第 3 章

实现企业存储解决方案 (Implementing enterprise storage solutions)

目录：

单元概述（Module Overview） 1

DAS、 NAS、和 SAN 概述（Overview of DAS, NAS, and SANs） 2

比较光纤通道，iSCSI 和以太网光纤通道（Comparing Fibre Channel, iSCSI, and Fibre Channel over Ethernet） 10

理解 iSNS、 DCB 和 MPIO（Understanding iSNS, DCB, and MPIO） 19

在 Windows Server 2016 中配置共享（Configuring sharing in Windows Server 2016） 24

实验: 规划和配置存储技术和组件（Planning and configuring storage technologies and components） 33

单元复习和作业（Module Review and Takeaways**）** 40

单元概述（Module Overview）

存储是在规划和部署 Windows Server 2016 操作系统时必须考虑的关键组件之一。 大多数组织需要大量的存储，因为用户工作经常使用创建新文件的应用程序，这又要求在中央位置存储。 当用户长时间保持文件时，一方面文件越加越多，另一方面对存储的需求就会增加。

在过去几年中，随着新技术的引入和现有技术的扩展，存储选项大大增加。 因此，在规划存储解决方案时，您必须考虑当前环境的技术以及引入新技术的影响。 许多组织已经对核心的硬件供应商和通信标准进行了标准化，虚拟化正在推动许多管理员重新评估这些标准，并开始考虑针对大量虚拟化基础架构的下一代存储解决方案。 本单元向您介绍各种存储硬件和通信技术。

目标（Objectives）

完成本单元后，您将能够：

- 描述直接连接存储（direct-attached storage ，DAS），网络连接存储（network-attached storage，NAS）和存储区域网络（storage area network，SAN）。
- 比较光纤通道（Fibre Channel），Internet 小型计算机系统接口（Internet Small Computer System Interface ，iSCSI）和以太网光纤通道（Fibre Channel over Ethernet）。
- 解释使用 Internet 存储名称服务（Internet Storage Name Service ，iSNS），数据中心桥接（Datacenter Bridging ，DCB）和多路径 I/O（Multipath I/O ，MPIO）。
- 在 Windows Server 2016 中配置共享。

第 1 课
DAS、 NAS、和 SAN 概述（Overview of DAS, NAS, and SANs）

在规划存储时，您需要确定服务器如何访问磁盘。 在某些情况下，您可以将磁盘直接连接到需要存储的服务器。 然而，在企业中，存储通常在 NAS 或 SAN 中，这提供了更多的灵活性。 在本课程中，您将学习可用于为服务器提供存储访问的不同方法。

课程目标（Lesson Objectives）

完成本课后，您将能够：

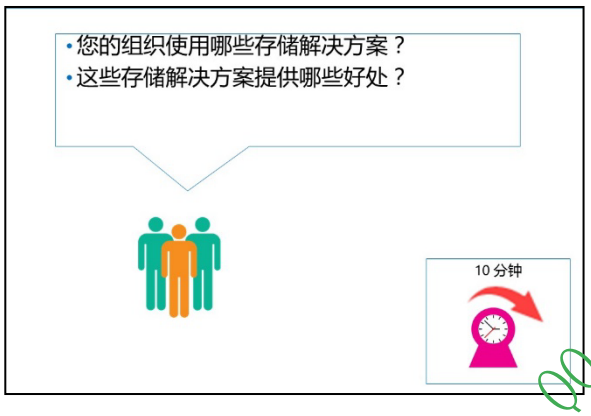
- 描述在您的环境中部署的存储解决方案。
- 描述 DAS。
- 描述 NAS。
- 描述 SAN。
- 确定何时应使用不同的存储类型。
- 列出块级（block-level）存储和文件级（file-level）存储之间的差异。

讨论：哪些存储解决方案部署在您的环境中？（Which storage solutions are deployed in your environment?）

组织有各种各样的存储选项，如 DAS，NAS 和 SAN。 这些选项中的每一个都适用于不同的场景。

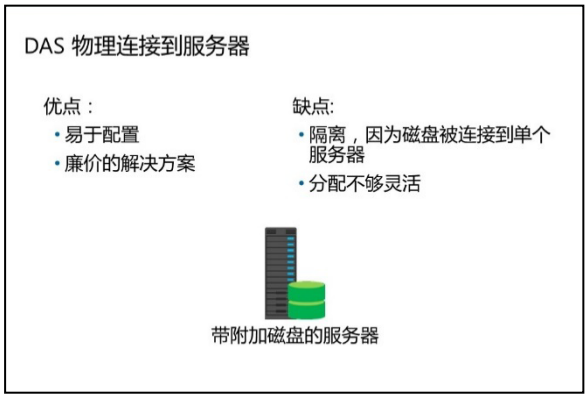
问题：您的组织使用哪些存储解决方案？

问题：这些存储解决方案提供什么好处？



什么是 DAS（What is DAS）?

几乎所有服务器都提供内置存储或*直接连接存储（direct-attached storage ，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，或者通过 USB 电缆或替代连接器（alternative connector）连接到服务器的磁盘。 但是，由于您将 DAS 存储器物理连接到服务器，如果服务器发生故障，则存储将不可访问。 DAS 具有各种磁盘类型，例如串行 ATA（Serial ATA ，SATA），串行连接 SCSI（serial attached SCSI ，SAS）或固态驱动器（solid-state drive ，SSD）。 这些磁盘类型都提供不同的速度和性能级别，并且具有各自的优点和缺点。.



使用 DAS 的优点（Advantages of using DAS）

典型的 DAS 系统具有包括多个硬盘驱动器的数据存储设备，其通过主机总线适配器（host bus adapter，HBA）直接连接到计算机。 在 DAS 和计算机之间没有网络设备（集线器，交换机或路由器），而是存储器直接连接到利用它的服务器。 因此， DAS 是最容易部署和维护的存储系统。

DAS 通常是可用的最便宜的存储，并且可以以各种速度和大小广泛使用以适应不同的安装。 此外，它的价格优势非常强，并且非常容易配置。 在大多数情况下，你只需简单插上设备，保证 Windows 操作系统能识别它，然后使用 Disk Management 功能来配置磁盘即可。

使用 DAS 的缺点（Disadvantages of using DAS）

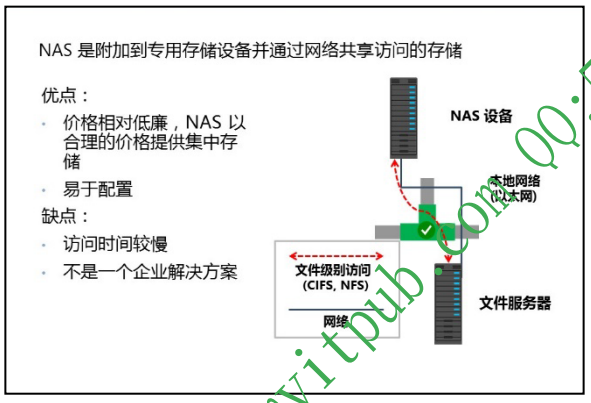
在 DAS 本地存储数据使数据集中化更加困难，因为数据在多个服务器上。 这可能会使备份数据更加复杂，用户可能会发现更难找到他们想要查找的数据。 此外，如果 DAS 连接的任何一个设备遭受电源中断，该设备上的存储将不可访问。

使用 DAS，向服务器分配更多存储可能比使用 SAN 更复杂。 使用 DAS，需要在服务器中安装物理磁盘，而使用 SAN，可以向服务器提供现有未分配的存储以扩展存储，而无需物理访问服务器。

什么是 NAS?（What is NAS?）

NAS 是连接到专用存储设备的存储，然后通过网络访问。 NAS 与 DAS 不同，因为存储不直接附加到每个单独的服务器，而是可以通过网络访问许多服务器。 NAS 有两个不同的解决方案：低端设备（仅限 NAS）和与 SAN 集成的企业级 NAS。

每个 NAS 设备具有专用操作系统，可以控制该设备上的数据访问，从而减少了与其他服务器服务共享存储设备所需的开销。 Windows Storage Server 是 Windows Server 2016 的一项功能，是 NAS 软件的一个示例。



NAS 设备通常提供对存储的文件级访问，这意味着存储中的数据只能作为文件和文件夹访问，您必须使用通用 Internet 文件系统（Common Internet File System ，CIFS），服务器消息块（Server Message Block ，SMB）或网络文件系统（network file system ，NFS）来访问文件。

要启用 NAS，您需要一个存储设备。通常，这些设备没有任何服务器接口，例如键盘，鼠标和监视器。要配置设备，需要提供网络配置，然后通过网络来访问设备。然后，您可以使用 NAS 的名称和您创建的共享在设备上创建共享文件夹。这些共享然后可由网络的用户访问。

使用 NAS 的优点（Advantages of using NAS）

NAS 对哪些正在寻找一个简单和具有成本效益的方式实现快速数据访问的组织来说是一个理想的选择，它应用在在文件级，多个客户端。 NAS 用户受益于性能和生产力的提高，因为 NAS 设备的处理能力专用于文件分发。

NAS 也适合作为中等价格的解决方案进入市场。它不贵，但它的以下方式比 DAS 适合于更多的需求：

- NAS 存储通常比 DAS 大得多。
- NAS 通常包括用于数据冗余的独立磁盘冗余阵列（RAID）。
- NAS 为所有关键文件提供单一位置，而不是通过使用 DAS 将其分散在各种服务器上。
- NAS 以实惠的价格提供集中存储。
- 可从任何操作系统访问 NAS 设备。它们通常具有多协议支持，并且可以同时通过 CIFS 和 NFS 提供数据。例如，Windows 和 Linux 主机可以同时访问 NAS 单元。

NAS 也是即插即用（*Plug and Play* ，PNP）解决方案，易于安装，部署和管理，无论您是否有 IT 人员。

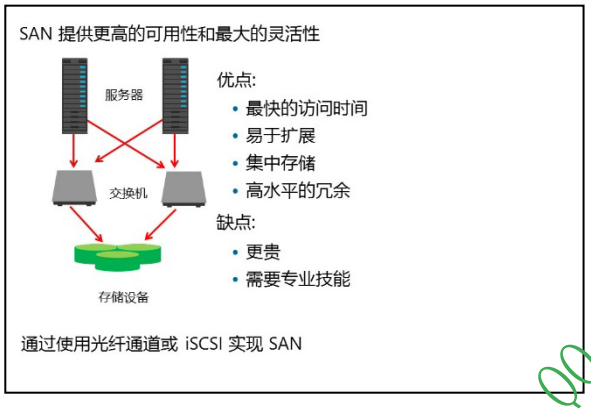
使用 NAS 的缺点（Disadvantages of using NAS）

NAS 从技术角度考虑比 SAN 慢。 您通常使用以太网协议（Ethernet protocol）访问 NAS，它主要依赖于支持 NAS 解决方案的网络。 因此，NAS 通常用作文件共享/存储解决方案，但您不能（并且不应该尝试）将其用于 Microsoft Exchange Server 和 Microsoft SQL Server 等数据密集型程序。

NAS 对于中小型企业来说是可负担的，但是提供较少的性能并且可能比 SAN 更不可靠。 因此，大多数大型企业使用 SAN 而不是 NAS。

什么是 SAN?（What is a SAN?）

第三种类型的存储是 SAN，其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 通常包括各种组件，例如 HBA，用于帮助路由流量的特殊交换机，以及具有用于存储的逻辑单元号（logical unit numbers ，LUN）的存储磁盘阵列。



SAN 允许多个服务器访问存储池，其中任何服务器都可以访问任何存储单元。但是，因为 SAN 使用网络，您可以使用它连接许多不同的设备和主机，并从几乎任何地方提供对任何连接的设备的访问。。

SAN 提供块级访问。这意味着，它不是使用文件访问协议来访问磁盘内容作为文件，SAN 通过使用协议，如以太网光纤通道（Fibre Channel over Ethernet）或 Internet SCSI（iSCSI）将数据块直接写入磁盘。

如今，大多数 SAN 解决方案提供 SAN 和 NAS。后端头单元（head unit），磁盘和技术是相同的，访问方法是唯一的变化。企业通常通过以太网或 iSCSI 上的光纤通道将块存储从 SAN 配置到服务器，而 NAS 服务通常通过 CIFS 和 NFS 才可用。

使用 SAN 的优点（Advantages of using SAN）

SAN 技术在块级别读写，这使得数据访问更快。例如，对于大多数 DAS 和 NAS 解决方案，如果您写入一个 8 GB 的文件，则必须读取/写入整个文件，并计算其校验和（checksum）。但是，使用 SAN，该文件将根据您配置 SAN 的块大小写入磁盘。此速度通过使用光纤通道和块级写入来实现，而不是通过使用校验和读取/写入整个文件。

SAN 还提供：

- 将存储集中到单个池中，这使得存储资源和服务器资源独立增长。它们还可以在必要时从池中启用动态存储分配。您可以根据需要增加或减少给定服务器上的存储，而无需复杂的重新配置或重新启动设备。
- 用于附加存储的通用基础架构，支持单个通用管理模型（common-management model）进行配置和部署。
- 多个系统共享的存储设备。
- 直接从设备到设备的数据传输，无需服务器干预。
- 高度冗余。您可以通过具有多个网络设备和路径的网络部署大多数 SAN。此外，存储设备包含冗余组件，例如电源和硬盘驱动器。.

使用 SAN 的缺点（Disadvantages of using SAN）

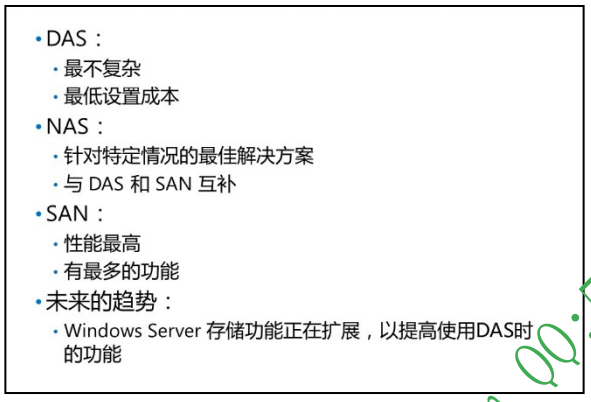
SAN 技术的主要缺点是，由于其配置复杂性，您可能需要使用管理工具并具有专门的技能。 此外，它比 DAS 或 NAS 贵得多。 入门级 SAN 通常花费与使用 DAS 或 NAS 设备的全负载服务器一样多的成本，并且没有任何 SAN 磁盘或配置。

要管理 SAN，您必须对底层技术（包括 LUN 设置，光纤通道网络，块大小和其他因素）有深入了解。 此外，每个存储供应商通常通过使用不同的工具和功能来实现 SAN。 因此，组织往往将人员专门用于 SAN 部署。.

注意： 您可以使用各种技术实现 SAN，最常见的选项是光纤通道和 iSCSI.

使用比较和使用场景（Comparison and scenarios for usage）

对 DAS，NAS 和 SAN 的良好了解是您在确定最适合您需求的存储解决方案时必须采取的第一步，您应该意识到，每种存储技术都扩展了其可用功能并增加了灵活性。 通常，你不会有一个明确的最佳选择，所以下一个主题再次检查三个拓扑，并比较它们，并解释哪一个是不同场景下的最佳解决方案。



DAS

您可能考虑使用 DAS，是因为它通常是最便宜，最不复杂的解决方案。 但是，DAS 可能需要比 NAS 和 SAN 更多的管理开销，特别是如果部署多个 DAS 解决方案。 例如，假设您的组织在 Windows Server 2016 中的故障转移群集中部署了 15 个 Microsoft Hyper-V 节点。如果使用 NAS 或 SAN，则单个高可用性存储解决方案可以容纳故障转移群集。 但是，如果使用 DAS，则可能需要 15 个设备。 在这种情况下，DAS 可以创建存储蔓延（storage sprawl），这意味着存在不断增加和扩展的存储岛（storage island），这可能难以管理和维护。

为了解决这个问题，最新的 DAS 解决方案有时包括一些关键的 SAN 功能，包括多种通信协议，企业管理软件和易于扩展。 您可以使用这些功能添加其他磁盘架（disk shelves）。 入门级 DAS 产品仅在每个设备中提供单个机架，并且不支持扩展。 这些限制导致存储蔓延。 但是，对于高端 DAS 系统，您可以扩展磁盘架和磁盘数，并轻松部署具有数百 TB 容量的存储空间的解决方案。 因此，这些解决方案可以处理前一节描述的 Hyper-V 故障转移群集方案。

在大型组织中，一些数据库管理团队和消息传递（messaging）团队倾向于使用 DAS 解决方案来减少对组织存储团队的依赖。 这让他们对自己的存储更多的控制。

NAS

大多数组织使用 NAS，虽然许多组织不将其共享文件夹解决方案称为 NAS。 第三方存储公司已经推出或扩展了其 NAS 产品，因此 SAN 解决方案通常也通过 CIFS 或 NFS 提供 NAS 服务。 因此，在许多组织中，SAN 和 NAS 通常共享相同的存储设备，磁盘架和支持基础架构。

NAS 是如此无处不在，它直接与 DAS 或 SAN 进行比较可能是没有用的。 DAS 和 SAN 经常直接相互竞争，但是 NAS 通常在还包含 DAS 和 SAN 的系统中起到互补作用。 最近，一些技术已经采用对 NAS 的支持。 一个这样的例子是 Hyper-V，现在支持在 SMB 3.0 共享上存储虚拟机。 如果其他技术开始支持 NAS，那么将来可能会与 DAS 和 SAN 进行更直接的竞争。

SAN

SAN 解决方案被广泛地称为最佳企业存储解决方案。 长期以来，SAN 是高性能存储的唯一解决方案。 不仅因为它灵活和高性能，而且它比 DAS 和 NAS 更容易扩展。

然而，DAS 和 NAS 最近扩大了它们的市场。 DAS 解决方案可以提供高性能存储，而没有 SAN 的复杂性，因为它利用了最新的磁盘和 SSD 技术。 对策是，SAN 解决方案可以在更大规模上提供相同的磁盘和 SSD 技术，规模是关键的区别。 尽管最大的 DAS 解决方案提供了数百 TB 的存储空间，但是顶级 SAN 解决方案提供了数千 TB 的存储空间。 此外，SAN 解决方案提供了更多的主轴（spindle），这通常会带来更好的性能。

最后，SAN 解决方案提供：

- 最好的管理工具。 SAN 管理工具通常提供单一的管理接口。
- 最具企业特色。 例如，一个共同的特征是在高速旋转磁盘的主轴之前的 SSD 缓存。
- 最大的灵活性。 SAN 在单个解决方案中提供 SAN 和 NAS 服务。

未来趋势（Future trends）

随着每个新版本的 Windows Server，微软正在使 Windows Server 中的 DAS 解决方案相比 SAN 存储解决方案更具竞争力的。 Windows Server 2012 引入了存储空间（storage space），为 DAS 提供冗余，而无需 RAID 控制器。但是，我们建议您使用缓存控制器（caching controller）来提高性能。Windows Server 2012 R2 引入了存储分层（storage tiering），允许最频繁访问的磁盘块自动存储在 SSD 驱动器上，而不是旋转磁盘（spinning disk）。 通过实现 Scale-Out 文件服务器（Scale-Out File Server）也可以实现共享文件夹的高可用性。 Windows Server 2016 还添加了存储副本（Storage Replica），以在使用 DAS 的两台服务器之间提供块级同步或异步复制。

Windows Server 所包含的存储功能正在稳步扩展，以包括之前只在 SAN 中可用的存储功能。 如果功能集满足您的需求，则将 Windows Server 与 DAS 配合使用通常比使用 SAN 更便宜。

使用 DAS, NAS, 或者 SAN 的场景（Scenarios for using DAS, NAS, or SAN）

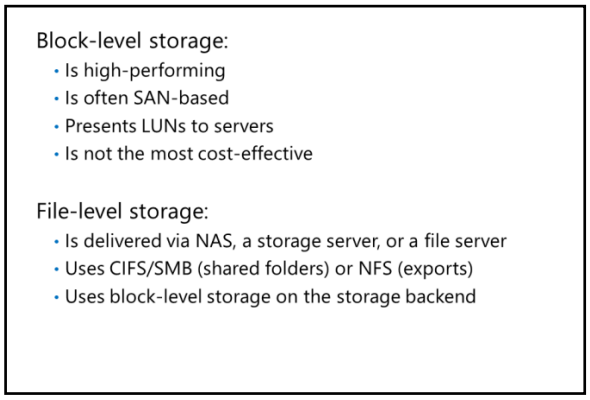
下表突出显示了一些常见的存储场景，并介绍了每种场景中 DAS，NAS 和 SAN 的能力。

场景	DAS	NAS	SAN
用于事务型数据库（transactional database）的高性能存储	• 性能非常好，成本最低的解决方案 • 可能在大型企业环境中增加显著的管理开销	不是大多数数据库服务器的有效解决方案	卓越的性能和功能使它成为事务型数据库的最佳选
用户主文件夹（home folder）	• 性能非常好，但可能扩展到分散的存储岛 • 许多DAS安装的企业管理的管理开销增加了	最适合用户主文件夹，因为它可以从任何计算设备提供 CIFS 访问，而不会导致昂贵的成本	• 出色的性能和功能，但超过用户主文件夹的需求 • 主文件夹可能需要集中 • 成本可能过高
虚拟机的存储	性能非常好，但是管理开销高于 SAN 解决方案	支持 Windows Server 2012 R2 或更高版本中的 Hyper-V，尝试降低成本和复杂性时，NAS 是一个不错的选择	出色的性能和功能使其成为大多数虚拟环境的最佳选择
分支机构共享文件夹	• 易于部署和低成本 • 通常是分支机构常规共享文件夹的最佳选择，因为您不需要分支机构有基础架构设施。	• 易于部署 • 中等成本 • 通常是现场具有小型基础设施的分支机构的好选择	通常成本过高，功能多于分支机构所需的功能
分层存储（Tiered storage）的应用程序	不像 SAN 那么灵活，但对于小的预算情况可行	与 SAN 相比，有限的通信协议，但一些解决方案是可行的，例如具有存储空间和分层的横向扩展文件服务器	• 最灵活 • 内置分层，缓存和其他性能增强功能使 SAN 成为应用程序的最佳选择
Microsoft Exchange 数据库和日志存储	最低成本，非常好的性能，是 SAN 的一个非常好的替代品，特别是对于喜欢管理自己的存储的消息传递团队	不是有效的选择	卓越的性能和功能其成为首选

块级存储与文件级存储（Block-level storage vs. file-level storage）

您可以通过两种方式在磁盘上排列数据：按块或按文件。 这些安排数据的方式是块级存储和文件级存储。 通常，一种布置或另一种布置是特定场景中的最佳解决方案。 然而，有时，它们在存储基础设施中互补。 例如，在大型企业环境中使用两种类型的存储是常见的。

通常，将块级存储与 SAN 结合使用，并将部分或全部存储分配给服务器。 通常，将文件级存储与 NAS 结合使用，NAS，存储服务器或文件服务器通过使用文件级协议（如 CIFS 或 NFS）来分配这些存储块（chunks of storage）。 此外，您通常将文件级存储放在块级存储上。



块级存储（Block-level storage）

块级存储通过 SAN 传递到服务器，最常见的是使用 SAN 通信协议之一，如 iSCSI，光纤通道（Fibre Channel）或以太网光纤通道（Fibre Channel over Ethernet）。 存储管理员从块级存储块中（chunks of block-level storage）创建存储卷。 在卷内，存储管理员创建 LUN，它们是虚拟存储区域。 您可以配置或呈现 LUN 以在一个或多个服务器上使用。 服务器将呈现的 LUN 看作物理硬盘驱动器，并且管理员根据 LUN 在 Windows Server 2016 中创建卷。 卷使用文件系统（如 NTFS 文件系统或复原文件系统（Resilient File System ，ReFS）格式化，然后以与物理或虚拟硬盘相同的方式访问。 块级存储具有以下特性：

- 它非常灵活。 例如，您可以将其用作操作系统卷，数据卷或共享文件夹的存储位置。
- 它不绑定到特定的操作系统或特定的文件系统。 所有核心操作系统和文件系统都支持它。
- 操作系统可以从块级存储 LUN 启动。 这意味着您的组织可以部署无盘物理服务器（diskless physical server）。 在这种情况下，服务器启动时使用光纤通道或 iSCSI HBA 连接到其引导 LUN。
- 您可以将块级存储直接呈现给虚拟机，以满足高性能存储需求。 在 Hyper-V 中，可以使用传递磁盘（pass-through disk）或使用虚拟光纤通道（virtual Fibre Channel）向虚拟机提供块级存储。

文件级存储（File-level storage）

CIFS 和 NFS 是文件级存储使用的主要通信协议。 CIFS 最初是 SMB 的增强版本。 然而，今天，术语 CIFS 和 SMB 通常可互换使用。 Microsoft 继续在 Windows Server 操作系统的许多主要版本中对 CIFS 进行增强。 文件级存储具有以下特性：

- 仅通过文件共享协议访问文件级存储。
- 文件级存储位于块级存储的顶部，并具有文件系统。
- 一些应用程序支持文件级存储，但其他应用程序不支持。 在 Windows Server 2012 R2 中，Hyper-V 开始在 SMB 3.0 共享文件夹中支持虚拟机存储。
- 文件级存储通常比块级存储更经济。

•

检查您的知识（Check Your Knowledge**）**

问题	
哪种类型的存储通常具有最低的实现成本？	
选择正确的答案。	
	DAS
	NAS
	SAN
	块级存储
	文件级存储

通过在右边的列中放置标记来验证语句的正确性。

声明	**回答**
SAN 提供文件级存储。	

第 2 课
比较光纤通道，iSCSI 和以太网光纤通道（Comparing Fibre Channel, iSCSI, and Fibre Channel over Ethernet）

您可以使用多种协议来配置 SAN，而为 SAN 选择的协议通常基于您组织的需求和技术人员的技能。 光纤通道是 SAN 的最佳性能解决方案，但它是实现最复杂和最昂贵的系统。 iSCSI SAN 的成本较低，因为设备的专业性较差，而且更易于实施和管理。 在本课中，您将了解到光纤通道和 iSCSI。

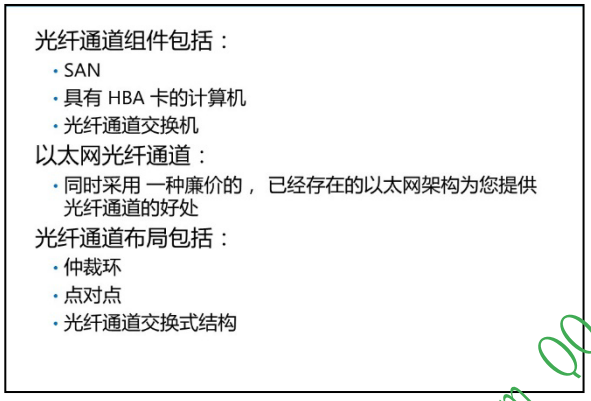
课程目标（Lesson Objectives）

完成本课后，您将能够：

- 描述光纤通道。
- 列出实现光纤通道的注意事项。
- 描述 iSCSI。
- 标识作为 iSCSI SAN 一部分的组件。
- 列出实现 iSCSI 的注意事项。
- 描述物理存储组件。
- 配置 iSCSI 目标。

什么是光纤通道（What is Fibre Channel）？

光纤通道是一种高性能网络技术，主要用于将计算机连接到 SAN。 它是一个历史悠久的标准，并于 1994 年获得批准。光纤通道依赖于通过网络传输 SCSI 命令的光纤通道协议。 典型的光纤通道实现包含以下组件：



- SAN。 在光纤通道实现中，SAN 是存储后端。它用作光纤通道目标，它是侦听计算机请求的组件。
- 带有 HBA 卡的计算机。 在光纤通道实现中，具有 HBA 卡的计算机是发起程序（*initiator*），因为它在需要访问 SAN 上的数据时发起请求。
- 光纤通道交换机（Fibre Channel switch）。 在光纤通道实现中，您通常使用光纤通道交换机，以使计算机不直接连接到 SAN。 SAN 通常具有非常有限数量的目标端口，并且那些端口几乎总是连接到光纤通道交换机。

以太网光纤通道是通过标准以太网网络的新型光纤通道实现。 它变得越来越受欢迎，因为它提供了出色的性能，特别是当你在廉价，并且经常预先存在的以太网基础设施中使用它。 您可以使用以太网光纤通道将您公司所有的不同通信机制融合到以太网。 使用以太网光纤通道来合并您的通信系统有三个主要优点，包括：

- 与复杂的多网络相比，管理单个网络拓扑更容易。
- 您可以使用以太网光纤通道的许多标准网络故障排除工具。

- 通常不需要专门的培训。

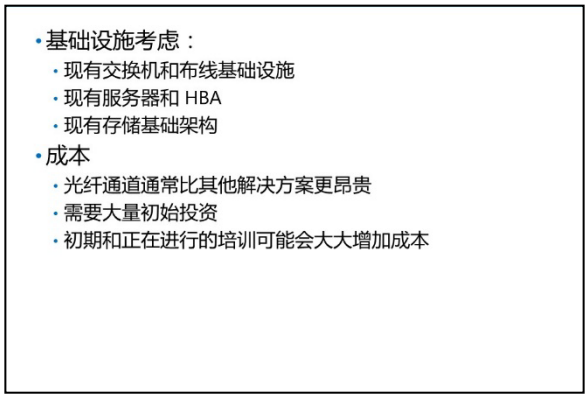
您可以使用以下三种布局之一安排光纤通道网络：

- 仲裁环（Arbitrated loop）。 在仲裁环路中，光纤通道主机和存储设备以环形连接，并且不需要开关（Switch）。 此选项是首次引入时开始使用光纤通道便宜方式。然而，由于光纤通道和融合交换机（converged switche）是非常实惠的，所以现在是非常罕见的。
- 点对点（Point-to-point）。 在点对点部署中，光纤通道主机直接连接到存储设备，并且不需要交换机。 但是，组织很少使用此选项，因为存储设备上可用的端口数量非常有限。
- 交换结构（Switched fabric）。 这是最常见的光纤通道部署。 交换光纤网环境（Switched fabric environment）使用光纤通道交换机（Fibre Channel switches）。 所有光纤通道主机连接到光纤通道交换机，光纤通道交换机连接到后端存储。

实现光纤通道的注意事项（Considerations for implementing Fibre Channel）

在决定是否在存储环境中使用光纤通道时，必须考虑几个重要因素，包括：

- 基础设施要求。
- 存储带宽要求。
- 连接可靠性和安全性。
- 资产和管理费用。



基础架构（Infrastructure）

光纤通道的基础架构要求通常适用于新的存储部署。 使用光纤通道时，通常为其安装特定且单独的基础架构。 该专用基础架构包括以下组件：

- 光纤或网络交换机。 在仅使用光纤电缆的网络中，可以使用光纤通道交换机。 但是，许多网络使用多种类型的电缆，您可以组合使用不同类型电缆的独立网络。 在这些融合网络中，交换机必须能够处理多种类型的业务和电缆。
- HBA。 HBA 是内置在计算机主板中的附加卡或功能，用于通过光纤通道或以太网进行通信。
- 附加布线（Additional cabling）。 布线是关键组件，它通常由光纤或以太网布线组成。
- 存储控制器（Storage controller）。 存储控制器或存储磁头（*storage heads*），管理到后端存储的通信。

新的光纤通道基础设施（Fibre Channel infrastructure）通常需要专门专用于存储环境的交换机。 专用网络通常提供更好的性能和安全性，因为交换机仅用于与主机和存储控制器之间的存储相关流量。 光纤交换机通常需要额外的小型可插拔收发器（form-factor pluggable transceiver），支持光纤通道布线。 这增加了基础设施的初始成本。 此外，每个主机还需要至少一个专用 HBA，并且通常需要两个用于冗余的 HBA，您必须与生产网络流量分开管理和连接它们。 最后，您使用的存储系统也必须支持光纤通道。

您可以使用具有多种电缆类型的光纤通道，其中最常见的是：

- 单模光纤（Single-mode fiber optic）。
- 多模光纤（Multi-mode fiber optic）。
- 以太网（Ethernet:）：
  - 以太网光纤通道（Fibre Channel over Ethernet.）。

  - IP 光纤通道（Fibre Channel over IP）。
- 以太网铜缆（Ethernet over Copper）。

专用光纤通道基础设施使用各种标准的光纤电缆。 多模光纤电缆比单模光纤电缆便宜，适用于大多数数据中心。 光纤通道的 128 吉比特每秒（Gbps）标准支持高达 100 米的多模光纤和高达 2,000 米的单模光纤。 大多数组织不需要 2,000 米的距离，但是当需要时，单模光纤提供了选择。

带宽（Bandwidth）

使用光纤通道连接到存储环境的最重要的好处之一是光纤通道可以提供的带宽和可靠性。 目前，每个端口的带宽速度高达 16 Gbps，光纤通道在每个端口上优于以太网。 这种额外的性能能力可能是决定是否使用光纤通道的主要因素。 最新的光纤通道标准是 32 Gbps。

可靠性和安全性（Reliability and security）

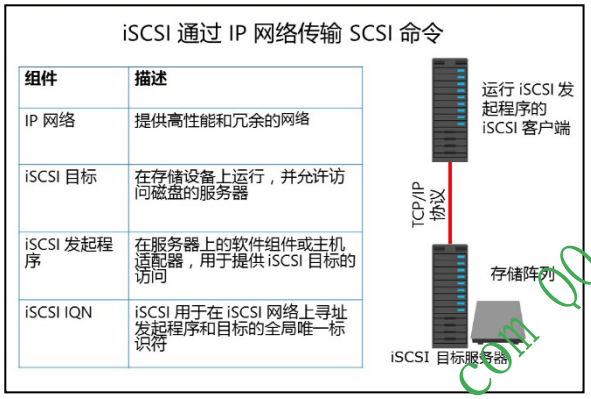
光纤通道提供良好的连接性，可靠性和安全性，这都是重要的好处。 光纤通道协议优于以太网协议，因为它要求以特定顺序接收帧（frame）。 基于传输控制协议（Transmission Control Protocol ，TCP）的协议不是这种情况，这可能会降低性能和可靠性。 此外，由于光纤通道部署通常使用专用基础架构，因此它更安全，更不易受攻击或恶化。 与光纤通道相比，如果系统的存储通信与其他网络流量共享，则主机的存储操作容易受到可能中断 TCP 通信的相同攻击。 例如，在具有融合基础设施的环境中的分布式拒绝服务（distributed denial of service ，DDoS）攻击可能会阻止 TCP 和存储通信。 当您使用专用光纤通道基础架构时，此漏洞会最小化。 在这种情况下中间层可能是以太网光纤通道，通过典型的以太网提供光纤通道的可靠性。

成本（Costs）

管理光纤通道解决方案的人员需要一组专门的技能，这可能使其比其他存储解决方案更昂贵。 内部人员可能需要额外的培训，以初步部署和管理解决方案，以及持续的培训，以保持技术变化的最新状态。 如果您使用第三方供应商来支持光纤通道解决方案，则您的成本可能与使用组织内的员工相同或甚至更高。

什么是 iSCSI（What is iSCSI）?

iSCSI 是支持通过传输控制协议/因特网协议（TCP /IP）网络访问远程基于 SCSI 的存储设备的协议。 iSCSI 通过 IP 网络传输标准 SCSI 命令，以便于数据传输，并管理远距离的存储。您可以使用 iSCSI 通过局域网（LAN），广域网（WAN），内部网（intranet）或 Internet 传输数据。



iSCSI 依赖于标准以太网网络架构。您可以选择使用专用硬件，例如 HBA 或网络交换机。 iSCSI 使用 TCP/IP，特别是 TCP 端口 3260.这意味着 iSCSI 使两个主机能够通过使用现有的以太网网络协商和交换 SCSI 命令。两个主机协商的示例包括会话建立（session establishment），流控制（flow control）和包大小。通过这样做，iSCSI 采用通用的，高性能的，本地存储总线子系统架构，并通过网络对其进行仿真，从而创建 SAN。

与某些 SAN 协议不同，iSCSI 不需要专门的布线。您可以通过现有的交换和 IP 基础设施运行它。但是，为了确保性能，您应该在专用网络上运行 iSCSI SAN 部署。否则，您可能会遇到严重降低的性能。

iSCSI SAN 部署包括以下内容：

- IP 网络。您可以使用标准网络接口适配器和标准以太网协议网络交换机将服务器连接到存储设备。为了提供足够的性能，网络应提供至少 1 Gbps 的速度，并且应为 iSCSI 目标（iSCSI target）提供多条路径（multiple paths）。我们建议您使用专用的物理和逻辑网络来实现快速，可靠的吞吐量。

- iSCSI 目标（iSCSI targets）。 ISCSI 目标呈现或宣传存储，类似于本地连接存储的硬盘驱动器的控制器。但是，服务器通过网络访问此存储，而不是在本地访问。许多存储供应商将硬件级 iSCSI 目标作为其存储设备硬件的一部分。其他设备或设备（如 Windows Storage Server 设备）通过使用软件驱动程序和至少一个以太网适配器来实现 iSCSI 目标。 Windows Server 2016 提供 iSCSI 目标服务器（*iSCSI Target Server*）作为 iSCSI 协议的驱动程序，作为文件和存储服务（File and Storage Services）角色的角色服务。
- iSCSI 发起程序（iSCSI initiators）。 iSCSI 目标将存储显示给 iSCSI 发起程序或客户端。 iSCSI 发起程序充当远程磁盘的本地磁盘控制器。自 Windows Server 2008 和 Windows Vista 以来的所有 Windows 版本都包括 iSCSI 发起程序，并且可以连接到 iSCSI 目标。
- iSCSI 限定名称（iSCSI qualified name ，IQN）。 IQN 是 iSCSI 用于在 iSCSI 网络上寻址发起程序和目标的唯一标识符。配置 iSCSI 目标时，必须为将连接到目标的 iSCSI 发起程序配置 IQN。 iSCSI 发起程序也使用 IQN 连接到 iSCSI 目标。但是，如果 iSCSI 网络上的名称解析可能成为问题，您可以通过其 IP 地址识别 iSCSI 端点（目标和发起程序）。

iSCSI 组件（iSCSI components）

本主题讨论 iSCSI 的两个主要组件：iSCSI 目标服务器和 iSCSI 发起程序.

iSCSI 目标服务器（iSCSI Target Server）

iSCSI 目标服务器角色服务提供基于软件和硬件独立的 iSCSI 磁盘子系统。您可以使用 iSCSI 目标服务器创建 iSCSI 目标和 iSCSI 虚拟磁盘，然后使用服务器管理器来管理这些 iSCSI 目标和虚拟磁盘。

Windows Server 2016 所包含的 iSCSI 目标服务器提供以下功能：

- 网络或无盘启动。您可以通过使用引导功能的网络适配器或软件加载程序快速部署无盘服务器，并且您可以通过使用差异虚拟硬盘来使得操作系统映像的存储空间节约高达 90%。这对于大规模部署相同的操作系统映像（如在运行 Hyper-V 的虚拟机上或高性能计算（HPC）集群中）是理想的。
- 服务器应用程序存储。某些应用程序（如 Microsoft Exchange Server）需要块存储。 iSCSI 目标服务器可以为这些应用程序提供持续可用的块存储。然而，由于存储可远程访问，它还可以将块存储组合在中央或分支机构位置。
- 异构存储（Heterogeneous storage）。 iSCSI 目标服务器支持不运行 Windows 的 iSCSI 发起程序，因此在混合环境中您可以共享在 Windows 服务器上的存储。
- 实验室环境。 iSCSI 目标服务器角色使 Windows Server 2016 计算机成为网络可访问的块存储设备。如果要在将应用程序部署在 SAN 存储上之前先对它们进行测试，这将非常有用。

Windows Server 2016 中的 iSCSI 目标服务器的功能包括：

- 身份验证。您可以启用质询握手身份验证协议（Challenge Handshake Authentication Protocol ，CHAP）以验证发起程序连接或启用反向 CHAP 以允许发起程序验证 iSCSI 目标。
- 查询发起程序计算机的 ID。要使用此功能，必须使用 Windows 8 或 Windows Server 2012 及更高版本的操作系统。
- 虚拟硬盘支持。您创建 iSCSI 虚拟磁盘作为虚拟硬盘。 Windows Server 2016 支持 .vhd 和 .vhdx 文件，.vhdx 支持高达 64 TB 的容量。您创建新的 iSCSI 虚拟磁盘为 .vhdx 文件，但您可以导入. Vhd 文件。

- 可扩展性。每个目标服务器的 iSCSI 目标最大数量为 256，每个目标服务器的最大虚拟硬盘数量为 512。

附加阅读： 有关详细信息，请参考：“iSCSI 目标服务器可扩展性限制”，地址为：http://aka.ms/dfxgja

- 可管理性。 您可以使用服务器管理器或 Windows PowerShell 管理 iSCSI 目标服务器。 Windows Server 2016 使用存储管理计划规范提供程序（Storage Management Initiative Specification）与 Microsoft System Center 2012 虚拟机管理器（Virtual Machine Manager）和更高版本来管理托管（hosted）和私有云（private cloud）中的 iSCSI 目标服务器。

您可以使用以下 Windows PowerShell cmdlet 来管理 iSCSI 目标服务器：

```
Install-WindowsFeature FS-iSCSITarget-Server
New-IscsiVirtualDisk E:\iSCSIVirtualHardDisk\1.vhdx –size 1GB
New-IscsiServerTarget SQLTarget –InitiatorIds “IQN:iqn.1991-
05.com.Microsoft:SQL1.adatum.com”
Add-IscsiVirtualDiskTargetMapping SQLTarget E:\iSCSIVirtualHardDisk\1.vhdx
```

附加阅读： 有关详细信息，请参阅：“Windows PowerShell 中的 iSCSI 目标 Cmdlet”，位于：http://aka.ms/j1iomo

当您启用 iSCSI 目标服务器提供块存储时，iSCSI 目标服务器将利用现有的以太网网络。 您需要专用的 iSCSI 网络来确保性能，或者您可以在现有网络上使用服务质量（QoS）标准。 如果高可用性对您的组织很重要，您应该配置高可用性集群。 但是，配置高可用性集群时，将需要用于群集的共享存储。 此存储可以是硬件光纤通道存储或串行连接的 SCSI 存储阵列。 您可以将 iSCSI 目标服务器配置为故障转移群集中的群集角色。 Windows Server 2016 引入了存储空间直通（Storage Spaces Direct）功能，该功能使用非共享存储来创建高可用性集群。 它仅通过使用本地非共享存储和常规硬件来实现。

iSCSI 发起程序（iSCSI initiator）

iSCSI 发起程序在 Windows Server 2008 和 Windows Vista 中引入，默认情况下已安装。 要将计算机连接到 iSCSI 目标，必须启动并配置服务。

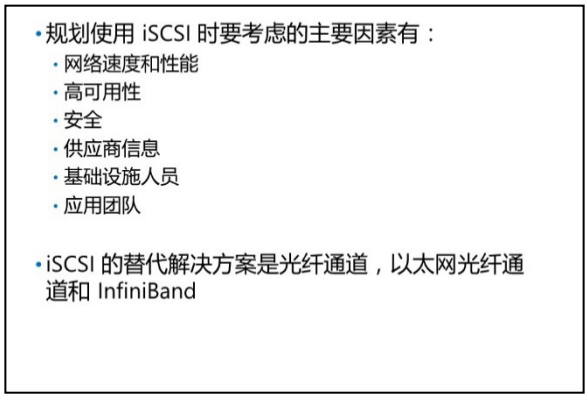
您可以使用以下 Windows PowerShell cmdlet 来管理 iSCSI 发起程序：

```
Start-Service msiscsi
Set-Service msiscsi –StartupType “Automatic”
New-IscsiTargetPortal –TargetPortalAddress iSCSIServer1
Connect-IscsiTarget –NodeAddress “iqn.1991-05.com.microsoft:netboot-1-SQLTarget-target”
```

实现 iSCSI 的注意事项（Considerations for implementing iSCSI）

在开始 iSCSI 部署之前，您应该查看基础架构，员工和客户需求，以确保选择适当的解决方案。以下是您应该考虑的主要注意事项：

- •网络速度和性能。网络速度应至少为 1 Gbps，但在许多情况下，现在数据中心的 iSCSI 网络为 10 Gbps，40 Gbps 或甚至 100 Gbps。
- 高可用性。网络基础架构必须高度可用，因为数据通过网络设备和组件从服务器发送到 iSCSI 存储。
- 安全。 iSCSI 解决方案应该有合适的安全级别。在需要高安全性的情况下，可以使用专用网络和 iSCSI 身份验证。在安全要求较低的情况下，您可能不必使用专用网络和 iSCSI 身份验证。
- 供应商信息。阅读有关使用 iSCSI 存储的不同类型部署和应用程序（如 Exchange Server 和 SQL Server ）的供应商特定建议。
- 基础设施工作人员。设计，配置和管理 iSCSI 存储的 IT 人员必须包括具有不同专业领域的 IT 管理员，例如 Windows Server 2016 管理员，网络管理员，存储管理员和安全管理员。这将帮助您设计具有最佳性能和安全性的 iSCSI 存储解决方案。它还将帮助您创建一致的管理和操作程序。
- 应用团队。 iSCSI 存储解决方案的设计团队应包括特定应用程序的管理员（例如 Exchange Server 管理员和 SQL Server 管理员），以便为特定技术或解决方案实现最佳配置。



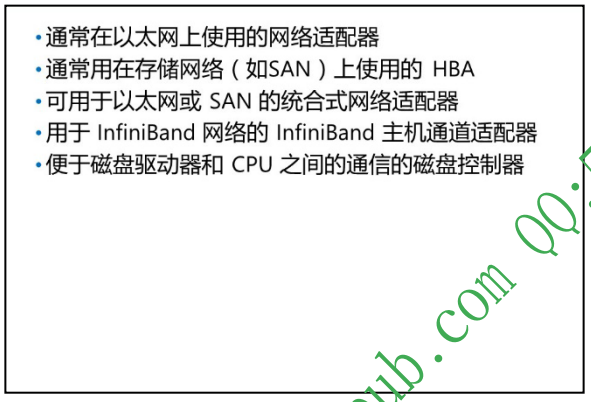
除了查看基础架构和团队之外，您还需要调查有竞争力的解决方案，以了解它们是否更好地满足您的业务需求。主要的 iSCSI 竞争对手是光纤通道，以太网光纤通道和 InfiniBand。

核心存储组件（Core storage components）

在存储基础架构中，几种类型的适配器和控制器构成存储系统的物理基础，包括：

- 网络适配器（Network adapter）
- HBA
- 融合式网络适配器（Converged network adapter）
- InfiniBand 主机通道适配器（InfiniBand host channel adapter）
- 磁盘控制器（Disk controller）

本主题考察这些组件的特性，并对每个组件最适合的场景进行概述。



网络适配器（Network adapters）

网络适配器由位于主板（motherboard）或扩展卡（expansion card）上的微芯片（microchips）和物理端口组成。 网络适配器主要提供到以太网的连接。 网络适配器通过使用 RJ-45 端口的有线网络或通过使用 802.11 无线网络标准的无线网络进行通信。 网络适配器是最具成本效益的存储连接解决方案。

当前的网络适配器以每端口高达 100Gbps 的速度运行，尽管 10Gbps 和 40Gbps 更常见。

您可以配置网卡组合（teaming）以实现性能，故障转移或两者。 使用组合时，作为组合的一部分的所有网络适配器组合起来创建虚拟网络适配器或组合网络适配器（*team network adapter*）。 您可以在组合网络适配器上配置设置。

注意：组合是一般网络连接的良好高可用性选项。 但是，对于 iSCSI 的特定用途，您应该考虑在多个网络路径中使用 MPIO 进行冗余，而不是使用网络组合。

HBAs

与网络适配器类似，HBA 由可以嵌入在主板或扩展卡上的微芯片和物理端口组成。 但是，与网络适配器不同，HBA 提供与 SAN 的连接。 HBA 比网络适配器更昂贵，虽然它们不是最昂贵的存储连接解决方案。光纤通道 HBA 在光纤通道网络上由万维网名称（World Wide Name ，WWN）唯一标识。 WWN 是每个光纤通道网络组件使用的可配置的 64 位地址，尽管它们不适用于 iSCSI HBA。

注意： WWN 是可配置的，因此仅依赖于 WWN 是一种安全风险。 一些攻击依赖于 WWN 欺骗，这是在未经授权的情况下使用另一设备的 WWN 来获得对后端存储的访问的过程。

对于性能，光纤通道 HBA 提供高达每端口 16 Gbps 的速度，而 iSCSI HBA 通常提供每端口 1 Gbps 或 10 Gbps。但是，您可以组合端口以实现更高的性能，这与其他存储扩展卡类似。通过允许您组合四个 16 Gbps 端口，该行业目前提供高达 64 Gbps 的理论光纤通道速度。

HBA 与软件进行负载平衡，它们的速度基于端口的总数和到后端存储的优化路径。在现实世界中，主机对于单个 SAN 控制器有两条以上的路径是不常见的。相反，当同时使用两个 HBA 时，公司通常选择使用多个 SAN 控制器的路径。业界已经宣布，即将推出的解决方案可以达到每端口性能 32 Gbps 的新标准。然而，随着光纤通道以太网和融合网络的普及，光纤通道和光纤通道 HBA 开始失去以太网和融合适配器解决方案的市场份额。

融合式网络适配器（Converged network adapters）

融合式网络适配器由微芯片和物理端口组成，有时嵌入在主板上，有时嵌入扩展卡。您可以配置融合式网络适配器以提供到以太网或 SAN 或两者的连接。融合式网络适配器的成本通常比 HBA 高一点，因为它们是以多端口和多协议支持构建的。融合式网络适配器通常同时支持多个协议，这使得它们成为可用的最灵活的存储适配器。

在性能方面，融合式网络适配器能够实现特定协议可以实现的最高速度。例如，如果其中一个端口是以太网端口，融合网络适配器可以实现高达 10 Gbps 的速度。然而，因为融合式网络适配器通常提供多种端口类型，所以它们通常不能实现专用单端口解决方案的组合速度。

目前，融合式网络适配器由于其灵活性而受欢迎，并且组织通常在现代数据中心中使用它们。

InfiniBand 主机通道适配器（InfiniBand host channel adapters）

InfiniBand 主机通道适配器与其他存储连接卡类似，由微型芯片和物理端口组成，通常位于扩展卡上。 主机通道适配器通过 InfiniBand 网络提供连接，并且提供当前最高级别性能。 然而，这种高性能是有代价的，因为主机通道适配器是可用的最昂贵的存储连接适配器。 一些当前的主机通道适配器工作在高达 56 Gbps。 InfiniBand 通过比竞争解决方案（例如以太网）具备更少的通信开销提供最低的延迟。 但是，组织很少使用 InfiniBand，通常是因为成本高，使用和管理它所必需的培训，以及低成本解决方案的竞争特性。

磁盘控制器（Disk controllers）

磁盘控制器是便于通过相关总线在硬盘和中央处理单元（CPU）之间进行通信的微芯片。早期版本的磁盘控制器嵌入在专用扩展卡上。今天，大多数磁盘控制器嵌入在磁盘驱动器中。此外，随着虚拟化的广泛采用，虚拟磁盘控制器是相当普遍的。虚拟磁盘控制器有时会模拟物理磁盘控制器，尽管较新的虚拟控制器是专门为虚拟实现而编写的，而且它们不依赖于仿真（emulation）。

磁盘控制器具有以下特性：

- 大多数服务器提供内置的 RAID 功能和专用磁盘控制器（specialized disk controller）或 RAID 控制器（*RAID controller*），这有助于 RAID 功能。
- 另一种类型的专用磁盘控制器或阵列控制器（*array controller*）有助于服务器和 DAS 设备之间的通信。
- 物理磁盘控制器通常通过串行 ATA（SATA）或串行连接 SCSI（SAS）接口进行操作。
- 虚拟磁盘控制器通常模拟（emulate）集成驱动器电子（integrated drive electronics ，IDE）或 SCSI 控制器。

演示：配置 iSCSI 目标（Configuring an iSCSI target）

在本演示中，您将了解如何：

- 添加 iSCSI 目标服务器角色服务。
- 创建两个 iSCSI 虚拟磁盘和一个 iSCSI 目标。
- 连接到 iSCSI 目标。
- 验证 iSCSI 驱动器的存在。

演示步骤（Demonstration Steps）

添加 iSCSI 目标服务器角色服务（Add the iSCSI Target Server role service）

- 在 LON-DC1，使用服务器管理器在 File and Storage Services 中添加 iSCSI Target Server 角色服务

创建两个 iSCSI 虚拟磁盘和一个 iSCSI 目标（Create two iSCSI virtual disks and an iSCSI target）

在 LON-DC1 上，在服务器管理器中的 File and Storage Services，浏览到 iSCSI.

使用以下设置创建新的 iSCSI 虚拟磁盘:

- 名称： iSCSIDisk1
- 磁盘容量： 5 GB
- iSCSI 目标： New
- 目标名称： LON-DC1
- 访问服务器： 172.16.0.21

使用以下设置创建第二个 iSCSI 虚拟磁盘：

- 名称： iSCSIDisk2
- 磁盘容量： 5 GB
- iSCSI 目标： LON-DC1

连接到 iSCSI 目标（Connect to the iSCSI target）

1. 在 LON-SVR1，打开 Server Manager，然后从 Tools 菜单中，打开 iSCSI Initiator.

在 iSCSI Initiator Properties 对话框中, 配置以下内容:

- 快速连接（Quick Connect:）： LON-DC1
- 发现目标（Discover targets）： iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target

验证 iSCSI 驱动器的存在（Verify the presence of the iSCSI drive）

1. 在 LON-SVR1，在服务管理器中， 从 Tools 菜单打开 Computer Management.

在 Computer Management 控制台中，从 Disk Management，验证是否存在两个 5 GB iSCSI 磁盘。

注意： 新磁盘已添加，但它们当前都处于脱机状态且未格式化。 这些磁盘列出为 Disk 11 和 Disk 12。

问题：您可以使用您组织的内部 TCP / IP 网络来提供 iSCSI 吗？

问题：您什么时候考虑从 iSCSI 目标实现无盘引导？

第 3 课
理解 iSNS、 DCB 和 MPIO（Understanding iSNS, DCB, and MPIO）

企业通常需要较小的组织不需要的存储功能，这些高级功能通常简化了存储管理。 iSNS 服务器是 iSCSI 目标的中心目录（central directory）。 DCB 有助于确保在承载多种类型数据的高速融合网络上满足 QoS 目标。 多路径 I/ O（MPIO）用于识别通过存储网络的多条路径，以实现冗余和性能。

课程目标（Lesson Objectives）

完成本课后，您将能够：

- 描述 iSNS。
- 描述 DCB。
- 描述 MPIO。
- 配置 MPIO。

什么是 iSNS?（What is iSNS?）

在复杂的 IT 系统中，有许多存储设备和许多需要访问存储的设备。 iSNS 服务器具有一个数据库，其中包含有关存储设备以及该存储在何处分配的信息的集合。该数据库和相关联的 iSNS 协议使得需要存储的设备可以查找分配的存储设备。也就是说，iSNS 客户端查询 iSNS 服务器以查找分配给它们的存储。

- iSNS 服务器服务是一个 Windows 功能：
  - 有三个主要组件：iSNS 服务器，iSNS 客户端和 iSNS 数据库
  - 有几个优点，包括：
    - 通过自动配置 iSCSI 客户端来减少管理开销
    - 与 iSCSI 和光纤通道兼容
    - 可以使 IP 网络功能像 SAN
    - 可以无缝集成 IP 和光纤通道网络
  - 还没有广泛使用

iSNS 是一种使用很少系统资源的灵活协议； iSNS 服务器和 iSNS 客户端使用 iSNS 协议来进行交互。客户端可以使用 iSNS 自动发现 iSCSI 存储设备，而您可以使用 iSNS 配置和管理 iSCSI 存储设备。 iSNS 还通过使用 Internet 光纤通道协议网关（Internet Fibre Channel protocol gateway）来促进光纤通道设备的相同操作。

但是，由于 iSNS 可以执行存储发现和配置任务，因此可以使用 iSNS 创建类似于 SAN 的 IP 网络功能。您还可以使用 iSNS 无缝集成 IP 和光纤通道网络，因为 iSNS 可以模拟光纤通道光纤网络服务（Fibre Channel fabric services），以及管理 iSCSI 和光纤通道设备。因此，如果 iSCSI 和光纤通道设备构成您的存储网络，这对您的组织非常有价值。

您可以使用 iSNS 来管理设备组，而不是单独管理这些设备，因为在 iSNS 数据库中注册设备后，不再需要手动配置。 iSNS 用作管理站可以配置和管理存储网络的中央配置点（central configuration point）。

iSNS 组件（iSNS components）

iSNS 有三个主要组件：客户端，服务器和数据库。

iSNS 客户端（iSNS clients）

当 iSNS 客户端尝试发现存储设备时，它通过使用 iSNS 协议启动与 iSNS 的通信。 iSNS 客户端通常是驻留在存储设备中的进程。 iSNS 客户端注册设备属性信息，下载关于发现域（Discovery Domains）中其他已注册客户端的信息，并接收在其发现域中发生的事件的异步通知。管理站（management station）是一种 iSNS 客户端，可访问 iSNS 中包含的发现域。

iSNS 服务器（iSNS servers）

iSNS 服务器响应 iSNS 协议查询和请求。 iSNS 服务器还启动 iSNS 协议状态更改通知。由注册请求提交的身份认证信息存储在 iSNS 数据库中。

iSNS 数据库（iSNS database）

iSNS 服务器使用 iSNS 数据库作为信息存储库。 iSNS 数据库包含有关 iSNS 客户端属性的信息。 通过使用启用目录的 iSNS 实现，可以将 iSNS 客户端属性存储在轻型直接访问协议（LDAP）目录中。

iSNS 功能（iSNS Functions）

iSNS 的四个主要功能是：

- 名称服务（name service）。 存储网络中的所有实体都可以使用此服务在数据库中注册其名称和其他信息。 所有注册的实体可以查询 iSNS 数据库以查找其他实体。
- 发现域（Discovery Domain）和登录控制服务（login control service）。 此服务有助于将存储节点分成组。 然后将这些组用于管理目的和控制登录活动。
- 状态更改通知服务（state change notification service）。 iSNS 服务器使用此服务发出有关网络上事件的通知。
- 将信息映射到 iSNS 数据库（Mapping information to an iSNS database）。 iSNS 将有关 iSCSI 和光纤通道设备的命名和发现信息映射到 iSNS 数据库。

iSNS 安装和配置（iSNS installation and configuration）

iSNS 服务器服务（iSNS Server service）是 Windows Server 2016 中包含的 Windows 功能。您可以通过在服务器管理器中添加功能或使用 Add-WindowsFeature cmdlet 来安装。

安装后，您可以从服务器管理器中的 Tools 菜单启动 iSNS 服务器。 然后，您可以注册 iSCSI 设备并将其分组到发现域（Discovery Domain）和发现域集（Discovery Domain Set）。 配置 Windows iSCSI 发起程序时，指定要使用的 iSNS 服务器 IP 地址或域名系统完全限定域名（Domain Name System fully qualified domain name ，DNS FQDN）。 启动程序将查询它以自动发现所有的 iSCSI 目标，基本上不需要为发起程序手动配置入口。

要执行 iSNS 服务器注册，请使用以下 Windows PowerShell 命令来管理 Windows Management Instrumentation（WMI） 对象：

要添加 iSNS 服务器，请使用以下命令：

```
Set-WmiInstance -Namespace root\wmi -Class WT_iSNSServer -Arguments
@{ServerName="iSNS-server-name"}
```

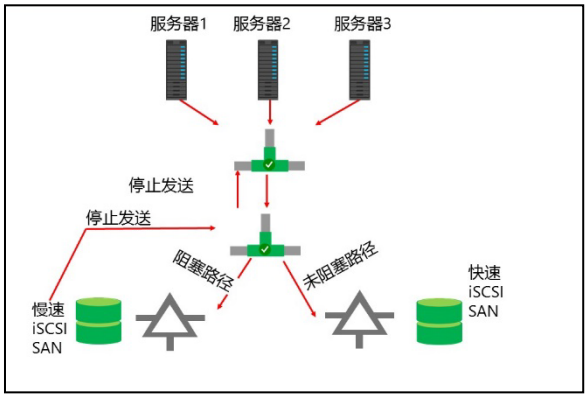
要查看 iSNS 服务器设置，请使用以下命令：

```
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer
```

要删除 iSNS 服务器，请使用以下命令：

```
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer -Filter “ServerName
=’iSNS -server-name’ | Remove-WmiInstance
```

什么是 DCB（What is DCB）？



大多数现有的数据中心通常具有适应不同组织需要的若干物理网络。例如，系统管理员和用户可能使用以太网，数据存储可能使用单独的物理光纤通道网络，高性能计算机可能使用 InfiniBand 网络。但是，在构建和维护网络时，使用单独的网络会增加成本和管理开销。

由电气和电子工程师协会（Institute of Electrical and Electronic Engineers ，IEEE）802.1 工作组开发的 DCB 提供了一种标准，通过该标准，您可以将这些网络组合成支持所有上述协议和 iSCSI 的单一物理基础架构。通常，当您使用融合式网络适配器（converged network adapter）或专用 iSCSI HBA 时，适配器供应商的软件包括配置基于硬件的 QoS 和 DCB 的其他功能的能力。此外，主机连接的网络交换机必须支持 DCB。

DCB 的特点包括：

- 拥塞通知（Congestion notification）。您可以使用它来管理没有内置控制机制的协议的拥塞。拥塞通知可以帮助设备发送数据以调节它们正在生成的流量，以避免拥塞。
- 基于优先级的流量控制（Priority-based flow control.）。这是一种链路层流控制机制，您可以根据网络上传输的数据类型进行控制。您可以使用此功能来定位流量控制，而不是不考虑正在传输的内容将数据流停止。最后一种做法是原始以太网流控制的一个特性。
- 增强的传输选择（Enhanced transmission selection）。这使系统能够为 iSCSI 和其他网络协议预留带宽。您可以使用增强型传输选择（enhanced transmission selection），根据您的需求或用途，为 iSCSI 预留特定的带宽量。这有助于提高性能。
- 数据中心桥接能力交换（Data Center Bridging Capabilities Exchange ，DCBX）协议。这使得诸如网络适配器和交换机的设备能够通信和共享能力和配置信息。

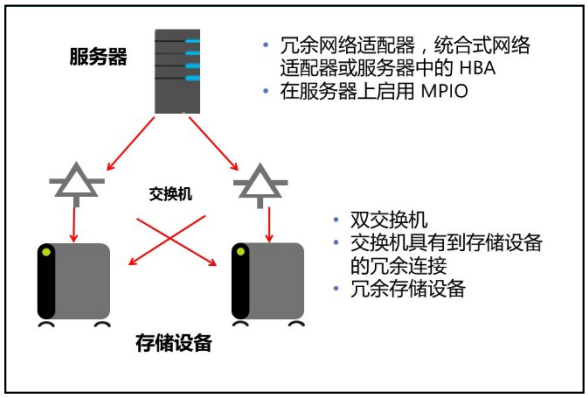
安装和配置 DCB（Installing and configuring DCB）

DCB 是 Windows Server 2016 功能，您可以从 Windows PowerShell 或使用服务器管理器安装。 要从 Windows PowerShell 安装 DCB，请打开命令提示符，键入 Install-WindowsFeature "Data-Center-Bridging"，然后按 Enter 键。

配置 DCB（Configuring DCB）

您使用 Windows PowerShell 来管理 DCB 中的 QoS 功能。 这些 cmdlet 位于 NetQos，DcbQos 和 NetAdapter 模块中。 要查看与 DCB QoS 相关的所有 cmdlet，请运行 Get-Help *Qos* 命令。 或者，要检索每个模块中可用的 cmdlet，请运行 Get-Command -Module DcbQos, NetAdapter, NetQos 命令。

什么是 MPIO（What is MPIO）?



MPIO 是一种存储网络增强，它提供从计算机到块存储提供程序的多个物理路径，而不管存储是直接连接到存储提供程序还是通过网络提供。自 Windows Server 2008 以来，MPIO 已内置到 Windows Server 中，并且在 Windows Server 2003 中作为 单独的组件提供。除了 Windows Server 操作系统内置的此支持外，许多存储供应商还提供自己的 MPIO 软件，可以安装在运行 Windows Server 的计算机上，连接到后端存储。你主要在这些情况下使用 MPIO：

- 创建或维护高可用性存储基础架构。在这种情况下，MPIO 与其他高可用性技术（如故障转移群集（failover clustering），网络负载平衡（network load balancing）和数据中心可用性（datacenter availability））相结合。数据中心可用性专门用于维护电源，冷却和网络。 Microsoft MPIO 可以处理最多 32 条到存储基础架构的路径。
- 最大化吞吐量（throughput）以满足高性能要求。在这种情况下，MPIO 使用 MPIO 负载平衡来最大化到存储的吞吐量。在大多数部署中，仍然配置高可用性，以便如果一个路径出现故障，则所有流量都使用备用路径，吞吐量会下降到单个路径级别。

MPIO 与其他软件并行工作。一个这样的软件是设备特定模块（device-specific module ，DSM）。 DSM 是一种存储供应商软件组件，可促进与后端存储的高效交互。 DSM 软件与 MPIO 软件协同工作，用于初始化事件，I/O 事件以及与后端存储通信的其他方面。与 MPIO 类似，存储供应商和 Microsoft 都提供自己的 DSM 软件。

演示: 配置 MPIO（Configuring MPIO）

在本演示中，您将看到如何配置 MPIO。

演示步骤（Demonstration Steps）

1. 在 LON-SVR1 上，在服务器管理器中，添加 Multipath I/O 功能。
2. 安装完成后，重新启动 LON-SVR1 ，以 Adatum\Administrator 身份登录，密码为 Pa55w.rd。
3. 在服务器管理器中的 Tools 菜单上，打开 MPIO。
4. 在 MPIO Properties 中，在 Discover Multi-Paths 选项卡上，添加对 iSCSI 设备的支持，然后在出现提示时重新启动。
5. 重新启动后，以 Adatum\Administrator 身份登录，密码为 Pa55w.rd。
6. 在服务器管理器中，打开 MPIO，然后验证 MSFT2005iSCSIBusType_0x9 是否列为设备。

通过在右边的列中放置标记来验证语句的正确性。.

语句	回答
您可以将 iSNS 同时用于 iSCSI 和光纤通道存储。	

检查您的知识（Check Your Knowledge）

问题	
Microsoft MPIO **可以拥有的最大路径是多少？**	
选择正确的答案	
	4
	8
	16
	32

第 4 课
在 Windows Server 2016 中配置共享（Configuring sharing in Windows Server 2016）

文件共享是 Windows Server 2016 提供的核心服务。每个新版本的 Windows Server 都会为非传统场景提供增强的文件共享功能，例如将虚拟机文件存储在共享文件夹而不是 SAN 或本地连接存储。 您可以使用服务器管理器为 Windows 客户端创建 SMB 共享或为 Linux 客户端创建 NFS 共享。 在本课程中，您将学习如何创建和管理共享文件夹。

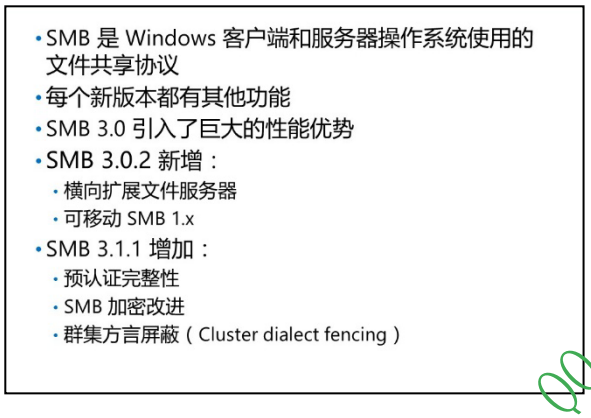
课程目标（Lesson Objectives）

完成本课后，您将能够：

- 描述 SMB 文件共享协议。
- 识别 SMB 的配置选项。
- 配置 SMB 共享。
- 描述 NFS 文件共享协议。
- 识别 NFS 共享的配置选项。
- 配置 NFS 共享。

什么是 SMB（What is SMB）?

SMB 是在 1984 年创建的客户端 - 服务器文件共享协议（client-server file-sharing protocol）。 Microsoft 修改了原始 SMB，并在 1996 年开始使用 CIFS 名称。今天，术语 SMB 和 CIFS 可互换使用，指的是相同的文件共享协议 。 本课程使用术语 SMB 来代表该技术。



SMB 被多个平台所支持，如在非 Windows 平台上支持 SMB 的开源版本，名称为 SAMBA，与 SMB 兼容。

有多个版本的 SMB，每个新版本都有其他功能和增强功能。 SMB 的版本随着新操作系统的发布而增加。 当两台计算机使用 SMB 时，他们协商使用哪个版本。 如果一台计算机能够使用 SMB 2.0，另一台计算机能够使用 SMB 3.0，则它们使用 SMB 2.0。 下表列出了不同 Windows 操作系统所包含的 SMB 的版本。

操作系统	SMB 版本
Windows 10 和 Windows Server 2016	SMB 3.1.1
Windows 8.1 和 Windows Server 2012 R2	SMB 3.0.2
Windows 8 和 Windows Server 2012	SMB 3.0
Windows 7 和 Windows Server 2008 R2	SMB 2.1

操作系统	SMB 版本
Windows Vista 和 Windows Server 2008	SMB 2.0.2
之前的版本	SMB 1.x

删除 SMB 1.x（Removing SMB 1.x）

当前 Windows 版本与 SMB 1.x 没有任何依赖关系。 如果您的网络不再包括 Windows XP 或 Windows Server 2003，则应考虑通过删除 SMB1 功能来禁用 SMB 1.x。

要确保您的网络没有使用 SMB 1.x 的设备，您可以启用对服务器上 SMB 1.x 的使用的审核。 事件存储在 Microsoft-Windows-SMBServer/Audit 中。 使用以下 Windows PowerShell 命令启用 SMB 1.x 审核日志记录：

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

要禁用 SMB 1.x，请使用以下 Windows PowerShell 命令：

```
Set-SMBServerConfiguration -EnableSMB1Protocol $false
```

SMB 3.x 功能（SMB 3.x features）

每个新的 SMB 版本提供了支持 Windows Server 中的新功能的附加功能。一些最重要的增强功能从引入 SMB 3.0 开始，它提供了显着的性能改进，包括支持在 SMB 3.0 共享上存储 SQL Server 数据库和 Hyper-V 虚拟机。

SMB 3.0.2 提供的功能使您能够为存储 SQL Server 数据库和 Hyper-V 虚拟机的高可用性文件共享实施 Scale-Out File Server 功能。此外，它启用带宽限制（bandwidth limitation），并且是允许禁用 SMB 1.x 的第一个版本。

SMB 3.1.1 具有以下新功能：

- 预身份验证（Preauthentication）。通过在会话建立期间使用安全散列算法 512（Secure Hash Algorithm 512，SHA-512）散列来验证数据包内容，从而防止中间人攻击（man-in-the-middle attacks）。
- SMB 加密改进。 SMB 加密现在默认使用 AES-128-GCM 加密算法，其性能明显优于在 SMB 3.0.2 中使用的 AES-128-CCM。
- Cluster dialect fencing.。要支持 Scale-Out 文件服务器集群的滚动升级，混合模式下的文件共享使用 SMB 3.0.2。在群集中的所有节点都升级后，文件共享开始使用 SMB 3.1.1。

附加阅读： 有关详细信息，请参阅： “Windows Server 中的 SMB 的新增功能” ，地址为：: http://aka.ms/Uthhq2

配置 SMB 共享（Configuring SMB shares）

文件共享的创建和配置长期以来一直是网络管理的核心部分。 共享文件的能力是计算机网络首先流行的原因之一。 大多数管理员知道您可以从文件资源管理器中创建共享文件夹。 但是，在 Windows Server 2016 中，您还可以使用服务器管理器和 Windows PowerShell 创建共享。 在服务器管理器中，术语*文件共享（file share）*和 *SMB* 指向相同的组件。

- 有三个 SMB 共享配置文件：
  - 快速
  - 高级
  - 应用程序
- 用于 SMB 共享管理的 Windows PowerShell cmdlet：
  - **New-SmbShare**
  - **Set-SmbShare**
  - **Remove-SmbShare**
  - **Get-SmbShare**
  - **Get-SmbSession**
  - **Get-SmbOpenFile**
  - **Set-SmbBandwidthLimit**

共享和 NTFS 权限（Share and NTFS permissions）

用户访问 SMB 共享上的文件的权限是共享权限和 NTFS 权限的组合。 最严格的权限集合始终适用。 例如，如果给予用户完全控制 NTFS 权限，但是他或她只有读取共享权限，则用户的访问权限为读取。

要简化数据访问，在使用 Quick 配置文件创建 SMB 共享时，共享权限设置为 Everyone 完全控制。 实际上，这意味着共享权限不限制对共享的访问，NTFS 权限用于控制访问。

SMB 共享配置文件（SMB share profiles）

您可以使用 Windows Server 2016 上的服务器管理器创建新共享。内置的新共享向导提供三个 SMB 文件共享配置文件，您可以从中选择，包括：

- **快速（Quick）。**这是在网络上共享文件夹的最快的方法。使用此方法，您可以选择卷或输入共享文件夹位置的自定义路径。您可以使用 New Share Wizard 配置其他选项，例如基于访问的枚举（access-based enumeration），共享缓存，加密的数据访问和权限。您可以在创建共享后手动配置这些选项和其他选项。
- **高级（Advanced）。**此配置文件提供与快速配置文件相同的配置选项，以及其他选项，如文件夹所有者，默认数据分类（data classification）和配额（quotas）。要创建高级配置文件，必须在至少一个使用服务器管理器管理的服务器上安装 File Server Resource Manager 角色服务。
- **应用程序（Applications）。**此专用配置文件具有适用于 Hyper V，数据库和其他服务器应用程序的设置。与快速和高级配置文件不同，在创建应用程序配置文件时，您无法配置基于访问权限的枚举，共享缓存，默认数据分类或配额。

下表列出了可用于每个 SMB 共享配置文件的配置选项

共享类型	基于访问的枚举	共享缓存	加密数据访问	默认数据分类	配额	权限
快速	是	是	是	没有	没有	是
高级	是	是	是	是	是	是
应用程序	没有	没有	是	没有	没有	是

Windows PowerShell 中 SmbShare 模块的 cmdlet（Windows PowerShell cmdlets in the SmbShare module）

Windows PowerShell 的 SmbShare 模块在 Windows Server 2016 中包含 35 个 cmdlet。这包括常用的 cmdlet，例如 New-SmbShare，Set-SmbShare 和 Remove-SmbShare。如果使用 SmbShare cmdlet，则可以配置任何共享属性，即使是那些在服务器管理器中不可用的共享属性。

如果要识别服务器上已存在的共享，并查看这些共享的属性，可以使用 Get-SmbShare。默认输出 Name, ScopeName，Path，和 Description，ScopeName 仅在服务器是集群的一部分时显示，对于未集群的文件服务器显示为*。

您可以使用 Get-SmbSession 来识别连接到 SMB 共享的用户。如果用户有打开的文件，则可以使用 Get-SmbOpenFile 来识别打开的文件。

如果您担心控制服务器上分配给 SMB 共享的带宽，则可以使用 Set-SMBBandwidthLimit 来定义为服务器上的不同类别的 SMB 流量分配最大吞吐量级别。这对 Hyper-V 主机很有用，以确保某些类别的流量不会压倒主机并影响其他类别，包括：

- 默认。这是指与 Hyper-V 或实时迁移无关的所有 SMB 流量，例如标准文件共享。
- Hyper-V。这指的是用于运行虚拟机的 SMB 流量，例如访问 SMB 共享上的虚拟硬盘驱动器。
- 实时迁移（Live Migration）。这是指在执行从一个 Hyper-V 主机到另一个 Hyper-V 主机的实时迁移时生成的 SMB 通信。

 **注意：** 要浏览 SmbShare 模块中的所有 cmdlet，请运行 Get-Command-Module-SmbShare 命令。.

演示: 使用服务器管理器和 Windows PowerShell 配置 SMB 共享（Configuring SMB shares by using Server Manager and Windows PowerShell）

在本演示中，您将了解如何：

- 使用服务器管理器创建 SMB 共享。
- 使用 Windows PowerShell 创建 SMB 共享。
- 查看 SMB 会话信息。

演示步骤（Demonstration Steps）

使用服务器管理器创建一个 SMB 共享（Create an SMB share by using Server Manager）

1. 在 LON-SVR1 上，在服务器管理器中的 File and Storage Services 中，浏览到 Shares.
2. 使用以下设置创建新共享：
    - 文件共享配置： SMB Share - Quick
    - 服务器： LON-SVR1
    - 按卷进行选择： D:
    - 共享名称： DemoShare
    - 启用基于访问的枚举： 选中
    - 权限： 默认

使用 Windows PowerShell 创建一个 SMB 共享（Create an SMB share by using Windows PowerShell）

1. 在 Windows PowerShell 提示符下，键入以下命令，然后按 Enter 键:

```
Mkdir D:\Shares\DemoShare2
```

2. 键入以下命令，然后按 Enter 键：

```
New-SmbShare -Name DemoShare2 -Path D:\Shares\DemoShare2 -FolderEnumerationMode
AccessBased
```

3. 键入以下命令，然后按 Enter 键：

```
Get-SmbShare
```

4. 键入以下命令，然后按 Enter 键：

```
Get-SmbShare DemoShare | FL *
```

查看 SMB 会话信息（View SMB session information）

1. 在 LON-DC1 上， 打开 File Explorer, 然后浏览到 \\LON-SVR1\DemoShare。
2. 在 LON-SVR1 上，在 Windows PowerShell 提示符下，键入以下命令，然后按 Enter 键：

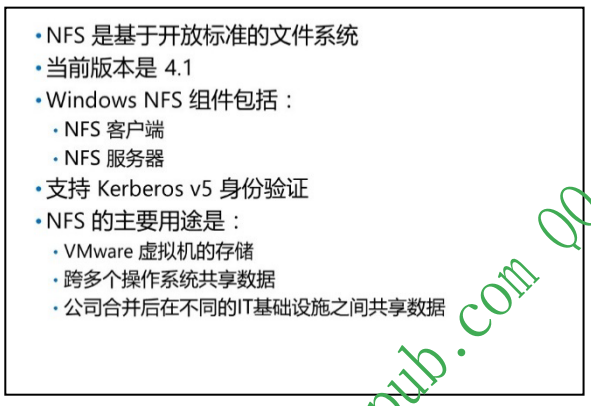
```
Get-SmbSession
```

3. 键入以下命令，然后按 Enter 键：

```
Get-SmbSession -ClientUserName Adatum\Administrator | FL *
```

什么是 NFS（What is NFS）?

NFS 是一种文件系统协议，它基于开放标准，允许通过网络访问文件系统。 NFS 已经积极开发，目前的版本是 4.1。 NFS 协议的核心版本和特性是：



- NFS 版本 1。Sun Microsystems 在 1984 年开发了版本 1，主要在内部使用。最初，NFS 在 UNIX 操作系统上使用，但随后在包括 Windows 在内的其他操作系统上受支持。
- NFS 版本 2。请求注解（RFC）1094，“NFS：网络文件系统协议规范”，定义了版本 2。此版本专注于提高性能。文件大小限制为 2 GB，因为它是一个 32 位实现。
- NFS 版本 3。RFC 1813，“NFS 版本 3 协议规范”，定义了版本 3，并引入了对较大文件大小的支持，因为它是 64 位实现。它还具有性能增强，例如更好地保护不安全写入，以及增加传输大小。它还包括安全增强功能，例如服务器的线上权限检查。
- NFS 版本 4。RFC 3530，“网络文件系统（NFS）版本 4 协议 “，定义了版本 4，它提供了增强的安全性和改进的性能。
- NFS 版本 4.1。 RFC 5661，“网络文件系统（NFS）版本 4 小版本 1 协议 “，定义了版本 4.1，增加了对集群的支持。

在 UNIX 中，NFS 基于导出（exports）工作。 导出与 Windows 中的文件夹共享类似，因为它们是共享的 UNIX 文件系统路径。

Microsoft 通过在 1998 年推出了 UNIX Add-On Pack 的 Microsoft Windows NT 服务开始支持 NFS。该产品用于将基于 Windows 的计算机与基于 UNIX 的计算机集成。 一个这样的集成功能是支持 NFS。 Microsoft 继续以原来的名称开发产品，直到 2004 年发布用于 UNIX 3.5 的 Microsoft Windows 服务。 此时，产品已重命名为“基于 UNIX 的应用程序的子系统”（Subsystem for UNIX-based Applications， SUA），功能拆分如下：

- UNIX 实用程序和软件开发工具包（SDK），可以从 Microsoft 下载中心免费和可选的下载。
- SUA 的一部分，Client for NFS 组件和 Server for NFS 组件器成为 Windows 功能。 SUA 功能在 Windows Server 2012 中已弃用，并且在 Windows Server 2016 中不再可用。但是，Client for NFS 和 Server for NFS 仍受支持并作为 Windows 功能使用。

Windows 中的 NFS 支持的两个组件是：

- Client for NFS。此组件使运行 Windows 操作系统的计算机能够访问 NFS 服务器上的 NFS 导出（exports），而不管服务器运行在哪个平台。
- Server for NFS。此组件使基于 Windows 的服务器能够通过 NFS 共享文件夹。任何兼容的 NFS 客户端都可以访问文件夹，而不管客户端运行哪个操作系统。绝大多数 UNIX 和 Linux 计算机都有一个内置的 NFS 客户端。

随着 Windows Server 操作系统的每次迭代，对 NFS 的支持得到了改进和扩展，如下所示：

- •Windows Server 2008 R2 在 Server for NFS 中引入了对 Kerberos 版本 5（v5）的身份验证支持。Kerberos v5 认证在授予对数据的访问权之前提供认证，它还使用校验和以确保没有发生数据篡改。

  •Windows Server 2012 引入了对 NFS 版本 4.1 的支持。此支持包括使用默认配置，本机 Windows PowerShell 支持以及在群集部署中更快速的故障转移来提高性能。

使用场景（Usage scenarios）

在许多场景下，您可以在 Windows 中使用 NFS，一些最受欢迎的用途包括：

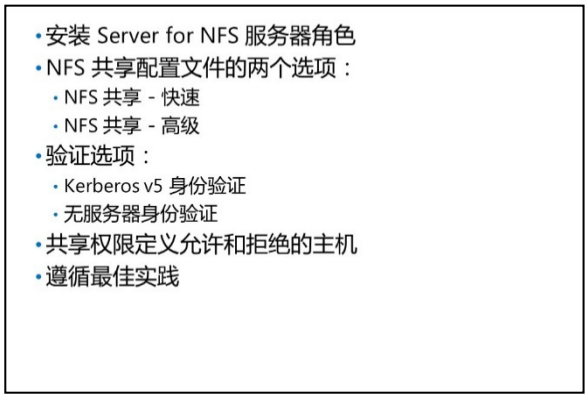
- VMWare 虚拟机存储。 在此方案中，VMWare 托管（host）NFS 导出（NFS exports）上的虚拟机。 您可以使用 Server for NFS 来托管 Windows Server 2012 R2 服务器上的数据。
- 多操作系统环境。 在这种情况下，您的组织使用各种操作系统，包括 Windows，Linux 和 Mac。 Windows 文件服务器系统可以使用 Server for NFS 和内置的 Windows 共享功能，以确保所有操作系统都可以访问共享数据。
- 合并或收购。 在这种情况下，两家公司正在合并。 每个公司都有不同的 IT 基础设施。 一个公司的用户使用 Windows 8.1 客户端计算机，他们必须访问其他公司的基于 Linux 和 NFS 的文件服务器托管的数据。 您可以将 NFS 客户端部署到客户端计算机，以允许用户访问数据。.

配置 NFS 共享（Configuring NFS shares）

内置的 New Share Wizard 提供两个 NFS 文件共享配置文件，您可以从中选择：

- **快速。** 创建快速配置文件是创建 NFS 共享的最快方式，但它没有高级配置文件可用的一些可自定义共享选项。 创建快速配置文件后，您可以在 New Share Wizard 之外手动配置高级共享选项。

  高级。 高级配置文件是创建 NFS 共享的最可定制的方式。 您可以使用它来设置文件夹所有者来帮助解决访问被拒绝的问题，配置默认数据分类，并启用配额。 要创建高级配置文件，必须在文件服务器上安装文件服务器资源管理器（File Server Resource Manager）角色服务。



在服务器上安装 NFS（Installing NFS on the server）

您可以使用服务器管理器或 Windows PowerShell 在服务器上安装 NFS。 使用服务器管理器时，必须添加 File and Storage Services 角色，然后安装 Server for NFS 角色服务。 要使用 Windows PowerShell 在服务器上安装 NFS，请运行以下命令：

```
Add-WindowsFeature FS-NFS-Service -IncludeManagementTools
```

创建 NFS 文件共享（Creating an NFS file share）

在服务器上安装 NFS 后，可以使用服务器管理器或 Windows PowerShell 创建 NFS 文件共享。 要使用 Windows PowerShell 创建 NFS 文件共享，运行以下命令为位于 d:\shares\share1 的目录配置名为 Share1 的 NFS 文件共享：

```
New-NfsShare -Name Share1 -Path d:\shares\share1
```

NFS 共享的身份验证可以使用 Kerberos v5 身份验证或使用无服务器（No server）身份验证。 当您使用 Kerberos v5 身份验证时，Active Directory 域服务（Active Directory Domain Services ，AD DS）用于验证用户账户。 使用无服务器身份验证时，可以将用户 ID（UID）和组 ID（GID）从 Linux 系统映射到 AD DS 帐户以分配权限。

为 NFS 共享配置共享权限时，通常定义允许访问共享的主机。 要允许所有主机，您可以选择 All Machines。 您还可以允许和拒绝指定主机。

最佳实践（Best practices）

在您的环境中实施 NFS 之前，应考虑以下几种最佳实践，包括：

- 使用最新版本的 NFS 服务器和客户端。目前，NFS 版本 4.1 是最新版本，在 Windows Server 2012 及更高版本以及 Windows 8 和更高版本上受支持。通过使用最新版本的服务器和客户端操作系统，您可以利用最新的性能和安全性改进，例如客户端/服务器协商和改进的对群集服务器的支持。
- 使用所有可用的安全增强功能。自从 NFS 版本 3.0 以来，NFS 提供了 Kerberos 安全选项来加强 NFS 通信。您应该尽可能使用以下选项：
  - Kerberos v5 认证协议。这是推荐的认证协议，以维持最高的认证安全性。
  - Kerberos v5 认证和完整性。这通过使用校验和添加完整性检查（integrity checking），以确保数据未被更改。
  - Kerberos v5 身份验证和隐私（privacy）。这会为身份验证流量添加加密。

- 不允许匿名访问。虽然匿名访问是 NFS 共享的一个选项，但不应使用它，因为它会降低文件共享环境的安全性。

Windows PowerShell 的 NFS 模块（NFS module for Windows PowerShell）

自 Windows Server 2012 以来，NFS 已经有自己的 Windows PowerShell 模块。要列出模块中可用的所有 42 个 cmdlet，请运行 Get-Command -Module NFS 命令。

来自 NFS 模块的一些最常用的 cmdlet 是：

- New-NfsShare。此 cmdlet 创建 NFS 文件共享。
- Remove-NfsShare。此 cmdlet 删除 NFS 文件共享。
- Get-NfsShare。此 cmdlet 检索有关 NFS 文件共享的配置的信息。
- Get-NfsSharePermission。此 cmdlet 检索共享的 NFS 文件共享权限。
- Get-NfsClientConfiguration。此 cmdlet 检索 NFS 客户端配置设置。
- Get-NfsClientGroup。此 cmdlet 检索在 NFS 服务器上配置的客户端组。
- New-NfsClientGroup。此 cmdlet 在 NFS 服务器上创建一个新的客户端组。
- Revoke-NfsSharePermission。此 cmdlet 从 NFS 文件共享中撤销 NFS 文件共享权限。
- Set-NfsShare。此 cmdlet 更改 NFS 共享的配置设置。
- Set-NfsClientConfiguration。此 cmdlet 更改 NFS 客户端的配置设置。

演示：使用服务器管理器配置 NFS 共享（Configuring an NFS share by using Server Manager）

在此演示中，您将看到如何使用服务器管理器配置 NFS 共享。

演示步骤（Demonstration Steps）

1. 在 LON-SVR1 上，在服务器管理器中的 File and Storage Services，浏览到 Shares。
2. 使用以下设置创建新共享：
   - 文件共享配置文件： NFS Share - Quick
   - 服务器： LON-SVR1
   - 按卷进行选择： D:
   - 共享名称： DemoNfsShare
   - 身份验证： Kerberos v5 authentication(Krb5)
   - 共享权限： All Machines, Read / Write
   - 权限： 默认

检查您的知识（Check Your Knowledge）

问题	
Windows 10 和 Windows Server 2016 使用哪个版本的 SMB？	
选择正确的答案。	
	SMB 2.1
	SMB 3.0.2
	SMB 3.1.1
	SMB 3.2

通过在右边的列中放置标记来验证语句的正确性。

语句	回答
您不能对 NFS 共享使用 Kerberos 身份验证，因为它们需要 AD DS。	

实验: 规划和配置存储技术和组件（Planning and configuring storage technologies and components）

场景（Scenario）

您是 A. Datum Corporation 的存储管理员，您的工作的一部分是确保您的数据存储系统满足短期和长期业务需求。

目标（Objectives）

完成本实验后，您将能够：

- 规划存储需求。
- 配置 iSCSI 存储。
- 配置和管理共享。

实验设置（Lab Setup）

估计时间：60 分钟

虚拟机：20470B-LON-DC1 和 20470B-LON-SVR1

用户名：Adatum\Administrator

密码：Pa55w.rd

对于本实验，您将使用可用的虚拟机环境。 在开始实验之前，您必须完成以下步骤：

1. 在主机计算机上，启动 Hyper-V Manager。
2. .在 Hyper-V Manager 中，单击 20470B-LON-DC1，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：Administrator
- 密码：Pa55w.rd
- 域：Adatum

5. 对 20470B-LON-SVR1 重复步骤 2 至 4。

练习 1: 规划存储需求（Planning storage requirements）

场景（Scenario）

A. Datum 公司希望设计新的存储解决方案以支持最近的几个更改。 这些更改包括：

- 外部客户更多地使用 Web 应用程序，这些客户需要更多和新的业务服务。
- 内部用户需要更多的支持和内部基础设施服务。
- 管理块级存储和共享文件访问的需求已经扩大。
- 最近收购的公司使用与 A. Datum 不同的 IT 基础架构。 IT 部门现在需要管理包括伦敦，纽约和日本的偏远地理区域的混合环境。
- 近年来存储成本大幅下降。
- A. Datum 业务集团生成的数据量增长得更快。

要求（Requirements）

一般来说，新系统应该是低成本，具有合理的性能，并且 A. Datum 和新收购公司的存储管理员应该能够轻松地管理它。

新的存储系统应包括：

- 集中管理和控制存储基础架构。
- 支持需要大量 SQL 数据库存储的应用程序。
- 一种简单，经济的方式来部署具有最小管理开销的块级存储。
- 配置 VMWare ESX / ESXi 虚拟机。
- 配置 Hyper-V 虚拟机。
- 支持需要访问共享文件夹的 UNIX 客户端。
- 如果需要，为旧客户端共享访问权限。
    - 作为履行此要求的一部分，您将确定较旧的客户端（包括 Windows XP 和 Windows Vista）是否需要访问共享，然后您将删除用户未使用的任何旧共享。.

方案（Proposals）

作为 A. Datum 的高级服务器管理员，您负责为组织实施新的文件存储技术。在审查要求后，您将根据以下问题的答案提出计划：

- 您计划评估 iSCSI，光纤通道和 InfiniBand 解决方案如何满足要求。你希望选择哪个解决方案？
- 您计划为 SQL 数据库实现哪些存储，块级存储或文件级存储？
- 您的解决方案将如何最大限度地减少存储管理员的管理开销？
- 您计划使用哪些服务器角色来配置 VMWare ESX / ESXi 虚拟机？
- 是否在 NFS 或 SMB 上运行 Hyper V 虚拟机？
- 哪个文件共享协议将用于需要访问的 UNIX 客户端？
- 如何计划禁用现有 SMB 文件共享的旧式 SMB 访问？

本练习的主要任务如下：

1. 阅读支持文档。
2. .记录您计划的行动方案。

▶ 任务 1: 阅读支持文档（Read the supporting documentation）

- 阅读实验练习场景中的支持文档。

▶ 任务 2: 记录你的计划的行动方案（Record your planned course of action）

记录您对以下问题的答案：

1. 您计划评估 iSCSI，光纤通道和 InfiniBand 解决方案如何满足您的需求。 你希望选择哪个解决方案？
2. 您计划为 SQL 数据库实现哪种存储类型，块级存储或文件级存储？
3. 您的解决方案将如何最大限度地减少存储管理员的的管理开销？
4. 您计划使用哪些服务器角色来配置 VMWare ESX / ESXi 虚拟机？
5. 您将在 NFS 或 SMB 上运行 Hyper-V 虚拟机吗？
6. 哪个文件共享协议将用于需要访问的 UNIX 客户端？

7. 如何计划禁用现有 SMB 文件共享的旧式 SMB 访问？

结果：完成此练习后，您应该已经成功规划了一个满足您组织要求的存储解决方案。

练习 2: 配置 iSCSI 存储（Configuring iSCSI storage）

场景（Scenario）

您需要使用 MPIO 实现高可用性的 iSCSI 存储。 文件服务器和 iSCSI 目标之间有两个独立的网络路径。 您将配置 MPIO 使用两个路径在网络级提供冗余。

本练习的主要任务如下：

1. 安装 iSCSI 目标功能。
2. 创建并配置 iSCSI 目标。
3. 配置 MPIO。
4. 连接到 iSCSI 目标。
5. 初始化 iSCSI 磁盘。

▶ 任务 1:安装 iSCSI 目标功能（Install the iSCSI target feature）

- 在 LON-DC1 上，在服务器管理器中，在 File and Storage Services 中安装 iSCSI Target Server 服务。

▶ 任务 2:创建和配置 iSCSI 目标（Create and configure an iSCSI target）

4. 在 LON-DC1 上，在服务器管理器中，在 File and Storage Services 中，浏览到 iSCSI。
5. 使用以下设置创建新的 iSCSI 虚拟磁盘:
   - 名称：iSCSIDisk1
   - 磁盘容量：5 GB
   - iSCSI 目标： New
   - 目标名称：LON-DC1
   - 访问服务器：10.100.100.3,10.200.100.3
6. 使用以下设置创建第二个 iSCSI 虚拟磁盘:
   - 名称：iSCSIDisk2
   - 磁盘容量：5 GB
   - 磁盘目标：LON-DC1

▶ 任务 3: 配置 MPIO（Configure MPIO）

1. 在 LON-SVR1 上，在服务器管理器中，添加 Multipath I/O 功能。
2. 安装完成后，重新启动 LON-SVR1，然后以 Adatum\Administrator 身份登录，密码为 Pa55w.rd。
3. 在服务器管理器中的 Tools 菜单上，打开 iSCSI Initiator。
4. 在 iSCSI Initiator 中，执行快速连接到目标 10.100.100.2。
5. 在服务器管理器中的 Tools 菜单上，打开 MPIO。
6. 在 MPIO Properties 中，在 Discover Multi-Paths 选项卡上，添加对 iSCSI 设备的支持，然后在出现提示时重新启动。

7. 重新启动后，以 Adatum\Administrator 身份登录，密码为 Pa55w.rd。
8. 在服务器管理器中，打开 MPIO，然后验证 MSFT2005iSCSIBusType_0x9 是否列为设备。

▶ 任务 4: 连接到 iSCSI 目标（Connect to the iSCSI target）

1. 在 LON-SVR1，在服务器管理器，在 Tools 中，打开 iSCSI Initiator
2. 在 Targets 选项卡上，断开所有会话。
3. 重新连接，选择下列选项，然后进入 Advanced 设置：
   - Enable multi-path
   - Add this connection to the list of Favorite Targets.
4. 在 Advanced Settings 对话框中, 选择以下设置:
   - 本地适配器：Microsoft iSCSI Initiator
   - 发起程序 IP：10.100.100.3
   - 目标门户 IP： 10.100.100.2/3260
5. 重新连接，选择下列选项，然后进入 Advanced 设置：
   - Enable multi-path
   - Add this connection to the list of Favorite Targets.
6. 在 Advanced Settings 对话框中, 选择以下设置:
   - 本地适配器： Microsoft iSCSI Initiator
   - 发起程序 IP：10.200.100.3
   - 目标门户 IP： 10.200.100.2/3260
7. 在 Volumes and Devices 选项卡中, 选择 Auto Configure 选项.
8. 在 Targets 选项卡中, 选择 iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target 作为目标, 然后查看 Devices。
9. 针对 MPIO, 确认以下配置：
   - 负载均衡策略： Round Robin
   - 路径详细信息与您为源地址和目标地址配置的 IP 地址匹配

▶ 任务 5:初始化 iSCSI 磁盘（Initialize the iSCSI disks）

1. 在 LON-SVR1 上，在服务器管理器中的 File and Storage Services 中，浏览到 Disks。
1. 选择一个总线类型为 iSCSI 的脱机磁盘，然后使其联机。
2. 右键单击该磁盘，然后创建具有以下属性的新卷：
   - GPT 磁盘
   - 驱动器号：J
   - 卷标签：SMBShares
   - 其他设置：默认
3. 选择一个总线类型为 iSCSI 的脱机磁盘，然后使其联机。
4. 右键单击该磁盘，然后创建具有以下属性的新卷：
   - GPT 磁盘

- 驱动器号：K
- 文件系统：NTFS
- 卷标签：NFSShares
- 其他设置：默认

5. 使用 File Explorer 验证 SMBShares 和 NFSShares 在 This PC 中是否可用。

结果：完成此练习后，您应已成功配置了使用 MPIO 进行冗余的 iSCSI 目标。

练习 3：配置并维护共享基础架构（Configuring and managing the share infrastructure）

场景（Scenario）

为 LON-SVR1 配置 iSCSI 存储后，需要创建共享以支持运行 Windows 和 Linux 操作系统的客户端。

本练习的主要任务如下：

1. 在 iSCSI 存储上创建 SMB 共享。
2. 在 iSCSI 存储上创建 NFS 共享。
3. 使用 Windows PowerShell 查看共享信息。
4. 禁用旧式 SMB1 协议。
5. 准备下一个单元。

▶ 任务 1：在 iSCSI 存储上创建 SMB 共享（Create an SMB share on iSCSI storage）

1. 在 LON-SVR1 上，在服务器管理器中的 File and Storage Services 中，浏览到 Shares.
2. 使用以下设置创建一个新的共享：
   - 文件共享配置文件： SMB Share – Quick
   - 按卷进行选择： J:
   - 共享名称：Data
   - Enable access-based enumeration
   - 添加权限： Domain Users, Modify

▶ 任务 2： 在 iSCSI 存储上创建 NFS 共享（Create an NFS share on iSCSI storage）

3. 在 LON-SVR1 上，在服务器管理器中的 File and Storage Services 中，浏览到 Shares.
4. 使用以下设置创建一个新的共享：
   - 文件共享配置文件：NFS Share – Quick
   - 按卷进行选择： K:
   - 共享名称： LinuxData
   - 验证模式： Kerberos v5 authentication(Krb5)
   - 添加权限：All Machines, Read / Write

▶ 任务 3：使用 Windows PowerShell 查看共享信息（Use Windows PowerShell to view share information）

1. 在 LON-DC1，打开 File Explorer, 然后浏览到 \\LON-SVR1\Data 。
2. 创建一个名为 NewFile.txt 的新文本文件，然后在 Notepad 中将其打开。
3. 在 LON-SVR1 上，打开 Windows PowerShell 提示符。
4. 在 Windows PowerShell 提示符下，键入以下命令，然后按 Enter 键：

```
Get-NfsShare
```

5. 键入以下命令，然后按 Enter 键：

```
Get-NfsShare LinuxData | FL *
```

6. 键入以下命令，然后按 Enter 键：

```
Get-SmbShare
```

7. 键入以下命令，然后按 Enter 键：

```
Get-SmbShare Data | FL *
```

8. 键入以下命令，然后按 Enter 键：

```
Get-SmbSession
```

9. 键入以下命令，然后按 Enter 键：

```
Get-SMBSession -ClientUserName Adatum\Administrator | FL *
```

10. 键入以下命令，然后按 Enter 键：

```
Get-SmbOpenFile
```

注意： Adatum\ Administrator 有两个条目。 文件资源管理器创建一个，记事本创建另一个。 如果不包括 NewFile.txt，那是因为文件连接只在最初打开文件或保存文件时保持很短时间。 如果你没有看到两个条目，切换到 LON-DC1，关闭记事本，然后双击 NewFile.txt。 然后，在 LON-SVR1 上，重复步骤 10。

11. 保持 Windows PowerShell 提示符的打开状态，用于下一个任务。

▶ 任务 4：禁用旧式 SMB1 协议（Disable the legacy SMB1 protocol）

1. 在 LON-SVR1 上，在 Windows PowerShell 提示符下，键入以下命令，然后按 Enter 键：

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

2. 键入以下命令，然后按 Enter 键：

```
Get-SmbServerConfiguration | FL enable*
```

3. 键入以下命令，然后按 Enter 键：

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4. 键入以下命令，然后按 Enter 键：

```
Get-WindowsFeature *SMB*
```

5. 键入以下命令，然后按 Enter 键：

```
Remove-WindowsFeature FS-SMB1
```

▶ 任务 5: 准备下一个单元（Prepare for the next module）

完成实验后，通过完成以下步骤将虚拟机还原到其初始状态：

1. 在主机计算机上，切换到 Hyper-V Manager 控制台。
2. 在虚拟机列表中，右键单击 28740B-LON-DC1，然后单击 Revert。
3. 在 Revert Virtual Machine 对话框中，单击 Revert。
4. 对 28740B-LON-SVR1 重复步骤 2 和 3。

结果：完成此练习后，您应该已成功创建 SMB 和 NFS 共享。

问题：为 iSCSI 实现 MPIO 并不像安装 MPIO 那么简单。 在本实验中，您执行了哪些其他步骤来启用 MPIO？

问题：当您使用 Get-SmbOpenFile 时，所有打开的文件是否显示？

单元复习和作业（Module Review and Takeaways）

复习问题（Review Questions）

问题：如果 DAS 提供与 SAN 类似的性能，它是否适合所有存储需求？

问题：在禁用 SMB1 之前，必须从环境中删除哪些操作系统？

工具（Tools）

下表列出了此单元引用的工具。

工具	用途	在哪里
Computer Management	• 管理 SMB 共享 • 管理磁盘 • 查看事件日志	在服务器管理器中的 Tools 菜单上
Disk Management	• 初始化磁盘 • 创建和修改卷	在服务器管理器中的 Tools 菜单上或 Computer Management 中
Fsutil.exe	• 管理 NTFS 卷；检查磁盘信息，创建特定大小的文件等等	命令提示符
File and Storage Services	• 执行基本存储管理任务 • 检查存储配置 • 创建卷	在服务器管理器中的 File and Storage Services 下