来, 这些设备中的每一个都表示单点故障。许多网络设备供应商提供了在安装冗余网络设备的情况下使用高可用性配置来配置网络设备的选项。如果单个组件发生故障, 冗余组件继续正常工作。
- 广域网 (WAN)。拥有多个分支机构的组织需要具有高可用性的 WAN 网络并将分支机构连接到公司网络的路由器。如果路由器故障, 第二个冗余路由器将继续提供连接。如果在单个 WAN 故障的情况下, 组织希望分支机构保持连接, 则组织可能考虑使用冗余 WAN 连接。
- 互联网连接。许多组织认为他们的互联网连接是业务关键组件。因此, 我们建议组织考虑部署两个 Internet 连接, 最好通过两个不同的 ISP。虽然 ISP 很少出现中断, 但通过另一个 ISP 提供辅助 Internet 连接提供了另一个级别的冗余。此外, 组织应将其路由器配置为冗余配置。如果单个路由器发生故障, 冗余路由器继续提供 Internet 连接。

规划网络的高可用性应包括冗余:

- 网络适配器
- 多路径 I/O
- 局域网
- 广域网
- 互联网连接

高可用存储 (Highly available storage)

计算机存储是每个应用程序最关键的组件之一。存储的数据应随时可访问。为了为存储提供高可用性, 企业可以根据业务需求在不同的存储解决方案和配置之间进行选择。

RAID

RAID 通过使用其他磁盘来确保磁盘子系统可以继续运行, 即使子系统中的一个或多个磁盘发生故障, 也能实现容错。RAID 使用两个选项来启用容错:

- 磁盘镜像 (Disk mirroring)。使用磁盘镜像, 写入一个磁盘的所有信息也会写入另一个磁盘。如果其中一个磁盘发生故障, 另一个磁盘仍然可用。

规划存储的高可用性时, 请考虑以下技术:

- RAID
- DAS
- NAS
- SAN
- 云服务

- 奇偶校验信息 (Parity information)。RAID 在磁盘故障时使用奇偶校验信息来计算存储在磁盘上的信息。服务器或 RAID 控制器计算写入磁盘的每个数据块的奇偶校验信息，然后将该信息存储在另一个磁盘上或跨多个磁盘。如果 RAID 阵列中的某个磁盘发生故障，服务器可以使用功能磁盘上仍然可用的数据以及奇偶校验信息来重新创建存储在故障磁盘上的数据。

直接连接存储 (Direct-attached storage)

几乎所有服务器都提供一些内置存储或**直接连接存储 (DAS)**。DAS 可以包括物理上位于服务器内部或直接与外部阵列连接的磁盘。应该使用 RAID 技术为 DAS 中的数据提供高可用性。但是，由于 DAS 存储器物理连接到服务器，如果服务器发生电源故障，则存储将不可用。

网络连接存储 (Network-attached storage)

网络连接存储 (NAS) 连接到专用存储设备，然后通过网络访问。NAS 与 DAS 的不同之处在于，存储不直接连接到每个单独的服务器，而是通过网络访问许多服务器。您可以在高可用 RAID 阵列中的 NAS 设备中的配置存储。组织受益于性能增益，因为 NAS 设备的处理能力专用于文件的分发。如果一个服务器发生故障，NAS 上存储的数据仍然可用，您可以从当前在线的另一台服务器访问它。



注意：在规划 NAS 解决方案时，请确保在 NAS 设备上存储数据的所有应用程序都支持 NAS。例如，Microsoft 不支持 Microsoft Exchange Server 在 NAS 上存储数据库的情况。

存储局域网 (Storage area network)

存储区域网络 (SAN) 是将计算机系统或主机服务器连接到高性能存储子系统的高速网络。SAN 通常包括诸如主机总线适配器 (HBA)，用于帮助路由流量的特殊交换机以及具有逻辑单元号 (LUN) 的存储磁盘阵列的组件。您可以在高可用性 RAID 阵列中配置 SAN 存储，其中 SAN 允许多个服务器访问任何服务器可能访问的存储池。由于 SAN 使用网络，因此 SAN 可以连接到许多不同的设备和主机，并提供对任何连接的设备的访问。SAN 还提供块级访问。SAN 不是通过使用文件访问协议作为文件访问磁盘上的内容，而是使用诸如以太网光纤通道 (Fibre Channel over Ethernet) 或因特网小型计算机系统接口 (Internet Small Computer System Interface, iSCSI) 之类的协议将数据块直接写入磁盘。

网络存储服务 (Cloud storage services)

在云环境 (例如 Microsoft Azure) 中运行应用程序的组织受益于已配置为高可用性的存储。此外，使用云服务 (如 Office 365) 的组织也可以从已在高可用配置中运行的存储和服务器受益，而这些组件不需要其他配置。已在 Office 365 中运行的应用程序 (例如 Exchange Online, Skype for Business Online 和 SharePoint Online) 已配置为高可用性。

高可用的计算或硬件功能 (Highly available compute or hardware functions)

Windows Server 2016 操作系统具有为不同类型的应用程序提供高可用性的功能。某些功能 (如故障转移群集) 对于许多应用程序 (如 SQL Server, Exchange Server 和 Hyper-V) 的高可用性操作至关重要。可以使用其他功能，如网络负载均衡 (NLB)，或者您可以部署等效的第三方设备。

在规划高可用性时，请考虑以下内置 Windows Server 2016 功能：

- 故障转移群集 (Failover Clustering) 使一组独立的服务器能够协同工作，以提高应用程序和服务的可用性。如果服务器群集或节点发生故障，则另一个节点开始提供服务。这是故障转

- 请考虑使用操作系统中内置的高可用性功能：
 - 故障转移群集
 - 网络负载均衡
 - RAID
- 遵循特定应用的最佳实践指南和建议

移, 并且导致很少或不会中断服务。

- NLB, 使一组独立服务器能够在运行 NLB 的服务器之间分发客户端请求。如果一个服务器不可用, 则其余服务器处理请求。
- RAID 功能内置在 Windows Server 2016 操作系统中, 并允许在 RAID 1 或 RAID 5 阵列中配置一组磁盘, 为存储的数据提供高可用性。但是, 管理员还可以考虑使用 DAS 控制器中内置的 RAID 软件。此外, 如果将服务器连接到 NAS 或 SAN 设备, 建议您在 NAS 或 SAN 设备上配置 RAID 阵列, 而不是在操作系统上配置。



注意：在决定部署哪个操作系统或硬件高可用性解决方案之前, 请始终阅读有关需要高可用性的特定应用程序的部署指南和最佳实践建议。此外, 请注意特定应用程序不支持的配置。

问题：高可用性应该为应用程序提供什么？

问题：连续可用性为应用程序提供了什么？

第 2 课

使用 Hyper-V 虚拟机规划高可用性和灾难恢复解决方案 (Planning high availability and disaster recovery solutions with Hyper-V virtual machines)

实施服务器虚拟化的一个好处是为具有内置高可用性功能的应用或服务以及不以任何其他方式提供高可用性的应用或服务提供高可用性的机会。使用 Windows Server 2016 Hyper-V 技术和故障转移群集，您可以使用几个不同的选项配置高可用性。

在本课程中，您将学习如何使用故障转移群集 Hyper-V 场景中为虚拟环境规划高可用性。

故障转移群集是一种 Windows Server 2016 功能，使您能够使应用程序或服务高度可用。要使虚拟机在 Hyper-V 环境中高度可用，应在 Hyper-V 主机计算机上实施故障转移群集。

本课程总结了基于 Hyper-V 的虚拟机的高可用性选项，然后重点介绍故障转移群集如何工作，以及如何为 Hyper-V 设计和实现故障转移群集。

课程目标 (Lesson Objectives)

完成本课后，您将能够：

- 使用 Hyper-V 虚拟机描述高可用性注意事项。
- 描述实时迁移 (live migration) 。
- 描述实时迁移要求。
- 使用存储迁移描述高可用性。
- 描述 Hyper-V 副本 (Hyper-V Replica) 。
- 规划 Hyper-V 副本 (Hyper-V Replica) 。
- 描述 Hyper-V 副本实现 (Hyper-V Replica) 。

Hyper-V 虚拟机的高可用性注意事项 (High availability considerations with Hyper-V virtual machines)

大多数组织都有一些应用程序是关键业务，必须高度可用。要使应用程序高可用，必须将其部署在为应用程序需要的所有组件提供冗余的环境中。要使虚拟机具有高可用性，您可以从几个选项中进行选择。您可以将虚拟机实现为群集角色，称为主机群集 (host clustering)，可以在虚拟机内部实现群集，称为来宾群集 (guest clustering)，或者可以在虚拟机中使用 NLB。

高可用性选项	描述
主机群集	<ul style="list-style-type: none"> • 虚拟机高度可用 • 不需要虚拟机操作系统或应用程序具有群集感知能力
来宾 (Guest) 群集	<ul style="list-style-type: none"> • 虚拟机是故障转移群集节点 • 虚拟机应用程序必须具有群集感知能力 • 需要 iSCSI 或虚拟光纤通道接口用于共享存储连接
网络负载均衡 (NLB)	<ul style="list-style-type: none"> • 虚拟机是 NLB 群集节点 • 用于基于 Web 的应用程序

主机群集 (Host clustering)

通过主机群集, 您可以使用 Hyper-V 主机服务器配置故障转移群集。为 Hyper-V 配置主机群集时, 可将虚拟机配置为高可用性资源。您在主机 - 服务器级别实施故障转移保护。这意味着在虚拟机中运行的客户机操作系统和应用程序不必具有群集感知能力。但是, 虚拟机仍然高度可用。

非群集感知应用的一些示例是打印服务器或专有的基于网络的应用, 例如财务应用程序。如果控制虚拟机的主机节点意外地变得不可用, 则辅助主节点获得控制权, 并尽可能快地重新启动或恢复虚拟机。您还可以以受控方式将虚拟机从群集中的一个节点移动到另一个节点。例如, 您可以将虚拟机从一个节点移动到另一个节点, 同时修补主机管理操作系统。

在虚拟机中运行的应用程序或服务不必与故障转移群集兼容, 他们不必知道虚拟机是群集的。故障切换处于虚拟机级别, 因此, 您在虚拟机中安装的软件没有依赖关系。

来宾群集 (Guest clustering)

来宾故障转移群集配置与物理 - 服务器故障转移群集类似, 除了群集节点是虚拟机。在这种情况下, 您可以创建两个或多个虚拟机, 并在客户机操作系统中启用故障转移群集。然后, 启用应用程序或服务以实现虚拟机之间的高可用性。因为故障转移群集在每个虚拟机节点的客户机操作系统中实现, 您可以在单个主机上查找虚拟机。这种配置在测试或分段环境 (staging environment) 中可以是快速和成本有效的。

但是, 对于生产环境, 如果将虚拟机部署在启用了故障转移群集的 Hyper-V 主机上, 则可以更好地保护应用程序或服务。在主机和虚拟机级别同时实现故障转移群集时, 资源可以重新启动, 而不管故障的节点是虚拟机还是主机。此配置也称为跨主机的来宾群集 (Guest Cluster Across Hosts)。它被认为是在生产环境中运行任务关键型应用程序的虚拟机的最佳高可用性配置。

在实现来宾群集时, 您应该考虑几个因素:

- 应用程序或服务必须是故障转移群集感知。这包括任何具有群集感知能力的 Windows Server 2016 服务以及任何应用程序, 例如群集 Microsoft SQL Server 和 Microsoft Exchange Server。
- Hyper-V 虚拟机可以使用基于光纤通道的连接到共享存储。但是, 这仅适用于 Microsoft Hyper-V Server 2012 及更高版本。或者, 您可以实现从虚拟机到共享存储的 iSCSI 连接。在 Windows Server 2012 R2 及更高版本中, 您还可以使用共享虚拟硬盘功能为虚拟机提供共享存储。


您应在主机计算机和虚拟机上部署多个网络适配器。理想情况下, 如果使用此方法连接到存储, 则应将网络连接专用于 iSCSI 连接。您还应该在主机之间专用一个专用网络, 以及客户端计算机使用的网络连接。

NLB

NLB 以与物理主机相同的方式处理虚拟机。它将 IP 流量分发到 TCP/IP 服务的多个实例, 例如在 NLB 群集内的主机上运行的 Web 服务器。NLB 在主机之间透明地分发客户端请求, 它使客户端能够通过使用虚拟主机名或虚拟 IP 地址访问群集。从客户端计算机的角度看, 群集似乎是回答这些客户端请求的单个服务器。随着企业流量的增加, 您可以向群集添加另一个服务器。

因此, NLB 是不必适应独占读取或写入请求的资源的适当解决方案。适用于 NLB 的应用程序的示例包括基于 Web 的前端, 数据库应用程序或 Exchange Server 客户端访问服务 (Client Access services)。

配置 NLB 群集时, 必须在将参与 NLB 群集的所有虚拟机上安装和配置应用程序。配置应用程序后, 在每个虚拟机的客户机操作系统 (而不是 Hyper-V 主机) 中的 Windows Server 2016 中安装 NLB 功能, 然后为应用程序配置 NLB 群集。旧版本的 Windows Server 还支持 NLB, 因此客户机操作系统不仅限于 Windows Server 2016; 但是, 您应该在一个 NLB 群集中使用相同的操作系统版本。类似于跨主机的来宾群集, 当您在不同的 Hyper-V 主机上找到虚拟机节点时, NLB 资源通常会从总体增加的 I/O 性能中受益。

 **注意:** 与旧版本的 Windows Server 一样, 您不应在同一操作系统中实施 Windows Server 2016 NLB 和故障转移群集, 因为这两种技术彼此冲突。

有几种情况下，您希望将虚拟机从一个位置迁移到另一个位置。例如，您可能希望将虚拟机的虚拟硬盘从一个物理驱动器移动到同一主机上的另一个物理驱动器。在另一个示例中，您可以将虚拟机从群集中的一个节点移动到另一个节点，或者只是将计算机从一个主机服务器移动到另一个主机服务器，而不是该群集的成员。与 Windows Server 2008 R2 相比，Windows Server 2012 和 Windows Server 2016 增强和简化了此过程的过程。

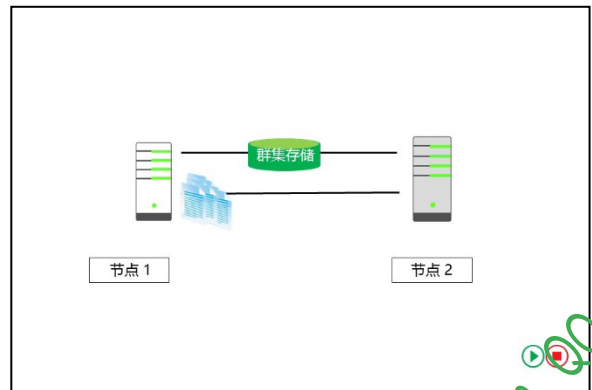
在 Windows Server 2016 中，可以使用以下方法执行虚拟机的迁移：

- **虚拟机和存储迁移 (Virtual Machine and Storage Migration)**。使用此方法，可以使用 Hyper-V Manager 中的 Move Virtual Machine Wizard 将已启动的虚拟机从一个位置移动到另一个位置或从一个主机移动到另一个主机。虚拟机和存储迁移不需要故障转移群集或任何其他高可用性技术。
- **快速迁移 (Quick Migration)**。此方法也可在 Windows Server 2008 中使用。它要求您安装和配置故障转移群集。在迁移过程中，当您使用快速迁移在群集节点之间移动虚拟机时，虚拟机将处于已保存状态。这会导致一些停机，直到它将内存内容复制到另一个节点，并从保存的状态恢复机器。
- **实时迁移 (Live Migration)**。实时迁移使您可以将虚拟机从一个主机迁移到另一个主机，而不会发生停机。在 Windows Server 中，您还可以执行不需要故障转移群集的 Shared Nothing Live Migration。此外，主机不必为要执行的此类型的迁移共享任何存储。
- **导出和导入虚拟机 (Exporting and importing virtual machines)**。这是一种建立的移动虚拟机而不使用群集的方法。您在一台主机上导出虚拟机，然后通过执行导入操作将导出的文件物理移动到另一台主机。这是一个非常耗时的操作。它要求您在导出和导入期间关闭虚拟机。Windows Server 2016 改进了此迁移方法。您可以将虚拟机导入到 Hyper-V 主机，而无需在导入之前将其导出。Windows Server 2016 Hyper-V 现在能够在导入操作期间配置所有必要的设置。

问题：您是否为您的环境中的虚拟机使用任何高可用性解决方案？

实时迁移概述 (Overview of Live Migration)

Windows Server 2016 Hyper-V 允许您在物理 Hyper-V 节点之间移动虚拟机，而无需关闭虚拟机。此过程称为实时迁移，您可以在群集或非群集环境中执行此过程。在故障转移群集中使用时，通过实时迁移，您可以将运行中的虚拟机从一个故障转移群集节点移动到另一个节点。如果在没有群集的情况下使用，Live Migration 将作为存储迁移执行，如前面的主题所述，它被称为**无共享实时迁移** (shared-nothing Live Migration)。使用实时迁移，用户在连接到虚拟机时不应遇到任何服务器中断。



注意：虽然您也可以使用虚拟机和存储迁移

(如本课前面所述) 执行虚拟机的实时迁移，但请注意，实时迁移基于一种称为故障转移群集的不同技术。与存储迁移方案不同，只有当虚拟机具有高可用性时，才会执行实时迁移。无共享实时迁移不使用或依赖故障转移群集。它通过将虚拟机从一个主机复制到另一个主机来移动虚拟机。


您可以使用以下某个方法启动实时迁移：

- 故障转移群集管理控制台 (The Failover Cluster Management Console)。

海量视频题库 myip.cn QQ:5565462

- 如果使用 VMM 管理物理主机, 则使用虚拟机管理器管理员控制台 (Virtual Machine Manager (VMM) Administrator console)。


Windows 管理规范 (Windows Management Instrumentation -WMI) 或 Windows PowerShell 脚本。

 **注意：**实时迁移使您能够在计划的故障切换期间显着减少虚拟机的意外中断。在计划的故障转移期间, 您可以手动启动故障转移。在计划外故障切换期间, 例如托管虚拟机的节点发生故障时, 实时迁移不会应用。

实时迁移过程 (The Live Migration process)

实时迁移过程包括四个步骤：

1. 迁移设置 (Migration)。当管理员启动虚拟机的故障转移时, 源节点将创建与目标物理主机的 TCP 连接。此连接将虚拟机配置数据传输到目标物理主机。实时迁移在目标物理主机上创建一个临时虚拟机, 并为目标虚拟机分配内存。迁移准备还会进行检查以确定是否可以迁移虚拟机。
2. 来宾内存传输 (Guest-memory transfer)。当虚拟机仍在源主机上运行时, 来宾虚拟机内存将反复传输到目标主机。源物理主机上的 Hyper-V 监视工作集中的页面。当系统修改内存页时, 它跟踪并将它们标记为已修改。在此阶段, 迁移的虚拟机继续运行。Hyper-V 多次迭代内存复制过程, 并且每次将较少数量的修改页复制到目标物理计算机。最终的存储器拷贝过程将剩余的修改的存储器页拷贝到目的物理主机。脏页数降至阈值以下或在 10 次迭代完成后, 复制将立即停止。
3. 状态转移 (State transfer)。要将虚拟机迁移到目标主机, Hyper-V 将停止源分区, 将虚拟机的状态 (包括剩余的脏内存页) 传输到目标主机, 然后恢复目标主机上的虚拟机。Hyper-V 必须在最终状态传输期间暂停虚拟机。
4. 清理 (Cleanup)。清理阶段通过拆除源主机上的虚拟机, 终止工作线程以及发出迁移完成的信号来完成迁移。

 **注意：**在 Windows Server 2016 中, 您可以通过使用服务器消息块 (SMB) 3.0 作为传输来执行虚拟机实时迁移。这意味着您可以利用关键的 SMB 功能, 例如流量压缩, SMB Direct (远程直接内存访问, remote direct memory access) 和 SMB 多通道, 这些功能可以提供高速迁移和低 CPU 利用率。

实时迁移要求 (Live Migration requirements)

要执行实时迁移, 必须配置主机计算机。此外, 您必须满足 Windows Server 2016 中实时迁移的特定要求：

- 应启用实时迁移; 默认情况下不启用。
- 主机计算机应具有相同的处理器体系结构。
- 用户账户必须是本地 Hyper-V 管理员组的成员或虚拟机的两个主机上的管理员组。
- 源主机和目标主机都必须安装 Hyper-V 角色。
- 源主机和目标主机都必须是同一域的成员, 或者是彼此信任的不同域的成员。

实时迁移要求包括：

- 启用实时迁移
- 主机计算机处理器要求
- 已配置主机计算机域成员资格和用户帐户
- 已安装 Hyper-V 角色和管理工具
- 已配置主机计算机身份认证
- 主机计算机性能, 网络和带宽配置

- 如果从源主机或目标主机运行工具，则应在源主机和目标主机上安装 Hyper-V 管理工具。否则，应在运行 Windows Server 2016 或 Windows 10 的计算机上安装管理工具。
- 您应为实时迁移流量配置身份验证协议。您可以选择以下身份验证协议：
 - Kerberos 要求您配置约束委派（constrained delegation）。启用 Kerberos 后，无需登录到服务器。
 - 凭证安全支持提供程序（Credential Security Support Provider-CredSSP）不要求您配置约束委派，但需要管理员登录到服务器。
- 您可以选择配置实时迁移的性能选项，以减少网络和 CPU 利用率，这可能会提高实时迁移的速度。
- 您应该在单独的网络上执行实时迁移，并且您可以使用诸如 Internet 协议安全（IPsec）之类的加密协议来保护实时迁移中主机之间的流量。
- 您可以配置实时迁移的带宽限制，通过使用 Windows PowerShell cmdlet Set-SMBbandwidthlimit 在实时迁移过程中优化网络带宽。

演示：配置实时迁移 (可选) (Configuring Live Migration)

在本演示中，您将了解如何启用和配置实时迁移

演示步骤 (Demonstration Steps)

1. 在 LON-HOST1 上，打开 Hyper-V 管理器。
2. 在 Hyper-V Manager Settings 中，打开 Live Migrations 并启用传入和传出实时迁移。
3. 如果要使用不同于 2 的数字，请指定实时迁移的同时数。
4. 查看使用特定网络连接以接受实时迁移流量的选项。
5. 选择 Advanced Features 以演示配置身份验证协议。
6. 在 LON-NVHOST2 上执行步骤 1 到 5。

通过存储迁移提供高可用性 (Providing high availability with storage migration)

在许多情况下，管理员可能希望将虚拟机文件移动到其他位置。例如，如果虚拟机硬盘所在的磁盘空间不足，则必须将虚拟机移动到另一个驱动器或卷。将虚拟机移动到另一个主机是一个非常常见的过程。

在旧版本的 Windows Server（如 Windows Server 2008 或 Windows Server 2008 R2）中，移动虚拟机会导致停机，因为虚拟机必须关闭。如果您在两个主机之间移动虚拟机，则还必须为该特定计算机执行导出和导入操作。导出操作可能很耗时，这取决于虚拟机硬盘的大小。

在 Windows Server 2012 和 Windows Server 2016

中，虚拟机和存储迁移使您可以将虚拟机移动到同一主机或其他主机计算机上的其他位置，而无需关闭虚拟机。

- 虚拟机和存储迁移技术使您能够将虚拟机及其存储移动到另一个位置，而不会停机
- 在迁移期间，虚拟机硬盘将从一个位置复制到另一个位置
- 更改将同时写入源驱动器和目标驱动器
- 您可以将虚拟机存储移动到同一主机，另一个主机或 SMB 共享
- 存储和虚拟机配置可以在不同的位置

要复制虚拟硬盘, 管理员可以使用 Hyper-V 控制台或 Windows PowerShell 启动实时存储迁移, 并完成存储迁移向导 (Storage Migration wizard) 或在 Windows PowerShell 中指定参数。这将在目标位置创建一个新的虚拟硬盘, 并且复制过程开始。

在复制过程中, 虚拟机完全正常工作。但是, 在复制期间发生的所有更改都将写入源位置和目标位置。您只能从源位置执行读取操作。

磁盘复制过程完成后, Hyper-V 会将虚拟机切换到在目标虚拟硬盘上运行。此外, 如果将虚拟机移动到另一个主机, 将复制计算机配置, 并将虚拟机与另一个主机相关联。如果在目标端发生故障, 则始终有一个故障恢复选项在源目录上运行。将虚拟机迁移到新位置并与其成功关联后, 该过程将删除源 VHD/VHDX 文件和虚拟机配置。

移动虚拟机所需的时间取决于源和目标位置, 硬盘或存储的速度以及虚拟硬盘的大小。如果源位置和目标位置在存储器上, 并且存储器支持卸载数据传输 (Offloaded Data Transfer, ODX), 则加速移动过程。

将虚拟机的 VHD/VHDX 和配置文件移动到其他位置时, 向导会显示三个可用选项:

- 将虚拟机所有的数据移动到单个位置。您可以指定单个目标位置, 例如磁盘文件, 配置, 检查点或智能分页 (smart paging) 。
- 将虚拟机的数据移动到其他位置。您可以为每个虚拟机项目指定单独的位置。
- 仅移动虚拟机的虚拟硬盘: 仅移动虚拟硬盘文件。

演示: 配置存储迁移 (可选) (Configuring storage migration)

在本演示中, 您将了解如何启用和配置存储迁移。

演示步骤 (Demonstration Steps)

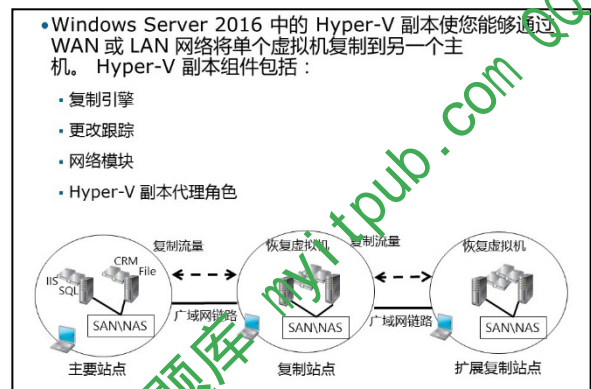
1. 在 LON-HOST1 中, 在 Hyper-V 管理器中, 打开 LON-HOST1 的 Hyper-V Settings 窗口。
2. 将存储迁移的同时数设置为 5。
3. 在 LON-HOST1 上创建一个名为 C:\VM 的文件夹。
4. 启动 Storage Migration 并显示移动存储的选项。
5. 将 LON-SVR1-B 虚拟机到 C:\VM 文件夹。

Hyper-V 副本概述 (Overview of Hyper-V Replica)

您可能希望有一个虚拟机的备份副本, 如果原始虚拟机发生故障, 您可以运行该备份副本。通过实现高可用性, 您有一个虚拟机的实例。高可用性不会防止在虚拟机内运行的软件的损坏。解决这个问题的一种方法是定期地手动复制虚拟机。您还可以备份虚拟机及其存储。虽然该解决方案实现了所需的结果, 但是它是资源密集和耗时的。此外, 由于您定期执行备份, 因此您不会拥有与正在运行的虚拟机相同的副本。

要解决此问题, 并允许管理员拥有单个虚拟机的最新副本, Windows Server 2012 及更高版本实现了 Hyper-V 副本 (Hyper-V Replica)。此技术使在主

站点, 或位置, 或主机上运行的虚拟机能够通过 WAN 或 LAN 链路有效地复制到辅助站点 (位置或主机)。Hyper-V 副本使您可以使单个虚拟机的两个实例驻留在不同的主机上, 一个作为主副本, 另一个作



为副本或脱机副本。这些副本会定期同步，您可以在 Windows Server 2016 中配置这些副本。您还可以随时进行故障转移。

在自然灾害，断电或服务器故障导致主站点故障的情况下，管理员可以使用 Hyper-V 管理器在几分钟内执行生产工作负载到辅助位置的副本服务器的故障转移，从而导致最少停机时间。Hyper-V 副本使管理员能够将虚拟化工作负载恢复到特定时间，具体取决于虚拟机的恢复历史记录配置设置。

Hyper-V 复制技术由几个组件组成：

- 复制引擎 (Replication engine)。此组件是 Hyper-V 副本的核心。它管理复制配置详细信息，并处理初始复制，增量复制，故障转移和测试故障转移操作。它还跟踪虚拟机和存储移动性事件，并采取必要的适当操作。例如，复制引擎将暂停复制事件，直到迁移事件完成，然后等这些事件停止后再恢复。
- 更改跟踪 (Change tracking)。此组件跟踪在虚拟机的主副本上发生的更改。它旨在使场景工作，无论虚拟机 VHD 文件或文件驻留在哪里。
- 网络模块 (Network module)。此模块提供了一种安全有效的方式在主机和副本主机之间传输虚拟机副本。默认情况下启用数据压缩。HTTPS 和基于认证的身份验证保护了此通信。
- Hyper-V 副本代理角色 (Hyper-V Replica Broker role)。这是在 Windows Server 2016 中实现的角色。在故障转移群集中进行配置，即使您正在复制的虚拟机具有高可用性并且可以从一个群集节点移动到另一个群集节点，也可以使用 Hyper-V 复制功能。Hyper-V Replica Broker 将所有虚拟机特定事件重定向到副本群集中的相应节点。Broker 查询群集数据库以确定哪个节点应处理哪些事件。如果执行快速迁移，实时迁移或存储迁移过程，这可确保 Broker 将所有事件重定向到群集中的正确节点。

当您规划站点上的硬件配置时，您不必使用相同的服务器或存储硬件。但是，重要的是确保有足够的硬件资源可用于运行 Hyper-V 副本虚拟机。



注意：Hyper-V 副本不是高可用性技术，而是灾难恢复技术。它不提供自动故障转移。

规划 Hyper-V 副本 (Planning for Hyper-V Replica)

使用 Windows Server 2016，管理员可以受益于以下新功能，可帮助优化 Hyper-V 副本并增加关键虚拟机的可用性。

- 更改复制频率。在早期版本的 Windows Server 中，Hyper-V 副本设置为五分钟的复制间隔，您无法更改此值。在 Windows Server 2016 中，您可以将复制间隔设置为 30 秒，5 分钟或 15 分钟。这意味着您可以根据真实环境配置复制流量。但是，请记住，具有较高延迟（例如 15 分钟）的副本会产生更多流量。
- 扩展复制。使用 Windows Server 2012 和更高版本的 Windows Server 操作系统，您可以将单个虚拟机复制到第三个服务器。因此，您可以将正在运行的虚拟机复制到两个独立的服务器。但是，不会从一个服务器到另外两个服务器进行复制。运行虚拟机的活动副本的服务器复制到副本服务器，然后副本服务器复制到扩展副本服务器。通过在被动副本 (passive copy) 上运行扩展复制向导 (Extend Replication Wizard) 来创建第二个副本。在此向导中，您可以设置与配置第一个副本时选择的选项相同的选项。

在 Windows Server 2016 中的 Hyper-V 副本功能可以：

- 将复制频率更改为 30 秒，5 分钟或 15 分钟
- 扩展复制以包括第三个主机

海量视频题库 www.it-ebooks.com QQ:5565462



注意：Hyper-V 副本现在允许管理员使用 Microsoft Azure 实例作为副本存储库。这使管理员能够利用 Azure，而不必建立灾难恢复站点，或管理异地备份磁带。要将 Azure 用于此目的，您必须具有有效的订阅。请注意，此服务可能不适用于所有世界地区。

问题：有没有扩展复制的方法可以有益于您的环境？

实现 Hyper-V 副本 (Implementing Hyper-V Replica)

在实施 Hyper-V 副本技术之前，请确保满足以下先决条件：

- 服务器硬件支持 Windows Server 2016 上的 Hyper-V 角色。
- 主服务器和副本服务器上存在足够的存储，以托管复制虚拟机使用的文件。
- 托管主服务器和副本服务器的位置之间存在网络连接。这可以是 WAN 或 LAN 链路。
- 正确配置防火墙规则，以在主站点和副本站点之间启用复制（默认流量超过 TCP 端口 80 或 443）。
- 存在 X.509v3 证书，以根据需要提供与证书的相互认证

Hyper-V 副本有以下先决条件：

- 服务器硬件支持 Windows Server 2016 上的 Hyper-V 角色
- 主服务器和副本服务器上存在足够的存储
- 在托管主服务器和副本服务器的位置之间存在网络连接
- 在主站点和副本站点之间正确配置防火墙规则以启用复制（默认为 TCP 端口 80 或 443）。
- 存在 X.509v3 证书以支持使用证书的相互身份认证

您不必单独安装 Hyper-V 副本，因为它不是 Windows Server 角色或功能。Hyper-V 副本作为 Hyper-V 角色的一部分实现。您可以将其用在独立的 Hyper-V 服务器上，也可以在作为故障转移群集一部分的服务器上使用，在这种情况下应配置 Hyper-V 副本代理（Hyper-V Replica Broker）。与故障转移群集不同，Hyper-V 角色不依赖于 AD DS。您可以将 Hyper-V 角色用于独立的 Hyper-V 服务器，或者是不同 Active Directory 域的成员，除非参与 Hyper-V 副本的服务器是同一故障转移群集的一部分。

要启用 Hyper-V 副本技术，请完成以下步骤：

- 在复制配置组（Replication Configuration group）中，将 Hyper-V 服务器作为副本服务器启用。
- 配置 Hyper-V 服务器设置。选择认证和端口选项，并配置授权选项。您可以选择从成功验证的任何服务器启用复制。在所有服务器都属于同一域的情况下，或者您可以键入作为副本服务器接受的服务器的完全限定域名（FQDN），这非常方便。此外，您必须配置副本文件的位置。您应在用作副本服务器的每个服务器上配置这些设置。
- 指定副本服务器名称和连接选项。
- 选择要复制的虚拟硬盘驱动器（如果虚拟机具有多个 VHD），并且还可以配置恢复历史记录和初始复制方法。在 Windows Server 2016 中，您还可以配置复制间隔 30 秒，5 分钟（这是 Windows Server 2016 中的默认值）或 15 分钟。
- 配置这些选项后，可以启动复制。在 Windows Server 2016 中创建初始副本后，还可以将扩展副本生成到运行 Hyper-V 的第三个物理或基于云的实例。扩展复制副本站点是从第一个副本站点而不是主要虚拟机构建的。可以为虚拟机的副本和扩展副本实例配置不同的复制间隔。

您可以使用 Hyper-V 副本执行三种类型的故障转移：测试故障转移，计划故障转移和故障转移。这三个选项提供不同的优点，并且在不同的场景中有用。

测试故障转移 (Test failover)

配置 Hyper-V 副本后，在虚拟机开始复制后，您可以执行测试故障转移。测试故障转移是一种无中断任务，使您能够在主虚拟机运行时测试副本服务器上的虚拟机，并且不会中断复制。您可以在复制的虚拟机

上启动测试故障转移，这将创建一个新的检查点。您可以使用此检查点来选择恢复点，从中创建新的测试虚拟机。测试虚拟机与副本具有相同的名称，但在末尾附加“- Test”。测试虚拟机未启动。默认情况下断开连接，以避免与正在运行的主虚拟机的潜在冲突。

完成测试后，可以停止测试故障转移。仅当测试故障转移正在运行时，此选项才可用。停止测试故障转移时，它会停止测试虚拟机并将其从副本 Hyper-V 主机中删除。如果在故障转移群集上运行测试故障转移，则必须手动从故障转移群集中删除测试故障转移角色。

计划故障转移 (Planned failover)

您可以启动计划故障转移以将主虚拟机移动到副本站点，例如，在站点维护之前或预期灾难之前。因为这是一个计划事件，没有数据丢失，但虚拟机在启动期间将不可用。计划故障转移确认在执行故障转移之前主虚拟机已关闭。在故障切换期间，主虚拟机将其尚未复制的所有数据发送到副本服务器。计划的故障转移过程随后将虚拟机故障转移到副本服务器，并在副本服务器上启动虚拟机。计划故障转移后，虚拟机将在副本服务器上运行，并且不会复制其更改。如果要再次建立复制，则应反转复制。您将必须配置类似于启用复制时的设置，并且它将使用现有虚拟机作为初始副本。

故障转移 (Failover)

如果主站点出现中断，您可以执行故障转移。仅当主虚拟机不可用或关闭时，才在复制的虚拟机上启动故障转移。故障转移是一种意外事件，可能导致数据丢失，因为在灾难发生之前，主虚拟机上的更改可能未复制。复制频率设置控制更改复制的频率。在故障切换期间，虚拟机在副本服务器上运行。如果从不同的恢复点启动故障转移并丢弃所有更改，则可以取消故障转移。恢复主站点后，可以逆转复制方向以重新建立复制。这也删除了取消故障转移的选项。

演示：实现 Hyper-V 副本 (可选) (Implementing Hyper-V Replica)

在本演示中，您将了解如何实现 Hyper-V 副本。

演示步骤 (Demonstration Steps)

1. 在 LON-HOST1 和 LON-NVHOST2 上，将每个服务器配置为 Hyper-V 副本服务器。
2. 使用 Kerberos (HTTP) 进行身份验证。
3. 从任何已验证的服务器启用复制。
4. 创建并使用文件夹 C:\VMReplica 作为存储副本文件的默认位置。
5. 在两台主机上启用名为 Hyper-V Replica HTTP Listener (TCP-In) 的防火墙规则。
6. 在 LON-HOST1 上，启用 28740B-LON-SVR1-B 虚拟机的复制：
 - 使用 Kerberos (HTTP)。
 - 允许 3 个同时存储迁移。
 - 选择仅具有最新恢复点 (only latest recovery point available)。
 - 将复制频率设置为 15 分钟。
 - 立即开始复制。
7. 等待初始复制完成，并确保 28740B-LON-SVR1-B 虚拟机出现在 LON-NVHOST2 上的 Hyper-V Manager 控制台中。
8. 在 LON-HOST1 上，查看 28740B-LON-SVR1-B 的复制健康状况。
9. 在 LON-HOST1 上，关闭 28740B-LON-SVR1-B，并执行计划故障转移到 LON-NVHOST2。验证 28740B-LON-SVR1-B 是否在 LON-NVHOST2 上运行。

问题： Windows Server 2016 中的虚拟机的迁移选项是什么？

问题： 什么是 Hyper-V 副本？

实验: 规划和实现高可用性和灾难恢复解决方案 (Planning and implementing a high availability and disaster recovery solution)

场景 (Scenario)

A. Datum Corporation 希望评估和配置他们可以利用的新的可用性特性和技术。作为系统管理员，您的任务是执行该评估和实施。

目标 (Objectives)

完成本实验后，您将能够：

- 配置 Hyper-V 副本。
- 为 Hyper-V 配置故障转移群集。
- 配置高可用性虚拟机。

实验室置 (Lab Setup)

估计时间: 75 分钟

虚拟机：28740B-LON-DC1-B，28740B-LON-SVR1-B

宿主机：28740B-LON-HOST1，28740B-LON-NVHOST2

用户名：Adatum\Administrator

密码：Pa55w.rd

要执行此实验，您应该继续使用在单元 2，5 和 6 中创建的 VM 环境，其中包括在物理主机 LON-HOST1，LON-HOST1 上运行的 LON-DC1-B 和 LON-SVR1-B 虚拟机，以及嵌套主机 LON-NVHOST2。

1. 在主机计算机上的任务栏上，单击 Hyper-V Manager。
2. 如果尚未启动，请在 Hyper-V 管理器中单击 28740B-LON-DC1-B，然后在 Actions 窗格中单击 Start。
3. 在 Actions 窗格中，单击 Connect。等待直到虚拟机启动。
4. 使用以下凭据登录：
 - 用户名: Adatum\Administrator
 - 密码: Pa55w.rd
5. 对于 28740B-LON-NVHOST2 和 28740B-LON-SVR1-B 虚拟机，重复步骤 3 到 5。
6. 在 28740B-LON-DC1-B，28740B-LON-SVR1-B 和 28740B-LON-NVHOST2 上，确保您的虚拟机被配置为使用 Host Internal Network (Internal Virtual Switch type)。
7. 在 LON-DC1-B 上，打开 DNS Management 控制台并验证分配给 28740B-LON-DC1-B，28740B-LON-SVR1-B 和 28740B-LON-NVHOST2 是虚拟机的实际 IP 地址。如果某些 IP 地址丢失，请根据 28740B-LON-DC1-B 上的 DNS Management 控制台中的信息进行配置。这些应该如下：
 - LON-DC1：172.16.0.10
 - LON-SVR1：172.16.0.21
 - LON-HOST1：172.16.0.160
 - NV-HOST2：172.16.0.32



注意：备注：您必须已完成章节 2，5 和 6 中的实验，才能完成此实验。

练习 1: 确定适当的高可用性和灾难恢复解决方案 (Lab Setup)

场景 (Scenario)

A. Datum 公司总部设在纽约。在伦敦一个偏远的办事处最近的火灾导致一些数据丢失后，它正在审查其当前的灾难恢复战略。还决定审查目前关于高可用性的战略。A. Datum 正在考虑升级到 Windows Server 2016，并希望确定是否有任何 Windows Server 2016 功能，它可以利用。预算也面临压力，管理层正在寻找是否有可以实现的任何成本节约，以帮助抵消目前用于 Hyper-V 群集的现有存储的支出。A. Datum 具有以下业务要求：

- 公共财务交易在线进行。
- 在应用/产品开发，人力资源，财务，客户服务，IT 和销售方面有 1000 名员工。
- 财务不能容忍在 Hyper-V 上运行的 SQL 和财务应用程序中的任何停机时间。
- 财务团队需要不到 1 分钟的停机时间为他们的 RTO 和零数据丢失作为他们的 RPO 对面向客户的交易。
- 财务部门也以非常快的速度增长，他们预计对应用和服务的需求将增加。

解决方案应该：

- 允许每月修补，无停机时间。
- 允许更换现有的旧存储，而无需使 Hyper-V 群集停机。
- 提供灾难恢复策略，允许在任何办公地点发生另一个灾难事件时恢复关键虚拟机。

这项工作的主要任务如下：

1. 设计适当的高可用性和灾难恢复解决方案
- **任务 1: 确定合适的高可用性和灾难恢复解决方案**
- **问题：**你应该采取什么行动，你应该考虑使用哪些技术？

练习 2: 实现存储迁移 (Implementing storage migration)

场景 (Scenario)

为了平衡在现有主机和新主机上运行的虚拟机数量，您计划在 Hyper-V 主机运行时移动虚拟机，而不会停机。首先，您将配置目标 Hyper-V 主机以允许实时迁移。接下来，您将使用移动向导将虚拟机存储，其虚拟硬盘及其检查点移动到合作伙伴的 Hyper-V 主机。

这项工作的主要任务如下：

1. 配置并执行存储迁移
- **任务 1: 配置和执行存储迁移**
1. 在 LON-HOST1 上，使用 Hyper-V 管理器确认 LON-SVR1-B 正在运行并配置了本地存储的 VHD。
 2. 使用 Move Wizard 将 28740B-LON-SVR1-B-Allfiles 虚拟机 VHD 移动到 C:\VMs\LON-SVR1-B，不要移动其他虚拟磁盘。
 3. 使用 Hyper-V 管理器确认 28740B-LON-SVR1-B-Allfiles 虚拟机 VHD 现在存储在 C:\VMs 文件夹结构下。



注意：在虚拟机运行时移动了 VHD。

结果：完成本练习后，你应该已经移动了 Hyper-V 存储和虚拟机。

练习 3: 配置 Hyper-V 副本 (Configuring Hyper-V Replicas)

场景 (Scenario)

在进行群集部署之前，您已决定评估 Hyper-V 中用于在主机之间复制虚拟机的新技术。如果活动副本或主机发生故障，您希望能够手动将虚拟机的副本挂载到另一个主机上。

本练习的主要任务如下：

1. 在两台主机上配置副本
2. 为 LON-SVR1-B 虚拟机配置副本
3. 验证计划的故障切换到副本站点
4. 准备下一个单元

► 任务 1: 在两台主机上配置副本

1. 在 LON-HOST1 和 LON-NVHOST2 上，将每个服务器配置为 Hyper-V 副本服务器。
 - 使用 Kerberos (HTTP) 进行身份验证。
 - 从任何已验证的服务器启用复制。
 - 创建并使用文件夹 E:\VMReplica 作为存储副本文件的默认位置。
2. 在两台主机上启用名为 Hyper-V Replica HTTP Listener (TCP-In) 的防火墙规则。

► 任务 2: 为 LON-SVR1-B 虚拟机配置副本

1. 在 LON-HOST1 上，启用 28740B-LON-SVR1-B 虚拟机的复制：
 - 使用 Kerberos (HTTP) 。
 - 将复制频率设置为 30 秒。
 - 选择仅具有最新恢复点。
 - 立即开始复制。
2. 等待初始复制完成，并确保 28740B-LON-SVR1-B 虚拟机已出现在 LON-NVHOST2 上的 Hyper-V Manager 控制台中。

► 任务 3: 验证计划的故障切换到副本站点

1. 在 LON-HOST1 上，查看 28740B-LON-SVR1 的复制健康状况。
2. 在 LON-HOST1 上，关闭 28740B-LON-SVR1-B，并执行计划的故障转移到 LON-NVHOST2。
3. 验证 28740B-LON-SVR1-B 正在 LON-NVHOST2 上运行。

► 任务 4: 为下一个单元做准备 (Prepare for the next module)

1. 在 LON-NVHOST2 上的 28740B-LON-SVR1-B 上取消故障切换。
2. 在 LON-HOST1 和 LON-NVHOST2 上删除 28740B-LON-SVR1-B 的副本。
3. 在 LON-HOST1 和 LON-NVHOST2 上禁用复制。

4. 在 LON-HOST1 上，将 28740B-LON-SVR1-B-Allfiles.vhd 移回 E:\Program Files\Microsoft Learning\28740\Drives\28740B-LON-SVR1-B\Virtual Hard Disks。
5. 重新启动主机。
6. 当出现启动菜单提示时，选择 Windows Server 2016，然后按 Enter。
7. 按照教师的指示登录主机。

结果：完成此练习后，您已配置 Hyper-V 副本。

问题：如何在 Windows Server 2016 中扩展 Hyper-V 副本？

问题：实时迁移和存储迁移有什么区别？

第 3 课

使用 Windows Server Backup 进行备份和还原 (Backing up and restoring by using Windows Server Backup)

数据保护描述了许多技术和方法, 允许您在计划外事件 (如数据损坏, 应用程序故障或由于泛滥或火灾导致站点丢失) 之后将数据, 服务和服务器恢复到运行状态。有效的数据保护策略可以满足组织的需求, 而不需要提供不必要的覆盖范围。虽然绝对保护似乎是可取的, 但在经济上是不可行的。当您制定数据保护策略时, 平衡组织中的特定类型数据丢失的成本与保护组织避免数据丢失的成本。

用于执行备份的软件也会影响备份过程。您可以在 Windows 操作系统中使用 Windows Server Backup 或 Microsoft System Center Data Protection Manager (Data Protection Manager)。您还可以使用第三方解决方案来备份 Windows Server 2016。

课程目标 (Lesson Objectives)

- 完成本课后, 您将能够 :
- 描述 Windows Server Backup
- 实施备份和恢复

Windows Server Backup 概述 (Overview of Windows Server Backup)

Windows Server Backup 是 Windows Server 2016 中的 Microsoft 管理控制台 (MMC) 管理单元, `wbadmin` 命令和 Windows PowerShell 命令组成一项功能。您可以使用 Windows Server Backup 中的向导来指导您完成运行备份和恢复。

您可以使用 Windows Server Backup 备份 :

- 完整服务器 (所有卷) 或仅选定的卷。
- 单个文件和文件夹。
- 系统状态 (System state)。
- Hyper-V 主机上的单个虚拟机。
- 群集共享卷 (Cluster Shared Volumes -CSV)

此外, Windows Server Backup 允许您 :

- 执行裸机还原 (bare-metal restore)。裸机备份至少包含所有关键卷, 并允许您在不首先安装操作系统的情况下进行恢复。您可以通过使用 DVD 上的产品介质或 USB 密钥以及 Windows 恢复环境 (Windows RE) 来执行此操作。您可以将此备份类型与 Windows RE 一起使用, 以从硬盘故障中恢复, 或者必须将整个计算机映像恢复到新硬件。
- 恢复系统状态 (Restore system state)。备份包含将服务器回滚到特定时间的所有信息。但是, 您需要先安装操作系统才能恢复系统状态。
- 还原单个文件和文件夹或卷。单个文件和文件夹选项使您能够选择备份和还原特定文件, 文件夹或卷, 或者您可以在使用重要的卷或系统状态等选项时将特定文件, 文件夹或卷添加到备份。
- 排除所选文件或文件类型。例如, 您可以从备份中排除临时文件。
- 将备份存储在多个存储位置。您可以将备份存储在远程共享或非专用卷上。

- 通过使用 Windows Server Backup, 您可以 :
 - 执行完整的服务器备份和裸机还原
 - 备份和恢复系统状态
 - 备份和还原单个文件和文件夹
 - 排除所选文件或文件类型
 - 从更多存储位置中选择
 - 执行 Windows Azure 在线备份

- 使用 Microsoft Azure 在线备份。Microsoft Azure 在线备份是 Windows Server 2016 的基于云的备份解决方案，可让您使用云服务备份和恢复异地的文件和文件夹。
- 如果发生硬盘故障等事件，您可以使用完整的服务器备份和 Windows RE 执行系统恢复。这将恢复您的完整系统到新的硬盘。
- Windows Server Backup 是单服务器备份解决方案。您不能使用 Windows Server Backup 的一个实例备份多个服务器。您需要在每个服务器上安装和配置 Windows Server Backup。

实现备份和还原 (Implementing backup and restore)

备份虚拟机 (Backing up virtual machines)

为虚拟机创建备份解决方案时，应考虑要备份的数据。您可以在主机上安装 Windows Server Backup，并执行主机级备份，也可以在虚拟机内安装 Windows Server Backup 以执行客户机内备份。在许多情况下，您可能要同时使用主机和来宾内备份。我们建议您阅读有关如何备份特定应用程序的技术文档和最佳实践。例如，SQL Server，Exchange Server 和 Skype for Business 服务器有不同的备份最佳实践。此外，一些应用程序仅支持客户机内备份。

- 备份和还原操作包括：
 - 备份和恢复 Hyper-V 主机
 - 备份和恢复虚拟机
 - 备份和恢复 AD DS，文件服务器和 Web 服务器
 - Azure 站点恢复

在执行完整服务器备份时，您使用主机级备份，其中备份中包含的数据包括虚拟机配置，虚拟机关联的快照和虚拟机的虚拟硬盘。从备份还原数据时，无需重新创建虚拟机或重新安装 Windows Server 角色。但是，备份不包括虚拟网络设置，这些设置需要重新创建并重新连接到虚拟机。为此，您可以创建 PowerShell 脚本，以自动化创建和连接虚拟交换机的过程。

在客户机操作系统中执行备份时，过程与为物理计算机执行备份相同。在执行主机级备份和虚拟机备份时，应在客户机操作系统中完成备份，然后在主机计算机上执行完全备份。

备份文件服务器和 Web 服务器 (Backing up file servers and web servers)

考虑这么一种情况：您希望为文件或 Web 服务器提供备份。为了在特定时间内快速恢复单个文件，客户机内备份就足够了。

如果要备份远程桌面会话主机服务器，主机级备份很可能比客户机内备份更有用。通过主机级备份，您可以快速地完整地恢复整个虚拟机，而来宾内备份则需要您在尝试恢复之前构建虚拟机并安装 Windows Server。

备份活动目录域服务 (Backing up AD DS)

备份 AD DS 角色是一个重要的过程，应该是任何备份和恢复过程或策略的一部分。您备份 AD DS 角色以在不同的数据丢失情况下恢复数据，例如删除的数据或损坏的 AD DS 数据库。


备份 AD DS 时，请考虑备份计划。请正确计划 AD DS 备份计划，因为您无法从早于 180 天的已删除对象生存期的备份进行还原。当用户从 AD DS 中删除对象时，它将保留有关该删除的信息 180 天。如果您有低于 180 天的备份，则可以成功还原已删除的对象。如果备份超过 180 天，则还原过程不会将还原的对象复制到其他域控制器，这意味着 AD DS 数据的状态将不一致。


了解虚拟机中的联机 and 脱机备份 (Understanding online and offline backups in virtual machines)

如果满足以下条件，则可以执行不会导致虚拟机停机的联机备份。

- 要备份的虚拟机已安装并启用集成服务 (integration services)。

- 虚拟机使用的每个磁盘都运行 NTFS 文件系统基本磁盘。
- 在虚拟机中的所有卷上启用 VSS，每个卷的快照存储在同一卷上。例如，卷 D 必须在卷 D 上存储卷影副本。

 **注意：**在 Windows Server 2012 中的 Windows Server Backup 向导中，选择要备份的 Hyper-V 虚拟机时，可用的备份类型是使用保存的状态（Saved State）（脱机）备份或使用子分区快照（Child Partition Snapshot）（联机）备份。这已在 Windows Server 2016 中更改为离线和在线。

 **注意：**在备份过程中，您将看到一条警告，提醒您不要将虚拟卷备份与物理磁盘备份混合。

高级设置（Advanced settings）

使用“备份计划向导”计划或修改备份时，可以修改以下设置：

- 排除。您可以排除特定文件夹及其子文件夹中的文件类型。例如，如果您备份有多个虚拟机的 Hyper-V 主机，则可能不想备份已附加的任何.iso 文件。
- VSS 备份。使用 VSS 备份选项，可以选择 VSS 完全备份或 VSS 副本备份。完整备份将更新备份历史记录，并清除日志文件。但是，如果您使用也使用 VSS 的其他备份技术，则可能需要选择 VSS 副本备份，以保留 VSS 写入程序日志文件。

Azure 站点恢复（Azure Site Recovery）

Azure 站点恢复是一个 Microsoft Azure 功能，提供将本地 Hyper-V 虚拟机和物理计算机复制到 Azure 的功能。Azure 站点恢复通过从单个位置执行复制，故障转移和恢复多个虚拟机，为组织提供业务连续性和灾难恢复服务（disaster recovery services，BCDR）。您可以将 Azure 站点恢复用于计划内的故障切换以进行测试或维护，在此您可以执行具有零数据丢失的故障转移。您还可以将 Azure 站点恢复用于计划外中断，其中根据复制频率，您预计最小的数据丢失。您可以执行故障转移和故障回复操作，并通过使用统一仪表板监视和管理虚拟机或物理计算机的 Azure 站点恢复操作。Azure 站点恢复无需使用本地辅助数据中心进行灾难恢复。

问题：列举您可能在组织中使用 Windows Server Backup 的几种场景。

问题：列举几个备份和恢复的方案。

第 4 课

Windows Server 2016 高可用性和故障转移群集 (High availability with failover clustering in Windows Server 2016)

Windows Server 2016 中的故障转移群集 (Failover clusters) 为许多服务器角色和应用程序提供了高可用性解决方案。通过实现故障转移群集，如果故障转移群集中的一台或多台计算机发生故障，您可以维护应用程序或服务的可用性。在实现故障转移群集之前，您应该熟悉常规高可用性概念。您必须熟悉群集术语，并了解故障转移群集如何工作。熟悉 Windows Server 2016 中的新群集功能也很重要。

课程目标 (Lesson Objectives)

完成本课后，您将能够：

- 描述故障转移群集。
- 使用故障转移群集描述高可用性。
- 描述群集术语。
- 描述群集类别和类型。
- 描述故障转移群集组件。
- 比较冗余技术

什么是故障转移群集 (What is failover clustering?)

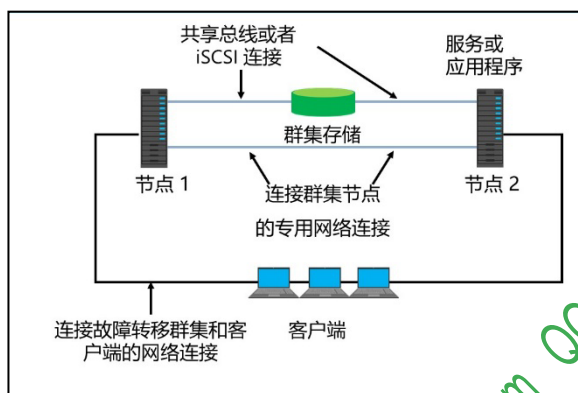
群集是一组计算机和存储设备，它们作为单个有组织的系统一起工作。您可以使用群集分配服务负载或提供高可用性的服务。您可以创建许多不同类型的群集以提供这些服务。在群集中，组件计算机通过高性能，可靠的网络彼此通信。它们可以共享一个或多个公共存储设备。您可以使用群集配置来解决可用性，可扩展性和可管理性。

一个**故障转移群集** (failover cluster) 是一组独立的计算机，它们一起工作以增加应用程序和服务的可用性。物理电缆和软件连接群集服务器，称为**节点** (nodes)。如果其中一个群集节点发生故障，另一个节点将开始提供服务。此过程称为故障转移。通过故障转移，您可以最小化服务中断。

在故障转移群集中，群集中的每个节点都具有以下属性：

- 与群集中的其他节点具有完全连接和通信。
- 意识到另一个节点加入或离开群集。
- 连接到客户端计算机可以通过其访问群集的网络。
- 通过共享总线或 iSCSI 连接连接到共享存储。
- 了解本地运行的服务或应用程序以及在所有其他群集节点上运行的资源。

问题：如果我可以将虚拟机从任何位置迁移到另一个位置，为什么需要实现群集？



高可用性和故障转移群集 (High availability with failover clustering)

故障转移群集通过提供数据, 应用程序和服务在不同故障情况下可用, 满足组织对高可用性的业务需求。但是, 应安装特定的硬件配置以满足故障转移群集的先决条件。此外, 您应安装特定的操作系统功能和应用程序组件作为故障转移群集部署的先决条件。

在为特定技术部署故障转移群集之前, 请阅读该特定技术的故障转移群集规划和部署指南和最佳实践文档。不同应用程序的高可用性部署可能有所不同。例如, Microsoft Exchange Server 在 Windows Server 操作系统中使用故障转移群集功能, 但是, 您使用 Exchange 服务器管理工具执行高可用性部署和故障转移群集安装的过程。您必须从服务器管理器控制台或 Windows Server 操作系统中的 Windows PowerShell 安装故障转移群集功能来部署 Hyper-V 的高可用性。

- 故障转移群集提供了数据, 应用程序和服务的高可用性
- 故障转移群集的注意事项 :
 - 硬件先决条件
 - 必备软件
 - 应用程序有特殊的故障转移群集配置
 - 应用程序必须是群集感知

应用程序必须具有群集感知功能, 才能使用故障转移群集。 Windows Server 操作系统中的故障转移群集为以下应用程序和功能提供高可用性 :

- DFS 命名空间服务器
- DHCP 服务器
- 分布式事务协调器 (DTC)
- 文件服务器
- Internet 存储名称服务 (iSNS) 服务器
- 消息队列
- 其他服务器
- 打印服务器
- 远程桌面连接代理 (Remote Desktop Connection Broker)
- 虚拟机
- WINS 服务器

群集术语 (Clustering terminology)

要部署故障转移群集, 您应该了解群集术语。故障转移群集术语在 Windows Server 和第三方故障转移群集产品中都是类似的。

此表显示故障转移群集术语。

故障转移群集术语包括 :

- 节点
- 服务或应用程序
- 共享存储
- 仲裁
- 见证
- 故障切换/故障恢复
- 客户

术语	描述
节点 (Node)	作为故障转移群集一部分的 Windows Server 2016 计算机，并已安装故障转移群集功能。
服务或者应用程序	可在群集节点之间移动的服务（例如，群集文件服务器可在任一节点上运行）。
共享存储	所有群集节点都可以访问的外部存储。
仲裁 (Quorum)	要继续运行群集必须联机的元素数量。当群集节点投票时确定仲裁。
见证 (Witness)	当节点数为偶数时，参与群集投票的服务器。
故障转移 (Failover)	由于节点故障或管理员的操作，将群集资源从第一个节点移动到第二个节点的过程。
回复 (Failback)	作为第一节点再次上线或管理员的动作的结果，将群集资源从第二节点移回到第一节点的过程。如果服务或应用程序从 Node1 故障转移到 Node2，则当 Node1 再次可用时，服务或应用程序将故障回复到 Node1。
客户端	连接到故障转移群集并且不知道该服务正在运行的节点的计算机。



注意：您将在第 8 单元“实现和管理故障转移群集”中更详细地学习故障转移群集术语。

群集类别和类型 (Clustering categories and types)

群集技术包括不同类型的群集，具体取决于为高可用性配置所需的应用程序类型。群集部署可能因群集节点的位置而异。此外，群集功能可以根据在每个群集成员节点上执行的活动而不同。

考虑根据组织的特定业务需求部署不同类别和类型的群集。群集类别和类型包括：

- 群集的类型。例如，通过部署故障转移群集实现 Hyper-V 高可用性，而使用 NLB 群集实现 Web 服务器的高可用性。
 - 为有状态 (stateful) 的应用程序 (如 SQL Server 和 Exchange Server) 部署故障转移群集。有状态应用程序具有长时间运行的内存状态，或具有大的，经常更新的数据状态。其他类型的故障转移群集应用程序包括 Hyper-V，文件服务器和打印服务器。
 - 为无状态 (stateless) 应用程序 (如 Web 服务器) 部署 NLB。无状态应用程序不具有长时间运行的内存状态，并且处理只读或不频繁更改的数据。无状态应用程序将每个客户端请求视为独立操作，它们可以独立地对每个请求进行负载均衡。无状态应用程序包括 Web 服务器，虚拟专用网 (VPN)，文件传输协议 (FTP) 服务器以及防火墙和代理服务器。NLB 群集支持不同的基于 TCP 或 UDP 的服务和应用程序。
- 单站点群集和多站点群集。群集部署可以包括所有节点都位于单个数据中心中的情形。但是，一些公司希望在主数据中心不可用时扩展其应用程序可用性。因此，组织部署伸展群集，在多个数据中心部署节点。多站点群集还可以包括组织在云环境 (例如 Azure) 中放置某些群集节点或见证服务器的情况。

- 应用程序的部署类型：
 - 故障转移群集
 - 网络负载均衡群集
- 节点位置：
 - 单站点群集
 - 多站点群集
 - 节点或见证服务器托管在云环境
- 活动服务器的数目：
 - 主动 - 主动集群
 - 主动 - 被动集群

- 主动 - 主动 (Active-Active) 和主动 - 被动 (Active-Passive) 群集。在主动 - 主动群集配置 (例如扩展文件服务器群集) 中，多个节点运行群集应用程序资源并接受客户端连接。在主动 - 被动群集配置中，一个节点运行群集应用程序，而其他节点是被动的，不接受客户端连接。如果活动节点由于任何原因失败，一些剩余的被动节点变为活动并运行应用程序，接受客户端连接。

故障转移群集组件 (Failover clustering components)

故障转移群集解决方案由此表中列出的几个组件组成。

故障转移群集组件包括：

- 节点
- 网络
- 资源
- 群集存储
- 仲裁
- 见证
- 服务或应用程序
- 客户

组件	描述
节点 (Nodes)	作为故障转移群集成员的计算机。 这些计算机运行群集服务以及与群集关联的任何资源和应用程序。
网络 (Network)	群集节点可以在其之间与客户端进行通信的网络。 我们在第 8 单元：实施和管理故障转移群集中更详细地讨论这些网络。
资源 (Resource)	节点托管资源。 群集服务管理资源，并可以启动，停止和将资源移动到另一个节点。
群集存储 (Cluster storage)	群集节点共享的存储系统。 在某些情况下，例如运行 Exchange Server 的服务器群集，不需要共享存储。
仲裁 (Quorum)	必须联机以允许群集继续运行的元素数。 当群集节点投票时确定仲裁。
见证 (Witness)	见证可以是文件共享或共享磁盘，用与维持仲裁。理想情况下，见证应该位于与故障转移群集使用的网络逻辑和物理上都分开的网络上。但是，它必须可以被所有群集节点成员访问到。
服务或程序 (Service or application)	Microsoft 提供给客户端和客户端使用的软件实体。
客户端	使用群集服务的计算机 (或用户) 。

我们会在第 8 单元：实现和管理故障转移群集中更详细地讨论故障转移群集组件。

冗余技术比较 (Technology redundancy comparison)

组织部署不同的技术用于数据保护，高可用性，站点恢复能力和灾难恢复。然而，没有一种技术可以覆盖每个故障或数据丢失情况。因此，组织应该知道什么组合的技术可以保护他们不同的故障情况。

例如，故障转移群集可保护组织免受服务器硬件故障的影响，但它不能保护组织免受数据删除或数据损坏所导致的数据丢失。 Windows Server Backup 可保护组织免受数据删除或数据损坏所导致的数据丢失，但不能保护组织免受服务器硬件故障的影响。因此，组织应选择使用故障转移群集来保护其应用程序不受服务器硬件故障的影响，并且还应用 Windows Server Backup 保护数据不被数据删除和损坏。

	零停机	硬件故障	站点故障	数据删除/损坏	自动故障转移
实时迁移	是	没有	没有	没有	没有
群集	取决于应用	是	取决于应用	没有	是
Hyper-V 副本	没有	是	是	取决于应用	没有
Windows Server Backup	没有	是	取决于具体场景	是	没有

此表列出了多种 Windows Server 技术及其如何响应不同的故障情况：

	零宕机时间	硬件故障	站点故障	数据删除或损坏	自动故障转移
在线迁移	是	否	否	否	否
群集	依赖于应用	是	依赖于应用	否	是
Hyper-V 副本	否	是	是	取决于应用	否
Windows Server Backup	否	是	依赖于应用	是	否

某些项目标记为“依赖”，因为具体的能力取决于应用程序和场景。例如，如果在部署 Exchange Server 时使用故障转移群集，则它为客户端提供零停机时间，并且还可以使用特定 Exchange Server 高可用性配置解决站点故障。但是，使用故障转移群集（例如文件服务器）的其他应用程序可能包括一些最小的停机时间，之后将还原应用程序，数据和服务。

问题：故障转移群集节点的属性是什么？

问题：故障转移群集解决方案的故障转移群集组件是什么？

海量视频题库 myitpub.com QQ:5565462

单元复习和作业 (Module Review and Takeaways)

最佳实践 (Best Practices)

- 在实施高可用性虚拟机之前开发标准配置。您应该将主机计算机配置为尽可能接近相同。要确保您具有一致的 Hyper-V 平台, 请配置标准网络名称, 并对 CSV 使用一致的命名标准。
- 使用 Hyper-V 副本中的新功能将复制扩展到多个服务器。
- 考虑使用横向扩展文件服务器群集 (Scale-Out File Server cluster) 作为高可用性虚拟机的存储。
- 实现 VMM。VMM 在 Hyper-V 和故障转移群集管理器之上提供了一个管理层, 可以阻止您在管理高可用性虚拟机时犯错误。例如, 它可能阻止您在群集中的所有节点无法访问的存储上创建虚拟机。

常见问题和故障诊断技巧 (Common Issues and Troubleshooting Tips)

常见问题	排错技巧
实施 CSV 并将共享存储迁移到 CSV 后, 虚拟机故障转移失败。	
虚拟机故障转移到主机群集中的另一个节点, 但丢失所有网络连接。	
重新启动作为主机群集成员的 Hyper-V 主机四个小时后, 主机上仍然没有运行虚拟机。	

复习问题 (Review Question)

问题：在 Windows Server 2016 中, 是否必须实现 CSV 以为 VMM 中的虚拟机提供高可用性?

工具 (Tools)

使用 Hyper-V 实现故障转移群集的工具包括：

工具	在哪里	使用场景
故障群集管理器 (Failover Cluster Manager)	管理工具	管理故障转移群集
Hyper-V 管理器 (Hyper-V Manager)	管理工具	管理虚拟机
VMM 控制台 (VMM Console)	开始菜单	管理 Hyper-V 宿主机和虚拟机

海量视频题库 myitpub.com QQ:5565462