Information Infrastructure Solution
领驭信息架构 创新存储时代

IBM

START FROM HERE

IBM企业信息架构技术白皮书—“真经”

欲得真精 必读此经

CONTENTS
目录

CONTENTS
目录

第五卷 IBM企业信息架构–信息安全方案群组

综 述

IBMSystemStorage:您的企业的未来就在这里

节省、增长、创新。借力IBMSystemStorage

前进

您的企业的未来就在这里。要充分利用IBM久经考验的创新技术和存储领先优势来提升您的最终效益，现在正是最佳时机。让我们鼓励您坚持到底，利用IBM简单、可扩展、智能化的存储来转变您的企业。

IBM System Storage™解决方案专为助您的企业取得成功而构建。端到端的存储独创性和IBM无与伦比的专业技术可帮助您降低成本、风险和复杂性，并同时提高您的基础架构和人员的效率与响应能力。节省、增长、创新。借力IBM System Storage。

为了我们的地球－以及您的最终效益实现环保

获得最高IT投资回报的迫切需求是企业日复一日面临的运营挑战－而节约能源则意味着节省资金。System Storage解决方案提供了高能效的工具和技术，可以帮助您保持专注于重要事项。此外，它仅对环境产生很小的影响，并同时优化您的数据中心以及改善IT成本结构。

通过消除存储中的低效之处实现节省。IBM预封装的存储套件和先进的系统虚拟化技术为您提供了非常方便的方式来降低成本、减少能源消耗以及大幅提高存储利用率－并同时不影响性能。自动化分层存储管理和卓越的数据移动性可以帮助您使应用程序和投资更符合存储数据的价值－既节省时间又节省资金。

通过实施IBM System Storage解决方案来降低电源、散热和空间方面失控的成本，您将会在环保方面作出“表率”。不论您的企业的规模如何，IBM均提供了高能效的策略和节省方案，帮助您实现可持续的企业。

借助灵活、响应迅速的IT基础架构实现轻松获取、轻松扩展

快速响应不断变化的业务需求，这句话通常说起来容易、做起来难。IBM System Storage 提供了易于使用且十分经济的存储产品，可以灵活地管理增长、复杂性和风险，从而帮助您发掘业务弹性并在企业日常运营所面临的挑战方面始终领先一步。

距离

解决存储增长难题。IBM System Storage允许您利用深入的基础架构灵活性大幅且可靠地对存储进行扩展，实现对数据增长的控制并消除昂贵的特殊存储采购。

简化存储管理并节省管理时间。借助图形界面和集成的系统，IBM存储平台允许您跨异构的环境来统一和管理物理和虚拟资源。

对于正常业务条件下企业的高效运营－以及发生紧急情况或中断事件时快速恢复，保护数据至关重要。System Storage凭借坚如磐石的数据保护工具和高可用性可以帮助您降低风险，在您最需要时更是如此。

借助IBM System Storage的强大功能和优异的简易性有效地管理您的业务数据。

通过至关重要的创新拓展您的业务空间

想象一下，突破性的创新将允许您更快、更好地运营您的企业，从而帮助吸引新客户并获得竞争优势。现在想象一下，久经考验的可靠性、顶级的服务和全面的专业技术支持将会使您在与业务需求的竞赛中始终领先一步。实现所有这一切，并同时降低您的总拥有成本以及保护现有的存储投资。IBM已经为您做到。

发展您的企业不仅仅意味着专注于优秀的创意－您想要获得更高的投资回报。System Storage可以帮助您通过重要的创新来转变您的企业。IBM System Storage平台拥有明确的技术路线图以确保平稳的升级和过渡，无论未来的技术如何变化，都能够满足最严格的数据存储要求。长期的二进制兼容性使得支持您的企业的设备、应用程序和技能拥有更长的寿命，即使在推出新的系统之后也不例外。

把握时机至关重要。System Storage解决方案可帮助您始终先人一步，这样您便可以就如何利用技术方面的进步作出战略决策，从而扩展您的企业并畅想无限可能。

在每一次的发展飞跃中我们将始终伴您同行

IBM了解创新并不能将大山移开－但可以简化攀登它的方式。并且我们也深知信任不会在一夜之间形成，而是通过无数次的交往逐渐建立起来的。我们遍布全球的本地技术专家和广泛的IBM业务合作伙伴网络相信协作就是“卷起袖管”并实现我们的价值。

IBM拥有广泛的资源、经验和专业技术来帮助您克服实际的行业挑战，并始终不懈地致力于为您的企业带来简单、可扩展、智能化的存储。

节省、增长、创新。借力IBM System Storage。

合适的

成为随需应变的企业需要在动态的业务环境中寻求新的增长、适应和响应方式，并同时管理成本。由于现在数据是企业的关键组成部分，因此高效地处理不断增长的信息量便成为取得成功的关键之一。存储环境是IT基础架构的重要部分，可以帮助实现随需应变企业的运营目标。

IBM存储产品和解决方案

- IBM System Storage虚拟化产品
- IBM存储管理软件
- IBM System Storage磁盘系统
- IBM System Storage磁带系统
- IBM System Storage SAN交换机
- IBM System Storage N系列

IBM System Storage虚拟化产品

虚拟化旨在通过将应用环境与物理存储基础架构相隔离来降低存储基础架构的复杂性。这有助于极大地提高管理异构存储环境的能力，从而可以更自由地根据需求选择最佳的产品，而不会增加支持成本。虚拟化还可以在对应用程序影响最小或无中断的情况下帮助实现对存储环境的改变，从而有助于更好地响应计划外的业务需求。从财务方面而言，简化的管理有助于降低运营成本，提高存储利用率则有助于降低资产成本。

IBM虚拟引擎TS7000系列

将硬件和软件结合到集成的解决方案中，旨在为通过光纤通道进行物理连接的服务器提供磁带虚拟化。TS7000系列融合了IBM服务器技术、磁盘技术和磁带技术，旨在虚拟化或模拟磁带库、磁带机和磁带介质。实际磁带资源之后便可以连接到TS7000，以帮助实现信息生命周期管理和业务连续性。TS7700虚拟引擎支持连接到Systemz™服务器。TS7500虚拟引擎™支持开放式系统连接。

IBM System Storage SAN卷控制器

旨在帮助降低在SAN环境中管理多个磁盘存储系统的复杂性和成本。它可以将多个磁盘存储系统的容量整合到一个可以单个位置进行管理的单一存储资源池。这可以帮助客户更高效地使用其资源，提高其应用程序的可用性并帮助提高相关人员的工作效率。

解决方案

IBM TotalStorage Productivity Center

IBM Total Storage®Productivity Center是一个开放的存储基础架构管理解决方案，旨在帮助简化对复杂存储基础架构的管理，提高存储容量利用率和管理效率。

IBM TotalStorage Productivity Center for Data

旨在实现存储基础架构中文件和数据库资源的自动化容量管理。它还提供了用于分析这些资源使用情况的多种功能。

IBM TotalStorage Productivity Center for Fabric

旨在实现存储网络中各种设备的自动化管理。它提供了资源发现、事件监视和更改、区域控制和SAN错误预测等多种功能。

IBM TotalStorage Productivity Center for Disk

旨在帮助管理员从单个点管理异构的SAN环境。它可以与多种支持SMI-S功能的存储设备协同工作，例如IBM TotalStorage Enterprise StorageServer®（ESS）和IBM SystemStorage DS4000™、DS6000™及DS8000™系列，以及使用IBM SystemStorage SAN卷控制器进行虚拟化的存储设备。

IBM TotalStorage Productivity Center for Replication

旨在简化和自动化复制环境的配置，从而有助于更有效地进行城域镜像、全球镜像、城域/全球镜像和IBM FlashCopy®管理。它还可以监视跨设备的复制操作，以帮助支持复制环境。

IBM Tivoli Storage Manager系列

IBM Tivoli® Storage Manager是Tivoli Storage Manager系列解决方案中的基础产品，通过在脱机存储层次结构中存储备份、归档、空间管理和裸机恢复数据，以及符合性数据和灾难恢复数据，来提供数据保护，以防止发生故障和其他错误。IBM Tivoli Storage Manager和IBM Tivoli Storage Manager扩展版使用集中、自动化和基于策略的管理，可以在发生硬件、软件或网络故障时为应用程序和关键数据提供全天候保护。Tivoli Storage Manager系列包含各种可选模块，这些模块可另行定购，用于邮件、数据库、复制服务、SAN、系统备份与恢复、空间管理Microsoft® SharePoint®和企业资源规划（ERP），从而实现全面的存储管理。

Tivoli Storage Manager

可以发生硬件、软件或网络故障时，提供关键数据和应用程序的企业可用性。它提供了移动与存储技术和基于策略的自动化，两者相结合可以帮助提高对数据和应用程序的保护，缩短灾难恢复时间并降低存储管理成本。它还可以管理不活动的数据并将数据的价值与有效的存储管理实践相关联。

虚拟化

IBM System Storage DS系列磁盘存储系统

高性能的IBM System Storage磁盘系统是行业中可靠性，可扩展性和互操作性最出色的产品。高可用性、多平台支持和对多种操作系统的支持有助于帮助您实施IBM的“随需应变企业”策略。

IBM SystemStorage连续企业磁盘存储器

IBM System Storage具有连续的企业磁盘存储。IBM System Storage DS6000系列，以及IBM System Storage DS8000系列，与更新后的IBM TotalStorage Enterprise Storage Server（ESS）800型一起在各种性价比选项范围内为大型机和开放式系统服务器提供连续的企业级存储系统，并提供了共享的复制服务和通用的管理接口。这些企业级产品可将企业级范围下移到以前的严格中端领域，并扩展涵盖了更高范围的性能与可扩展性需求。

IBM SystemStorage DS8000Turbo系列

为高性能关键任务工作负载可高度扩展且经济高效的数据存储设立了新的标准。DS8000支持非常大的高效缓存和高达512TB的物理磁盘容量，并且吞吐量达到了ESS 800的7倍。DS8000提供了顶级的高性能、可扩展性和长期经济性。DS8300还可提供在存储系统LPAR（逻辑分区）中运行等效于两个独立存储阵列的成本优势，全部在单个物理DS8300中完成。DS8000还提供了业务持续性解决方案，包括IBM SystemStorage Flash Copy、IBM Flash CopySE、城域镜像、全局镜像以及城域/全局镜像。DS8000是用于存储整合的绝佳系统，可支持通过FC/IBM FICON®和IBME SCON®连接到各种服务器，包括IBM System z、System i™、System p™、System xi™以及其他运行UNIX®、Linux®、Windows®等操作系统的平台。

IBM System Storage DS6000系列

在价格合理的小型模块化套件中提供了高可用性和高性能。该系列以及DS8000系列提供了具有共享复制服务和通用管理接口的企业级连续存储系统。DS6800以其高效的空间设计提供了卓越的性能。DS6800具备出色的吞吐量和I/O处理能力，非常适用于高速率的事务型和带宽密集型应用程序，并可满足渴求性能的工作负载的需求。DS6800支持各种服务器（大型机和开放式系统），包括IBM System z、System i、System p、System x以及运行UNIX、Linux 和Windows操作系统的非IBM平台，可以帮助简化IT基础架构。

存储

IBM TotalStorage Enterprise Storage Server Refurbished with Warranty

是企业级可靠性和功能的原始基础。ESS Refurbished with Warranty 800型最高可提供55.9TB 的物理磁盘容量，为您带来均衡的性能。它提供了极为强健的业务连续性解决方案，包括Flash Copy以及城域和全球镜像。ESS是为测试或备用系统提供存储或者为需要ESCON或SCSI连接的系统提供存储的绝佳系统。它可通过FC/FICON、ESCON和SCSI与各种服务器（包括大型机和开放式系统）连接，支持许多新旧版本的常用操作系统。

IBM System Storage DS4000系列

可以帮助满足如今随需应变时代不断增长的高性能或高容量存储要求。IBM System Storage DS4000系列采用通用的存储管理软件和高性能硬件设计，从而有助于以低成本为客户提供企业级的功能。高可用性、多平台支持、广泛的开放式操作系统支持和综合管理工具均有助于应对不断变化的存储要求和挑战。

IBMSystemStorage DS3000系列

旨在提供串行连接SCSI（SAS）技术的灵活性。

DS3400在直连或SAN解决方案中可提供4-Gbps速度的光纤通道性能。DS3300为IP SAN提供了1 Gbps的iSCSI连接，而DS3200在直连解决方案中则可提供3-Gbps点对点拓扑结构。DS3000系列支持基于SAS的扩展机箱EXP3000，此机箱可将容量最多增至48个磁盘，而无需另行投资控制器。

磁盘

IBM TotalStorage Expandable Storage Plus320（2104）

非常适合于要求采用最新小型计算机系统接口（SCSI）Ultra 320技术的中小规模IBM AIX®环境。它可以实现使用一条SCSI总线的双主机连接，以便借助IBM高可用性群集多处理（HACMP™）故障转移软件实现非并发的高可用性配置；或是实现使用两条SCSI总线的双主机连接。Expandable Plus 320非常适合于与IBM System p的多主机连接。

IBM System Storage归档和保留

IBMSystemStorage DR550和DR550易捷版

旨在提供预配置的集成产品，以帮助存储、检索、管理、共享和保护管制数据和非管制数据。DR550可以通过单处理器或双处理器IBM POWER5+服务器支持高性能的数据访问，或者支持极高的存储容量（从1.1TB扩展至112TB联机存储容量，通过连接光盘或磁带库最高可扩展至数PB的分层存储容量），此外还具有低于仅磁盘归档产品的总拥有成本。DR550还支持数据加密，旨在防止对记录进行未经授权的访问，并有助于保护隐私，企业版DR550还可提供同步或异步复制选项，以实现灾难恢复。DR550基于策略的归档数据保留功能可以支持不可擦除、不可重写的数据存储。借助已确立归档应用程序编程接口（API）连接到IBM内容管理器或非IBMISV内容管理器或归档软件，DR550可以提供长期数据保留、归档和保护功能，从而满足管制行业和其他行业的需求。

存储

IBM System Storage磁带存储系统

磁带存储系统在业务连续性和信息生命周期管理计划中充当着关键角色。利用IBM完整系列的磁带机、自动加载机和磁带库，即可轻松存储、归档和检索数据。

磁带库

IBM System Storage TS3500磁带库

是大容量开放式系统和IBM Systemz环境的卓越之选。它可以与高性能、高容量的IBM LinearTape-Open™（LTO）Ultrium第3代或第4代磁带机结合配置，以提供出色的数字线性磁带（DLT）替代方案。IBM TS1120磁带机可进行组合，以提供快速访问以及高性能与高容量特性。TS1120和LTO第3代和第4代磁带机均支持WORM以及标准数据磁带。TS3500还支持TS1120和LTO第4代磁带机加密。

IBM SystemStorage DR550

IBM System Storage TS3310磁带库

设计为高性能、可靠、可扩展的磁带子系统，最多可自动化396盘盒式磁带（TS3310）。磁带库采用获得专利的IBM多路架构，旨在允许在单个物理库内定义多个逻辑库，并允许异构应用程序同步共享单个物理库。控制和数据路径故障转移还增加了额外的自动化功能。TS3310最多可使用18个第3代和/或第4代LTO磁带机。此外，还支持WORM数据磁带（通过LTO 第3代和第4代磁带机）。TS3310还支持LTO第4代磁带机加密。

IBM System Storage TS3400磁带库

可以在较小的自动化空间内为System i、System p、System x、System z及其他开放式系统环境提供IBM SystemStorage TS1120磁带机的高容量与性能优势。TS3400磁带库是外部5U独立安装或机架安装单元，最多可以支持两个TS1120磁带机。对于已经在其数据中心采用TS1120磁带机，同时希望在远程位置采用同一技术的组织来说，TS3400磁带库是理想的磁带存储解

决方案。TS3400还适用于IT环境的实际空间较为狭小的组织。

磁带

IBM System Storage TS3200磁带库

为4U高度，结构极为紧凑，最多可容纳48盒LTO磁带以及1个或2个LTO第3代和/或第4代磁带机，并且采用了可拆卸的磁带盒插槽，以便进行批量加载和卸载。该磁带库最多可支持两台异构服务器对其同步共享访问，并且无需其他硬件或软件。标配有条码阅读器和三磁带输入/输出插槽。通过可选的Web界面，用户可以使用Web浏览器来监视磁带库状态。TS3200是满足中小企业不断增长的存储需求的理想之选。LTO第3代磁带机还为TS3200磁带库提供了WORM功能，LTO第4代磁带机还支持数据加密。

IBM System Storage TS3100磁带库

是外部独立安装或机架安装的24磁带2U高自动加载机，使用一个具有两个可拆卸磁带盒插槽的IBM LTO第3代或第4代磁带机。对于使用磁带并要求大容量或高性能磁带备份（带有或不带有随机访问）的客户而言是不错的选择。标配有条码阅读器、远程管理功能和单个磁带输入/输出插槽。TS3100为自动化存储管理软件提供了选择所需磁带的能力。WORM功能也适用于LTO Ultrium 3磁带机，LTO第4代磁带机还支持数据加密。

IBM System Storage LTO系列存储产品

存储

磁带机

IBM System Storage TS1120磁带机

旨在提供快速性能与高容量，以帮助降低异构服务器环境中的客户资源要求。TS1120可以同时提供对数据的快速访问和备份大型数据库所需的高容量，因此支持采用单一的磁带技术。这有助于降低成本并允许将数据整合到较小的空间，而这反过来又有助于降低存储环境的复杂性和管理开销。TS1120提供WORM功能，有助于支持数据保留需求和要求审计跟踪的应用程序。此外，TS1120还提供了加密和关键管理功能，这些功能使其成为理想的数据保护解决方案。

IBM TotalStorage 3580磁带机

可为现有的Linear Tape Open（LTO）盒式磁带用户或在一盘盒式磁带上通常存储少于400GB数据的用户提供便利。这种独立的单个第3代LTO磁带机可以采用机架安装，也可置于桌面上，是出色的SDLT、DLT、1/4英寸、4毫米或8毫米磁带机替代方案。LTO Ultrium 3磁带机还提供了WORM功能。

IBM 3580磁带机

IBM System Storage TS2340磁带机

是不断增长的存储要求和不断缩短的备份窗口的最佳解决方案。TS2340磁带机融入了最新一代的高级LTO技术，适合满足各种小型系统的备份、保存、恢复，以及归档数据存储需求。此外，TS2340还支持通过3Gbps SAS连接进行数据加密，从而提供更多安全功能。

补充的磁带存储产品

产品包括7206（4毫米和VXA-2格式）、7207SLR格式）和7212（多磁带技术格式），旨在帮助保护、访问和管理任何规模组织的关键业务数据。

网络

IBM System Storage SAN 交换机

尽管不为大多数用户所知，但IBM SAN基础架构组件为所有类型和规模企业的可扩展、可靠存储提供了出色的连接能力。IBM存储网络通过将存储资源整合到池中，提高了存储资产的利用率并改善了信息的共享和访问，从而在帮助简化基础架构方面发挥了关键的作用。

存储区域网络（SAN）

解决方案提供了出色的基础架构，可帮助使企业保持

迅捷、灵活，以应对随需应变企业中不断流动、高压力和快速变化的情形。IBM提供来自SAN交换机供应商Brocade和Cisco的各种SAN基础架构产品。这些产品可将服务器和存储连接为高可用性的存储网络，以支持可扩展性，从而帮助满足快速且无法预测的增长需求。

IBM System Storage SAN路由器

旨在为大型企业的磁盘、磁带、虚拟化和软件解决方案提供灵活、高性能、安全的城域和全局网络光纤通道和FICON SAN扩展。

- IBM System Storage SAN18B-R路由器交换机
- 适用于IBM System Storage的Cisco MDS 9222i路由器交换机

IBM System Storage SAN 企业导向器

旨在为全球性企业的磁盘、磁带、虚拟化和软件解决方案提供超高可用性、性能和可扩展性的光纤通道和FICON连接。

- IBM TotalStorage SAN256B导向器
- IBM TotalStorage SAN140M导向器
- IBM TotalStorage SAN256M导向器
- 适用于IBM System Storage的Cisco MDS9506导向器
- 适用于IBM System Storage的Cisco MDS9509导向器
- 适用于IBM System Storage的Cisco MDS9513导向器

IBM System Storage SAN 入门级交换机

旨在为中小企业（SMB）的磁盘、磁带、虚拟化和软件解决方案提供价格合理、易于使用且高性能的连接。

- IBM TotalStorage SAN16B-2易捷型号网络交换机
- 适用于IBM System Storage的Cisco MDS9124易捷型号网络交换机

IBM System Storage SAN中端交换机

旨在为SMB和大型企业的磁盘、N系列、磁带、虚拟化和软件解决方案提供价格合理、灵活且高性能的光纤通道和FICON 连接。

- IBM System Storage SAN32B-3网络交换机
- IBM System Storage SAN64B-2网络交换机
- 适用于IBM System Storage的Cisco MDS9134网络交换机

存储

统一存储－网络连接存储（NAS）、IP SAN（iSCSI）和FC SAN

IBM System Storage N系列（N3700、N3300、N3600、N5200、N5300、N5500、N5600、N7600、N7800）

提供多功能的统一存储架构，可同时满足各种需求－SAN和NAS、主存储和辅助存储－同时具有高可用性。IBMN系列以真正简化存储基础架构和提高生产效率的方式应对复杂的要求。

统一存储－网络连接存储（NAS）、(IP SANiSCSI）和FC SAN

- N系列产品组合中的每个产品在整个平台上均采用单一操作系统，并且提供多种高级功能的软件组合，从而带来了行业中最为多样化的存储平台之一，用于提供综合系统管理、存储管理、板载和板外复制服务、虚拟化技术、灾难恢复以及备份解决方案。
- 所有N系列产品均提供完全相同的广泛网络连接功能，可以通过包括文件系统NAS协议（CIFS、NFS）在内的多种网络访问协议，以及包括iSCSI和FCP在内的块I/O协议连接到各种主机和客户端系统，并且全部通过单个硬件平台完成。
- 所有的N系列产品均具有极高的灵活性，可以通过光纤通道磁盘驱动器和SATA磁盘驱动器扩展至高达504TB。
- 此外，可选的合规性和数据保留软件还可在管制环境中提供数据安全性，在此数据必须以不可擦写和不可重写格式进行存储，以满足行业对保留公司数据资产最新的严格法规要求。

IBM System Storage N 系列产品组合提供了目前行业内最为多功能的存储平台之一。

利用强大优势

	存储管理软件	系统管理软件	系统管理软件	磁盘存储/N系列	磁带存储	SAN	业务合作伙伴解决方案中心
IBM	●	●	●	●	●	●	●
HP[6]	●	●	●	●	●	●	●
EMC[7]	●	●	●	●		●	●
Dell[8]		●		●	●	●	●
Hitachi[9]	●		●		●	●	●

IBM存储产品与其他供应商产品的比较

IBM System Storage N3600和N3300

将所有部分组合到一起

IBM System Storage Proven™可以证明IBM服务器和存储与其他供应商的硬件及软件产品的兼容性与互操作性。IBM System Storage Proven计划为客户确定预先符合条件的存储解决方案和配置与IBM产品的互操作性。

要查看预先符合条件的IBM System Storage Proven解决方案的完整列表，请访问：ibm.com/storage/proven

IBM Systemx和Blade Center存储服务器

最新的IBM System x存储服务器产品提供了各种价格合理的、基于Windows的网络连接文件服务器解决方案。这些解决方案将IBM成熟的System x和Blade Center® 服务器技术与Microsoft Windows Storage Server 2003操作系统相结合，为各种规模的大型和小型企业提供了出色的网络连接存储解决方案。每台服务器的硬件均已预先配置，并预安装了Windows Storage Server 2003操作系统，从而实现快速部署并方便使用。

利用强大优势

遍布全球的顶级销售与技术支持服务网络为每一个IBM存储产品提供强大支持。IBM提供本地、专注的支持服务，以帮助促进从开始到保修等各个阶段的系统开发。除客户支持、验证和集成协助之外，IBM还提供各种融资选项、培训及咨询服务，旨在提供完整的数据存储解决方案。

IBM与IBM业务合作伙伴以及其他领先的技术公司合作，共同提供合适的存储解决方案，以帮助您的企业在如今的动态市场中取得成功。您也可以访问IBM业务合作伙伴创新中心，亲自测试IBM存储解决方案。选择IBM作为您的技术供应商，您将能够充分利用最新和新兴的技术，这对于企业的成功至关重要。

现在就开始吧

这是一个简单的决定。一个全球性的端对端存储解决方案供应商就可为您的组织完成的工作，何必不断寻找多个供应商来重复进行？坚持采用行业领导厂商所提供的出色的存储解决方案、产品和服务。

IBM x346 NAS 存储服务器

创新

	数据库软件	托管	咨询和实施服务	磁盘融资	Microsoft Windows服务器	UNIX服务器	其他大型机	应用程序服务器
IBM	●	●	●	●	●	●	●	●
HP[6]			●	●	●	●		
EMC[7]		●	●	●				●
Dell[8]		●	●	●	●			●
Hitachi[9]			●	●				

信赖IBM提供您所需的帮助

IBM提供：

- 全面的、可定制的开放式IT存储解决方案，以满足您特定的业务需求和预算
- 广泛的模块化硬件和软件产品组合
- 卓越的保修支持
- 国际化服务和支持
- 灵活的融资选项
- 以上全部适用于中小企业

选择IBM提供您所需的存储设备

这些全面的IBM存储产品有助于IT组织突破数据管理、保护和使用的传统模式，从而实现随需应变信息的灵活性和强大优势。服务器和存储技术的融合可提供最新的强大基础，以简化基础架构，实现灵活增长并降低总拥有成本。

从这一更广的方面来说，IBM处理简化问题的能力居于行业领导厂商之一。IBM着眼于整个环境－服务器、网络和存储。这样做可以帮助您创建更经济、灵活和弹性的环境，在该环境下资源和信息可以自由流动，容量和配置可快速更改以满足业务需求。

什么是IBM优势？当然，IBM提供全面的产品组合，包括服务器、网络组件、管理软件和存储产品。但是，IBM还提供各种服务，以帮助取得基础架构简化、业务连续性和信息管理计划的成功。

IBM全球服务和IBM业务合作伙伴可融合从咨询到实施和运营整个范围的技能，来帮助开发根据您的独特需求和预算进行定制的解决方案。这些服务有助于简化IT运营，从而帮助降低成本、提高弹性并增加灵活性，以支持随需应变的信息。

IBM环保数据中心信息基础架构解决方案

在当今环保意识日益增强的时代，业务主管非常关注为企业树立环保形象。同时，许多IT管理人员正面临着信息处理历史上前所未有的多方面危机。这些企业正经历着处理和存储信息的虚拟爆炸性增长，并且能源成本也飙升至历史记录水平。

为满足这种呈指数增长的信息需求，IT企业意欲向数据中心添加更多服务器和存储设备，而大多数数据中心的可用空间、电力和不断增多的设备的所有散热能力均已达到极限。根据《Business Standard》发表的“Going Green with Storage”文章，在过去的15年中，基于磁盘的存储设备所消耗的电力已从1992年的200瓦/设备平方英尺飙升至现在的1,100瓦/平方英尺。[1]

数据中心已成为企业资产负债表上的主要能源消耗方式。更有效的节能数据中心有助于减小对环境的影响，并降低IT成本。

我们不能低估数据中心所消耗的能量。数据中心的效率提高20%将节约数十亿度电。

除信息爆炸性增长以及能源成本和需求不断攀升之外，还有其他诸多因素迫使对数据中心转型，其中包括：

- 业务和技术创新节奏加快。
- 为企业资产和客户信息提供更好的安全保护的需求不断增大。
- 系统和网络操作的成本日益增加。
- 对遵守政府环境保护法规的需求增大。

新企业数据中心- 环保竞争先锋

就企业而言，数据中心的成本越低，企业在市场中的竞争力越强。同时，整体环保IT特性必须包括减少二氧化碳排放量。实际上，因能源成本提高而无法在数据中心中实现“环保”可能会使您的IT基础架构无法支持业务需求的增长。IBM根据综合全面的数据中心方法，开发了新企业数据中心（NEDC），作为有效IT 交付的渐进新模型。新企业数据中心侧重于优化系统和网络，以打破IT资源和业务服务之间的锁定，同时提供快速的服务交付并与业务目标保持一致。新企业数据中心降低了电力要求，极大地减少了高效、环保和经过优化的基础架构所排放的热量，此外，其优点还包括提高了资产利用率，缩短了灾难恢复的时间并降低了地面空间的要求。

信息存储是目前数据中心中发展最快的的技术之一。据《Business Standard》上的文章报道：存储将很可能成为数据中心信息基础架构中耗电最多的元素之一。当今业务环境中信息的飞速增长促进了这一发展。

借助新企业数据中心，IBM根据IBM System Storage™提供了有助于削减能源成本并更有效地使用可用存储空间的信息基础架构解决方案。了解IBM信息基础架构策略的相关信息对理解IBM如何具备上述优点很有帮助。

IBM信息基础架构：环保方案的关键

如果客户能够及时揭示信息的业务价值，从而做出更好的决策并提供宝贵的基于信息的服务，信息则可以成为一项资产，为企业带来竞争优势。信息也可能带来风险。如果未采用适当的安全措施、章程和过期策略，不必要的开支和责任则可能有悖于企业的原有任务。您需要在两者之间进行权衡，以便在利用信息的同时管理风险。

多年以来，IBM一直致力于使用有助于解决信息可用性、数据保留和安全要求的解决方案来协助客户管理其信息基础架构。IBM提供行业领先的产品和服务，使客户能够揭示信息的业务价值。IBM帮助客户增强核心功能，从而实现对信息可用性、信息保留、信息安全和信息规范的可量化服务级别改进。

在IBM信息基础架构解决方案支持您的环境的情况下，您可以使您的进程更加有效和经济合理，并减少整体排放的二氧化碳量。IBM 提供存储虚拟化、信息生命周期

管理、归档和大量IBM 硬件和软件等解决方案，这些解决方案将提高运营效率以及电力和散热效率作为核心。利用IBM的一系列综合环保服务解决方案，您可以建立相关策略，以便在基础架构中更准确地传递信息。

以最快速度访问最需要的信息是基础架构效率的关键。使用IBM信息基础架构解决方案，您可以对信息的创建、捕获、修订、路由、审批、发布、归档或销毁方式进行更精细地控制。这些解决方案与应用程序和信息的生命周期的所有阶段相关。

节约能源成本，并借此更好地实现数据中心的环保是IBM信息基础架构解决方案的优点之一。通过这些解决方案，您能够访问基于大众认可的IBM最佳实践的无缝集成系统中的所有数据。

用于更好地实现数据中心环保的构建模块

IBM已开发了四种构建模块，用于提供在减少运营存储成本的同时管理业务增长的工具。事实证明，这些步骤可以在使用相同能源的情况下增加IT容量、减少多至55%的散热量、降低运营成本并通过采用更少的资源对环境产生正面影响。[2]这些构建模块包括：

- 诊断：评估对存储的使用情况。获取相关信息，了解能源使用情况并确定改进空间。
- 构建：计划、构建和升级至节能数据中心。根据存储的信息，使用最适当的介质或介质组合部署更节能的存储设备。
- 虚拟化：实现虚拟化和其他创新性技术，以便更高效地利用存储设备。消除重复、未使用、非活动和临时数据。
- 散热：使用创新性散热解决方案可以更有效地冷却存储设备。

诊断

为了解能耗问题所在，IT主管必须首先从能源使用方面对数据中心进行评估。IBM Systems and Technology Group和IBM全球技术服务制定的IBM数据中心评估提供了各种服务，以支持能效目标。IBM可以提供：

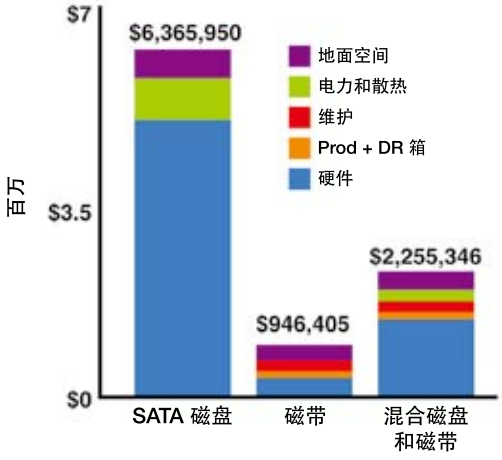
- IT系统能效和数据中心效率评估。
- IBM服务器和存储设备电力/散热趋势评估。
- 数据中心最佳实践评估。
- 数据中心温度分析和优化。
- 存储优化和集成服务。

就能耗而言，IT管理人员必须考虑物理数据中心和IT 基础架构的成本。IBM评估不仅涉及提高物理工厂的电力和散热效率，还涉及对服务器和存储设备进行整合和虚拟化。

构建

升级现有数据中心或构建新数据中心使IT企业可以节约大量能源。大多数数据中心的IT基础架构每两年至四年更换一次，添加这一新设备后，旧数据中心可能无法以节能方式为基础架构供电或散热。这就是构建或升级数据中心是以更好方式实现企业环保的重要基石的原因之一。

使用混合磁带和磁盘减少 50% 的 TCO
10 年 TCO 示例。假定有 250 TB 的存储空间，并且每年的增长速度为 25%



更改数据中心并非总是可行，但是您可以随时间更改您的基础架构。IBM提供的硬件和软件存储解决方案

可以通过整合和虚拟化服务器和存储设备，从而极大地节省能源开支。

客户信息基础架构目标可能包括提高性能、合规性、数据安全和灾难保护，并减少总拥有成本和能源开支。全部磁盘或全部磁带存储基础架构可能无法实现这些目标，但是IBM提供的分层混合基础架构解决方案可以帮助IT企业优化能源节约。

虚拟化

存储虚拟化是IBM帮助客户构建信息基础架构这一策略的关键部分。通过虚拟化存储基础架构，客户可以隐藏存储环境的复杂性，从而实现提高利用率、简化管理和提高存储管理员的生产效率等优势。虚拟化技术可以帮助企业极大地减少数据中心中所需物理存储设备的数目和成本。

使用IBM System Storage SAN卷控制器（SVC），IT企业可以将多个磁盘系统中的存储卷整合到一个容量存储库，从而进行集中管理。SVC是专为实现以下目的而设计的：

- 不间断地迁移数据。
- 简化分层存储设备的部署。
- 提高存储设备性能。
- 帮助提高存储设备的利用率并控制增长。

IBM还提供了虚拟磁带库产品－IBM Virtualization Engine™ TS7500和TS7700。磁带虚拟化技术整合了磁带模拟软件和磁盘阵列，以使多个磁盘显示为主机备份应用程序的一个磁带库和/或磁带驱动器。虚拟磁带库可以使多个备份应用程序服务器共享一个磁盘。作为分层磁盘/磁带解决方案，您可以使用这些虚拟引擎：

- 管理将数据从在线应用程序存储设备传输到离线的永久归档介质。
- 安全存储长期归档，以实现记录保留和灾难恢复。
- 实现完全集成的分层磁盘和磁带存储器层次结构。
- 消除在仅包含磁带的环境中可能存在的瓶颈。
- 帮助缩短批处理时间，并降低总拥有成本和管理开销。

重复数据删除软件是进一步扩展IBM信息基础架构策略的又一关键技术，使客户能够消除冗余数据并简化满足其业务需求所需的基础架构，这可以极大地提高数据中心的效率。

IBM的ProtecTIER™重复数据删除技术和解决方案可以帮助企业：

- 满足企业客户特有的重复数据删除需求，以最大程度地提高在线性能、伸缩性和数据完整性。
- 与现有备份和恢复应用程序（如Tivoli® Storage Manager及其他程序）相辅相成。
- 缩短备份和恢复信息所需的时间。
- 减少所需的物理存储设备的数目，进而有助于降低成本和减少能耗。

散热

散热是目前数据中心能源成本的重要组成部分。使用IBM RearDoor Heat eXchanger等技术，IBM可以帮助您降低相关成本。

eXchanger是水冷热交换机门，用于在计算机系统后部所产生的热量进入室内以前排除这些热量。它适用于服务器和存储设备。eXchanger降低了数据中心的热量负载，并且有助于避免出现热点。

环保转折点

鉴于IT必须处理和存储的信息量每18个月增加一倍，IT主管和管理人员正面临着这样一种不断变化的新情况：对数据中心进行革命性变革，或者承担能源开支超支且无法满足业务需求的风险。

基于对目前能源挑战的深刻理解，IBM提供的解决方案和服务在深度和广度方面使企业能够以可度量方式帮助降低能耗和对环境的影响程度，而不会使服务级别受到损害。借助一系列综合性环保服务管理解决方案，IBM提供了相关技术和专业知识，为了对能源管理予以一定程度的关注，这些技术和专业知识是必需的。

IBM提供了相关解决方案、服务，并提供了可能相对更重要的相关策略，这些产品和服务有助于优化数据中心空间、电力、散热和灵活性，其结果超乎客户的期望，同时还可以降低成本并支持业务增长。

选择的有助于构建更环保的数据中心的IBM节能技术

IBM 解决方案	业务优势
IBM System Storage SAN 卷控制器	• 启用能有效利用空间的虚拟磁盘存储（"自动精简配置"） • 旨在提高存储利用率，进而帮助减少能源的使用 • 允许不间断地迁移数据，以便更方便快捷地实现更节能的存储 • 旨在简化分层存储的部署并提高存储性能 • 提供能有效利用空间的 IBM FlashCopy ? 快照功能
IBM TS7500 和 TS7700 磁带虚拟引擎	• 提高操作简便性和能效的级别 • 简化备份和恢复过程 • 管理数据增长和成本 • 启用虚拟化物理磁带资源以帮助提高能效 • 为"磁带"归档或者需要实时访问数据的情况提供低成本的存储选件
ProtecTIER 重复数据删除解决方案	• 最大程度地提高在线性能、伸缩性和数据完整性 • 扩展现有备份和恢复应用程序 • 减少备份和恢复窗口 • 降低存储要求并减少相关能耗
IBM System Storage 磁带	• 每千兆字节具有最低的能源成本，与旋转磁盘相比需要较少的电力和散热 • 提供完全自动化的库，用于在能源成本较低的非峰值时间内执行备份操作 • 为长期数据归档或者不需要实时访问数据的情况提供最低成本的存储选件
IBM System Storage DS8000	• 旨在提供存储效率和利用率 • 提供能有效利用空间的复制服务 • 具有可选的容量优化驱动器 • 采用新型串行先进技术连接 （SATA） 和光纤先进技术连接 （FATA） 驱动器，其运行速度仅为 7200 RPM ，同 10 K 或 15 K RPM 性能优化光纤通道驱动器相比，新型驱动器消耗的能源较少
IBM TotalStorage? Productivity Center	• 有助于减少浪费的磁盘空间 • 利用 Storage Resource Manager 工具高效使用存储空间 • 识别可被删除的数据，以便在现有存储上创建空间 • 识别可移至更能高效利用能源的存储的数据 • 能够启动自动化任务以释放空间
IBM System Storage DR500	• 提供高效的创新性信息保留平台，从而管理增长、降低风险并支持符合法规要求 • 提供运营效率 • 保护长期保留且符合法规要求的业务信息
IBM 企业模块数据中心	• 能够支持高达 12x 的电力和散热能力增长 • 使企业能够在需要所需能力之前延迟高达 40% 的资产成本以及高达 50% 的运营成本 • 与现有数据中心相比，可以节约多至 50% 的能源 • 为 OEM 创新提供开放式架构

IBM企业信息架构—法规遵从方案群组

Information Infrastructure Solution

领驭信息架构 创新存储时代

IBM System Storage DR550: 帮助金融服务行业满足法规合规要求

信息增长和法规合规的交叉点

为了在全球合法开展业务，公司需要满足超过1万个规章制度的规定。由于全球经济波动多数都围绕着一个明确的货币系统，因此，这些法规中很多都适用于金融服务业。金融服务机构(如证券公司、个人和企业租赁公司及保险公司等)都受到多个法规的约束。

在当今商业环境中开展业务时，金融服务机构必须考虑与银行合并、什么记录必须严格建立，数量以及抵押贷款保证金等相关的法律。此外，许多金融机构都涉足多个银行业领域，因此，他们的法规合规面临独特挑战。美国证券交易委员会、金融业监管局和美国律师总署等机构的成立都是为了保护并执行规章制度(这些只是美国的联邦机构证券/监管机构)。金融机构如出现违规行为将付出惨重代价—从高额罚款到丧失经纪资格。

值得庆幸的是，大多数金融服务公司(与规模或收入无关)都通过某些类型的业务流程来帮助满足所有这些规则的要求。遗憾的是，这些规章制度很少附带说明，使法规合规官员很难：1)解释规则；2)决定用于满足规则的最佳业务流程和支持技术。因此，金融服务公司在法规合规投入上面很容易出现尺度拿捏不准的问题。

管理机关开展审计时常涉及到信息收集、访谈和业务流程审核等工作。此外，由于金融服务公司所从事的工作很容易引起法律诉讼，如租赁及股票保险，因此，公司必须遵从不同政策的几率非常高。例如，美国联邦民事诉讼规则(FRCP)规定了民事案件必须遵从的步骤，包括案件提审和取证过程。这意味着金融服务公司的法律顾问必须满足更多规章制度的要求，包括在取证期间管理电子形式保留的信息。

数字信息量不断增长使金融服务机构面临全新法规合规问题。用户对在线交易网站、电子贷款申请和客户电子邮件的日益使用创建了更多需要处理、保留和管理的数字内容。IT部门必须确保系统能够运行可创收的应用、促进与法规合规相关的业务流程，并满足不断增长的数据需求。

由于与商业记录的创建、保留和保护相关的规章制度数量太多，因此，信息存储解决方案经常是法规合规官员、公司法律顾问首先关注的、希望藉此提高法规合规流程。现在有许多金融服务记录都是数字内容，例如，公司与经纪业务客户之间的电子邮件往来或影像检查等。因此，公司可更新基于纸张的现有记录管理程序来捕获并打印这些记录或者实施可扩展的在线存储系统通过电子方式保留信息。IBM System Storage DR550是将磁盘和磁带集成到单一归档库中的唯一产品——意味着其能够通过成本效率的方式大幅度扩展。金融服务公司可将数据在线保留更长时间，以便满足审计或取证要求时节省大量时间。

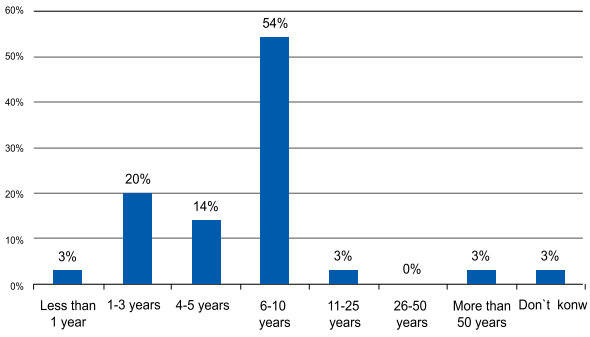
IBM DR550提供许多功能来帮助金融服务公司立刻解决与法规合规相关的问题，例如在单一系统中同时支持磁盘、磁带和光盘存储。本文将介绍与金融服务业相关的某些主要的国际法规、金融服务机构面临的挑战以及如何通过实施IBM DR550系统来即刻满足法规合规和业务流程要求。

金融服务行业的规章制度

从存储的角度简化规则

尽管法律条目和执行机构非常多，且稍有不慎就面临处罚的风险，但通过实施适当的存储系统来改进整个法规合规流程是相对简单的工作，原因有二。第一，大多数规章制度都要求金融服务机构创建商业记录作为审计跟踪依据。商业记录可包括证券交易确认函、购车贷款申请、经纪人与客户之间的往来电子邮件或储蓄账户提款活动等信息。对于这些商业记录，法律明文规定了哪些实体必须遵从哪些特殊规则。第二，规章制度规定特定记录必须保留的时间。某些情况下，保留期可能是6个月，有时也可能长达30年—美国住房贷款的常用年限。金融服务记录一般保留6-10年，如图1所示。

图1. 金融服务机构归档内容的平均保留年限



如果金融服务公司没有适当的归档战略以及支持实施战略的存储解决方案，那么，创建并长时间保留大量信息的成本极高。50%的金融服务公司归档数据主要是为了满足法规合规要求。存储系统能够大幅度扩展，并帮助保留信息来降低法规合规总成本，并提高效力。1

SEC Rule 17a-4及此后的规则

大多数与金融服务公司相关的记录法规多明文规定了为什么需要创建商业记录、商业记录必须保留的时间，还规定了记录的保留格式。由于许多规章制度都不会告诉公司如何去遵从它们，因此这种情况实属罕见。一般的规则都只是简单地指出公司必须满足的要求—允许公司采用多种方法和流程去确保法规合规。

17CFR Sec. 240.17a-4，俗称SEC Rule 17a-4，是附带说明的唯一记录保留法案。总之，这个法案明文规定经纪人/代理人必须将某些商业记录保留在不可擦除、不可重复写的存储介质中，并且对什么是不可擦除、不可重复写的介质，提供了SEC给出的多个解释，还解释了哪些类型的磁带、光盘和磁盘系统能够满足这个要求，指出您也可通过软硬件组合来满足这个要求。不可擦除、不可重复写的格式可帮助确保商业记录的完整性/真实性。此外，法案还规定经纪人/代理人必须将商业记录和记录索引的拷贝保留在单独位置(关于SEC Rule 17a-4的具体说明，请见附录A)。

SEC和NASD有着不同的记录和记账要求，但这些要求都满足SEC 17a-4法案对于数据保留方法的规定。1940年投资顾问法案、1940年投资公司法案和住房抵押贷款披露法案所规定的记录创建和保留要求都适用于各种类型的金融服务公司(图2)。这些法案都不要求通过任何特殊格式保留记录。

图2. 投资顾问法案和投资公司法案节选

规章制度	相关章节的标题/说明
17CFRSec. 275.204-2 (1940年投资顾问法案)[2]	账本和记录均有投资顾问保留。
17CFR Sec. 270.31 a-1- 3 (1940年投资公司法案)[3]	1. 记录由注册投资公司、多数股东所拥有的附属公司或者与注册投资公司有交易往来的其他人员负责维护。 2. 记录由注册投资公司、多数股东所拥有的附属公司或者与注册投资公司有交易往来的其他人员负责保留。 3. 记录由全球维护和保留记录的请求人以外的其他人员负责准备或维护。
12 CFR Sec. 203.4 (住房贷款披露法案)[4]	汇编贷款数据。 • (a) 数据格式和逐条记录。金融机构每个日历年都应收集与住房贷款申请、申请人、购房、家用购房贷款、装修贷款和重新募集资金相关的数据。金融机构应根据预审计划的规定收集申请数据(见Sec. 203.2(b))，前提是预审申请被拒绝或者发放了住房贷款。所有可报告的交易都应在交易完成当季结束后30天内记录在案(如购房贷款申请人或购房以及申请的拒绝或撤销等)，格式应满足附录A中的规定。

美国信用合作社管理局等多个其他规则均对小型金融服务公司具有约束力(图3)。许多小公司都熟知这些规则，知道‘记录’现在还包括客户往来电子邮件、在线表单和其他数字内容(附录A列出了与金融服务公司相关的更多规章制度)。

图3. 美国信用合作社管理局颁布的法规节选

规章制度	相关章节的标题/说明
12CFRSec. 749.1-5	1. 什么是关键记录？ 2. 信用合作社如何处理这些关键记录？ 3. 什么是关键记录中心？ 4. 信用合作社使用什么格式来保留记录？信用合作社可将记录保留在允许重新构建记录的任何格式中，包括纸张原始文件、机器拷贝、微缩胶片或底片、磁带、或能够准确体现记录中所含信息的任何电子格式，这些记录必须可供根据法律、法规或规则要求拥有访问权的所有用户进行察看，并且应该允许复制用于传输和打印等目的。 5. 信用合作社应使用什么格式来维护其他NCUA制度所要求的书面资料、记录或信息？ 6. NCUA不建议使用特殊格式来保留记录。如果信用合作社将记录保存在微缩胶片或电子格式中，被保存的记录必须是准确的、可复写的、可供NCUA检查人员察看的。如果将记录保留在信用合作社位置，应允许检查人员随时访问察看；如果记录保留在第三方或场外，则应在检查人员提出申请后在合理时间将这些记录提供给他们进行察看。信用合作社必须维护必要的设备或软件以便允许检查人员根据申请审核并复制记录。信用合作社还应确保复制品可作为法律诉讼时的合法证据被法院采用。

在英国，金融服务局负责管理所有的银行业和保险活动。根据FSA手册，不同的金融服务公司应根据多个记录保留规定维护记录。图4举例说明了这些规则。总之，记录保留规则涉及到从账户申请到广告计划的所有信息，保留期通常是1-6年。

图4. 英国金融服务局(FSA)规章制度节选

规章制度6	相关章节的标题/说明
MCOB2.8 抵押贷款和住房贷款的记录保留：企业原始资料规范	• MCOB 2.8具体说明了公司根据MCOB要求保留足够记录以确保法规合规的行为标准。MCOB Sch 1中概述了MCOB的记录保留要求。 • MCOB要求记录必须随时可供FSA访问以便开展检查工作。 • 公司接到要求后必须在两个工作日内提供可访问的记录以供检查。 (1) 公司可将记录保存在自己选择的格式中，但必须确保记录可供FSA访问。 (2) 如果公司选择通过电子格式保存记录，应采取合理的措施来确保： • (a) 电子技术能够准确反应原始信息； (b) 电子记录不会被有意或无意更改。 • MCOB与记录相关的所有规则都包含记录保留期要求。虽然MCOB没有硬性规定，但公司应选择延长记录保留时间，以便用于解决客户投诉或法律诉讼等问题。
MCOB Sch 1记录举例说明7 MCOB 4.7.17R(1)(a)	具体的客户信息，包括客户需求和环境，用于评估抵押贷款合同的合理性(3年保留期)
MCOB Sch 1记录举例说明8 MCOB11.3.1R(2)	证明公司在发放贷款时已经考虑到客户还款能力的证据(抵押贷款)。(保留期：自抵押贷款合同生效之日起一年或者提前达成协议)

在日本，金融服务机构必须遵从金融商品交易法(由于类似于美国的Sarbanes-Oxley，因此常被称为J-SOX)。上面我们提到的国际记录保留制度并不是跨国公司开展业务时所需遵从的唯一法律，因为任何国家的中央银行、经纪公司和资本市场体系都制订了相应的法律来管理这些实体的运营。如果这些银行在美国开展业务，则必须遵从SEC制订的规则。因此，SEC规则被广大经纪人/代理人所熟知。对于美国银行。他们还必须遵从FSA和其他管理机构发布的规则。

迁移到电子记录管理、保留和存储环境中

将几千页纸的规章制度浓缩成几页纸的通用总结对于提高法规合规能力看似帮助不大，但是，公司可通过将精力集中在一部分IT基础设施领域来提高法规合规能力。从存储的角度研究对金融服务业有影响的规章制度，不难看出商业记录必须保持一段时间。随着电子商务、供应链和其他应用创建了越来越多的数字形式的记录，金融服务公司必须决定如何保留它们来满足法规合规要求。在股票交易靠填表来完成或者客户必须返回银行填写存款单的时代，基于纸张的记录管理是可行的。时过境迁，现在的金融服务公司不再使用基于纸张的流程来保留IT系统创建的记录。通过归档软软件和硬件实现电子记录管理程序半自动化，允许金融服务公司轻松获取特定记录，规定保留期并自动执行任务。

现在，许多金融服务公司都使用备份磁带来满足记录保留规定。磁带介质以电子格式保留商业记录，对于SEC特定的规章制度来说，一次写入多次读取(WORM)的磁带格式可用于防止所有的篡改或删除操作。磁带的缺点在于写入磁带的数据不保存在标准格式中，意味着您在访问数据之前必须先恢复它们。当公司需要持续搜索和使用记录时，由于磁带需要先恢复再访问，而磁盘系统的检索速度较快，因此，磁盘是更好的选择。

各公司为满足审计要求而处理商业记录的要求各异。小型社区银行可能永远不会被审计；证券公司和投资银行可能必须证明自己每年多次备份商业记录。将信息保存在磁盘系统上将提高记录的可访问性— 促进加速响应审计要求。

虽然磁盘是用于保存最新记录来满足审计要求的理想选择，但将多年的数据保存在磁盘上代价很高。金融服务机构可选择将陈旧的商业记录转移到磁带甚至光盘上以降低采购和运行成本。因此，结合了磁盘和磁带的归档策略才是金融服务公司满足多个规章制度要求、长时间保留记录、并定期出示记录来满足审计要求的理想选择。

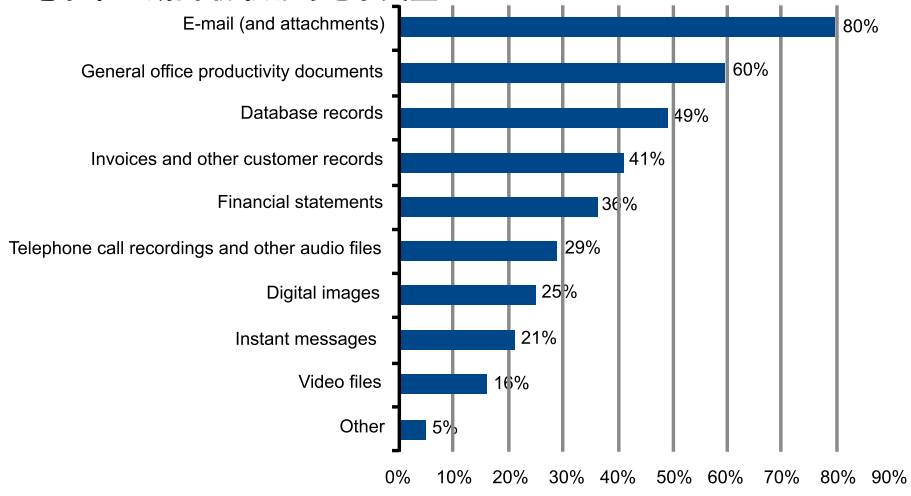
电子取证提高了法规合规要求

不仅关乎时间，还关乎数量

虽然原因在变，但金融服务机构易于卷入诉讼风波的严酷事实却始终不变(现在的罪魁祸首是不负责任的贷款控制；过去则是松懈的经纪人/代理人控制)。因此，金融机构需要设法找到并保留可能成为电子取证要求的任何及全部信息，包括电子邮件、贷款申请、客户报告及电报往来等。虽然大多数此类信息都是通过电子格式生成和保留的，但只占金融机构全部数据中的一小部分。

由于计算机系统日益应用到日常商务活动中，立法机构和管理机构在诉讼期间将目标集中在通讯应用、数据库记录和其他来源的电子证据上(图4)。其中某些取证是在审计期间开展的，有些则是在民事案件后提交后进行的。无论什么原因，金融服务公司的法律顾问都会迅速成为IT高手，以便得心应手地处理法律诉讼流程。

图5. 电子取证期间最常用的记录类型



做好持久战的准备

无论是大型证券公司还是小型社区银行，任何金融服务公司都必须准备好以满足电子取证要求。查找数据只是金融公司在电子取证期间必须满足的诸多要求之一。一旦发现可能的证据来源—包括备份磁带和PC上的文件—金融公司必须长期保留数据，直到诉讼或审计工作完成为止。保留证据可帮助确保数据完整性，但许多公司都发现很难将大量数据保留多年不被滥用、篡改或删除。法律诉讼结案可能需要一段时间，尤其是涉及到大量原告或有着重大金融影响的诉讼案件—特别是进一步加剧电子证据保留需求的诉讼。

考虑到记录保留法要求金融公司将这些信息保留多年(抵押贷款最多30年)，再加上数据的持续增加，我们不难想象找到所需的电子证据是多么困难的事情，更不用说长期保留它们了(即确保完整性)。您可阅读2006年12月颁布的以管理电子证据为重点的美国联邦民事诉讼规则增补本来了解详细情况。

通过归档确保法规合规

做出明智投资

为了满足记录保留和电子取证要求，金融公司需要通过不同方式归档信息。由于没有人知道法院何时会取证数据，因此，将所有信息都保存在磁带上不再行得通。但把所有数据都保存在磁盘上也因成本问题而行不通。金融公司在选择归档产品时，应考虑归档解决方案不仅能够满足现在和将来的数据保留、数据真实性和灾难恢复需求，而且还必须足够灵活地支持应用和存储(例如，解决方案可支持电子邮件、数据库和文件等多种类型的应用数据)并能够结合多层存储系统。

IBM帮助金融服务机构解决主要的法规合规问题

经济高效地长期保留大量数据

ESG调查发现，数据库信息年增长率达25%，电子邮件和非结构化数据的增长速度更是高达这个数字的2-3倍。去年，一家大型跨国银行的信息量从1PB增长至2PB。并非所有这些信息都是商业记录，但这个增长率却将受到记录保留制度和电子取证制度约束。再加上平均6-10年的数据保留期，金融公司必须通过新方法来保留所有数据，且不用大幅度增加IT预算。

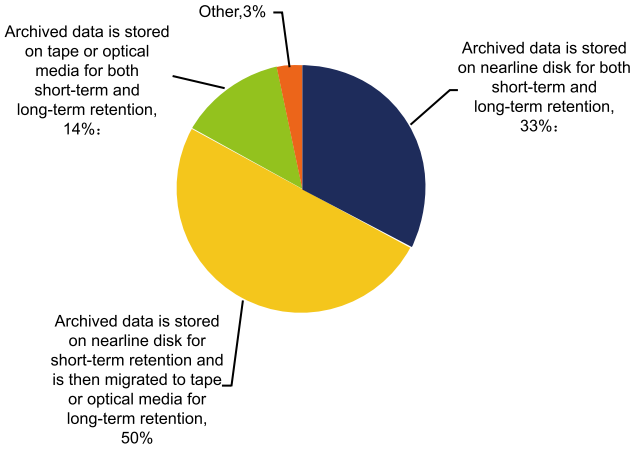
IBM深知金融服务公司规模不同，因此提供两款DR550—具体取决于用户环境的规模。DR550 DR1是单一服务器的单一机柜(25U高)系统，最多提供30TB的可用磁盘容量，专为中小企业而设计，是社区银行、信用合作社或大公司的部门的理想选择。DR550 DR2是企业级解决方案，最适合大型金融机构，可用磁盘容量可从8TB扩展到136.5 TB，允许用户实施两个DR550服务器来实现高可用性。企业版本还提供同步或异步复制选项用于灾难恢复。

设计用于在单一归档系统中支持多层介质是DR550的主要区别因素之一(磁盘、磁带和光盘)。两款机型都支持可选的TS1120 WORM/加密、LTO 3/4 WORM和LTO4加密，可帮助降低归档成本(根据实际情况选择保存数据的介质)并允许金融公司将归档的容量扩展到PB级。数据迁移自动完成，基于策略或基于事件。一般情况下，公司可将陈旧的或者不经常使用的数据迁移到磁带中。迁移工作由DR500中的System Storage Archive Manager(SSAM)负责。

对于金融服务公司来说，同时基于磁盘和磁带保存数据的可扩展性和灵活性，允许公司法律顾问告诉IT法律取证时可能用到哪些数据，从而确保此类数据随时可供访问。对于抵押贷款申请等商业记录，使用磁带长期保留可更为经济高效。总之，结合使用磁盘和磁带是金融服务公司归档数据时最常用的存储基础设施(图5)。

图6. 金融服务机构使用的归档存储基础设施

金融服务机构现在使用的归档存储基础设施（回答人百分比，N=36）



来源：ESG调查报告：Electronic Discovery Requirements Escalate, 2007

集中保留商业记录以便实施一致的管理

商业记录可能包括电子商务、即时消息传递和其他应用生成的电子邮件、数据库数据和文件。所有这些数据都必须是准确无误的，因为您不知道调查人员会调查哪些来源的数据。尝试为每个应用部署特定的档案存储系统将给IT带来沉重负担。IBM DR550为所有这些类型的数据创建了集中的多层档案库，从而简化了这个流程。并且，数据迁移由DR550的SSAM自动执行和管理。

SSAM API与超过40个归档和内容管理应用相集成。记录的保留期由档案应用决定，由DR550负责执行。这个系统还提供网关功能，允许用户将NFS和CIFS文件放到档案库中并使用SSAM为数据分配保留策略，同时基于策略或特定事件在归档介质之间自动迁移数据。

记录的保留和安全性

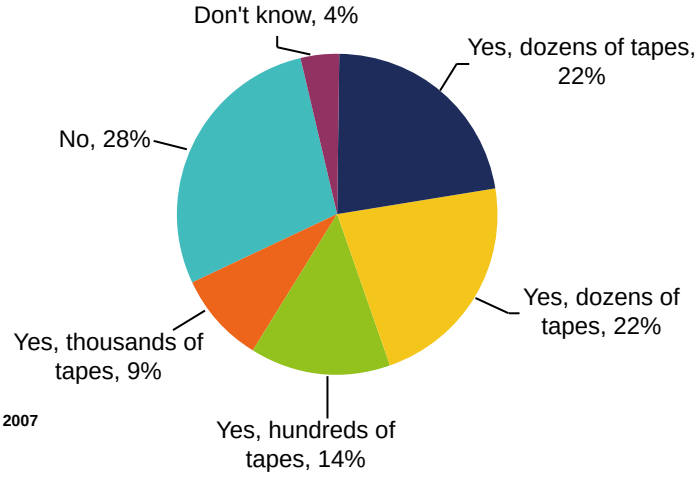
将记录归档与数据保留完全是两码事。自动执行这两项任务对于金融机构来说至关重要。鉴于金融服务公司需要保留大量数据，因此，必须自动保护关键业务数据。

DR550提供自动WORM功能，适用于所有存储层(磁盘、磁带和光盘)。一旦数据被写入DR550，在到期前便不能被篡改或删除。这意味着终生保护记录，更重要的是，数据能够在DR550多个层次之间迁移。金融机构可通过DR550设定记录保留策略，或者直接从数据库、电子邮件或归档应用设定记录保留策略。此外，DR550还支持基于WORM的磁带库或驱动器以满足SEC 17a4的要求。

由于磁带是保存IT数据的主要存储库，因此，许多金融公司都利用磁带来依法整合信息(图6)。DR550为金融服务客户提供选择性，可将电子证据保存在磁盘及/或磁带上，这对公司法律顾问与IT部门合作，在信息存储成本与可访问性要求之间找到最佳均衡点、然后选择适当的DR550产品至关重要。

图7. 许多公司都将依法将信息保存在磁带上

据您所知，您的公司是否因为法律或规章制度不明确而不敢确定到底需要保存哪些备份磁带？(回答人百分比,N = 107)



来源：ESG调查报告：Electronic Discovery Requirements Escalate, 2007

DR550还支持内置加密功能，允许金融服务机构通过在磁带上加密数据以保护运输到离线站点的记录。远程磁带存储(如同基于磁盘的复制一样)可满足SEC Rule 17a-4的一个要求，但客户可能还需要为灾难恢复目的而运输磁带。为了防止非法访问，包含账户或信用卡数据等敏感信息的磁带必须加密。

保护公司档案

DR550集成了介质管理功能，作用不仅局限于归档。您可使用SSAM从DR550直接将数据备份到磁带，这一点非常重要，因为：1) 允许用户轻松保护档案；2)无需更多的备份软件，因此具有经济高效性。对于业务连续性，DR2 (企业级机型)提供可选的同步或异步归档数据镜像功能，能够进一步保护用户最关键的归档数据。在这里，镜像也是通过DR550内置软件完成的。

大多数金融服务公司都必须公布业务连续性计划来证明自己遵守规章制度。通过在离线站点同步或异步复制数据，DR550帮助金融机构确保不会因灾难而丢失关键记录，从而满足业务连续性计划中的关键要求。

结语

记录保留制度可追溯到20世纪初期，但是，就像SEC规则一样，现在的记录包括电子邮件和其他数字文件等多种新形式。针对电子证据管理而制订的全新美国FRCP法案也是金融服务机构必须遵从的规章制度。遗憾的是，无论规模大小，金融服务公司都必须设法确保通过经济高效的、有助于提高运行效率的方式满足所有这些规则的要求。

试图寻找万能的法规合规解决方案是不切合实际的做法。与其耽误时间，您不如去投资能够提供所需功能来帮助您迎接法规合规挑战并且能够兼容现有IT基础设施的解决方案。您可将存储环境作为切入点，因为许多规则都要求创建数据并将数据保留一定的时间。随着数字化数据越来越多，记录保留流程也必须同步演进，从文件箱迁移到磁盘和磁带等更容易查找和访问的存储介质中。

无论是远程复制、设置和强制保留期限，还是构建经济高效的档案库并确保数据的终生完整性，DR550都提供丰富的功能来帮助金融服务公司迎接法规合规挑战。从法规合规的角度看，DR550并不是帮助金融服务公司解决全部问题的万能解决方案，但它的确能够凭借卓越的可扩展性和配置灵活性来帮助公司满足记录保留和取证要求，允许公司通过经济高效的方式更长时间地保留更多信息。

附录A -举例说明金融服务行业的记录保留制度

下面的表格描述了金融服务机构必须遵从的部分规章制度，具体取决于他们现在所属的业务领域。

1934年证券交易法案 - Rule 17a

规章制度9	相关章节的标题/说明
17CFRSec. 240.17a-1	面向全国证券交易所、证券联合会、注册清算代办处和市级证券规则制订委员会的记录保留规则。
17CFRSec. 240.17a-2	与稳定化活动相关的记录保留要求
17CFRSec. 240.17a-3	特定交易人、经纪人和代理人的记录创建要求。
17CFRSec. 240.17a-4	特定交易人、经纪人和代理人的记录保留要求。 第(f)段： 根据Sec. 240.17a-3和240.17a-4要求进行维护和保留的记录应立刻在“显微照片介质”上面(定义见本节)或者通过“电子存储介质”(定义见本节)创建或复制，以满足本段提出的要求并以适当格式在规定时段内维护并保留记录。 (1)对本节来说： (i) 术语显微照片介质是指微缩胶片或者类似介质； (ii)术语电子存储介质是指根据本节第(f)(1)(i)和(f)(1)(ii)段的规定，满足(f)段条件要求的任何数字存储介质或系统。 (2)如果电子存储介质由交易人、经纪人和代理人使用，应满足以下要求： (i) 交易人、经纪人和代理人在使用电子存储介质前必须根据法案17(d)节的规定(15 U.S.C. 7 8q(d))，通知法案指定的权威监管部门。如果是使用除光盘技术外的任何其他电子存储介质(包括CD-ROM)，交易人、经纪人和代理人都必须至少提前90天通知指定的权威监管部门。无论在任何情况下，交易人、经纪人和代理人都必须提供自己的演示文稿或者存储介质供应商或其他合格第三方的演示文稿来证明所选的存储介质满足(f)(2)的要求。 (ii) 电子存储介质必须能够： (A)只将记录保存在不可擦除、不可重复写的格式中； (B)自动验证存储介质记录流程的质量和准确性； (C)给原始记录排序，如果适用的话，还能复制存储介质的单元并提供此类电子存储介质上对信息的保留期信息。 (D)提供足够的容量，允许根据证券交易委员会或交易人、经纪人和代理人所属自管理机构的要求，将电子存储介质上保存的索引和记录轻松下载到(f)段允许的任何介质中。

接上表

规章制度[9]	相关章节的标题/说明
17CFRSec. 240.17a-4	(3)如果交易人、经纪人和代理人使用显微胶片介质或电子存储介质，请注意： (i)所有记录必须可供证券交易委员会或交易人、经纪人和代理人所属自管理机构的工作人员随时轻松访问，以便轻松制作可读取的放映片、显微胶片或电子存储介质图像以及可轻松读取的图像。 (ii)所有记录都可随时提供并允许放大传真件，以便证券交易委员会以及交易人、经纪人和代理人所属自管理机构的工作人员、或者对交易人、经纪人和代理人拥有司法权的任何州级证券机构根据需要进行察看。 (iii) 只要不是原始文件所在的位置，交易人、经纪人和代理人可将记录的拷贝保留在满足Sec. 240.17a-4规定的任何介质上并满足保留期要求。 (iv)组织原始信息和存储介质上复制的信息并准确编制索引。 (A)无论任何时候，交易人、经纪人和代理人都必须能够将此类索引提供给证券交易委员会或交易人、经纪人和代理人所属自管理机构的工作人员进行检查。 (B)每个索引都必须复制且复制的拷贝必须保存在远离原始拷贝的位置。 (C)原始的和复制的索引必须根据被编成索引的记录的要求保留一定时间。 (v)交易人、经纪人和代理人必须根据Sec. Sec. 240.17a-3和240.17a-4的规定运行审计系统，以确保为维护和保存而输入到电子存储介质的数据的可察性以及对这些被维护和保留的任何原始和复制记录所做的任何修改的可察性。 (A)无论任何时候，交易人、经纪人和代理人都必须能够将此类审计系统提供给证券交易委员会或交易人、经纪人和代理人所属自管理机构的工作人员进行检查。 (B)审计结果必须根据审计记录的要求保留一段时间。 (vi)交易人、经纪人和代理人必须维护、更新并根据证券交易委员会或交易人、经纪人和代理人所属自管理机构的工作人员及时提供全部所需信息以便他们访问保存在电子存储介质中的记录和索引；将电子存储介质的物理和逻辑格式保存在由第三者保存附带条件委付盖印的契约中并保持副本的时新性；将所有不同类型的信息的字段格式写在电子存储介质和源代码中；并提供相应的文档和信息以便支持访问记录和索引。 (vii)对于根据本节要求只使用电子存储介质保存部分或全部记录的每名交易人、经纪人和代理人，至少需要一名能够访问交易人、经纪人和代理人的电子存储介质并将信息下载到符合本节规定的任何介质上的第三方("请签名")向交易人、经纪人和代理人所属检查权威机构提交文件，对此类记录做出如下承诺。

NYSE和NASD与SEC Rule 17a-3&4相一致的记录保留规则

NYSE规章制度[10]	章节标题
Rule 410	记录的排列顺序
Rule 123	记录的排列顺序
Rule 440	账本和记录

NASD规章制度[11]	章节标题
Rule 3110	账本和记录

银行保密法案 / 反洗钱法案

规章制度[12]	章节标题
31 CFR Sec. 103.32-38	记录由在国外金融账户上拥有金融权益的个人创建和维护 记录由金融机构创建和维护 由银行创建和维护更多记录 由证券公司经纪人或代理人创建和维护更多记录 由货币代理人或交易人创建和维护更多记录 记录的性质和保留期

面向国有证券公司经纪人和代理人的记录创建和维护制度

规章制度[13]	章节标题
17CFRSec. 404.2-4	2.记录由注册的国有证券公司的经纪人和代理人创建和维护；非常驻的国有证券公司经纪人和代理人的记录。 3.记录由注册的国有证券公司的经纪人和代理人保留 4.R记录由国有证券公司的身份是金融机构的经纪人和代理人保留

面向国家银行的记录保留规则

规章制度[14]	相关章节的标题/说明
12CFRSec. Sec. 12.3	记录保留。 通用规则。影响客户准确交易的国家银行至少应将下面的记录保留三年： (1) 序时记录。按时间先后顺序排列的带编号的日证券交易记录，包括： (i) 每次交易涉及到的账户或客户名； (ii) 证券说明； (iii) 买卖价格的单位和总计； (iv) 交易时间； (v) 参与证券买卖的经纪人/交易人或其他人员的姓名或其他标记； (2) 账户记录。每名客户的账户记录，体现了： (i) 证券的买卖； (ii) 证券的接收和交付； (iii) 现金收入和支出； (iv) 与证券交易相关的其他借记和信贷记录； (3) 买卖契约书的顺序。每个证券买卖订单的单独的契约书(订单票据)(无论交易是被执行还是被取消)，包括： (i) 交易涉及到的账户或客户名； (ii) 订单类型(市场订单、限价订单或特殊订单)； (iii) 交易人或负责交易的其他银行员工接收订单的时间； (iv)交易人向经纪人/代理人发单的时间；如果在经纪人/代理人不存在的情况下，订单的执行或取消时间； (v) 订单执行价格； (vi) 相关经纪人/代理人姓名； (4) 经纪人/代理人的记录。被银行指定参与证券交易的所有经纪人/代理人的记录，提成金额，或者每名经纪人在当前日历年的分红； (5) 通知。根据Sec. Sec. 12.4和12.5. (b)规定的维护方法所提供的书面通知的拷贝。根据本节要求，记录必须能够清晰准确地提供所需信息，以便满足审计要求。记录维护措施可能包括使用自动或电子记录，前提是记录必须支持检查人员轻松检索和访问并允许轻松复制到硬拷贝上。

英国金融服务局的记录保留规则及定义摘录

术语	定义
MiFID	欧洲议会和理事会金融工具市场指令
MiFID制度	遵从欧洲议会和理事会2004/39/EC指令的佣金制度，规定了投资银行的组织要求和营业调节并为遵从这个指令规定了条款
MiFID投资公司	适用于MiFID的公司，包括满足以下条件的信贷机构和UCITS投资公司 1. 总部设在EEA的投资公司(或者在EEA设立了注册办公室的投资公司) 2. BCD信贷机构(只限提供投资服务或根据MiFID Article 1(2)的规定开展相关活动的机构) 3. UCITS投资公司(只限根据UCITS指令Article 5(3)及MiFID Article 5(4)提供相关服务的公司)；除去根据MiFID Article 2 (例外)或Article 3 (可选例外)享有豁免权的公司

规章制度15	相关章节的标题/说明
高级管理活动、系统和控制 SYSC 9.1.x	通用记录保留要求 1. 公司必须安排有序地保留商业和内部组织记录，包括相关的所有服务和交易，记录必须足够充分以便满足FSA或任何其他相关权威机构根据MiFID监视公司法规合规情况的要求，尤其是用于证明公司对客户已经履行了所有的法规合规义务。 2. 公司必须根据MiFID的要求将所有商业记录至少保留五年时间。 3. 对于MiFID，通用平台公司用于保留记录的介质必须允许FSA或任何其他相关权威机构随后更据MiFID轻松访问信息，因此必须满足下面的条件： (1)FSA或任何其他相关权威机构必须能够根据MiFID轻松访问记录并重新构建交易处理过程中的每个主要阶段； (2)支持任何纠错或其他补遗活动，开展此类纠错或其他补遗活动之前允许轻松访问记录内容； (3)否则绝不允许使用或更改记录。 4. 记录保留指导原则。记录保留应遵循手册中的全部指导原则，应允许以英文的形式复制在纸张上。如果公司被要求保留非英文的通信记录，应满足要求。然而，公司应能够根据要求提供翻译支持。如果公司将商业记录转移到英国以外的国家或地区，应使用这些国家或地区的正式语言而不是英语。 5. 对于非MiFID商业记录的保留，公司应运行适当的系统和控制机制来确保记录的可访问性和安全性，以便满足规章制度和法律法规的要求。关于保留期，通用原则是只要记录有用就应一直保留它们。 6. 手册在每个模块的Schedule 1中都提供了这个模块的记录保留要求的汇总信息。 7. 欧洲证券监管委员会(CESR)已在MiFID实施指令Article 51(3)中针对最少记录数量提供了建议，请参见：http://www.fsa.gov.uk/pubs/other/CESR_Minimum_List_Recommendations.pdf

FSA的记录保留规则及保留期制度摘录

规章制度	记录及其保留期的举例说明
高级管理活动、系统和控制- SYSC Sch 116	提供足够的会计和其他记录以便公司能够向FSA证明： (1) 公司在经济上是健全的，并实施了适当的系统和控制措施； (2) 公司的经济地位和风险暴露级别(确保准确性)； (3) 公司满足GENPRU、INSPRU和SYSC的要求(将记录保留3年或更长时间)。
客户资产 - CASS Sch 1.317	公司代替客户保管或接收的或者公司安排其他公司代替客户保管或接收的客户财产(3年)。
集体投资计划- COLL Sch 118	会议纪要(6年)。
商业经营最新规范-COBS Sch 119	关于公司、服务和信息的信息(5年)。
银行、建房互助协会和投资公司之谨慎规范- BIPRU Sch 120	法律审核记录，向所有相关的权威机构证明公司信贷保护措施的可执行性(根据需要进行审核)。
保险公司之谨慎规范 -INSPRUSch 121	与公司每笔长期保险基金相关的单独的会计记录(未规定)。
电子货币- ELM Sch 1	证明公司不再与某人存在密切关系的记录(在公司停止使用ELM 3.5.10 R后保留3年)。
培训和能力- TC Sch 1	公司必须制作适当记录来证明遵从这个规范中的规则并在员工停止活动后将这些记录保留一段时间： (1) 对于MiFID商业记录至少保留5年； (2) 对于非MiFID商业记录至少保留3年； (3) 养老金转移专家的记录年限不确定。

附录B – 保险行业的法规合规

美国提供多种形式的保险服务：健康、汽车、人寿、残疾等。许多保险公司还在资产管理等其他金融服务领域开展业务。因此，保险经纪人和承保人所必须满足的制度要求许多都与银行相同。例如，保险公司必须满足个人声明制度的规定。此外，他们还必须遵从HIPAA (医疗保健)等行业特定的规则。毫无疑问，保险公司将大量资源用在了法规合规上。

虽然保险公司表面上与证券公司及其他金融服务公司有所区别，但是，对于规章制度和存储要求，他们适用的规则非常相似。保险公司必须将特定记录保留一定时间，因为政府经常需要审计这些记录，或者这些记录经常因保单持有人修改了保险范围而需要进行修改。保险公司的记录创建和保留制度如此复杂是这个行业的供应链所致。在每个保险子领域，都会有经纪人、代理人、承保人、处理人/清算所和其他各方参与‘纸张工作’流程。

无论保险公司在特殊流程中扮演怎样的角色，都必须保留与理赔、支付和保险费相关的信息。并且必须允许多个不同群体在整个流程中轻松访问这些信息。许多情况下，此类数据都必须在审计或电子取证期间出示，这是因为保险公司经常会牵扯到法律诉讼中。因此，保险公司必须根据要求长期保留证据。

任何保险公司都能受益于IBM System Storage DR550。这个系统可扩展到几百兆兆字节的内部磁盘、磁带或光盘存储容量。可扩展性对保险公司来说至关重要，因为现在的理赔工作流中包括汽车事故照片、洪水受灾视频和其他丰富媒体内容。保单和理赔记录可能需要保留多年，具体取决于各州的规定。对于涉足医疗保健行业的保险公司来说，必须根据HIPAA安全规定终身保留病人数据，因此，支持加密功能的DR550是理想选择。

由于参与工作流的其他各方需要轻松访问保险记录，因此，DR550基于SSAM的数据迁移和复制功能可供大型保险公司用于高效地将信息保留到适当位置。

许多保险公司都利用内容管理应用来管理包含记录管理流程的工作流。通过SSAM API，DR550能够与多个内容管理平台进行通信，从而减轻IT部门的工作负担。保险公司可将DR550用作记录管理档案库，不必改造现有流程—这对正在从书面程序向数字记录保留程序迁移的公司来说无疑是巨大优势。

与许多其他公司一样，保险公司也必须遵从记录创建、保留和取证法律。随着丰富媒体和电子表单逐渐被应用到理赔流程中，存储设施将在法规合规方面发挥关键作用。作为预定义的工作流的一部分，信息归档是不可或缺的环节，这个流程现在逐步走向数字化。IBM DR550能够随容量需求的增长而扩展，并且能够转移和拷贝数据，从而允许您轻松访问和保护数据。

注释：

[1] ESG调查报告：2007年电子邮件数据库/文件归档调查，11/2007

[2] http://www.access.gpo.gov/nara/cfr/waisidx_06/17cfr275_06.html

[3] http://www.access.gpo.gov/nara/cfr/waisidx_06/17cfr270_06.html

[4] http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr203_06.html

[5] ' http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr749_06.html

[6] http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr749_06.html

[7] http://fsahandbook.info/FSA/html/handbook/MCOB/Sch1?searchtext=MCOB%20Sch%201&searchtype=boolean

[8] http://fsahandbook.info/FSA/html/handbook/MCOB/Sch1?searchtext=MCOB%20Sch%201&searchtype=boolean

[9] 美国档案记录管理局联邦法典 — http://www.access.qpo.gov/nara/cfr/cfr-table-search.html#paqe1

[10] http://rules.nyse.com/NYSE/

[11] http://www.finra.org/RulesRegulation/FINRARules/index.htm

[12] http://www.access.gpo.gov/nara/cfr/waisidx_07/31cfr103_07.html

[13] http://www.access.gpo.gov/nara/cfr/waisidx_06/17cfr404_06.html

[14] http://www.access.gpo.gov/nara/cfr/waisidx_06/17cfr404_06.html

[15] http://fsahandbook.info/FSA/html/handbook/SYSC/9/1

[16] http://fsahandbook.info/FSA/htm l/hand book/SYSC/Sch/1?searchtext=record%20keeping&searchtype=boolean

[17] http://fsahandbook.info/FSA/html/handbook/CASS/Sch/1?searchtext=record%20keeping&searchtype=boolean

[18] http://fsahandbook.info/FSA/html/handbook/COLL/Sch/1?searchtext=record%20keeping&searchtype=boolean

[19] http://fsahandbook.info/FSA/html/handbook/COBS/Sch/1?searchtext=record%20keeping&searchtype=boolean

[20] http://fsahandbook.info/FSA/html/handbook/BIPRU/Sch/1?searchtext=record%20keeping&searchtype=boolean

[21] http://fsahandbook.info/FSA/html/handbook/INSPRU/Sch/1?searchtext=record%20keeping&searchtype=boolean

[22] http://fsahandbook.info/FSA/htm l/handbook/ELM/Sch/1?searchtext=record%20keeping&searchtype=boolean

[23] http://fsahandbook.info/FSA/html/handbook/TC/Sch/1?searchtext=record%20keeping&searchtype=boolean

20 Asylum Street
Milford, MA 01757
电话: 508-482-0188
传真: 508-482-0218
www.enterprisestrategygroup.com

中等规模企业E-mail归档与合规解决方案

仔细考虑下列e-mail挑战：

- 核心可用性要求
- 为了应对诉讼而延长e-mail保留期限
- 在发送给20个人的e-mail附件中查找文本
- 合规性战略

对那些需要在满足内部用户和外部审计要求的同时对e-mail数量和存储进行控制的中等规模企业来说，面对所有这些挑战，可能令他们感到畏惧。

目前，E-mail是企业实现内外沟通的主要途径。许多客户通过e-mail进行合同和协议谈判和磋商，交换发票和付款信息。e-mail常常是有关重要交易的唯一记录，因此必须对e-mail进行保护和保存。

如果您的e-mail系统变慢甚至出现故障陷入瘫痪，对业务造成的影响是十分严重的，尤其是这种故障造成您的e-mail丢失，而且这些丢失的e-mail包含您在外部审计过程中需要用来证明自己符合相关法规要求的关键信息或附件。

通过传统的备份解决方案在系统出现故障时（例如，磁盘系统故障）对系统进行恢复已经无法适应现在的需求。

比如说，您和您的员工无法在数千封浩如烟海的e-mail中轻松找到有关付款的信息。他们还很可能只在一个地方备份e-mail，因此，如果备份地点发生什么事情的话，就会面临失去已归档的e-mail和文件的风险。

让这些e-mail中的文件和信息能够被内部和外部审计部门用来进行审计或者满足相关法规要求对企业来说是一个巨大的挑战。

e-mail归档和合规解决方案能够帮助您解决这些难题。然而，市场上的解决方案如此之多，以至于企业难以根据自己的环境选择真正适合自己的解决方案。 而且，许多解决方案往往都是面向大型企业而开发的，而不是面向中等规模企业而开发。

来自IBM的e-mail归档和合规解决方案能够帮助中等规模企业以合理的成本解决自己面临的e-mail挑战。

这些解决方案还可以在帮助您满足有关数据保留的法规要求的同时降低数据复杂性以及数据丢失的风险。通过这些解决方案，您可以：

- 在e-mail中查找特定的消息。
- 定义e-mail保留策略，根据内部要求和政府要求e-mail指定不同的保留周期。
- 自动化的数据备份和恢复功能。
- 实现存储的集中管理。

e-mail归档和合规再也不仅仅是可有可无。 它现在是任何业务基础架构和业务连续性战略的一个关键组成部分。因此，它应该满足某些特定的核心要求。e-mail归档解决方案必须能够按照不同的策略存储e-mai正文l以及任何相关的附件（例如Microsoft® Word文档或PowerPoint®演示文稿），而且保留期是不同的。

对这些e-mail进行查找和检索的能力也非常重要。e-mail存档可能在短时间内变得非常大。 您还可能需要在数千封e-mail中查找与某个特定问题有关的一封或两封邮件。您的e-mail归档软件必须能够按照标准文本字段 （例如，发件人、收件人、抄送、秘密抄送、主题和日期）对所有e-mail建立索引。

其它需要考虑的要求是，延长保留期限，控制存储增长，处理个人文件夹，对即时消息进行归档，定制策略，操作系统以及进行更加复杂的查找。 您还需要制定一个能够与您的e-mail归档解决方案整合并对其形成互补的合规战略。

为了帮助类似贵公司这样的企业解决这些挑战，IBM

和我们的业务合作伙伴已经为中等规模企业开发出了e-mail归档解决方案，通过软件、硬件和服务整合起来，满足您包括法规遵从在内的所有需求。

IBM E-mail归档和合规解决方案是一套集服务、硬件和软件于一体的解决方案，其规模和定价都完全面向中等规模企业，满足这类企业的e-mail归档管理需求和相关法规遵从的需求。

它们包括：

- 一个e-mail归档核心组件
- 一个便于e-mail检索的内容管理程序
- 集成e-mail记录管理
- 一个方便审计的数据库的设计
- 多种存储和硬件的选项
- 由了解您的当地市场和您特殊需求的经验丰富的IBM业务合作伙伴提供的增值服务

带给您的好处是：

- 对e-mail归档和内容管理程序组件进行集中管理
- 支持长期信息保留的法律法规和公司标准的合规性要求
- 通过策略驱动的或用户发起的自动化的归档控制企业邮件系统长期数据增长和系统性能
- 在您选择的存储设备上对e-mail进行长期归档并轻松安装到适合自己业务的IBM硬件上。

通过IBM CommonStore让E-mail归档变得轻松简单

IBM e-mail归档解决方案的一个核心组件是IBM CommonStore for Exchange Server/Lotus® Domino®。IBM CommonStore与Microsoft Exchange或IBM Lotus Domino无缝整合，对e-mail正文和相关的附件进行长期的安全的归档保管。 您可以通过邮件中嵌入的链接查看或检索消息并调用相关的附件。

基于规则的归档和保留策略可以帮助您严格遵守相关法律法规等合规性的要求。

您可以制定归档策略，自动将所需的文档拷贝至相应的存储库，削减管理成本。 解决方案中的IBM e-mail查找技术能够让您超越关键词、名称和日期范围，利用短语、布尔表达式、近似、模糊以及通配符进行查找。 在法律发现过程中，这种查找对节省时间来说至关重要。 如果e-mail属于审计或调查的一部分，您还可以暂缓对e-mail的自动删除。

另外一个被称为“单实例存储”的功能可以减少您的存储需求。 如果某封带有很大附件的邮件被发送给很多人，系统会只储存一份拷贝。

所有这一切用户都是透明的，他们可以继续无需培训使用自己的e-mail客户端界面或Web客户端进行邮件的访问。 归档的邮件仍然在收件箱内，用户可以轻松点击这些邮件而“重新找回”它们，无需对它们创建本地拷贝或者为了保持在磁盘占用极限范围内而删除它们。 这样不仅提高了工作效率，而且还降低了成本。

通过IBM Email Management Express为您的e-mail功能提供无间断的保护

IBM Email Management Express能帮助您保持e-mail对用户的连续性，包括那些通过手持设备等无线设备上网的用户。 通过这些服务，您和您的员工可以恢复已删除的e-mail，使用有效的e-mail归档功能，在保持正常业务运作和生产力的同时持续保持与供应商、客户和业务伙伴的沟通，既便在您的主e-mail系统发生故障无法使用时也能保持这种正常的沟通。无需专用的软件或投资，因此，您可以确定哪些服务和功能最适合您特殊的需求、环境和预算。

通过Tivoli Storage Manager保护您已经归档的e-mail

为了保持业务的连续性并遵守相关的法规要求，您必须对关键的e-mail或者与它们有关的数据和文档加强保护，防止丢失。同时，您还希望尽量避免增加对IT资源的投资。

这就是为什么IBM和我们的业务伙伴面向中等规模企业推出将IBM Tivoli® Storage Manager作为e-mail归档解决方案的一部分的原因。

IBM Tivoli Storage Manager提供集中化的自动数据保护功能，可以减少由于数据丢失而带来的风险，同时还可帮助您在遵守相关数据保留合规性的同时降低数据的复杂性、管理成本，解决一致性问题。 这是一个用来对您的关键数据（包括您的e-mail存档）进行保护的解决方案，管理起来非常方便，不仅安全，而且可以恢复，帮助您在最大限度上减少存储管理所需的员工时间和对网络带宽的占用。

通过IBM DB2 Express 9.5轻松做到遵守相关法规

从容应对不断变化的威胁或者政府以及企业内部法规要求，对信息资产进行全面保护，确保企业的成功。IBM DB2® Express 9.5提供众多专门为了实现这些目标而开发的功能。

其中包括简单的审计管理功能，能够为审计活动提供适当层次的信息，同时还提供一套工具为审计流程提供支持，更好地将DB2整合到您的审计战略中去。

这些功能不仅能够对发生的情况进行跟踪，而且还能通过基于角色的安全模型，三层环境中可靠的上下文关系以及整个数据生命周期过程中的高级加密功能，最大限度地减少对敏感数据的非法或意外访问。

在可靠的IBM硬件和磁带解决方案基础上实现集中式e-mail存储和访问

您希望在最大限度上降低e-mail存储成本并确保调整后的数据拥有正确格式的同时提高e-mail存储能力。 因此，我们面向中等规模企业的e-mail归档解决方案包括了IBM System Storage™ DR550、IBM BladeCenter® S Express、System x™和System Storage Tape Library Express产品家族。

面向IBM CommonStore研发的System Storage DR550通过先进的技术对数据保留策略进行管理和加强，能够对e-mail、数字图像、数据库应用、即时消息、业务交易、合同或保险索赔以及其它类型的存储记录进行归档。它通过基于数据保护政策的、不可删除、不可重写等存储功能来解决您的法规遵从问题。 此外，它还提供先进的数据保护功能，例如数据加密和保护策略加强功能，以及一套基于策略和事件的数据管理软件功能。

IBM System x和BladeCenter S Express通过提供模块化、积木式的基础架构能够随着您的业务需求一起扩展的架构来满足您基础架构的需求。 它通过简化基础架构来帮助您降低成本，减少耗电量和设备占地面积。受IBM一流的大型机和超级计算机技术的启发，它实现了性能、可靠性和控制的完美结合，通过IBM领先的技术帮助您获得竞争优势。

IBM System Storage Tape Library Express产品家族通过出众的性能和可用性满足您在备份、保存/恢复和归档方面的数据存储需求。 有多种模型可供您选择，所有这些模型都采用线性磁带开放技术，具有很高的性价比。

来自IBM业务合作伙伴的增值服务

IBM拥有广泛的本地业务合作伙伴网络，他们拥有面向各个中等规模企业行业的丰富经验和专业知识。 在IBM的支持下，他们能够在IBM产品的基础上和您可承受的投资范围内为您提供简单、价格合理而且可定制的应用与解决方案，满足您的各种需求。 现在，我们的业务合作伙伴具备更高的能力，帮助您找到正确的IBM资源。

您的正确之选

E-mail归档和合规不仅对开展业务来说是一个关键需求，而且也是业务连续性的一个基础组成部分。IBM面向中等规模企业的解决方案将软件、硬件和服务适当组合起来，全面满足您的e-mail归档需求，包括法规遵从需求在内。而此解决方案的所有组件在规模和价格方面都完全符合您的预算要求。

IBM是连续性和恢复解决方案领域公认的领袖。 实际上，全球各种规模的企业都在利用我们的解决方案来保证他们业务的正常运行。 我们在业务咨询、托管、数据安全和管理方面为您提供方便使用、易于管理而且可以根据您不断变化的业务需求进行调整的解决方案。IBM能够以适合中等规模企业的定价为企业提供各种所需的功能，使我们成为区别于其它公司的一流企业。 现在，随着您可以更轻松地与IBM专家和业务合作伙伴联系，您可以比以往更轻松地与我们合作。

规避风险 完善管理

——IBM IT风险管理与IT治理

IBM全球信息科技服务部

1993年，纽约世界贸易大厦爆炸，使大厦内绝大多数企业丧失了全部商业数据，相关业务活动几乎全部中断；2005年末，东京证券交易所因软件故障导致交易无法继续进行，给瑞穗证券带来超过300亿日元的直接损失。在全球，由于IT系统故障导致金融市场动荡的事例已经发生多次，在中国，类似现象也屡见不鲜。正如中国银监会主席刘明康指出的，金融电子化给银行业风险管理提出的新挑战已经成为银行业金融机构面临的四大挑战之一。

为了应对这一挑战，协助企业增强抗风险能力，《银行业金融机构信息系统风险管理指引》、《银行业金融机构内部审计指引》和《关于开展2006年度信息科技风险内部和外部审计的通知》等相关法规、管理条例陆续出台……因此，对于众多银行和金融机构来说，尽快完善IT风险管理机制、已经成为他们的当务之急。

从上述事例可以看出，金融行业在进行信息系统建设时，需要引入一种新的管理机制来对信息系统的安全性、投资效果、实施进程和实施效果进行评估、指导和改进，这种机制就是我们现在所说的IT风险管理机制。

虽然很多金融行业为了满足外部监管机构要求和自身信息化建设的实际需要而在IT建设投入了大量资金和精力，但结果却并不乐观。在IT建设过程中，金融行业往往面临下列困扰：

- IT风险识别完成前：
  - 企业的信息系统现状与监管机构的要求之间存在一定差距；
  - 企业信息系统的风险管理能力亟待加强；
  - 企业信息系统虽已具备一定的风险管理能力，但仍需要对各方面进行强化，才能满足外部监管机构需求。
- IT风险识别完成后：
  - 多项信息系统的严重缺失需要立即改善；
  - 企业内部没有足够的资源来支持和推进改善工作；
  - 企业信息系统存在多项重要缺失，
  - 企业信息系统存在少数缺失，需要后续的持续追踪。

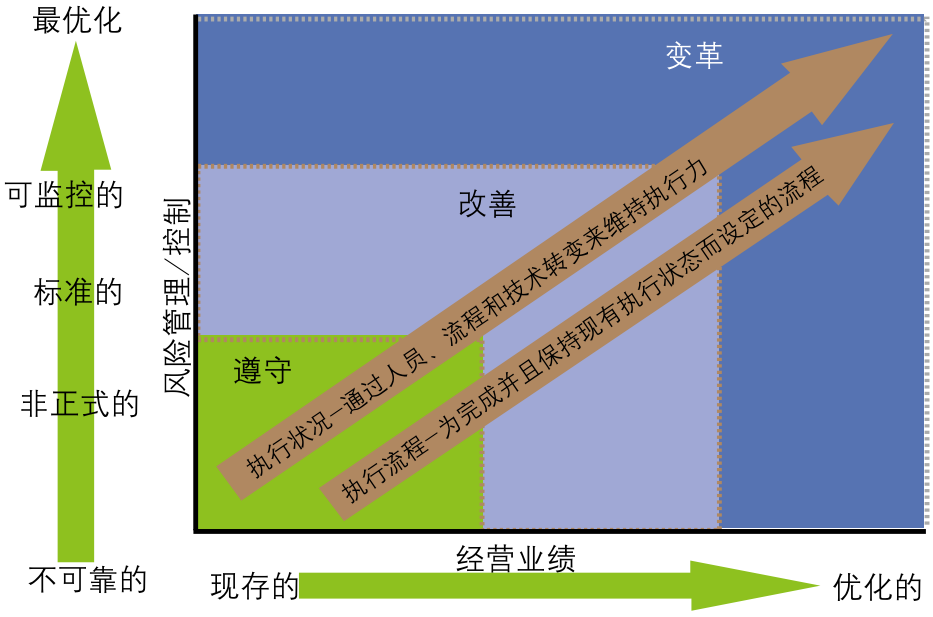
如果您正面临上述困扰， IBM IT风险管理与IT治理服务将为您提供完善的解决方案。

为您量身定制同时满足短期和长期需要的模型

在协助您实现短期外部监管合规的过程中，IBM将依据成熟的方法论模型以及监管机构的要求来为您定义IT系统的现状、目标，并依据您企业IT系统的战略发展蓝图，制定出符合IBM IT风险管理需要的实施路线图。

IBM IT风险管理将从IT整体风险管理以及行业监督委员会的关注要点两个角度来实施，并参考国际最佳实践准则，如COBIT、ISO20000,ISO 27001、ISO 17799、ISO 13335-3以及ISO 13335-4,CMM等。同时，IBM还基于行业相关法律法规，从技术、管理层面上评估机构内部信息风险控制的现状，制定IT风险管理方案。

IBM将为您制定同时满足企业短期外部监管要求和长期企业风险管理机制发展需要的整体解决方案。这一解决方案既能够适合您短期外部监管要求的需要，同时又符合企业长期发展的蓝图。



信息系统风险管理与治理服务

目前，众多银行业金融机构正面临着紧迫的信息系统内部和外部审计的任务。如何顺利通过严格的监管机构要求？IBM信息系统风险管理与治理服务将为您提供端到端的IT风险管理方案，协助您的企业顺利满足监管机构要求。

依据相关外部监管机构所出台的条例的范围，IBM信息系统风险管理与治理服务分为一般控制和应用控制。其中，一般控制的内容包括：

- IT组织与管理控制，基本要求是权责的划分和职能的分离；
- 系统开发与维护控制，即为了保证信息系统开发过程中各项活动的合法性和有效性而进行的控制；
- 信息系统操作控制，包括操作计划、机房守则、操作规程和上机日志记录等，其目的是通过标准的操作规范来保证信息处理的质量，减少差错的发生；
- 硬件和软件控制，即通过对硬件和软件的控制，尽可能及时发现错误，避免损失；
- 系统安全控制，发现并解决系统中存在的安全方面的问题，防止其危害系统安全。
- 数据安全的控制，数据的生命周期，数据的备份与存储
- 网络风险控制,网络体系的架构，网络流量监控
- IT运维系统的控制，变更管理，问题管理，事件管理等

应用控制的内容则包括输入控制、系统处理与数据文件以及输出控制，它们分别需要达到以下要求：

- 输入控制

第一，经济业务在系统处理之前经过适当的批准；
第二，经济业务被准确地转换为机器可读形式并记录于系统数据文件；
第三，经济业务没有丢失或不适当地增加、复制、改动；
第四，拒绝、改正不适当的经济业务，必要时及时重新补救。

- 信息处理与数据文件控制

第一，经济业务（包括系统生成的）由系统正确处理；
第二，经济业务没有丢失或不适当地增加、复制或改动；
第三，系统处理的错误能够被及时鉴别并改正。

- 输出控制

第一，系统处理的输出结果准确无误；
第二，输出结果仅限经过批准的人员审阅；
第三，输出结果应及时提供给适当的、经过批准的人员。

建立在风险分析基础上的IT风险补救计划

首先，IBM会根据外部监管要求和企业IT系统的现状进行风险分析，在分析的基础之上，创建和制定IT风险补救计划，并提供和定制IT风险控制模板，从而辅导企业顺利通过外部监管要求以及建立自己的信息系统风险管理与治理体系实际需求。

- 整理评价遵从外部监管的风险控制相关文档
  - 汇总整理相关文档，包括各类规范、规定、制度、流程、管理报表、改善追踪记录等；

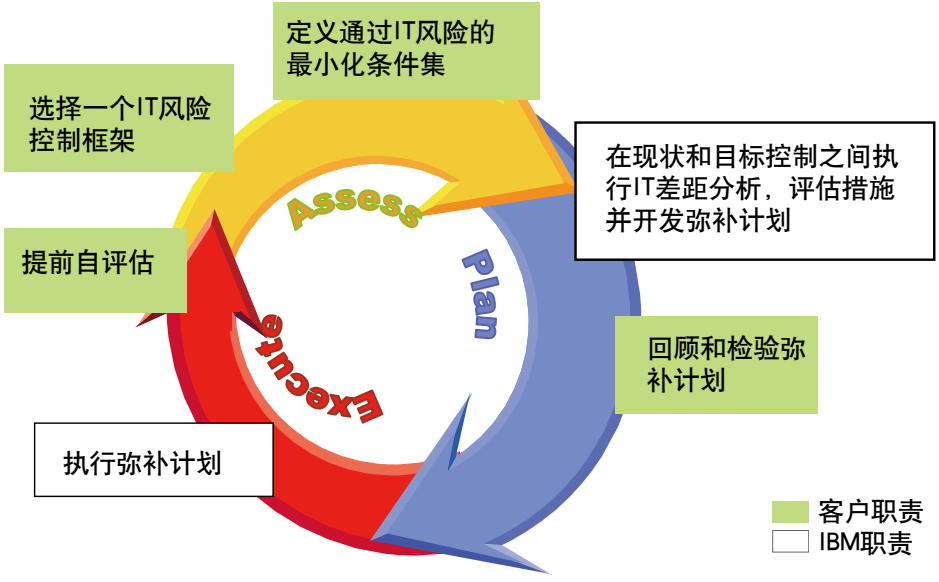
- 建立风险管控模板，完善内控记录；
- 强化评价外部评价文档内容
  - 分析现况与外部监管要求的差距；
  - 强化既有文档的可审性；
- 拟定改善计划来回应外部监管要求
  - 检验既有的结果与现况；
  - 针对企业信息系统的重大缺失拟定补救计划；
- 进行短期快速的改善措施
  - 针对需要立即改善的缺失进行补救；
  - 协助企业改善信息系统风险管理与治理体系现况。

通过IBM IT风险管理与IT治理服务，您将获得的价值有：

- 成功通过外部监管机构要求；
- 对自身的IT系统风险状况有了清晰的了解；
- 信息系统风险获得了暂时的缓解。
- 建立了有效的信息系统风险管理与治理体系

与您通力合作，获得外部监管合规与IT风险管理建设的成功

在您的企业进行IT外部监管合规与内部信息系统风险管理建设的过程中，IBM将与您同心协力，紧密合作，努力获得IT外部监管合规与内部信息系统风险管理建设的成功。在初始的准备阶段，IBM将协助您进行提前的自评估，选择一个IT风险控制框架，并定义通过IT风险控制的最小化条件集；在随后的计划阶段，IBM将在您完成对弥补计划的回顾、检验后，在企业信息系统现状和目标控制之间进行IT风险分析，评估措施并开发弥补计划；之后，IBM将严格执行弥补计划，以确保您的企业信息系统顺利通过外部监管合规要求与内部信息系统风险管理建设。



IT外部监管合规性要求与企业信息系统风险管理体系的完善是一个循环的过程。IBM将为您提供一系列的后续解决方案，包括信息科技治理解决方案（EA）、业务持续性解决方案（BCP&DRP）、信息系统运行和操作管理解决方案（ITSM）、项目开发和变更管理解决方案（PMO）和信息安全管理解决方案（ISMS）等。

外部监管合规性要求对企业而言并不是一个责难，而是一个改善IT运维的契机。IBM将与您通力合作，把握这一契机，使您的信息系统保持螺旋式上升，从而促进业务的良性发展。

选择IBM，选择值得信赖的合作伙伴

IBM作为最大的IT服务提供商，为全球70多个国家的客户提供稳定可靠的服务。与IBM合作，您不仅可以拥有先进的IT风险管理设计解决方案，而且还将获得来自IBM的专业技术和管理支持。IBM IT风险管理咨询服务的优势在于：

- **业界领先的方法论**

作为全球领先的服务提供商，IBM每年投入大量资金和人力，对IT架构等相关技术进行深入研究，拥有了包括独特的7个域优化分析方法论等内容在内的业界领先方法论，并据此开发了一套整体的智力资产和实施方法，能够帮助各行各业的用户制订出切合实际的、投资合理的、完整可靠的解决方案，或提供具指导性的建议。

- **丰富的项目管理经验**

IBM是一个以管理著称的公司，在全球范围内拥有大量的成功实施案例，自身也是IT优化的典型范例。IBM具有全球和国内范围不同行业、不同复杂程度项目的实际成功经验。在IT风险管理服务领域，IBM凭借丰富的实践经验和深厚的理论研究，能够为您提供包括咨询、设计、开发、管理及产品在内的全方位服务，提高IT系统在支持业务运营、促进发展创新中的实际效果与效率。

- **实力雄厚的技术专家队伍**

IBM拥有一支实力雄厚的技术专家队伍和富于项目管理经验的人员，包括超过300位咨询及IT技术服务专业人员，以及IBM全球资源的支持。IBM拥有超过100位IT架构工程师，超过400位系统服务工程师，为您提供大型系统的集成服务；超过500位系统服务工程师负责信息系统的安装和售后维护支持工作。IBM在全国十多个城市设有分公司，能够在全国范围内提供及时、周到的支持和服务。

- **整合的IBM职能支持**

IBM不仅拥有极富经验的成熟专家队伍，还拥有咨询、规划、实施三位一体的项目团队，既具备咨询公司的丰富经验，又兼具技术公司的强大实践能力。我们的专业团队背后有IBM整合业务的强大支持，更有全世界IBM业务合作伙伴的网络协助，职能涵盖行业和IT咨询、应用管理、实施服务等各方面，为您提供端到端的解决方案。

IBM企业信息架构-信息高可用方案群组

信息高可用方案群组

Information Infrastructure Solution

领驭信息架构 创新存储时代

N series Data ONTAP 7G操作系统

2008年9月

在当今快速变化的商业环境中，您的企业需要经济高效的、灵活的数据管理解决方案来处理异构环境中不可预知的爆炸性存储增长。随着业务的发展，您需要让数据为您工作。您希望提高效率。您希望数据管理能力能够随着存储需求的增加而扩展。它要足够灵活，能够适应和保护您的多样化业务环境。您需要一款简单而经济的系统，而且能够支持您有效地管理资源。

一、主要优势

适应变化

通过灵活的资源分配为您的业务和技术应用提供最高水平的服务，以支持您的存储适应不断变化的要求。

增强数据可用性

支持数据在企业中即时可用的同时，我们将帮助保护您的关键任务数据

节省存储、能源和空间

用更少的磁盘空间保存更多信息，从而节省能源、散热成本和空间。

提高生产力

通过针对虚拟化而优化的操作环境，最大限度地提高员工的工作效率，加快上市速度。

降低总体拥有成本

通过简化的部署和管理来降低总体拥有成本。

二、DataOntap 操作系统

实施可扩展的、灵活的 Data ONTAP 7G操作系统

N series存储解决方案能通过可扩展的灵活操作系统（我们称为 Data ONTAP 7G）帮助您管理企业环境中的数据。

Data ONTAP 7G可提供：

- 更加高效的存储
- 高可用性
- 业务连续性
- 优质的服务
- 减少存储管理复杂性

满足各种需求

我们创新的 Data ONTAP 7G架构与存储系统相互配合，能够满足从小型工作组到企业数据中心等各种规模用户的需求。我们的软件能够无缝集成到 UNIX、Windows和 Web环境中。您将得到可扩展的性能和灵活的存储环境，其中包括能够存储和支持您的应用、整合数据、并为您的企业提供可靠的数据存取能力的解决方案。

Data ONTAP 7G操作系统将简化您的管理工作，通过结合使用已获专利的文件系统和微核设计，为您带来下列优势。

迅速而轻松地适应变化

灵活的数据卷不需要预先分区。现在您可以更加轻松地定制数据来满足您的需求。更理想的是，您可以使用更少的开支来更迅速地完成工作。更迅捷的响应意味着更快地获得业务。

提高服务质量

通过 FlexShare，您可以将完全不同的应用整合在一起，对不同的数据集进行优先级划分，并根据需求的增加动态地调整优先顺序。对同一N series系统上的多种工作负荷，您均可以使用FlexShare来承载N series设定不同的优先级别。

降低成本

现在您可以将更多数据保存在更少的磁盘空间中，因为我们将重复数据删除技术和精简配置技术融入 Data ONTAP 7G之中。FlexVol技术可确保您以最高效率使用存储系统，从而将硬件投资降至最低限度。您不仅可以减少物理存储的数量，还能大量节省能源、散热和数据中心空间方面的成本。

购买更少的存储空间

您可以将数百个TB的数据整合到一个存储系统上，因为我们的操作系统非常善于充分利用多个处理器。它是任何商业或技术应用的理想选择。

在您的公司内共享异构数据

通过 Data ONTAP 7G，您可以使用数据块级和文件级的协议无缝地访问单一存储系统上的数据。通过使用FCP协议的光纤通道SAN网络结构或者使用iSCSI协议的IP网络结构，均能提供数据块级别数据存取能力。我们的 Secure Share跨协议锁定技术有助于确保您在共享异构数据时不需要牺牲安全性、兼容性或性能。

增强数据可用性

我们还可以帮助您减少昂贵的停机时间，并最大限度支撑关键任务数据访问。现场测试表明 Data ONTAP 7G 通过其可选软件能力可提供 99.999% 可用性。

支持这一高级数据可用性的 Data ONTAP 7G 标准特性及可选能力包括：

- 任意位置写入文件布局（WAFL）文件系统
- Snapshot
- FlexClone
- 多路高可用性
- 在线－在线控制器故障切换
- RAID-DP
- SyncMirror
- 块级别数据校验能力（专利申请中）

确保业务连续性和法规遵从性

我们知道您的业务运营中不能容忍长时间信息访问中断或者不符合记录封存法规等情况出现。Data ONTAP 7G具有创新的数据容灾保护和恢复特性。您可以获得业务连续性和基于磁盘的数据长久封存特性，以支持受控数据和静态参考数据。

扩展数据保护

通过N series Snapshot技术，您可以提供接近即时水平的文件级别全数据集恢复能力。

对于每个数据卷，您可以得到多达255张数据原位（data-in-place）及时间点（point-in-time）镜像。与其他厂商的快照方案不同，N series Snapshot副本几乎达到实时，因此只需要最低限度的磁盘空间费用。这是保护您的生产数据独一无二的选择。

集成 RAID可为您提供经济高效的保护，免受多种磁盘故障和错误的干扰。我们的双奇偶校验 RAID-DP（高性能 RAID 6应用）能帮您避免用户服务中断现象发生。

降低总体拥有成本

Data ONTAP 7G能够简化存储基础设施的部署和管理，从而支持您的企业拥有更高的效率和生产力。

迅速而轻松地进行部署

使用我们的设置向导，您可以迅速配置并安装我们的操作系统。由于我们使用了标准的命名和身份验证服务，因此您会发现我们的软件易于部署，可以无缝地集成到您现有的 UNIX和 Windows环境中。

软件/特性	功能	优势
Deduplication	通用的重复数据删除技术可删除冗余的数据对象	减少您需要购买和维护的存储器的数量
FlexCache	高速缓存NFS卷可支持远程办公室中加快文件存取和服务器计算群的速度	提高系统的性能、响应速度和数据可用性
FlexClone	即时创建LUN和数据卷副本（不需要额外的存储空间）	节省测试和开发时间，增加存储空间
FlexShare	向负载最重的系统上最重要的工作负载优先分配存储资源	为您提供来自指定高优先级应用的出色性能
FlexVol	在大容量的磁盘空间池至上，创建LUN和文件系统卷，其空间可以根据需要灵活调整。	确保您的存储系统以最高效率运行，同时减少硬件投资
LockVault	将SnapLock与SnapVault相结合，为非系统化的文件创建WORM保护档案	确保您符合记录封存法规，从而避免长时间的业务中断
MetroCluster	集成的高可用性/灾难恢复解决方案，完全支持园区等区域的部署	确保在站点发生故障时立即提供数据
MultiStore	安全地将存储系统划分到多个虚拟存储设备中	支持您整合多个数据域和文件服务器
Operations Manager	从单一管理控制台管理多个N series系统	简化 N series 部署并支持您整合多个 N series 系统的管理
Protection Manager	N series磁盘到磁盘环境的备份和复制管理软件	使您实现自动化数据保护，确保您拥有无差错的备份方案
SnapDrive	从 Windows、UNIX 和 Linux 服务器提供基于主机的N series存储数据管理方案	支持您在服务器出现故障时启动无差错的系统恢复机制
SnapLock	数据卷内的写入保护结构化应用数据文件可提供WORM磁盘存储能力	支持您完全遵守记录保存相关规定，使您高枕无忧
SnapManager	为数据库和业务应用提供基于主机的N series 存储数据管理方案	让您自动进行无差错的数据恢复并为您提供应用感知型灾难恢复能力
SnapMirror	支持系统间的自动化增量数据复制：同步或异步	为您提供数据分配镜像和灾难恢复的灵活性和高效率
SnapMover	支持在系统内的控制器之间快速重新分配磁盘（不会产生干扰）	让您在在线－在线控制器系统上进行负载平衡，而且不会干扰数据流
SnapRestore	从任何Snapshot备份迅速恢复单独的文件、目录或整个LUN和数据卷	从备份立即恢复您的文件、数据库和完整的数据卷
Snapshot	以最低的性能影响程度对LUN或数据卷进行增量数据原位及时间点复制	支持您定期创建节省空间的备份（不干扰数据通信）
SnapValidator	最大限度提高 Oracle Database 的数据完整性	支持您增强 Oracle Database 的灵活性，从而符合 Oracle HARD 计划的规定
SnapVault	向另一个N series系统输出Snapshot副本，以提供增量数据块级备份解决方案	为您提供经济高效的、基于磁盘的长期数据备份
SyncMirror	在镜像的每一侧都保存2份数据的在线副本（带有RAID-DP保护）	保护您的系统免受各种硬件故障（包括三重磁盘故障）的干扰
VFM	将多个Windows和UNIX文件服务器虚拟化至一个逻辑存储池（命名空间）中	为您提供异构文件服务器环境中非破坏性的自动化容量扩展、数据复制和数据管理能力

经济高效的N series灾难恢复解决方案

2008年9月

全球范围内最近发生的安全事件表明，人们迫切需要一种简单而经济高效的灾难恢复解决方案。由于某些灾难在任何时候都无法避免，因此企业的关注重点已由过去的如何避免灾难转向了如何减轻灾难的影响。尽管长期以来，人们对完整的灾难恢复的讨论和关注从未降温，但出于成本和复杂性的考虑，许多企业还是仅仅为那些重要性居前的5%至10%的关键任务关键应用部署了基于磁盘的DR。

一、主要优势

满足各种需求

对不同的灾难保护等级进行选择时，您可以使用光纤通道协议或者IP网络协议。

加快应用恢复速度

利用基于磁盘且应用一致性的Snapshot副本来加快恢复速度。

增加价值

利用镜像副本中快速且拥有存储效率优势的克隆来加快其它业务流程，如应用测试和开发。

节约存储成本

利用重复数据删除技术，并将数据由FC向更廉价的ATA 磁盘复制，最终达到降低存储成本的目的。

降低网络成本

仅传送被改动过的数据块，从而降低带宽需求。

二、解决方案

利用经济高效的复制解决方案为更多数据提供保护

利用N series的整套复制解决方案，您可以通过合理的投入为更多应用提供保护。为了使您的大量应用免受站点和区域性灾难的破坏，我们的解决方案可以支持一系列恢复点目标（RPO）。我们的统一存储架构采用了一组通用软件，可处理所有层级和类型的存储，令您的部署和管理更简单、更经济高效。网络和存储效率的提高可帮助您进一步降低成本。

防范站点灾难

同步复制解决方案采用了MetroCluster或SnapMirror，可实现零数据丢失。利用MetroCluster，您可以支持在任何组件出现故障时进行自动化故障切换，以及在主站点故障时进行单命令故障切换。

防范区域性灾难

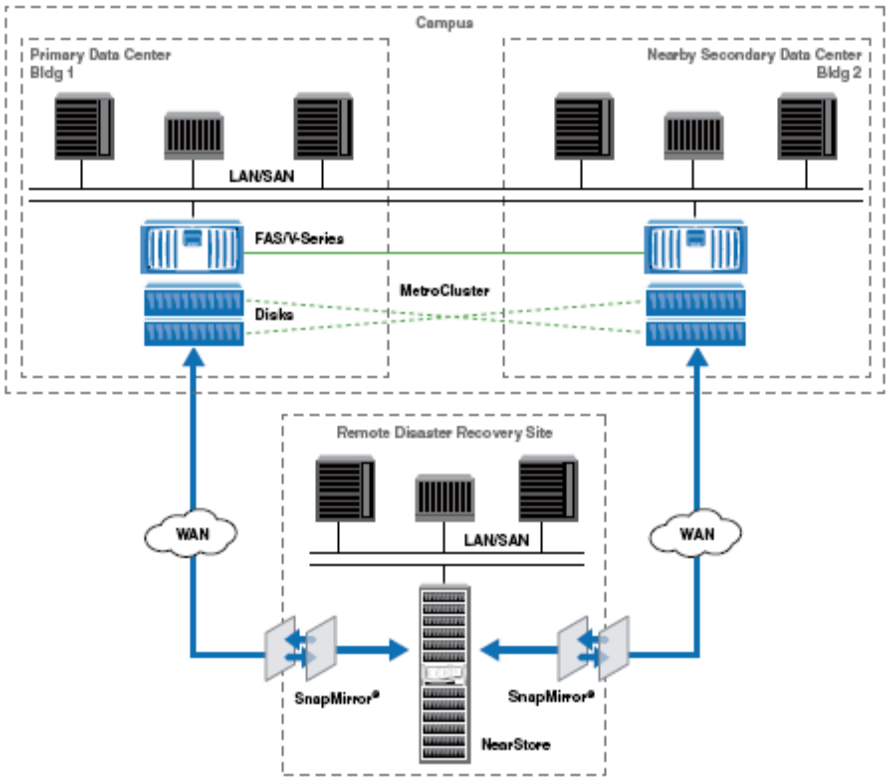
异步复制解决方案采用了SnapMirror Async，可满足从一分钟到一天范围内的RPO要求。利用该解决方案，您可以将数据从FC存储复制到更经济的 ATA 存储，从而节约资金。通过重复数据删除技术，您还可以最大限度地降低存储利用率。您还能够充分利用 N series Snapshot技术，仅在网络中发送改动过的数据块，从而降低网络带宽需求。利用FlexClone和SnapMirror Async的组合，您可以在您的灾难恢复存储中为其它应用创建额外副本，如测试、开发和质量保证（QA）。创建这些克隆的过程非常简单，既不会对您的生产系统造成影响，也不会消耗额外的灾难恢复存储空间。

降低成本，保护更多数据

在 N series 灾难恢复解决方案的帮助下，您可以通过以下方式节约资金：

- 降低部署成本
- 减少存储及网络带宽成本
- 充分利用现有网络基础设施
- 将灾难恢复存储用于运作中的业务

依靠N series，您将充满信心，因为您知道数据将会得到可靠的保护，而且企业能够实现快速备份，从而在灾难发生时保持正常运作。



三、N SERIES 灾难恢复解决方案组件

常用组件

组件	描述
N series 存储	提供高性能网络化存储。
MetroCluster	防范园区内各种类型的硬件中断和站点灾难。
NearStore	提供基于 SATA 的企业级存储。
SnapMirror	防范站点及区域性灾难。
G 系列	对分层异构存储阵列进行虚拟化。

可选组件

组件	描述
FlexClone	支持从镜像副本创建克隆时无需使用额外空间。
MultiStore	在带有多个文件服务域的两个 N series 系统间实现非中断性故障切换。
Protection Manager	提供自动化复制管理功能
SnapManager	创建应用一致的 Snapshot 副本
SnapVault 和 SnapLock	复制不可重写、不可擦除的 WORM 数据卷
VFM	充分利用全球命名空间，在文件服务中实现非中断性故障切换

N series 全面的解决方案

2008年9月

N series提供一应俱全的产品系列，从企业数据中心到分支机构，全面照顾到企业运营的需求。提供切合所需的数据管理解决方案。通过这些解决方案，企业可以简化运作，有效控制数据的增长，提高存储利用率，革新数据中心，降低风险和总体拥有成本，并在瞬息万变的商业环境中，体现无与伦比的性能及扩展性。凭借丰富完善、傲视同群的产品阵营、技术和合作伙伴，N series的企业存储解决方案为客户解决最关键的IT和业务难题，满足客户最苛刻的应用环境需求，缔造最大的投资回报（ROI）。以下我们从企业应用和存储基础架构两个不同的角度，全面了解N series的企业解决方案如何帮助客户提升速度和效率，实现业务突破，走得更快、更远。

一、面向应用的存储解决方案

商务应用程序

面向Oracle E-Business Suite、SAP、FileNet、Documentum、IBM Content Manager等应用，企业一直在寻找能够降低应用程序宕机时间，提高员工工作效率，同时节省成本的解决方案。

N series一应俱全的解决方案提供了兼具高可用性和可靠性的基础设施，确保用户和管理员能够全面提高工作效率；独特的Snapshot、SnapRestore应用有助于企业加快测试开发流程，快速占有市场的先机；先进的FlexClone能够快速克隆真实的生产环境，以革新传统的商业业务流程。

数据库

信息是企业的命脉；但是，数据的快速增长驱使企业从战略角度思考对信息的使用及存储基础设施的运作效率。N series存储解决方案与业界领先的企业数据库（Oracle、Microsoft SQL Server、IBM DB2、Sybase等）融会贯通，使企业收到事半功倍的效果。

N series的数据库解决方案针对数据库的空间配置管理、备份恢复、容灾、业务流程、数据相关应用等方面，利用Appliance的设计理念和独特的数据自动管理功能，彻底革新传统的数据库管理模式，从而帮助企业减少投资、提升运作效率及创造成本效益。通过 N series的基础设施，企业能够适应日新月异的业务状况与流程，并在减少宕机时间的前提下实现数据可用性，提高用户和管理员的工作效率。

消息传送与协作

电子邮件系统及协同工作系统日益成为支撑企业正常运转的关键系统。除了考虑可靠性、稳定性以外，如何快速备份和恢复更细粒度的数据，如何有效保存为应对法规要求而保留的海量数据，都成为企业在构建系统时的重大挑战。

N series致力于提供灵活、易于扩展的综合解决方案，为企业实现高效的消息传送与协作，打造出稳定、可靠的存储平台；同时对备份策略进行优化，并进行更细粒度的恢复。这些解决方案所占的空间极少，却可以完全满足实现归档、法规遵从等要求。

文件服务

企业的非结构化数据（文件）呈指数式增长，导致服务器的数量不断增加，而文件分散存储的情况又日益严重。N series存储整合解决方案不仅具有极高的可用性和扩展性，可以跨越所有开放平台，进行安全可靠的共享文件访问，并有效整合企业的服务器和存储资源，以达到最高的资产利用率；同时在文件防误删除、备份恢复、防病毒感染、法规遵从、重复数据删除等方面为企业提供最可靠最高效的解决方案。

技术应用程序

对于运行机械设计、电子设计、软件开发、油气开采以及媒体娱乐等业务的企业，一般都需要采用十分专业的

高性能应用软件。它们渴求能够加快产品上市速度、削减研发成本的技术。

N series的存储解决方案可以同时满足这两方面的需求。N series解决方案有助于改善业务流程、缩短设计周期，同时为工程、设计、开发和勘探团队提供无可比拟的协调性，从而提高工作效率；同时，通过改善资产利用率减少运作成本，为存储环境提供所需的灵活性——这一切都有利于降低总生产成本。

数字媒体内容

据估计，企业内有80%的数据属于非结构化信息，如文档、图像、音频和视频内容。对于视频监控或数字放射等应用程序，授权用户必须能够妥善管理、保护和轻易访问视频和图像数据；而在媒体、娱乐和互联网市场中，能否快速创建和发布独特的数字内容，往往成为了发展核心业务的关键。

N series针对PACS、DVS、媒体和娱乐应用程序等主要领域，提供完善的数字内容存储和管理解决方案，特别

着重于实现更快捷的多媒体信息创建和捕获、轻松的共享和可靠的发布。N series解决方案的优点不胜枚举，包括无可匹敌的性能及可扩展性、高容量存储应对内容增长、高可用性存储实现了最高的工作效率和最长的运行时间，同时达到业内一流的易管理性，有效降低TCO。

二、基于基础架构的存储解决方案

服务器虚拟化

为提高企业服务器资源的利用率和动态扩展计算性能，市场上出现了向内和向外两种服务器虚拟化技术。向内进行服务器虚拟化，包括像 VMware 和 Microsoft 的强大企业商业解决方案和许多开源产品；向外进行服务器虚拟化，则实现了网格计算的模型。为了给虚拟服务器提供存储，首先必须具备共享的能力，并且达到简单、灵活且具有成本效益的要求。如果在服务器虚拟化设计的规划和部署中未能考虑高效的存储优化，则只会将成本从服务器转移到存储基础设施上。

N series 的统一存储解决方案能够在异构存储环境之间进行灵活的存储聚合，独一无二地迎合了虚拟化服务器环境。存储系统并且具有高可扩展性，有助于提高利用率，充分满足虚拟服务器增长的 I/O 需求；同时为虚拟机提供全面的自动数据保护，而对性能的影响几乎为零。统一的跨平台数据管理手段，加上高效的自动管理能力，可以大大简化存储的配置与管理工作。

业务连续性

企业必须能够在计划或突发性宕机期间保持应用程序的可用性，并能够在出现灾难的情况下，迅速重新构建全

部功能。只有保证业务的连续性，才能创造收益，保持竞争优势。

N series 的存储解决方案能够全面应对设备故障、逻辑错误和环境灾难等多层次的灾难问题，解决导致应用程序宕机的所有因素。它可以防止操作出错，又能够快速从操作错误和应用程序错误中恢复，减少计划宕机时间，让企业从灾难中恢复运作。N series的业务连续性方案，包括能够切合实际应用要求的双盘故障防护、本机时间点瞬时备份恢复、同异构数据远程复制等多个子项。N series以简洁的结构提供了卓越的数据可用性、快速的数据恢复、存储弹性和经济实用的恢复解决方案，使企业可以利用更少的资源，为应用程序提供更周全的保护。

备份和恢复

数据正在以惊人的速度增长。传统的备份和恢复机制已经发展到了极限，加上激烈的市场竞争，要求企业不断提高服务水平和质量。

N series提供全方位的备份和恢复解决方案，包括本机时间点瞬时备份恢复、跨机长期在线备份恢复、分支机构远程备份恢复、数据块级增量备份恢复、虚拟磁带库备份恢复、传统磁带备份恢复、磁盘到磁盘备份恢复等。这些解决方案可以从多角度、多方位优化现有的磁带备份，减少对传统磁带的依赖，简化备份恢复的管理，提高企业的服务水平和质量。

归档与法规遵从

企业希望通过智能化的途径，对快速增长的数据进行有效的分类和归档，同时以科学的方法，提高存储资源的利用率，并且降低大量数据对存储空间的投资需求。企业更必须确保数据的安全、完整和一致性，以避免由于违规而遭受巨额的罚款或影响声誉。

N series归档和法规遵从解决方案以综合的运作模式，消除了单独存储库的需要，弥补了归档和法规遵从的单点解决方案之间的缺口。它们把本机跨机的分级存储平台、多功能数据拷贝应用、信息综合管理、开放式标准的方法等内容兼收并蓄，更排除了写入专有应用程序接口的需要，能够面对千变万化的数据归档和法规遵从要求，从而降低了集成成本，并且让企业把所有归档和法规遵从计划，合并到灵活的公共平台上。

存储安全

数据安全一直是企业信息系统面对的一大问题。

N series的数据安全解决方案可满足企业对法规遵从、安全存储整合、数据加密、安全备份及灾难恢复、知识产权保护及安全信息共享等不同方面的需求。

N series除了提供本身的产品外，还积极推动旗下 Decru 公司先进的存储安全性解决方案。这些解决方案已经在世界各地得到广泛部署，让企业和政府客户可以利用最强大的安全技术来保护存储数据。

异构存储管理

N series的解决方案能够把企业不同的存储设备，整合到统一的存储平台内，实现统一数据管理的功能，从而简化数据中心内的存储和数据管理；还可以针对第三方的存储设备，实现统一的集中备份和容灾流程。

三、方案魔力矩阵

N series解决方案	面向应用的存储解决方案						基于基础架构的存储解决方案					
	商务应用程序	数据库	消息传送与协作	文件服务	技术应用程序	数字媒体内容	服务器虚拟化	业务连续性	备份恢复	归档与法规遵从	存储安全	异构存储管理
存储架构												
主存储	•	•	•	•	•	•	•	•	•	•	•	
近线存储	•	•	•	•	•	•	•	•	•	•	•	
统一网络存储架构	•	•	•	•	•	•	•	•	•	•	•	•
FC SAN 存储模型	•	•	•		•	•	•	•	•	•	•	
iSCSI SAN存储模型	•	•	•		•	•	•	•	•	•	•	
NAS 存储模型	•	•	•	•	•	•	•	•	•	•	•	
FC/SATA 分级数据存储	•	•	•	•	•	•	•	•	•	•	•	
V-Series 异构存储虚拟器	•	•	•	•	•	•	•	•	•	•	•	•
高可靠性												
RAID 6（RAID DP）	•	•	•	•	•	•	•	•		•	•	
SyncMirror	•	•	•	•	•	•	•	•			•	
空间管理												
FlexVol	•	•	•	•	•	•	•	•		•		•
FlexClone	•	•	•		•		•	•				•
De-duplication重复数据删除			•	•	•	•	•			•		•
Virtual File Manager			•	•	•	•		•		•		•
数据保护												
Snapshot	•	•	•	•	•	•	•	•	•			•
SnapRestore	•	•	•	•	•	•	•	•	•			•
SnapVault	•	•	•	•	•	•	•	•	•	•		
OSSV	•	•	•	•	•	•	•	•	•	•		•
数据复制												
Metro-Cluster	•	•	•		•		•	•				•
SnapMirror	•	•	•	•	•	•	•	•				•
ReplicatorX	•	•	•	•	•	•		•				•
高效窄带初始化	•	•	•	•	•	•		•				•
智能断点恢复	•	•	•	•	•	•		•				•
全局一致点组	•	•	•	•	•	•		•				•
数据安全												
MultiStore 虚拟多存储	•	•	•	•							•	•
按需病毒防护			•	•							•	•
SnapLock		•	•	•	•	•				•	•	•
LockVault			•	•	•	•			•	•	•	•
性能管理												
FlexCache			•	•	•	•						•
FlexShare	•	•	•	•	•	•						•
SnapMove	•	•	•		•	•						•
应用管理												
SnapDrive for Windows/Unix	•	•	•		•	•		•	•			•
Single Mailbox Recovery			•						•			•
SnapManager for Exchange			•					•	•			•
SnapManager for Oracle		•						•	•			•
SnapManager for SAP	•							•	•			•
SnapManager for Sharepoint			•					•	•			•
SnapManager for SQL Server		•						•	•			•
系统管理												
Operation Manager	•	•	•	•	•	•	•	•	•	•		•
Protection Manager	•	•	•	•	•	•	•	•	•			•
SAN Manager	•	•	•	•	•	•	•	•	•			•
远程管理	•	•	•	•	•	•	•		•	•	•	•

N series多元化的解决方案，使现代企业的信息管理难题迎刃而解。

VMware环境下存储、备份解决方案

2008年9月

服务器整合与虚拟化为企业基础设施带来了高效、灵活和可扩充性。要想尽可能快地响应市场和业务需求并充分利用服务器虚拟化的优势，您需要满足虚拟化服务器对您的存储基础设施提出的更高要求。采用虚拟服务器后，备份工作将变得更加困难，而快速恢复也会愈加紧迫。为了能够充分利用与服务器虚拟化相关的所有优势，您的数据中心移植战略必须同时兼顾存储设备和服务器。

一、主要优势

加快上市速度

快速分配存储资源，就像快速配置虚拟服务器；将测试和开发周期从几周缩短到几分钟，对虚拟机进行即时存储资源分配和克隆。

降低成本

采用我们的重复数据删除技术，削减50% - 90%的 VMware存储需求；运用我们的精简配置技术，购买更少存储设备，节约50%的功耗、散热和空间。

管理风险

瞬间备份，符合备份窗口。恢复时间是EMC和惠普产品的两倍。

增强数据保护

在不影响系统性能的情况下执行频繁而完整的备份。

缩短恢复时间

使用我们基于磁盘的Snapshot技术，以较少的停机时间和更高的服务水平恢复您的数据。

节省存储、能源和空间

通过实施我们的重复数据删除技术来提高您的存储利用率。您可以最大限度地利用现有的存储，并且会因为不必购买额外的存储而节省大量成本。

提高生产效率

可以为几百个数据集简化复杂的备份和复制的配置任务。使用我们的Protection Manager，您可以将具有相同保护要求的数据分组到数据集中，从而可以对其采用和定制响应的保护策略，并为其生成详细的报告。

二、解决方案

借助N series虚拟化解决方案简化VMware环境

将N series的统一存储架构纳入您的虚拟化解决方案采用N series产品构建一套完善的虚拟化基础设施。我们侧重存储设备而VMware侧重服务器。我们的自动化备份和恢复解决方案能够提供一流的数据保护能力。借助我们的解决方案，您可以有效保护基础设施，使其在VMware环境中实现较其它解决方案两倍的恢复速度。此外，您还可运用我们的重复数据删除技术和自动精简技术，最大程度地提高利用率、降低总体拥有成本且确保性能不受影响。我们还可借助业界使用最广泛的统一存储架构，帮您简化管理工作和管理复杂性。我们面向生产、测试、开发和桌面环境的虚拟化解决方案可有益补充您VMware部署的可管理性、利用率和成本节约优势。

管理风险

现在，您可借助备份、复制、恢复和灾难恢复解决方案保护您的虚拟化基础设施和数据，这些解决方案均不会对您系统的性能产生不利影响。采用我们的解决方案，您在VMware环境中恢复虚拟机的速度是采用EMC或惠普产品的两倍。

我们面向存储和网络的高效数据保护解决方案无需企业购买价格高昂的灾难恢复（DR）基础设施。鉴于我们所提供的高成本效率，您完全能够以更低廉的成本保护更多的数据。我们简化的解决方案能够帮您快速、可靠地恢复所有应用层级。采用N series解决方案，您可利

用您的DR基础设施进行应用测试，充分发挥其优势。您甚至还可利用它有序测试DR站点本身。

实现存储设备的最高利用率

我们可以帮助您通过多种方式最大程度地提高资产利用率、降低成本。采用我们的自动精简技术和Snapshot技术可助您获得较高的效率，帮助您削减50%的功耗、散热和空间需求。通过在您的主存储器、备份以及归档存储设备上使用我们的重复数据删除技术，可以减少您50% - 90%的VMware存储需求。

提高运营效率

借助面向数据保护和虚拟机（VM）恢复的自动化解决方案，您的VMware管理员再也无需亲自处理大多数劳动力密集型任务。我们为您提供面向Oracle、SQL、Microsoft Exchange、Microsoft SharePoint和SAP的其它数据管理解决方案，帮助您自动化完成特定应用备份和恢复操作，提高您的生产力。

快速响应变更

为响应不断变化的业务需求，您需要具备部署新的虚拟机，并为其快速供应存储设备的能力。采用我们的解决方案，您可以缩短 40% 的资源分配时间，且对服务器没有丝毫影响。我们近乎即时的低开销存储设备克隆和资源分配功能完全能够帮您实现上述目标。此外，这些功能支持瞬间配置存储设备和克隆您的虚拟机，可帮助您将测试开发周期从几周缩短至短短的几分钟。

最大程度地实现您的业务优势

我们不仅提供了更卓越的解决方案，同时还提供了专为虚拟化环境特别打造的专业服务和支持。N series专业服务运用业经验证的方法、工具和最佳实践，帮您部署最恰当的虚拟化解决方案，满足您的业务需求。我们前瞻的支持服务采用创新的N series技术，能够帮助您排除隐患。我们还可专门针对您的特定需求优化您的虚拟化解决方案，帮助您降低总体拥有成本（TCO），享受更快的投产时间和更可靠的性能。采用我们的专业服务作为您的虚拟化向导，您就能获得恰当地满足您需求的强大关键技术组合。

针对 VMware 环境的 N series 备份解决方案

实施适合所有恢复类型的 N series 备份基础设施

VMware ESX Server支持多种不同的备份方法，其中包括 VMware Consolidated Backup 提供的基于代理的免服务器备份。许多组织选择采用多种备份解决方案来满足不同的恢复需求：一种用于文件级恢复，一种用于虚拟服务器完全映像恢复，还有一种用于对数据库和应用程序进行应用程序一致的备份。提供应用程序一致备份（确保备份数据处于可恢复状态）的解决方案会增加复杂性，因为它可能需要您在备份过程中关机或者停顿您的数据库或应用程序。具有多个流程的多种解决方案可能会带来数据管理上的麻烦。

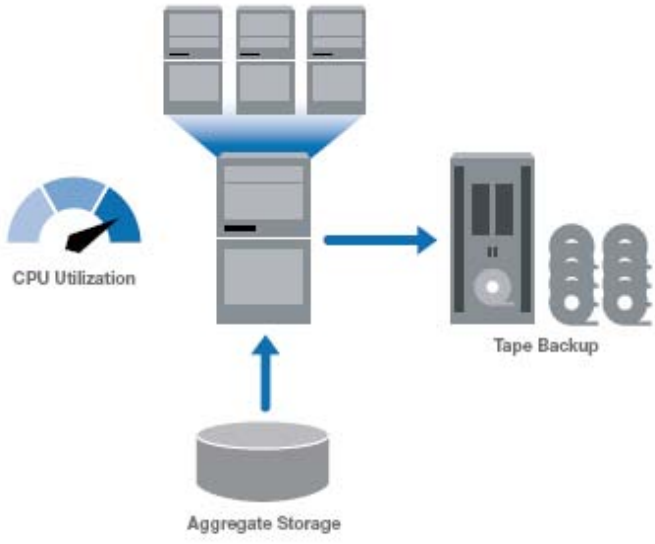


Figure 1) Backing up all data places an excessive load on the CPU. Traditional backup methods might become impractical in a virtual environment because of their affect on CPU performance.

传统的备份方法在虚拟环境中可能会变得不切实际，因为它们会影响CPU的性能。

您可以采用我们的数据管理基础设施来简化您的备份决策。我们为文件、虚拟机和数据仓库提供高效的备份和恢复。使用我们的解决方案，您可以轻松地执行热备份（一种流程，可在执行应用程序一致备份的同时，保持虚拟机运行并提供请求的服务）、快速恢复和精细恢复。

消除备份窗口

借助我们的快照和复制解决方案，您将获得虚拟基础设施所应有的业务优势，还可以按您的业务要求来备份文件和应用程序。

加快备份和恢复速度

您可以确保满足备份窗口的一种方式是完全消除备份窗口。与其它快照实现技术不同，N series Snapshot技术可以实现近乎即时的高空间效率的免服务器备份。因为N series Snapshot副本的速度和空间效率很高，所以客户可以频繁执行备份而不会影响系统性能。

快照副本驻留在存储上，可以保护数据免遭损坏。要在出现主系统故障时保护数据，您可以使用N series SnapVault技术来存储基于Snapshot副本的备份。如果您部署的内容涉及远程系统的集中备份，或者您要将备份数据移到场外或磁带上来实现灾难保护，那么，我们的SnapVault解决方案是理想之选。

在过去，您可能会觉得硬盘到磁盘的备份在经济上不可承受，因为增加存储容量可能需要很高的成本。这种情况已经不复存在了。我们可以帮助您显著减少要备份的数据量，从而改变您的成本结构。我们的SnapVault技术仅传送自上次备份以来发生了更改的数据块级数据，从而可以提高备份速度，并且所用的网络带宽和存储容量都变得更少。因此，您现在可以经济实惠地在磁盘上存储更多的数据。您可以使用我们的Open Systems SnapVault，将我们的Snapshot技术扩展到第三方存储。这种轻型的基于主机的软件代理可以将数据保存在直接连接的第三方存储上，并将其以Snapshot格式存储在二级N series存储中。

快速恢复数据

N series在考虑可用性时，恢复和备份的重要性是一样的。您需要在尽可能少地中断服务的情况下快速恢复数据。您可以利用基于磁盘的Snapshot副本方便直接地访问数据，缩短恢复时间，以及提高服务水平。如果将 N series Snapshot技术与SnapRestore结合，您将实现针对各种情形的快速恢复：

- 您的最终用户可以在几分钟时间内恢复单个文件或整个虚拟机。
- 您可以从克隆的备份存储直接运行虚拟机以实现快速恢复。
- 您可以使用与关键企业应用程序（包括 Oracle 以及Microsoft的Exchange、SharePoint和SQL Server）集成的N series SnapManager产品恢复应用程序一致的备份。

简化备份和恢复

备份自动化

借助我们的备份解决方案，可以更轻松地满足您的服务级别协议。您可以使用Protection Manager实现复杂备份和复制配置的自动化；该管理器拥有自动化的设置和基于策略的管理功能，可以帮助您简化企业数据保护的过程。通过将具备相似保护要求的数据分组成数据集，可以快速地对特定类型的所有数据应用特定的保护策略。您也可以使用Protection Manager创建详细的定制报告。

最大程度提高存储效率

减少存储购买量

您可以通过使用我们的重复数据删除技术，极大地提高存储利用率。利用该项技术，您可以以透明的方式删除任何卷中的重复数据，而不必考虑数据的类型。您可以减少高度冗余的重复虚拟机和虚拟台式机映像数据，从而降低VMware环境中的存储成本。

降低总拥有成本

利用我们的高存储效率和简化的数据管理，实践证明，相对于传统备份系统，您将节约大量的资源。通过缩短恢复时间，您可以降低停机带来的成本。根据最近的 Mercer研究1，N series SnapVault解决方案可以帮助您降低影响总体成本的三种要素中每个要素的成本。根据接受Mercer研究的受访者报告，SnapVault的易用性、改进的管理和增强的稳定性可以使工作效率提高三至八倍。

降低运营成本

我们的备份解决方案可以降低您的介质成本，并使您能仅增加少量的软件投资就让实现通过WAN连接进行

远程办公室备份，从而让您有机会获得显著的成本优势。对于使用典型备份循环和计划的典型备份环境，与具有相似容量的磁带备份解决方案相比，使用N series SnapVault解决方案的支出可以减少54%。

加快恢复速度，提高备份可靠性

当您对您的服务器环境进行虚拟化时，与物理服务器关联的备份环境的重要性将更加突出，因为即使在备份环境中只出现一次故障，也可能会影响对环境中每个应用程序和虚拟服务器的保护。因此，提高备份系统的可靠性特别重要。绝大多数情况下，对虚拟化环境来说，传统的磁带备份的速度不够快，也不够强大和稳定。因此作为磁带备份的替代方式，我们提供了高成本效益的磁盘存储技术和高效的数据管理软件，它们可以提供可靠且易于管理的数据备份和恢复。

提高可靠性

数以千计的组织依靠我们的磁盘到磁盘备份解决方案提供可靠的备份，并实现高于99.99% 的可用性。这些组织使用 RAID-DP 提供额外的驱动器故障保护。无需在RAID 5需要的驱动器用量之外增加驱动器，它们可以支持其存储系统同时承受两个驱动器故障（或者在较为现实的情况下，承受一个驱动器故障和重建过程中的一个介质错误）。

让您的备份架构发挥作用

如果您能快速完成测试、开发和部署活动，您就可能获得重要的竞争优势。但要做到这点，通常需要生成数据或虚拟机的物理副本，而这要花费时间，并且可能会消耗大量的磁盘空间。通过在您的备份系统中使用 N series FlexClone，您可以创建数据的即时空间优化副本，其中包括服务器实例、虚拟机和应用程序数据。除了测试和开发以外，您还可以将您的备份架构用于各种其它生产业务目的，如数据挖掘、最终用户恢复、灾难恢复测试，等等。

全新企业级数据中心的业务弹性

简介

2002年11月，IBM宣布推出“随需应变计算”，这项计划能够帮助信息技术（IT）高层管理人员深入了解信息系统基础设施的构造并为他们提供指导，为高效的业务流程流提供透明而动态的支持。 随需应变计算鼓励IT战略规划者和设计者：

1. 对他们的信息系统进行合并和虚拟化；
2. 实施服务导向架构（SOA），以便执行服务请求；
3. 对系统、存储、网络、数据库和应用管理实现自动化；
4. 通过虚拟化、以SOA为支持的信息系统对业务流程流进行协调。

现在，六年过去了，IBM提出了进一步的指导。 随着市场条件（例如，能源成本的不断上升，全球扩张和不断上升的IT管理成本）的不断变化，以及根据自己帮助数千家客户对通过SOA实现的基础架构以及合并的虚拟化系统进行部署的经验，IBM正在呼吁广大行业客户从现有的分布式计算数据中心模式向所谓的“全新企业级数据中心（NEDC）”模式转变。

> 和随需应变计算相类似，这种全新的企业级数据中心模式以企业信息系统架构和资源虚拟化为重点。 除此之外，新的企业级数据中心模型还非常注重能效、基础架构优化、设施管理、业务驱动的服务管理、安全和业务弹性。

此Advisory对全新企业级数据中心的业务弹性做了更加透彻的分析。 第1部分对全新企业级数据中心是什么，它旨在解决哪些问题以及NEDC实施的三个阶段做了说明。 第2部分对业务弹性做了定义，并对业务弹性需要满足的四个关键需求做了描述。 这部分内容还对业务弹性如何融入NEDC的三个阶段做了说明。 第3部分属于总结部分，为那些希望在全新企业级数据中心环境内实施弹性业务服务的IT设计者和规划者提供循序渐进的指导建议。

第1部分：什么是“全新企业级数据中心”？

由于设计不合理，全球许多数据中心现在已经变得效率非常低下而且高度分散。 松散分布的系统设计使得数据中心变得极为复杂而且管理成本非常高，难以保证其安全。

为了解决这些问题，IBM推出了一种全新的数据中心设计模式（NEDC），这种模式的核心理念是通过更有效的信息系统和数据中心设计，通过更合理的资源利用，改善程序与程序之间的通信以及更加先进的服务管理实践来控制数据中心成本。

旧的数据中心设计方面存在的问题

旧的、分布式数据中心在设计方面存在的主要问题包括：

接入点增多 – 分布式设计导致网络接入点不断增多，形成数十、数百甚至数千个端口，这些端口都需要防入侵安全保护。 向上扩展和集中化设计（如同设计全新企业级数据中心时建议的那样）能够极大地降低接入点数量，从而在降低成本的同时降低管理的复杂性；

资源利用效率低下 – 分布式数据中心的系统和存储利用效率低下已经是众人皆知的现象，这种利用效率低下会导致存储容量的浪费（在许多情况下，分布式应用服务器为了给计算高峰期间留出容量余地，往往只能利用总存储容量的10-20%）。 通过提高利用率，可以降低购置成本（IT购买者可以从现有系统获得更多的计算资源），简化管理，提高可用性，等等。

电源利用效率低下 – 分布式系统消耗大量的电力。 从直流电转变为交流电需要浪费大量的电能。 为了给CUP、内存和其它组件降温，风扇需要不断地送气。 网络接口卡（NIC）和相关的网络交换机、集线器和路由器也需要耗电，即使在不使用的时候也要耗电。 向上扩展设计能够提高系统利用率，在保证同等计算能力的同时，通过减少耗电机器的数量来达到节能的目的。 而且，向上扩展

设计还能极大地减少耗电NIC以及相关网络设备的数量，原因在于大量的分布式计算都通过某个规定的系统机箱内的背板或总线实现的）；程序模型的复杂性－旧的数据中心设计在很大程度上依靠紧密耦合的编程模型，这些编程模型高度灵活，难以维护，从而使得企业无法充分发挥它们的效率，而采用新的、松散结合的“服务导向”编程模型则可以充分发挥它们的效率；而且，劳动密集型的流程流管理－在旧的数据中心内对业务流程流进行管理，需要大量的人为干预操作，因此属于劳动密集型管理。而NEDC设计中所提倡的更好的，自动化的服务管理可以极大地降低人员密集型管理的劳动力成本。

NEDC模型帮助您解决这些问题

为了帮助企业克服这些分布式计算设计的复杂性问题，并且帮助企业大幅降低IT运作成本，IBM NEDC模型重点放在：

1. 通过资源合并和虚拟化，提高信息系统资源利用率；
2. 高能效、环保而且优化的基础架构和设施；
3. 业务驱动的服务管理；
4. 提高安全性和业务弹性；
5. 采用能够解决信息可用性、保留、安全和依从问题的信息基础架构战略。

NEDC设计的三个阶段

一般来说，向新的企业级数据中心计算模型转变需要涉及到三个阶段（见图1）：

1. 简化；
2. 共享；和
3. 动态。

图1：NEDC设计的三个阶段

简化阶段重点放在通过合并和虚拟化来降低IT购置和运营成本。 在此阶段，企业开始将分布式资源集中至更少的数据中心、服务器、存储和网络设备（以便简化管理）。 企业还对资源进行虚拟化（创建逻辑分组、池或物理服务器、存储和网络设备），提高利用率。

共享阶段将IT管理员和经理的工作重点从对个别系统的管理转到对“类似”资源的集结和共享上来。 这些相似的资源是经过虚拟化和集结的同种类型资源的集群或集合体，经过集结后作为一个共享的资源池对其进行管理，仿佛就是一个单一的系统。 此阶段还提出一个名为“管理服务流”的概念。 通过打破相似或类似资源（例如，x86服务器或者孤立的存储设备）之间的壁垒，将这些设备分组至逻辑资源池，然后采取端到端的系统、存储和网络管理，企业可以在很大程度上降低IT运营成本。 通过向服务导向架构转变，企业可以把重点转移到对流程流进行协调和对服务进行管理上来，而不是对全异的系统、存储、网络设备进行管理。

共享的架构允许跨越“相似”环境对工作负荷和数据进行移动、控制和平衡。 在此阶段，IT经理和管理员开始将更多精力集中到流程流和服务管理上来（原因在于，对基础信息系统的管理和配置在很大程度上变得更加自动化）。

在采用全新企业级数据中心的动态阶段，完全消除了服务交付和基础IT架构特点之间的物理联系。信息系统变成一个IT“集合”，用户在请求服务时无需担心基础信息架构的复杂性问题。

在此阶段，由于服务不再与特定的孤立技术联系在一起，因此，IT经理可以对资源的分配情况进行改动，确保IT系统在不影响一般业务流的正常运行前提下尽可能地高效运行。在此阶段，通过对政策、流程和过程实现标准化和自动化能够进一步优化运作。

从业务弹性角度看，高度虚拟化的系统、存储、网络资源有助于提高运作灵活性（原因在于备份、冗余、可用资源都可以在一个集合内轻松找到）。 所有这些工作前面阶段都已经做过，目的是为了提高可用性，建立容错机制，对异构业务和同类业务进行融合，为实现成本有效、完全自动化的弹性业务提供基础。

> 在动态阶段，信息系统变得对特定业务需求高度响应。信息系统不再硬性规定业务流，相反，它们会根据预先制定的业务规则自动服务于业务流。 而且，这些规则可以根据不断变化的市场情况或竞争压力实时进行修改。

第2部分：将业务弹性融入到全新的企业级数据中心模型

术语“业务弹性”描述的是一种全面的战略，它能让企业快速对风险和机遇进行适应并做出反应，以便保持业务运作的连续性，成为客户更加可靠的合作伙伴并实现自身发展。 有关业务弹性更加深入的描述，见IBM业务连续性和弹性服务首席技术官Richard Cocchiara的《超越灾难恢复：成为弹性企业》：

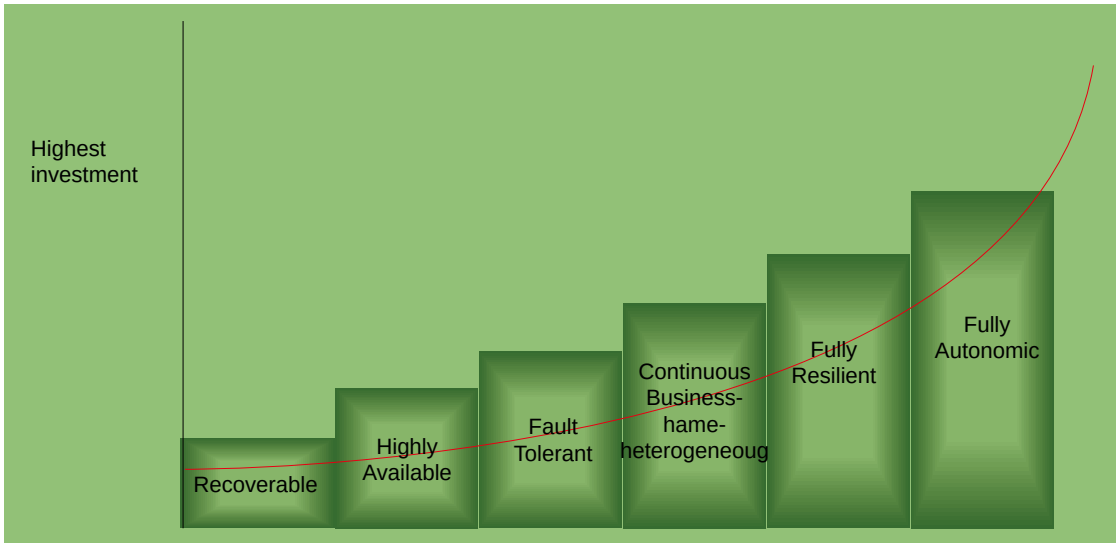
http://www-935.ibm.com/services/us/bcrs/pdf/wpbecoming-a-resilient-business.pdf

在设计弹性环境时，最终的目标是实现一个可完全恢复、高度可用的容错架构，无论发生何种类型的业务中断事故都能提供持续的计算服务。（系统故障可能像应用响应时间、内部或外部安全违规问题一样简单…）在实施的最后阶段，应该对这一具有高度弹性的环境进行自动化，以保证能够对故障快速做出反应，并大大降低IT管理方面的人力成本。

> 在谈到业务弹性时，最主要的影响因素是投资资本成本（有关实施完全自动的、弹性业务环境的最佳实践专业知识、产品和相关的服务）。 企业需要按照业务弹性特色和功能的成本对他们的业务需求进行权衡。

弹性业务环境的实施可以分为几步（见图2）。

图2 通过逐步投资实现完全自动化的业务弹性



在建立弹性系统时满足四大关键客户需求

实施NEDC的每个阶段都需要不同层次的业务弹性。 比如说，在简化阶段，要求能够以最低的成本从故障（硬盘故障、电源故障，等等）中恢复。 在更先进的动态阶段，需要高度可用而且具有容错能力的完全弹性的信息系统来满足业务服务需求。 动态阶段可能需要自动化的管理服务（政策和流程）对动态资源的管理进行简化。

总之，建立一个充满弹性的全新企业级数据中心需要具备下列前提条件：

1. 灾难恢复计划，产品，策略和流程。 灾难恢复计划和相关的策略及流程能够让企业快速从故障中恢复过来。 这些计划能够在最大限度上减少无法预料的事件造成的影响，让企业快速对故障做出反应，同时在最大限度上减少与此类故障有关的成本、时间和风险。
2. 高可用性和/或容错系统/存储/网络环境。 可用性要求因行业不同而异，但都必须制定相应的计划，确保信息系统具备适当水平的可靠性，以满足24x7的内部需求或法律规定的恢复和正常运行需求。
3. 高可用性/容错监督/管理系统。 企业可用性需要监督和管理。 通过在组件业务系统层次上的可用性管理来提高弹性。 通过对资源进行监督有助于减少故障；而简化管理则有助于降低管理的人工成本。
4. 通过确保业务连续性实现一个在最大限度上减少运行中断的环境。 所有前面的活动都旨在帮助企业在遇到中断性事件时保持业务的正常运作，以及满足相关的法律监管要求。

图3对这四个“关键的客户需求”做了详细说明。

图3：建立业务弹性：4个关键的客户需求

资料来源：IBM公司，2008年7月

将业务弹性融入到全新企业级数据中心设计的三个阶段

如同前面所说的，建立新的企业级数据中心需要三个实施阶段。 每个阶段都对业务弹性具有不同的要求。

简化阶段的重点在于合并和虚拟化、能源评估、高能效系统的部署和电源监控、以及基本的服务管理（系统/存储/网络/应用/数据库监督、资源自动发现以及工作负荷自动化）。

> 在此阶段，从业务弹性/安全角度看，主要重点是实施备份和恢复系统，确保服务器高度可用以及提供安全加密服务。

共享阶段的重点是将系统和存储整合为一个更容易管理的整体（对相似资源进行分组），以便对它们实现进一步的虚拟化和更好的管理。 在此阶段，企业向服务导向的架构进行转变，并对这种架构进行优化，使之提供更好的服务。 环保活动超越对系统环境的评估和监督，将整个数据中心（冷却器、电源管理系统、空调，等等）都包括进来。 而且，由于在此阶段充分利用了以服务为导向的服务提供方法，因此，需要对服务管理战略进行完善，并推出基础的业务服务管理功能。 推出变化和配置管理数据库（该数据库在简化对资源的监督、控制和管理以及信息系统环境向动态阶段的发展中起着重要作用）也很重要。

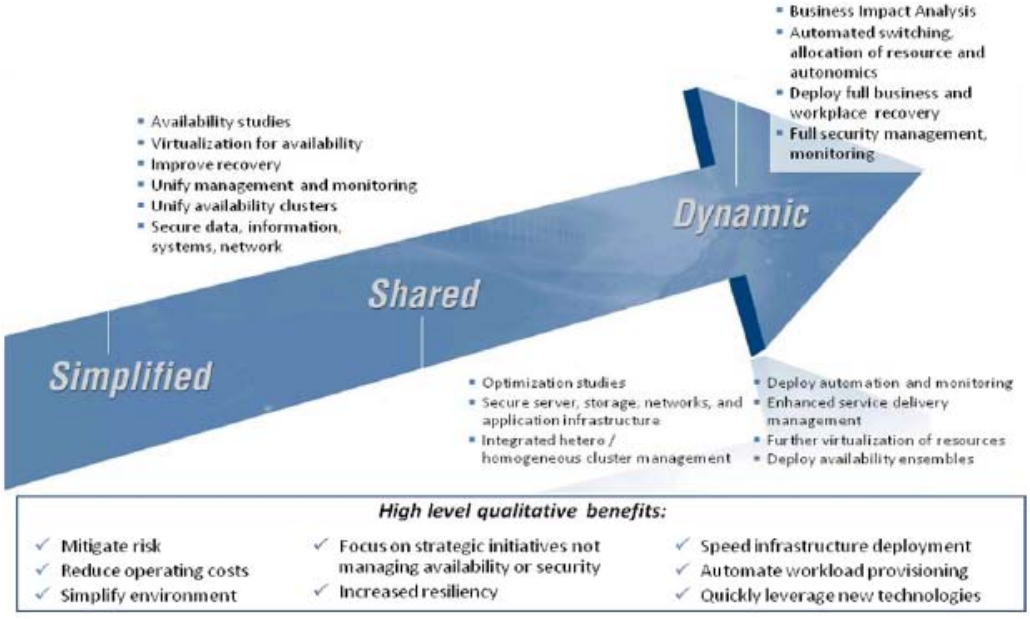
> 在此阶段，业务弹性和安全活动需要把重点放在确保地理上分散的集群能够正常运行；需要建立隔离/完整性/身份安全机制；同时还需要提供业务连续性和弹性服务。

在动态阶段，整个集体被分成多个合作性集合，通过动态地提供资源（动态配置）来满足业务需求。 整个IT环境基本上变成流程流的一个服务点。 在此阶段可以实施高级能效管理，包括根据工作负荷类型对电源进行优化，准时容量交付（未使用的资源可以在不使用的时候关闭），可以通过Internet来实现更高的可扩展性。 在此阶段，服务管理高度自动化：数据中心在节能模式下运行，自动化的资源调度得到协调，可以对复合应用（将各种应用集中起来实现某种业务结果）进行透明管理。

> 在此阶段，业务弹性表现出持续的可用性，持续数据保护和自动归档功能。

有关建立业务弹性NEDC的整个阶段性方法在图4中做了详细说明。

图4－将业务弹性融入NEDC的阶段性方法



资料来源：IBM公司，2008年7月

第3部分：有关建立全新企业级数据中心的循序渐进的指导建议

这部分内容对业务弹性规划“大的形势”做了说明，然后对部署弹性业务系统的5个具体的行动计划做了深入的说明。

图5对业务弹性如何跨越整个企业，到达企业需求，流程支持，应用/数据设计，技术部署以及设施管理做了具体说明。

图5：跨组织的多维业务弹性规划

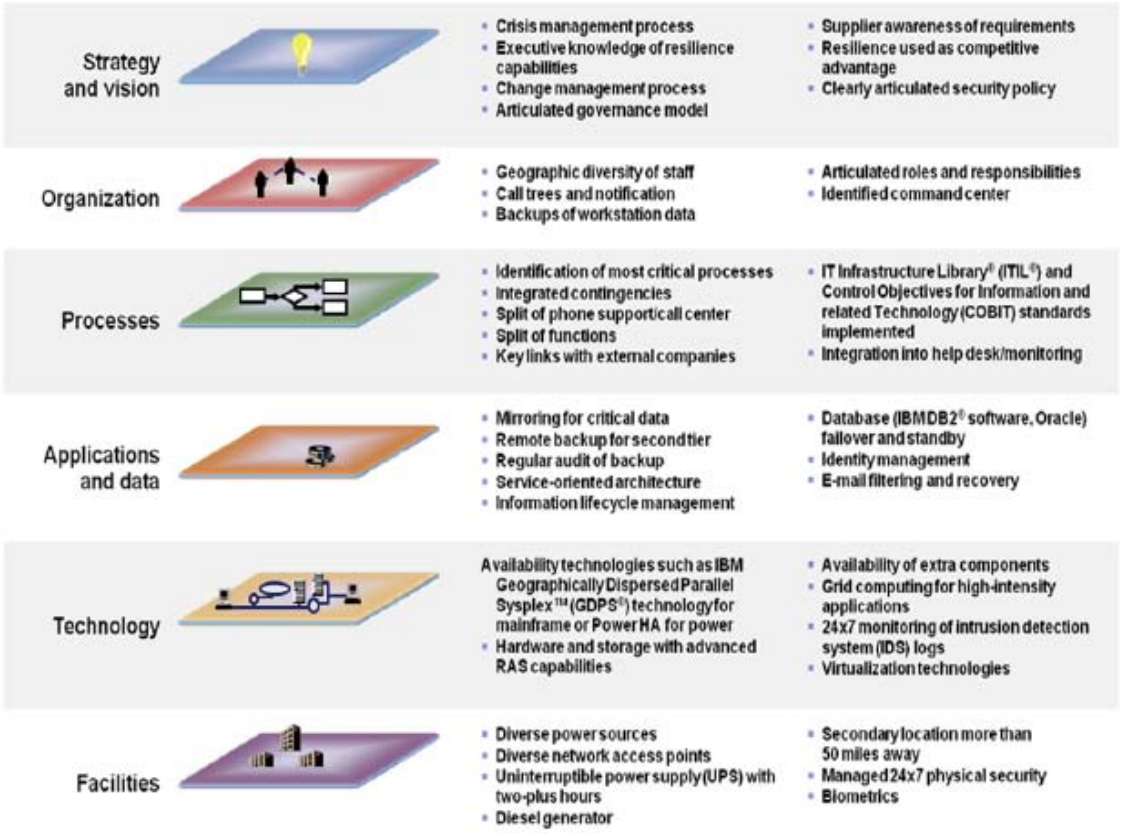


图5中某些关键功能和最佳实践的举例包括：

- 在制定业务弹性战略计划时，类似危机管理、变化管理和安全这些要素以及高层管理人员的支持，都必须考虑到。 而且，需要注意的是，弹性战略的实施往往是为了帮助企业满足相关的要求（有关系统正常运行或服务时间的要求，对在线数据的访问要求）。
- 从企业角度看，需要对员工的地理位置加以考虑，而且，一旦发生业务故障，需要明确规定对业务故障负责的人员角色及其职责。
- 在制定业务弹性计划时，流程流同样也很重要。 流程需要评估，因此，企业如果需要对故障做出反应，最关键的是要制定一个列表，列出哪些流程是最重要的。而且，需要制定应急计划，确保流程流的正常运行。
- 必须对关键数据进行备份，并确保即使在发生故障时关键应用也能正常运行；
- 从技术角度来说，需要决定对哪些应用进行监督（以及应该对哪些应用提供高可用性支持或者容错支持）。 而且，应该制定有关镜像系统的登录、身份认证和安全策略；
- 从设施角度来看，应该提供不同的电源，以及不同的网络连接选项。为了确保信息系统的正常运行，应该提供无间断电源，而且应该在距离主计算站点至少50英里远的地方设立备用计算站点，以应对灾难事故的发生。

循序渐进业务弹性设计需要考虑的因素

在到目前为止建立全新企业级数据中心经验的基础上，IBM建议IT系统设计者/战略规划者在建立完全弹性的业务系统时把重点放在以下四个方面。 这四个方面包括：

1. 对数据恢复进行完善（更快地从意外故障或灾难性故障中恢复回来）；
2. 提高正常运行时间/可用性（提高服务器和应用的正常运行时间和可用性）；
3. 推行企业可用性管理（提高运作效率，缩短故障时间）；
4. 实施一个能够持续运作的业务环境（通过建立一个能够消除故障时间，提供完整的业务恢复功能而且高度安全的高度自动化的信息系统/服务管理环境来实现业务连续性）。

后面的内容对这几点做了更加详细的说明。

提高恢复能力：制定灾难恢复计划

对建立业务弹性而言，首先，也是最重要的一点，就是实施全面的灾难恢复计划。 在制定此类计划时，应该按照以下5个步骤进行：

1. 根据您存在的漏洞、法规遵从需求、业务需求和风险容忍水平来制定计划
2. 制定相应的计划，在灾难过程中降低系统发生故障的风险以及相关的收入损失。
3. 将灾难恢复扩展至新的组件、系统和地点。
4. 将现场、工作场所和整个企业的恢复计划包含进来。
5. 定期对计划进行测试和更新。

提高正常运行时间和可用性：集群、高可用性和容错

一个集群、高可用性和/或容错计划需要通过对应用、系统和业务部门需求进行分析并将可用性要求与具体的业务需求统一起来，对备份/恢复和可用性需求进行评估。 建议方法如下：

1. 按照应用、系统和业务部门的要求对现有实施计划进行评估。
2. 巩固当前实施（集群、虚拟化、自动重启、容错、集合）。
3. 对关键的业务或任务应用采取冗余措施。
4. 支持新的业务需求。
5. 将可用性与业务需求统一起来。

引入企业可用性管理

企业可用性管理不仅意味着对活动进行监督/控制以确保系统正常运行，它还包括有关对需求进行协调、对系统健康状况进行评估的设施，等等。 在实施企业可用性管理环境时，应该考虑以下几个步骤：

1. 对现有的实施情况进行评估，以便进行改进。
2. 设计并实施高度可用的弹性解决方案。
3. 做好需求波动的准备，以便在必要时无缝增加容量。
4. 通过仪表板查看业务性能以及服务和流程的运行健康状况。
5. 充分利用这些信息，按照业务影响确定响应和投资重点。

实施业务连续性环境

IT设计者需要通过对业务弹性水平进行分析（这种分析是它们各自环境内的应用和信息系统所必需的）来开始这一阶段的业务弹性实施工作，并将这些需求与现有的灾难恢复和可用性计划融合起来。 还必须注意信息系统硬件的可扩展性特点以及企业不同应用软件解决方案的可扩展性要求。 在此阶段，IT设计者还应该考虑在提高存储利用率的同时，通过适当的解决方案对存储与信息系统进行整合，以简化管理。 此外，他们还需要制定计划，对信息系统环境的管理实现自动化，一旦发生故障，能够自动启动容灾和业务连续性功能。

因此，这一阶段的5个步骤包括：

1. 按照现有的灾难恢复和可用性计划实施情况对弹性需求进行分析。
2. 设计并实施必要的弹性加强措施。
3. 采用可扩展而且能够适应您业务模式的整合的硬件和软件解决方案。
4. 采用整合的数据恢复和可用性存储解决方案。
5. 通过快速服务器、存储、网络和应用恢复功能实现自动化的系统/站点故障恢复。

提高恢复能力，实现各种层次的可用性，并实施企业可用性管理环境的最终目的都是为了实现一个完全自动的、安全的、弹性的、以服务为导向的信息系统环境。 若想实现这一目标，必须实施上述所有建议措施。

总结

“全新企业级数据中心”是一个旨在帮助企业在对信息系统进行统一，为那些与企业目标密切相关的服务流提供支持的同时降低IT运作成本的模型。 此模型高度依赖于基础计算设施一致而可靠的服务交付能力。 相应地，系统硬件需要保持可靠、可用而且安全。

特别是，新的数据中心模型倡导灵活的IT基础架构，能够对不断变化的工作负荷进行动态地处理。为了确保服务交付，可能需要冗余组件（采用高可用性/容错配置）。还必须建立一个服务管理环境来确保服务交付水平。在整个企业内采取多级安全策略是必要的。最终，可能需要工作场所/数据中心/全面业务恢复服务。

为了确保企业能够从意外故障中恢复回来，IBM强调必须制定全面的业务恢复计划。IBM可以帮助您制定这种全面的计划。 公司的业务弹性背景包括：

- 100%的灾难恢复成功率；

在安全和弹性业务系统设计和部署领域的丰富经验，以及严格的、经过现场实际检验的方法和技术支持；

- 可靠、可用而且安全（RAS）的系统和存储环境，在降低风险（IBM系统和存储具有一流的可用性和安全功能，信息和数据保护功能，提供广泛的全球技术支持，等等）的同时，确保无与伦比的安全和业务正常运行时间。
- 在40年提供高可用性解决方案经验的基础上，拥有行业一流的软件、服务器、存储和操作环境；
- 获奖的软件，一流的硬件技术以及行业一流的服务和容错系统；
- 获奖的安全和隐私软件与服务。（IBM比全球任何其它一家公司拥有的安全和隐私版权都要多）；
- 面向特定地区和特定行业定制设计的、业务弹性和安全性解决方案。

就产品和服务的竞争角度而言，某些供应商只能提供部分这些产品和服务，只有IBM一家供应商能够为客户提供一站式服务，为他们提供全面的硬件、软件、战略规划、部署和测试服务，帮助他们降低运营的复杂性，提高安全性，在整个全新的企业级数据中心确保业务弹性。

Clabby Analytics http://www.clabbyanalytics.com 电话：001 (207) 846-0498 ©2008 Clabby Analytics公司版权所有 保留所有权利。 2008年7月	Clabby Analytics是全球一家独立的技术研究和分析组织，专业从事信息基础设施与业务流程整合/管理研究。有关Clabby Analytics开展的其它研究和分析，见www.valleyviewventures.com

图1

Simplified	简化
Shared	共享
Dynamic	动态
Drives IT efficiency	提高IT效率
Rapid deployment of new infrastructure and services	快速部署新的架构和服务
Highly responsive and business goal driven	高度响应并且以业务目标为动力

图2

Highest investment	最高投资
Recoverable	可恢复
Highly Available	高度可用
Fault Tolerant	容错
Continuous Business-Homo-Heterogeneou	持续业务－同构－异构
Fully Resilient	完全弹性（容灾）
Fully Autonomic	全自动

图3

Disaster Recovery Recover Quickly	**灾难恢复** 快速恢复 • 在最大限度上降低不可预测事件的影响－从次要事件到灾难性事件－目的是更有效地对事件做出反应并最大限度减少系统故障造成的时间和成本损失
High Availability or Fault Tolerant Critical Systems Availability	**高可用性或容错** 关键系统的可用性 • 实现适当水平的可用性，满足日益增长的24×7的企业内部或法律规定的系统恢复和正常运行时间要求
Enterprise Availability Management Manage and Monitor	**企业可用性管理** 管理和监督 • 通过在组件、业务系统和企业层次实施可用性管理来提高弹性 • 通过监督减少系统故障中断 • 简化管理，降低管理费用
Business Continuity Minimize Disruption	**业务连续性** 在最大限度上减少业务中断 • 通过业务连续性规划，在发生对业务造成中断性影响的事件时保持业务持续运作，正常提供服务， 并遵守行业和政府法规要求。

图4

简化	共享	动态
• 可用性调查 • 为实现可用性而进行虚拟化 • 统一管理和监督 • 对可用性集群进行统一 • 确保数据、信息、系统、网络安全	• 优化调查 • 确保服务器、存储、网络和应用架构安全 • 整合的同构/异构集群管理	• 业务影响分析 • 自动化的交换、资源分配和自治 • 全面业务部署与工作场所恢复 • 全面安全管理、监督 • 自动化部署与监督 • 增强的服务交付管理 • 部署可用性数据库
高质量的收益		
• 缓解风险 • 降低运营成本 • 简化环境	• 把重点放在战略性的计划上而不是对可用性或安全的管理上 • 提高弹性	• 提高基础架构部署速度 • 对工作负荷的配置实现自动化 • 快速利用新的技术

图5

战略和愿景	• 危机管理流程 • 管理层对弹性能力的了解 • 变化管理流程 • 分级管理模式	• 供应商对需求的意识 • 作为竞争优势的弹性 • 明确分级的安全策略
组织	• 员工的地域分散性 • 呼叫树和通知 • 工作站数据备份	• 分级的角色和职责 • 确定的指挥中心
流程	• 识别最关键的流程 • 整合的应急计划 • 电话支持/呼叫中心分开 • 职能分开 • 与外部公司的主要关系	• 有关实施的信息和相关技术（COBIT）标准的IT架构库（ITIL®）和控制目标 • 整合至帮助台/监控系统
应用和数据	• 关键数据镜像 • 2层远程备份 • 定期对备份进行检查 • 服务导向架构 • 信息生命周期管理	• 数据库（IBM DB2®软件、Oracle）故障恢复与备份 • 身份管理 • E-mail过滤与恢复
技术	诸如用于大型机的IBM Geographically Dispersed Parallel Sysplex™（GDPS®）技术和用于电力的Power HA的可用性技术 • 带有高级RAS功能的硬件和存储	• 额外组件的可用性 • 面向高密度应用的网格计算 • 对入侵检测系统（IDS）日志的24×7监控 • 虚拟化技术
设施	• 不同的电源 • 不同的网络接入点 • 24×7×365的无间断电源（UPS） • 柴油发电机	• 50英里以外的备份地点 • 管理下的24×7物理安全 • 生物测量技术

通过IT优化实现高可用性

Jean S. Bozman

2008年1月

概述

对保持业务连续性以及为企业最终用户和最终客户持续提供服务来说，一个高度可用的企业系统必不可少。在技术快速变化的时代，实现高可用性（HA）对许多客户来说是一个挑战，他们在众多服务器之间以及整个企业范围内确保高可用性会遇到太多的障碍。

IT转型流程为改善高可用性带来了新的机会，尤其是对涵盖整个企业并且充分利用整个网络中众多服务器计算能力的端到端的应用来说，更是如此。这是因为IT转型为我们开启了以不同方式做事的大门，它打破了阻碍在不同业务单位之间的信息孤岛，实现更加深度整合，并为所有联网的服务器的管理提供统一界面。通过这么做，还可以通过对工作负荷进行合并来减少服务器的数量，从而提高计算效率并节省电力/冷却成本。在IT转型过程中，IT架构得到优化，因此，工作负荷运行的平台能够以最佳的性能和最高的效率为它们提供支持。

那些希望让最终用户能够全年365天实现对关键业务系统24 x 7无间断访问的企业正在研究如何为正在部署的工作负荷采用可靠的服务器和HA软件对重要的应用进行保护。有关这些系统的运作效率对降低有关IT人员时间、系统故障时间以及已部署系统的电力/冷却运营成本来说至关重要。

IBM提供全面的硬件和软件解决方案，确保在众多服务器和存储系统以及众多服务之间保持高可用性，通过高可用性对应用提供全面保护。 特别是，IBM在销售（直接销售或者通过合作伙伴）提供虚拟化、合并和自动化功能的软件的同时还销售具有可靠性、可用性和可服务性（RAS）三大特征的硬件，这些功能都已经内置在平台内。 比较重要的一点是，IBM提供具有先进的端到端的系统管理功能的软件，为整个网络中众多服务器应用提供端到端的支持。此方法旨在确保企业内的最终用户以及最终客户能够持续使用整个IT架构内的数据服务，即使在平台或网络发生故障时也不会受到中断影响，确保业务弹性和业务连续性。

简介

系统和数据的高可用性对企业来说是一个非常重要的目标。企业本身高度关注业务流程（与向最终客户提供商品和服务直接相关的流程）和随时随地接入全球业务系统的能力。此白皮书对这些目标和支持各种应用和业务系统可用性的IT基础架构之间的关系做了说明。

在当今联网的、以Internet为支持的世界里，企业对IT架构随业务变化而改变的能力的期望值越来越高。然而，他们对确保业务流程业务连续性所需要付出的代价还没有考虑。随着支持通过手机、个人数字助理（PDA）和PC实现接入的以Web为支持的系统高级功能的不断发展，人们不禁要问：如何为这种端到端的业务流程提供支持呢？

此白皮书对我们日常看到的业务流程与IT系统（提供数据和业务流程所依赖的业务系统）高可用性需求之间的关系做了概括说明。如何将这些IT系统整合起来是本白皮书的重点内容，因为每个企业都根据自己企业当前的IT技术情况以及企业在利用IT技术方面的偏好来部署自己独特的IT系统。

此白皮书重点关注对当前IT架构进行改革的业务经理和IT经理，他们相信，当前自动化孤岛之间的障碍可以消除，可以将基础的数据和系统联系起来。随着这些情况的发生，我们必须确保通过硬件、软件和服务的组合对系统进行保护，确保高可用性，从而使用户能够在需要的时候随时随地通过网络接入系统。

通过业务合并实现高可用性

全球化、上市速度以及面临降低运营成本的压力都是促使企业需要以高度可靠、可用的方式实现对IT系统访问的原因。我们再也不能说业务与IT之间没有联系，或

者说业务不会受IT的影响。IDC早已观察到这样一个现象，全球许多企业由于认识到计算机对实现新的业务计划的重要推动作用，因此，在制定有关新的业务方向的决策时，都要让业务负责人和IT负责人参与到系统采购委员会。因此，新一代的应用正在得到开发，将原先只存在于特定业务部门的数据散布到整个企业的各个角落。实际上，这些数据往往只局限于那些为它提供支持的IT系统内，与真正需要使用这些数据的系统之间的联系有限。

今天，一系列新的应用开发技术，包括那些针对服务导向架构（SOA）的技术在内，都能够开发出可以在整个企业内对数据加以充分利用的端到端的应用。有关这方面的一个例子是，我们可以通过Web服务器提供Internet数据，通过应用服务器来运行业务线（LOB）应用（例如，ERP、CRM、HR），通过数据库服务器来保存客户数据、库存数据、商务智能（BI）数据以及交易数据。 这种方法能够在整个网络内提供端到端的架构，以一种全新的方式支持任务关键型应用，并且显示当今企业IT转型的方法。当这些服务器通过软件、公司网络以及Internet连接在一起时，当今以Web为支持的企业引擎已经可以立即供业务使用。

一旦这种端到端的应用部署完毕，对其加以保护，防止发生任何类型的中断事故就变得非常重要。其中的某些原因如下：

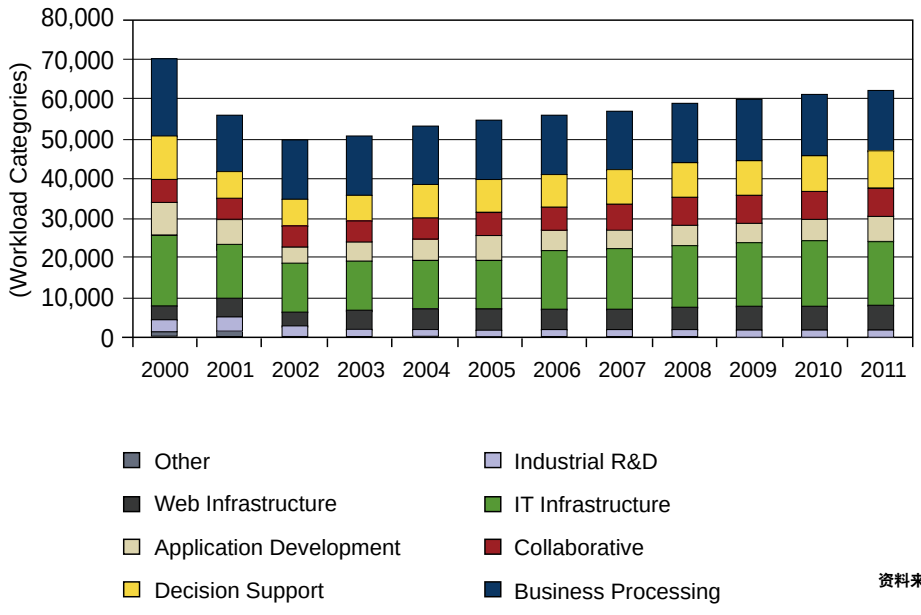
- 端到端的应用如果发生中断或者故障就可能影响对数据的持续访问，使业务运作发生中断，从而影响企业收入
- 导致订单延迟，收入推迟，影响企业盈利能力
- 可能由于客户决定选择其它的服务提供商而失去最终客户
- 对企业当前的业务情况了解不准确

确保业务连续性（避免由于系统故障而造成业务中断影响）的能力是业务弹性的主题，而它是以IT为支持的，确保业务流程（包括覆盖整个企业的端到端的应用）对企业内的最终用户以及企业的最终客户高度可用、可访问。如果支持关键流程的应用和数据不可用，或者性能下降到可能对最终用户造成影响的程度，就会严重影响业务运作。

许多任务关键型工作量很容易识别，包括为银行、制造和零售运作提供支持的系统在内。如果没有这些系统，交易中的业务就会陷入停顿。然而，随着业务流程通过企业网络和Internet与IT服务交付实现整合，应用和数据越来越多地进入业务关键或者任务关键范畴。比如说，许多企业把email看成是一种业务关键型的工作量。这不是15年前的事，而是现在的事，说它是一个任务关键型的业务组件是因为客户通过email发送采购订单或者在持续的email商讨的基础上做出购买决策。

IDC有关工作量类型的数据显示，许多系统能够为现代企业提供支持。从1999年开始每年都开展的这项调查对1,000名或1,000名以上的IT经理进行调查，向人们展示现代企业通过开展哪些工作来为他们的企业运作提供支持（见图1）。

2000-2011年服务器工作量收入预测 (图1)

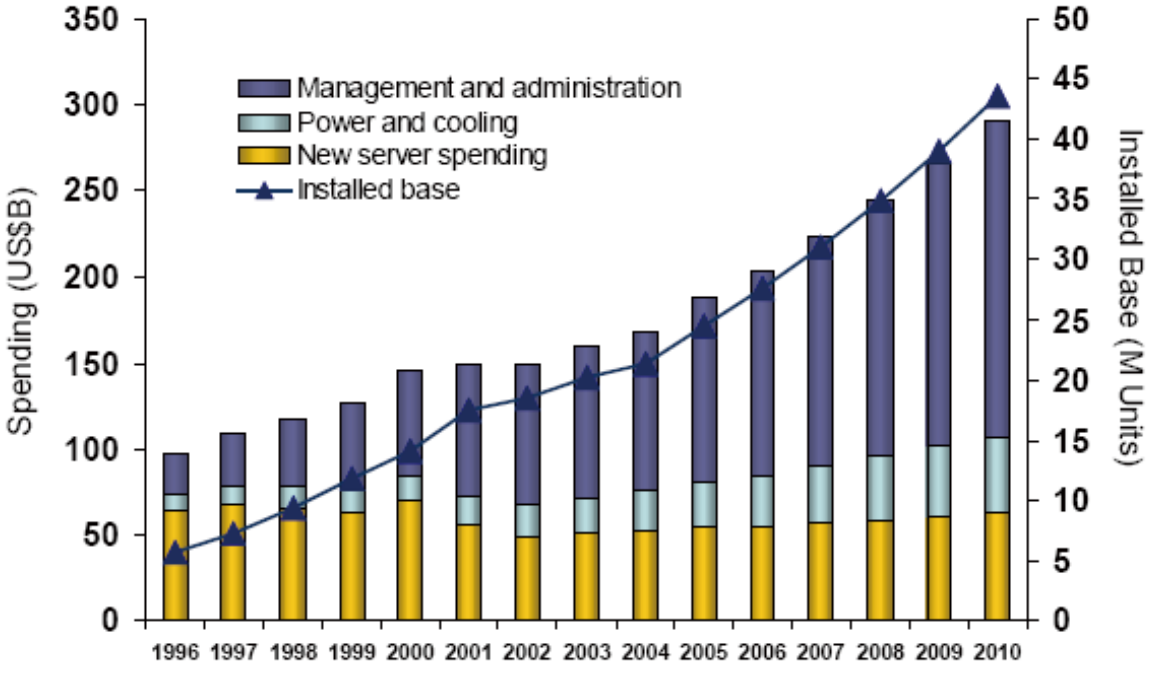


资料来源：IDC，2008年

对高度响应的业务应用的需求正在为高度可用的系统带来新的需求。当IT服务、应用和数据发生中断时，这种中断可能导致业务运作变慢甚至停止。由于这些任务关键型和业务关键型系统响应速度慢或者发生故障不能使用，导致最终用户受到挫折，可能选择在其它地方开展业务。当系统不可用时，任何类型的系统故障都会导致运营成本上升。

从图2中我们可以看到，自1996年以来，IT运营成本一直在上升；从2001年开始，随着小型服务器的增多，成本开始急剧增加。目前，全球已安装的服务器数量在3000万台以上，与1996年的400万台相比增长幅度非常大。不仅服务器数量增多，而且许多服务器的位置都靠近最终用户和客户。

全球已安装服务器的购置、管理、电力和冷却成本 (图2)



资料来源：IDC，2008年

企业必须采取措施来降低他们IT基础架构的运营成本，而且他们目前正在通过多种方法实现这一目标，包括：

- 将工作量合并至更少的服务器，以降低电力/冷却成本和IT管理成本
- 利用虚拟化技术，通过在任何一台服务器平台上完成更多的工作来支持合并
- 通过使用高可用性软件对这些工作量加以保护

上世纪90年代以来，随着Web服务器首次被广泛采用，卷服务器（价格在25,000美元以下的小型服务器）在IT架构中得到快速增长和发展。 2001年这种增长速度进一步提高，当时，有关资本支出的担忧主要集中于如何在小型服务器上而不是在中型和高端企业服务器上部署工作量来降低采购成本。 服务器的这种扩展带来了意外后果，然而，由于系统管理方面的IT人员成本以及大量小型服务器的管理成本高于大型服务器的管理成本，更多可扩展的服务器提供更先进的系统管理和控制以及更多的RAS功能来确保应用的正常运行。

探索降低运营成本的方法

近年来，人们关注的重点有所改变：运营支出比服务器本身的成本增长得更快。企业正在寻找能够降低他们IT部署复杂性的方法，以便降低成本。有关这方面的一些方法包括：

- 降低电力/冷却成本。例如，据IDC估计，目前在新服务器上每花1美元，就需要在电力和冷却方面额外花费0.50美元。2010年，在新服务器上每花1美元，就需要在电力和冷却方面额外支出0.70美元。

- 降低复杂性。客户现在可以选择将多个操作系统镜像合并到更少的服务器上，从而更有效地对它们进行管理。与在独立的物理服务器上对如此众多的镜

像进行管理（每台服务器都可能由于硬件组件故障而导致服务中断）相比，通过这种合并，可以降低运营风险和成本。很重要的一点，通过集群，用户可以在发生故障时将工作量恢复到虚拟服务器上，从而减少由于部署备用物理服务器（这些服务器在“被动”模式而不是“主动”模式下运行）而引发的运营成本。总之，这些用来降低基础架构复杂性的方法提高了IT系统的响应能力，整个企业的任何人在访问这些IT系统时都能确保高度的可用性并且降低业务风险和运营支出。

- 改善物理和虚拟服务器的管理。通过减少需要管理的系统总数，可以简化IT运作并对IT人员配备需求、员工对软件进行升级、打安全补丁以及其它形式的例行维护产生影响。比较重要的一点是，随着管理点的下降，系统故障时间大大缩短。例如，刀片服务器系统以统一的方法对十几个独立的刀片进行管理，从而避免对每台独立的刀片进行布线或者连接电缆。这种方法不仅降低了运营成本，而且提高了一个机箱内所有刀片服务器的正常运行时间。

- 在整个基础设施中实现环保。同时，我们在许多方面鼓励企业“走向环保”：制造业生产的带包装的产品，这些产品的报废回收，以及整个企业的能效，等等。IT转型流程为改变IT基础架构带来了机会，通过将工作量分配到运行效率最高的服务器和存储设备上为“环保”计划提供支持，通过对工作量进行合并来减少服务器的数量。

通过了解IT数据服务对最终用户和最终客户的可用性，企业可以考虑如何对自己当前的数据中心进行改造来提高能效，同时，知道如何将HA功能融入到即将投入使用的硬件和软件中去。 例如，通过工作量合并，将更多的工作量合并到更少的服务器，可以减少企业需要管理的机器的数量，因此使得数据中心的电力和冷却成本将下来。IT优化流程通过将IT资源放到利用效率最高的地方并将工作量映射至适当的系统资源来降低IT部署的复杂性以及运营成本。

在需要的地方实现高可用性

企业以及那些为这些企业提供支持的IT组织该如何着手提高可用性和业务弹性？最好的答案是采取循序渐进的方式，每次只走一步，因为在整个企业内实现高可用性不是通过一个项目或者只在一个站点就能实现的。

相反，它是随着时间的推移众多步骤的结果，通过各种高可用性技术在整个企业内提高系统的可用性，每种技术都与支持的工作量类型以及最终用户有关这些工作量可用性的期望相适应。

不同的工作量需要不同的可用性水平。某些工作量可能需要非常99.999%的可用性，每年只有几分钟的停机时间。其它工作量可以轻松承受数分钟的停机时间而不会对企业造成不可挽回的损失。这里有一系列高可用性解决方案，每个解决方案都必须与它支持的应用适当对应。

对IT基础架构进行改变需要仔细考虑这些改变可能影响到的工作，以及如果这种改变没有解决IT效率问题的话，会造成哪些后果。在“淘汰和更换”战略都被大家摒弃的时代，能够正确识别哪些系统需要立即更新的方法无疑是最有效的。通过打破“信息孤岛”，将它们联系起来，在无需对整个企业范围内多年来建立起来的硬件和软件架构进行淘汰的前提下解决IT低效某些方面的问题。

系统供应商和服务合作伙伴可以提供评估服务并举行座谈会，帮助企业对业务优先级和高可用性/灾难恢复（HA/DR）要求之间的联系以及企业跨越复杂的、多供应商异构环境对现有资产的利用情况进行评估。这有助于帮助客户制定实现可用性目标的计划或发展策略。

一旦制定了对IT架构实现现代化的计划，就必须采取相应的措施将高可用性技术运用到现有的众多服务器、存储和软件系统。高可用性技术非常多，由于某些系统需要在完全无间断的情况下运行，而在其它情况下，通过多台服务器之间的工作量均衡和集群以及数据复制来确保数据可用性，这些都将为业务系统提供足够高的可用性水平。

通过IT合并实现高可用性

随着业务流程通过企业网络和Internet与IT服务交付实现整合，应用和数据越来越多地从非关键范畴进入业务关键范畴。对高度响应的业务应用的需求正在为高度可用的系统带来新的需求。

当IT服务、应用和数据发生中断时，这种中断可能导致业务运作变慢甚至停止。最终客户面对迟缓的响应速度和系统故障而倍感挫折，因此可能决定在别处开展业务。因此，必须对服务水平协议（SLA）概念进行更新，以反映通过Internet向最终客户提供的实时服务的真实情况。

业务的开展地点再也不必局限于实际的业务场所，而是可以通过在线银行服务和在线零售“店面”昼夜不停地进行。在这种业务环境下，如果缺乏对客户的响应能力就可能导致暂时或永久性地失去客户业务，从而影响企业的收入和利润。

业务弹性这一术语指的是企业在提高IT灵活性（应用部署方式）并确保这些重要应用对全球最终客户保持24 x 7 x 365可用的同时对自己业务系统进行改变的能力。通过对服务器进行有效部署，能够让IT组织在多个方面提高成本效益。帮助IT组织实现这一目标的方法很多，其中包括：

- 对工作量进行合并，以节约成本和能耗，这意味着剩下的系统和基础设施必须高度可用，以确保最终用户和最终客户能够对它们进行访问。近年来，大量的工作量已经被部署到机架密集型服务器上，包括面向机架优化的服务器和采用多核处理器的刀片服务器。随着小型服务器密度的提高，使得更多企业应用可以运行在这类服务器上，然而，为了对这些应用提供保护，它同时也增加了对高可用性软件的需求。用户还可以通过其它方式将众多小型服务器上的工作量合并到已经支持高可用性、扩展能力更强的系统上。

- 将某些工作量重新部署至可扩展的服务器上也可以是工作量合并的一个重要组成部分。 对异构、多供应商架构向外扩展是一项非常复杂的工作，尤其是对大型企业来说－许多企业不具备根据自己的业务需求来设计和开发最佳解决方案所需的IT技术和资源。用户还可以通过其它方式将众多小型服务器上的工作量合并到已经支持高可用性、扩展能力更强的系统上。

- 能够让应用跨越IT架构进行移动并且让单台服务器支持更多应用的虚拟化意味着企业可以更有效地利用IT投资。在许多情况下，小型服务器（价格在25,000美元以下的卷服务器）的使用时间只有15%，甚至更低。某些中型企业服务器（价格在$25,000到$500,000之间）的使用时间往往在40%，甚至更低。包括大型机在内的高端服务器（服务器价格在500,000美元或以上）的利用率可以高达90%，为任务关键型工作量确保非常高水平的资源利用率。大型机和Unix服务器中的虚拟化已经非常成熟（见“变革的技术动力”），随着客户希望提高对已安装服务器的利用率，对x86服务器中虚拟化正在加速进行。由于虚拟化能够提高应用或工作量的集中程度，减少服务器的数量，因此，为了确保业务弹性，高可用性支持变得更加重要：确保即使在发生硬件、软件或者网络故障时，业务流程仍然能够正常运行。

- 对资源进行随需向上扩展的能力。随着工作量的增加，应用需要更多的资源－处理器、内存和I/O。在可扩展的系统上，可以随需增加额外的容量，根据季节、时间或者对机器的在线访问量情况满足高峰时期工作量的需求，尤其是通过Web实现的应用（例如，在线银行、有关消费品和零售商品的在线订单）。在向外扩展的部署中，可以通过集群或者工作量均衡的方式增加额外的容量。这一点通常通过采用集群和可用性软件来实现，这些软件通过高速连接和共享的存储将多台物理服务器连接起来。此外，还可以通过集群或工作量均衡软件将多台物理或虚拟服务器连接起来，实现资源扩展，为整个企业内正在被访问的特定应用或数据服务提供支持。另外一种被广泛采用的方法就是在刀片服务器系统上部署工作量，随着应用对处理能力需求的提高增加更多的刀片。

- 高级系统管理功能可以跨越局部或整个企业的IT架构对所有计算层进行管理。整个企业范围的工作量管理在多个层次上都非常有效，它充分利用现有的投资，通过“代理”软件对运行在本地服务器上的工作量进行管理，它还能让企业对整个企业内的工作量进行全面管理。它能够跨越多个地点提高所有被管理工作量（物理服务器和虚拟服务器的工作量）的能见度，全面了解网络和应用情况。这种对所有服务器（包括物理服务器和虚拟服务器）和网络进行可视化的能力提高了它们日常的可用性，而且，随着系统重新进入正常运行状态和数据服务得以恢复，它还能增强为灾难恢复流程提供支持的能力。如果没有它，随着虚拟化在整个企业范围内被越来越广泛地采用，虚拟服务器的蔓延会为系统管理员带来越来越多的挑战。通过对虚拟环境进行更有效地管理，客户可以通过故障恢复对资源（物理资源或虚拟资源）进行更改，在工作量需求需要额外的容量时，对新的虚拟资源进行分配。系统管理软件需要把重点放在全面了解运行在网络上的物理和虚拟服务器，实现可视化的虚拟化，为系统管理员提供支持，让应用持续满足绩效目标和业务部门的SLA要求。由于服务器和存储已经整合在一起，因此，

为了在整个IT架构内为工作量提供支持，这种功能很重要。

- 数据复制。为了保持高度可用，端到端的应用需要访问企业数据。如果通过对多台服务器进行集群或者通过在整个IT架构内对工作量进行均衡将工作从一台服务器迁移到另一台服务器，为了保持工作的正常进行，数据必须保持可用。这就是为什么必须注意在不止一个地点对数据进行复制或者镜像的原因。如果一个数据存储源发生故障不可用，另外一个数据库就可立即接管。这样就保证了业务系统的持续可用性。

- 在整个企业范围内对服务器工作量进行配置。随着新技术的出现，对工作量的配置（在整个IT架构内对工作量进行迁移）比以往更加轻松、简单。有关这方面改进的例子包括：实时迁移功能，该功能可以将工作量从一台服务器迁移到另一台服务器，从一个刀片迁移至另一个刀片，或者从刀片服务器内的一个分区迁移至另一个分区。工作量管理软件为IT提供了一个控制点，用户可以通过它对工作负荷的运行情况进行监督，看它们是否需要额外的资源（处理器、内存或I/O）来继续运行，而且响应时间符合正在被访问的系统最终用户约定的SLA要求。

变革的技术动力

技术的不断发展推动了数据中心的变革。这些技术使得企业开始重新思考如何提高数据中心的能效，改善对工作量的管理，从而降低运营成本。以下是IDC供方和需方（基于客户的）调查报导的全球服务器市场上一些最主要的技术趋势，以及它们对客户部署新IT架构的影响。IT转型流程为客户提供了新的机会，让他们可以充分利用现有的技术并对其加以完善，在降低与IT人员时间、意外故障停机和实时系统管理有关的成本的同时对下一代数据中心进行优化。

虚拟化

虚拟化在大型机上已经有40年的应用历史，在Unix服务器上有近20年的应用历史，它能够更有效地对系统资源加以利用，在让工作负荷运行在可用计算资源上的同时对这些系统的IT投资加以保护。

最近，在来自VMware, XenSource和Microsoft的ISV产品（这些产品为x86服务器增加了管理程序，支持多操作系统镜像运行在同一个服务器平台上）基础上，x86服务器领域掀起一股新的虚拟化浪潮。此流程能够将更多应用和工作负荷集中在同样的服务器上，从而增加每个虚拟化服务器平台对高可用性的需求。在其它类型的结构上，由于系统的逻辑视图已经抽象化，因此，系统平台已经高度虚拟化（例如，基于RISC的服务器和大型机）。就已经实现的虚拟化而言，对工作负荷进行配置现在变得更加简单，因此，工作负荷可以从系统的一个区域移动到另一个区域。新技术还可以让工作负荷从一个系统移动到另一个系统，从而实现在数据中心层次上对工作负荷进行配置和重新分配。

合并

随着为了保持特殊架构所需的成本和复杂性的上升，使得企业运营支出不断增加，在与新的虚拟化技术结合时，这些合并工作将为客户带来巨大的投资回报。如同前面所说的，随着更多的应用或工作负荷通过机架密集型服务器来处理，只会提高对工作负荷保护的需求，并且要求在必要情况下能够从其它资源对这些工作负荷进行恢复。在高度可靠的硬件平台（这些平台通过RAS功能以及高可用性软件解决方案加以保护）上进行合并的能力是全面、整合的高可用性方法的一部分。

走向环保

同时，我们在许多方面鼓励企业走向环保：制造业生产的带包装的产品，这些产品的报废回收，以及整个企业的能效，等等。通过了解IT服务的可用性，企业可以考虑如何对自己当前的数据中心进行改造来提高能效，同时，知道如何将HA功能融入到即将投入使用的硬件和软件中去。例如，通过工作量合并，将更多的工作量合并到更少的服务器，可以减少企业需要管理的机器的数量，因此使得数据中心的电力和冷却成本将下来。

随着IT数据中心的转型（通过跨越各个计算层次的端到端的系统取代“信息孤岛”，将工作量合并到更少的服务器上），企业可以通过向能效更高的平台进行合并来“走向环保”。通过减少服务器数量还可以节约能源，例如，通过让工作负荷运行在有管理的刀片式服务器机箱内的刀片上，可以减少电能消耗。 与采用面向机架优化的扩展槽的服务器（每台服务器都单独布线和架设电缆）相比，通过在刀片式服务器机箱内实现与所有刀片和冷却组件都进行电力连接，以这样的机箱来取代冗余布线，可以降低整体耗电/冷却成本。

IBM产品和服务

IBM系统和技术集团（STG）产品－System x x86服务器，基于POWER的系统（System p、System I和System z大型机） – 提供广泛的可以在整个企业范围

内部署的服务器和存储解决方案，满足各种系统的需求。由于客户需求的变化，客户有关IT技术使用偏好以及各种计算工作负荷需求的不同，这一点很重要。 虽然服务器平台和软件堆栈在企业内随部署情况不同而异，企业需要始终如一地满足每个被支持的应用或工作负荷的可用性需求，同时也要满足整个企业各个业务部门规定的服务水平。

这部分内容列出了IBM旨在满足这些业务和IT可用性需求的硬件、软件和服务：

- x86服务器－IBM System x－ 是IBM与全球主要ISV紧密合作，推出运行在IBM服务器平台上最先进的高可用性解决方案的产品线。这些来自Microsoft, Oracle, Symantec, IBM Tivoli以及其它供应商的高可用性解决方案运行在System x硬件上，可以与由高度可用的设备（这些设备的硬件平台本身具有RAS功能）组成的存储设备（SAN和NAS）进行链接。有关软件堆栈方面，通过打包软件和IBM系统软件以及中间件的组合，形成多层高可用性解决方案，对应用和数据提供可靠的保护。IBM在其大型机和可扩展服务器设计经验的基础上设计System x和BladeCenter产品，包括为数据完整性、安全性固件和软件增加RAS功能，以及通过系统管理对System x服务器的处理能力进行优化。

- IBM POWER系统（System p和System i）是基于RISC的系统，能够支持IBM POWER处理器上的IBM AIX Unix和多个Linux分布，同时支持IBM i5/OS for System i应用。面向大型企业的可扩展POWER系统和面向中小企业的System i能够为客户提供高水平的RAS、安全和高度细致的系统管理。这些系统具有内置的服务器虚拟化功能，支持逻辑分区（LPAR）和工作负荷分区（WPAR），必要时，能够将工作负荷迁移到其它资源上。现在，随着IBM AIX 6 for POWER系统的推出，客户能够通过WPAR在系统内部对工作负荷进行移动，或者将工作负荷移动到其它系统，访问运行这些工作负荷的资源。这种将工作负荷移动到其它资源的能力对发生硬件或软件故障时确保应用的可用性来说非常关键。而且，这种能力对消除“计划维护”的影响来说也非常关键，这种维护往往是影响业务持续运作的一个关键因素。当由于自然灾害、电力故障、网络故障或者人为原因引发其它类型的系统故障时，来自IBM的集群和可用性软件（例如，HACMP、IBM Cluster 软件和IBM Tivoli System Automation [SA] Base）能够将多个服务器节点连接起来，为故障恢复提供支持。对IBM HAGEO来说，还提供地理集群支持功能，根据地理距离来分散服务器节点。

- IBM System z大型机支持Parallel Sysplex集群，将多台System z服务器组合为一个集群，发生故障时，该集群通过Sysplex Timer瞬间切换至Sysplex内的其它资源，从而确保99.9999%甚至更高的正常运行率（每年的故障停机时间低于5分钟）。这就使得Sysplex部署和容错服务器一样在IDC Availability Spectrum、Availability Level 4 (AL4)中处于最高层次，因为最终用户在访问数据服务时不会发生任何中断。System z大型机的IBM Geographically Dispersed Parallel Sysplex (GDPS)配置是为跨越整个企业的端到端的工作负荷提供支持的一个重要组成部分。GDPS支持多站点或者端到端的应用可用性。它与IBM TotalStorage Enterprise Storage Server协同工作，对Parallel Sysplex操作任务实现自动化，并通过单一控制点开展故障恢复工作。此功能能够实现近乎无间断的数据操作，并且在企业架构内各个站点之间确保业务连续性。

- IBM Storage系统支持虚拟化存储，因此，多台服务器可以通过逻辑方式而不是物理方式向“虚拟存储”空间内写入信息。这意味着，这些存储设备可以在整个企业内成为各种服务器的共享存储资源，在每个共享的服务器资源上保留逻辑分区的同时确保应用重启时数据能够恢复。

- IBM TotalStorage Productivity Center。 此产品能够在整个企业内对服务器和存储进行整合配置，以便对新的计算能力进行快速部署。 共享的工作流和常见管理工具的组合使得配置工作比以往更加简单而且高效。TotalStorage Productivity Center充分利用IBM Tivoli系统管理软件的功能来控制数据、结构和硬盘的分配。它充当先前IBM Storage Resource Manager和IBM Tivoli SAN Manager产品的角色，为存储建立一个统一的管理框架。其自动化功能可以减少由于存储管理过程中的手动干预而引发的错误，其工作流自动化功能可以提高存储容量的配置速度。

- IBM System Software。IBM提供众多服务器操作系统，包括面向System z大型机的IBM z/OS, z/VSE和z/VM，以及面向基于IBM POWER的系统IBM AIX和IBM i5/OS。此外，System z支持特种处理器，包

括Integrated Facility for Linux (IFL)，它能够在大型机系统上支持Linux数据库应用（例如，IBM DB2和Oracle Database 10g and 11 g）。此IFL功能意味着目前所有IBM系统（POWER, x和z）都支持Linux，从而让Linux应用对企业来说可以写入并且能够运行在联网的、以Web为支持的计算环境中的服务器上。用于为应用提供服务的IBM WebSphere和IBM Lotus Notes/Domino可以运行在所有IBM服务器的Linux上。

- IBM Management Software。IBM提供管理软件，满足基础架构硬件层和软件层的需求。IBM Director是一个用于对x86服务器系统上的硬件组件进行管理的软件，它与IBM PowerExecutive协同工作来减少“贴近硬件的”电力/冷却需求。IBM Director支持不局限于x86；它还支持其它IBM平台，包括基于POWER的系统在内。IBM Director可以与IBM Tivoli企业管理框架实现链接，在整个企业内对系统管理进行协调。它能够帮助用户从系统层次上了解整个企业以及IT架构的情况。IBM Tivoli软件能够在整个企业范围内支持端到端的管理，在数据中心内部以及在地理上分散的数据中心之间对系统进行链接。此功能支持地理分散的集群，支持在整个企业范围内或者跨越数据中心之间的网络链接对工作负荷进行故障恢复。IBM提供各种IBM Tivoli产品来支持端到端的应用。这些产品包括IBM Tivoli工作负荷管理系列产品、IBM Tivoli系统自动化系列产品、IBM Tivoli配置管理程序，它们是帮助企业对应用可用性进行管理的关键产品。

- IBM Services。来自IBM全球技术服务部（GTS）的主要产品包括：IBM高可用性评估讨论会，旨在对特定性业务需求的可用进行评估，对当前能力进行评估，并制定在跨越多供应商异构环境充分利用现有资产的同时满足这些需求的计划；IBM Geographically Dispersed Open Clusters，提供类似于GDPS的功能，建立一个支持来自多供应商硬件的开放系统环境；以及IBM Business Continuity and Resiliency Services。

挑战和机遇

IBM在提供支持数据和应用高可用性的硬件、软件和服务方面拥有丰富的经验。这些高可用性解决方案面向所有的IBM服务器和存储产品提供，而且，IBM在全球范围为这些解决方案提供支持。此外，IBM还提供软件，包括Tivoli SA Base (集群功能)和Tivoli SA End-to-End（支持覆盖整个企业的端到端的应用），在各种服务器和集群之间提供高可用性支持。随着客户部署的SOA和端到端的供应链应用越来越多，对此高可用性支持进行全面协调的能力将越来越重要。

鉴于IT行业快速变化的市场动态，新技术正在不断地被推向市场。例如，面向x86服务器的虚拟化软件正在被广泛采用，并且为高可用性提供支持，尤其是对有计划的停机和灾难恢复。然而当前正在部署中的许多向外扩展的虚拟化系统没有内置的支持功能，而且x86虚拟化领域的某些软件供应商正在通过与服务器OEM（例如IBM及其服务器竞争对手）合作的方式对他们的解决方案进行扩展，通过ISV为所有的高可用性解决方案提供有关计划内和计划外系统停机的高可用性保护。

对IBM的挑战是，如何向客户表明自己对各种高可用性解决方案的支持能够与建立在卷服务器、中型服务器和高端服务器上的各种企业解决方案实现整合，并且从全局角度实现整合，以简化整个企业的管理。机会在于充分利用服务器和存储系统先进的虚拟化功能向客户展示如何将向外扩展虚拟化与高可用性解决方案结合起来实现业务连续性和业务弹性。IBM还向客户表明自己了解这一挑战的尺度，并且正在向市场推出一系列产品和服务，以便通过更加统一的方法在整个技术范畴内确保高可用性。

结论

企业为了降低与IT人员配备、电力/冷却以及服务器和存储系统故障停机有关的运营成本，正在对数据中心进行转型。这种转型以新的IT架构实施方法为标志，

第三页图

Workload Categories	工作负荷范畴
Other	其它
Web Infrastructure	Web基础设施
Application Development	应用开发
Decision Support	决策支持
Industrial R&D	行业研发
IT Infrastructure	IT基础设施
Collaborative	协作
Business Processing	业务处理

第五页图

Spending (US$B)	支出（单位：10亿美元）
Management and administration	管理
Power and cooling	电力和冷却
New server spending	新服务器开支
Installed base	已安装设备数量
Installed Base (M Units)	已安装设备数量（单位：百万台）

通过这种方法对基础架构进行优化，从而使那些为运行在自身上面的工作负荷提供支持的平台具有更高的性能和效率。

IBM提供相应的硬件、软件和服务，让客户采取全面的方法，通过平台内置的具有RAS功能的硬件在各种服务器和存储系统内确保高可用性；通过先进的端到端的系统管理为众多服务器上的应用提供支持。此方法还能使企业内的最终用户以及使用整个IT架构内数据服务的区域或全球最终客户从中受益。

为什么虚拟化对当今的企业非常重要

2007 年12 月

IBM提供了一套丰富、多样化、并且集成的虚拟化解决方案，涵盖了从x86 系统到System z™ 大型机乃至存储区域网络（SAN） 卷控制器。

在今天的IT领域，唯一不变的就是变化本身。对于一个复杂的企业级IT基础设施来说，要想实现最佳的业务结果，所需要的并不仅仅是部署新解决方案；这还意味着要将IT重新定义成一个多功能的、并且可以随需求一起变化的企业战略工具。

为此，许多企业都追求全局性战略，比如整合－以减少为支持IT服务而所需要的服务器数量－和虚拟化－以解除那些来自特定系统的服务所受的束缚，并用更动态的虚拟形式重新提供它们。

通过整合和虚拟化，企业可以实现更为简单、更为可扩展、更加经济有效、并且可以更加灵活地与新的企业目标保持一致的IT 基础架构。

大约40年前，IBM在特定的背景下（即，在共享大型机上并列运行单独的逻辑分区）率先提出了虚拟化概念。如今在新的背景下，虚拟化又被赋予了新的生命。这些新背景包括：虚拟服务器到虚拟存储，虚拟化环境中的网络和工作站优化，以及应用程序虚拟化。与业务方面的任何重大转型一样，虚拟化也获得了成功，因为它提供了有助于提升业务核心价值的切实优势。通过虚拟化可以：

- 减小IT成本和业务风险
- 提高运作效率和灵活性
- 简化部署和管理
- 增强总体业务弹性
- 使得新型创新成为可能。

随着当今的公司越来越认可虚拟化技术，了解这些技术的含义、它们之间的相互关系以及它们的通常实现方式将具有重要意义。在追求通过融合各种以虚拟化为中心的产品、行业最佳实践和先进专长从而使IT部门更具效率、弹性、灵活性以及更加务实的全局性虚拟化战略中，IBM已成为当前业务领域中的杰出解决方案提供商之一。

IBM提供了一套丰富、多样化、并且集成的虚拟化解决方案，涵盖了从x86系统到System z大型机乃至存储虚拟化以及这些领域之外的范畴。此外，为了充分利用这些解决方案的优势，IBM还可以与客户进行高效合作，共同开发关键业务战略和流程－所有这一切都将以既定的最佳实践作为指导。

IBM还在虚拟化的观念、理论和实践方面积累了长期经验，这些可以追溯到上个世纪60年代以及虚拟化自身的起源。一些竞争对手在拿到合同后会将解决方案的细节外包并且咨询第三方，但IBM不会这么做。这对客户意味着什么好处呢？在战略实施过程中，全面实践所做的承诺，在发生问题时可以用单一标准来回答和解决问题，使新业务流程和技术解决方案之间的联系更紧密。

在IBM的帮助下，当今的企业可以利用在整个组织内全方位改进IT工作方式的过程中发现的许多良机来应用虚拟化技术。

虚拟化可以通过将众多服务器的功能转移到较少的服务器上（整合）从而发挥作用。

什么是虚拟化?

虽然某些形式的虚拟化会比其它一些更为常见，但每一种情况下的总体目标都是相同的：将某种（实际、物理）形式的技术从其原始环境中分离出来，然后用虚拟形式重新提供它。如果实施得当，这种虚拟形式可以提供与原始形式一样的功能，但此外还能大幅度增加控制性和灵活性。简而言之，当目标变化时，这种虚拟版本显然更易于作出适应性变化，因为它已经摆脱了它曾遭受的物理约束。在必须不断修订和调整IT服务或为了满足新需求而必须从头开发IT 服务的商业环境下，这是一个巨大优势。

近些年来，由于服务器虚拟化可以将众多的物理服务器整合成数个可以部署在少量物理服务器上的逻辑服务器，从而受到广泛关注。

服务器整合：当今企业的必然选择

当今的许多最大型组织发现，“服务器的无序扩展”－IT基础架构中的服务器数量快速增长－ 形成了一个与日俱增的问题。虚拟化可以将众多服务器的功能转移到较少的服务器上（整合），从而有助于这些情况的改善。

IBM Systems Director平台管理系列可以增加易用性，同时帮助降低复杂程度和削减成本。

自从上个世纪80 年代中期逐渐用微型计算机替代大型机以来，IT 部门越来越多地将许多服务转移到小型服务器上，并且为了满足不同情况下的特定业务需求而在这些低廉的服务器上部署了越来越多的服务。

但事实证明，这种做法造成了隐性成本和复杂性。不妨想象一下，如果一家企业拥有多个典型的数据中心，每个数据中心可能有1000 台服务器。每台服务器都可能是一个潜在故障点；一旦发生故障，IT 部门就必须花费宝贵的时间来着手处理，而IT 部门往往在时间和预算方面本来就比较紧张。另外，这还会造成停机，给最终用户带来影响。

同样还存在逻辑管理问题。在各种环境中逐一跟踪数以百计的服务器，比如跟踪它们拥有的应用程序和它们提供的服务，是一个巨大挑战。换句话说，当初仅通过部署越来越多的小型低廉服务器来创建越来越多的IT 功能是一种递减回报的战略。在达到某种程度后，管理上的复杂性和其它成本使得所部署的每一台服务器所具有的业务价值越来越低。

或者也可以考虑一下资源利用问题。为了实现最佳的投资回报，企业需要从服务器获得最高的业务价值，但很多服务器在绝大多数时间里都处于闲置状态。但不论服务器是否在完成业务任务，它们都会耗费多种类型的成本，包括管理成本、耗电及散热（必须用冷却系统散热，因此需要更多的能源）。

通过在一台物理服务器上部署多个虚拟服务器，企业级IT部门可以简化管理和削减成本。

这一问题的解决方案是，通过虚拟将多台服务器的功能整合到一台服务器上。例如，一台基于现代x86架构的服务器，比如IBM System x™服务器，可以轻松寄存多个虚拟服务器－ 每一个服务器都在逻辑上独立于其它服务器并且同其它服务器分开。由于每一个虚拟服务器都被添加到主机计算机上，因此其软件会对底层硬件提出要求，这样可以减少空闲时间，并且确保硬件能发挥出尽可能多的业务价值。

这些优势并不只是与硬件/软件有关，因为它们都有直接的业务影响。通过在一台物理服务器上部署多个虚拟服务器，企业级IT部门可以简化管理、削减成本和大幅度提高服务器的灵活性，可以根据新业务目标的需要来转移或修改虚拟服务器。跟踪、更新和维护一台物理服务器要比对多台服务器执行这些工作容易并且省成本。但每个虚拟服务器仍可以有效提供旧模式下需要有专用计算机的服务器所提供的那些服务，这一点对IT基础架构的其余部分非常重要。但对于IT基础架构的其余部分而言，每个虚拟服务器仍可以有效地提供旧模式下需要有专用计算机的服务器所提供的所有服务。

这样一来，从物理服务器到虚拟服务器的蜕变就使得总体业务价值得到大幅度提升。

虚拟化存储方法将存储设备视作抽象资源，可以根据新的业务需求来分配（或收回）。

虚拟化存储：摈弃静态的物理存储，实现动态的虚拟存储

存储是探讨虚拟化概念并体现其业务价值的另一个平台。当今的大型组织需要更多的存储空间来保存比以往任何时候都要多的数据，旨在为这些数据提供支持的旧战略和解决方案已显得力不从心。

例如，我们可以考虑一下部署灵活性方面的问题。增加存储容量的传统方法需要在业务服务器上部署新的硬盘驱动器，这无论从开销还是从时间和能源方面来说，都是一个高成本消耗过程。在这种情况下，宝贵的IT 人才不得不牺牲时间来将当前驱动器上的数据迁移到新驱动器上－ 通常还需要涉及临时性的中间位置－ 然后再重新配置服务器来使用这些新驱动器，而他们原本有可能需要将时间放到更重要的任务上。当企业需要更多存储容量时，这个过程将不得不重复。

另一方面，虚拟化存储方法将存储设备视作可根据新的业务需求来分配（或收回）的抽象资源，而不是硬盘驱动器什么的。借助适当的解决方案，比如IBM的SAN卷控制器，虚拟化的服务器存储系统可以被视作一个笼统的、与物理存储系统在IT基础架构中的位置无关的逻辑池。当IT服务功能需要更多的存储容量时，旨在执行存储分配任务的、并且经过优化的软件和硬件解决方案可以动态分配存储空间。任务要求的越多，它可以得到的也就越多。系统会自动将那些不再需要的存储空间返还给公用池。

IBM全球技术服务可以帮助客户规划、设计和实施先进的虚拟化技术。

就长期而言，这种方案对企业来说显然是合算的，尤其是在管理成本方面。此外，它还具有更快捷和更灵活的特点。它可以用与服务有关的、可配置的逻辑政策来控制，或者由自动监视解决方案（比如可以确定针对如果不为某个数据库服务器提供逻辑存储空间，该服务器很快就可能发生存储问题的解决方案）触发。实际上，虚拟化存储在这种方式下可以被看成一个增加总体业务弹性的工具，因为它提供了用于预见和预防问题而不是等到问题发生再解决的机制。当然，对存储问题作出的最快反应莫过于首先阻止问题发生。监视和虚拟化存储解决方案使得这种想法变成活生生的现实。

这种背景下的虚拟化还提高了投资回报。由于存储系统被视作可分配的资源，因此为服务器或其它依赖存储空间的IT资产购买超过所需水平的存储空间从而“为将来做准备”的想法在很大程度上显得不必要。借助虚拟化，服务器的配置可以显得更为适度，而IT经理也可以放心，因为存储空间在任何给定环境下只需根据任何需要它的给定应用程序或服务即可进行伸缩。

因此，虚拟化在存储领域体现出的总体业务优势类似于它在计算方面表现出的业务优势：降低成本、增加弹性和灵活性、通过自动化来简化管理和增强能力。

网络性能优化领域充斥着众多元素；如果优化是最终希望的结果，那么就必须尽量减少各种形式的潜在性能瓶颈及多余技术。

虚拟化和整合可以为网络优化提供帮助

对当前复杂的企业级IP网络来说，网络优化的重要性与日俱增。在许多情况下，这种优化将涉及某些类型的虚拟化、服务整合或者同时涉及这二者。

假设一家企业收购了另一家企业。两家企业以前拥有完全不同的网络基础架构，涉及到不同的解决方案、配置和拓扑。合并后的新企业若要实现IT性能和弹性目标，则必须预测并解决大量涉及这两个网络的服务质量问题。网络元素需要整合，而他们的IT服务将被连接起来。例如，两个公司可能在公共Internet上利用经过高级加密的虚拟专用网络（VPN）来提供员工和东道组织之间的安全网络访问。根据业务合并的全面程度，这两种不同的虚拟网络实现方法可能需要执行全面的整合和集成。

而仅涉及一个公司的情况也可能具有类似的复杂性。网络性能优化领域充斥着众多元素；如果优化是最终希望的结果，那么就必须尽量减少各种形式的潜在性能瓶颈及多余技术。如果不借助专业分析、不执行网络调整，那么这些难题非常容易造成最终的IT服务水平、可用性和总体业务弹性无法达到最优化。许多处于这种情况下的企业都需要从信任的合作伙伴那里获得专业咨询，以便评估和解决这些这些复杂问题。IBM的网络战略和优化服务是一个广泛的解决方案模型，特别适用于这种背景，它也许可以为上述企业提供一个答案，因为它融合了服务生命周期和IT基础架构的所有元素，因此是一个异常完整的网络优化方案。

工作站功能由一个中央的虚拟主机提供，因此也可以轻松地用集中方式对它们进行监视、管理和备份/恢复。

虚拟服务器使得工作站更加方便和易于管理

当今企业越来越多地使用的另一种虚拟化形式是在虚拟化环境中部署的虚拟工作站。与传统的工作站环境相比，虚拟工作站具有许多显著优势。

传统的工作站环境包含拥有本地存储、本地处理、本地应用程序和本地数据的高端桌面计算机。虽然可以按照需要将它们转用于新的业务功能，但这个过程通常需要IT人员提供新软件和新配置。同样，在将工作站转给其他人使用时也需要调换工作站或用户的位置。从这些意义上看，它堪称实际IT系统实施的“经典”范例：资产被绑缚在专用硬件上，因此相对缺乏灵活性。

相比之下，虚拟环境中的工作站借助全然不同的配置而改善了这些不足。与该工作站相关的整个工作站环境被寄存在远程，可以在IP网络上借助提供该环境的软件来访问。最终用户在一个窗口中访问工作站，以前在实际工作站上提供的应用程序和数据现在将通过虚拟服务器来提供。

这种虚拟化方法可以为最终用户的业务带来相当大的好处。由于处理过程发生在远程，因此不论本地用户的本地硬件性能如何，他们都可以享受到远程主机的高水平

性能。由于虚拟化环境中的工作站是通过网络实现的，因此位于IT基础架构上任何位置的任何用户在理论上都可以访问这些工作站；事实上，一个虚拟工作站可以供多名位于完全不同的地理环境中的人员使用。

从IT人员的角度上看，其优势也同样明显。与传统的桌面环境相比，虚拟环境中的工作站更易于创建、配置和部署。此外，虚拟工作站功能是由一个中央的虚拟主机提供的，这意味着可以轻松地用集中方式对它们进行监视、管理和备份/恢复。

其优势叠加在一起为：极大地简化了IT人员的管理工作；使用户可以获得更高的性能和更大的便利；并且为企业创建了更灵活、更强大的解决方案。

IBM虚拟化解决方案和服务：在现场解决业务问题

IBM与全世界数以百计的公司进行了合作，并提供了娴熟的咨询、专业化的服务或一流的技术，以帮助他们获得通过虚拟化来应对各种业务挑战的全面解决方案。许多公司都成功利用虚拟化和整合来实现了自己的业务目标，这里仅介绍了其中的两例。

“借助p5 系统和DB2®，我们创建了一个可以实现扩展和快速响应以及降低许可证和运作成本的SAP应用环境。” Francois van der Merwe，Pick‘n Pay

Pick’n Pay

Pick′n Pay是一家在南非并且正在全球取得成功的零售企业。该公司有多个品牌，如Boxer、Franklins、Pick′n Pay和Score，经营着500多家大商场、超市和小商场，员工逾40,000人，年收入近320亿南非兰特（约50亿美元）。

Pick′n Pay用一个自主开发的零售系统跟踪配送、销售、库存和财务。该解决方案运行在多个供应商系统上，这使得其扩展成本日趋昂贵，它往往需要新硬件来应付工作负载增加问题。随着Pick′n Pay在南非和澳大利亚的不断扩张，这种提供信息服务的方法开始成为增长的制约因素。

Pick′n Pay选择了纯IBM的IT基础架构。该基础架构基于2台IBM System p5™ 590服务器和1台p5-550服务器，运行IBM AIX 5L™ v5.3，并且采用IBM System Storage™ DS8100存储系统。“通过增加服务器来实现增长是一种费力而不讨好的扩展方法”，技术运营经理Francois van der Merwe评论道。“过去，随着应用工作负载的增加，我们会将工作负载转移到新服务器上，但这蕴藏着未知风险和延时问题。”

“p5解决方案赋予了Pick′n Pay根据需求进行扩展的能力，为此只需添加虚拟服务器和处理器能力，并且没有延迟。当生产工作负载较高时，我们从测试和开发环境向生产环境分配更多的能力，以确保各项工作能够按时完成，而无需添加新服务器来处理临时需求或季节性需求。”

Pick′n Pay的2台p5-590服务器运行SAP零售和SAP ERP软件，每台服务器安装了32颗处理器，并且所有处理器都投入到使用当中。p5-550服务器运行SAP NetWeaver BI，它使用了4颗处理器，可以扩展到8颗。Pick′n Pay借助On/Off Capacity on Demand功能来根据要求添加额外的处理器，从而只需为自己需要的容量付费。

IBM System Storage DS8100负责管理所有SAP应用程序的数据。Pick′n Pay 将使用IBM SAN卷控制器来虚拟化其存储卷。通过这样做，该公司将可以在不考虑物理设备自身的情况下增加、减少和升级其存储池－ 这是在让IT基础架构符合不断变化的业务需求方面迈出的另一步。

“我们的IT目标可以用三个词来形容－‘快速’、‘小型’和‘简单’，我认为我们当前已经实现了‘简单’这一目标。当需要作出新的经营安排时，如果起支持作用的IT 系统足够简单，那么我们有望在短时间内用较低成本准备好系统。” SusumHasegawa, Lawson Inc.

Lawson, Inc.

Lawson, Inc.便利店一天大概要接待700万名顾客。各家商店都秉承“邻近的热门购物地点”这一理念来提供自身的服务。该公司正在以NATURAL LAWSON和LAWSON STORE100等形式和那些从事常规业务的企业一起逐步构建适应社会环境变化的商场。该公司的CIO和IT站信息系统主管Susumu Hasegawa说，“为了在不断变化的社会环境下实现持续增长，我们必须思考如何构建能将通常位于我们客户群之外的购物者吸引过来的商场。为此，我们不仅要改变我们的货物范围，而且还要研究传统零售之外的服务。也就是说，

如果我们不改变我们的经营方式，我们的业务将无法实现持续增长。”

该公司的IT站系统工程领导Yamamoto先生在谈到Lawson的业务支持系统时这样说道：“我们的4个中心曾分布着200多台来自不同厂商的服务器。它们的运营由几个不同承包商负责，没有统一的规则或水平。为了应对高峰期，我们为每个工作系统提供了备用服务器，但这个备用系统完全就是浪费。通过简化这方面的安排，我们不仅降低了成本，而且在需要新系统时还可以加快系统部署。”

Lawson选择的系统是IBM System z。Yamamoto说明了作出这种选择的原因。“我们希望获得一种允许从包含一系列不同服务器的环境中有效迁移应用程序的方法。我们一直重视基础架构的可靠性和集成性，因此物理硬件的耐用性和可靠性也是一个重要因素。此外，通过在System z上用VM设置虚拟服务器，可以用单元形式在上面开发所需的应用程序，并可以根据需求来共同利用添加的CPU，以弥补整个系统中的薄弱环节。这种配置不仅简单，而且还降低了成本。”

Lawson的IT站系统工程高级经理Kobatake先生认为，采用System z的优点之一是便于实现服务器集成。“以前分布在2个数据中心内的大型机应用程序现在被寄存在一个System z 机房内。此外，8个工作系统，包括此前运行在分布式服务器和其它若干系统上的财会、同商店之间的通讯系统、同交易商之间的数据交换系统等，也被迁移和集成到System z上。借助System z，我们可以动态利用每个系统的CPU空闲时间。因此除了应对高峰期外，日常的利用效率也得到提高。批处理时间也被大幅度缩短，这使得财务处理时间仅为以前的五分之一。”

在迁移到System z时，现有的系统职能和响应得以保持，并且采取了旨在实现平稳过渡的措施。广泛的测试和准备使得整个迁移过程几乎没有对用户造成任何不利影响。

Yamamoto说，“主机切换和其它操作可以提前完成。其性价比令人极为满意，这在类似的系统迁移中是不多见的。”

“我们4个中心的集成工作当前已几乎完成了1个，并将继续根据我们的完成计划依次对其它中心进行集成。从现在开始，我们准备最充分地利用System z，并且继续沿用有助于实现集成优势的方法，包括降低总拥有成本（TCO）。”

优化IT：虚拟化如何适应全局性战略

优化IT是一个通过创建高效和动态的基础架构来实现IT投资的最大业务价值的过程。通过优化IT基础架构，可以实现符合业务价值的成本结构改善，获得节能环保型的绿色数据中心，以及实现一个响应及时、可靠、灵活并且可以为实现服务承诺提供支持的基础架构。

为了创建这样的动态基础架构，则需要使用虚拟化技术来整合现有的基础架构，从而允许您增加资产利用率，并且减少物理位置的数量。其它使用虚拟化的活动则能帮助实现标准化（以减少不同架构的数量）和简化（以消除重复的或未得到充分利用的基础架构元素）。实现手工过程的自动化也有助于降低运营成本。通过部署和维持高度可用的基础架构，计划的事件或意外事件便不会影响到关键的业务应用程序和数据。

虚拟化可以帮助降低成本、提高IT资产利用率、增强服务一致性并且提高总体的IT投资回报，从而实现一个优化的IT基础架构。

为什么选择IBM?

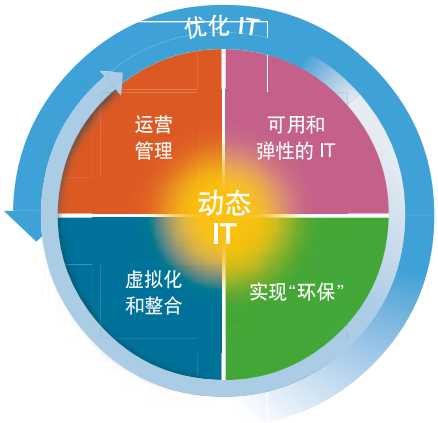
对于那些为了利用整合的、虚拟化的IT基础架构所带来的全部优势而寻找信得过的合作伙伴的组织，IBM提供了一整套服务器、存储、应用程序和工作站虚拟化技术和能力，以及网络优化解决方案－IBM全球技术服务为所有这一切提供了计划、设计和实施先进虚拟化技术的帮助。

在企业级虚拟化解决方案类别中，IBM提供了涵盖不同类别企业功能的多样化套件。

比如IBM服务器就融合了旨在满足各种虚拟化战略需求的一流功能、性能和集成能力。

- IBM System x服务器在行业标准基础上进行创新，提供了带有X-Architecture® 技术的x86服务器。它们运行速度更快，发热量更小，耗电更低，因此是实现虚拟化的理想平台。IBM System x 和IBM BladeCenter® 解决方案帮助降低总成本，以便数据中心可以在最高效率下运行。通过连同使用VMware和其他供应商的管理程序，System x和BladeCenter产品可以提供全功能的企业级解决方案。

- 基于UNIX® 的IBM System p™服务器是用IBM自己的POWER™处理器架构和Advanced POWER Virtualization来驱动的。借助它们最多可以将现有基础架构的成本降低72%。1 IBM System p虚拟化技术，比如Micro-Partitioning™，为实现服务器整合提供了许多令人激动的新机会。
- IBM System i™经过了虚拟化能力方面的专门调整，可以用子系统工作负载管理器、基于POWER-hypervisor的Micro-partitioning以及分区性能自动平衡来管理多个应用程序和过程。
- IBM System z大型机为经过整合及虚拟化的服务器提供了异常高级的性能和安全水平。它们可以同时在完全分开的分区中运行多个单独的操作系统或应用程序实例，从而实现逻辑上隔离的、优化的虚拟化环境。



在IBM System Storage组合的优势中，首当其冲的当属IBM SAN卷控制器（SVC）。它允许企业将存储视作一个可以按需分配和控制的增量资源，从而确保了最大化的服务灵活性以及几乎所有IT 任务的性能和可靠性。借助SVC，当今的组织还可以提高存储系统的利用率，从而充分发挥现有硬盘空间的作用，并且优化依赖存储系统的IT任务的效率。

IBM网络优化解决方案所包括的IBM服务器（比如IBM BladeCenter）通常连同领先提供商的专用网络电话交换机一起使用，以实现网络融合。电话和数据网络在逻辑和物理意义上的组合可以简化管理、降低成本并且利用组织中可能已有的IP架构服务质量专长。

IBM虚拟工作站解决方案，比如Virtual Desktop Infrastructure和Virtual Infrastructure Access Service，利用IBM x86服务器的优势以托管资源的方式重新创建可以在组织中的任何位置访问的物理工作站。在虚拟化环境中可以将工作站提供给网络上的任何用户，哪怕这些用户仅配备了具有最低本地资源的瘦客户端。

IBM软件解决方案旨在轻松地监视、管理和最大限度优化虚拟化技术。IBM以虚拟化为中心的平台管理工具系列（统称为IBM Systems Director）为企业提供了以全局方式协调所有虚拟和物理资源而所需的全面查看和控制能力，通过让业务技术与业务目标保持一致来实现最高水平的灵活性和弹性。这一模块化的、基于开放标准的系列集成并利用了其它相关产品，比如IBM Director、IBM TotalStorage®Productivity Center和IBM Tivoli® Storage Manager，目的是为组织提供服务器和存储系统中所有相关资源的统一视图，并且提供关键类别的信息，如配置、发现、状态监视和自动响应。

但无论解决方案如何能最好地满足您的特定业务需求，虚拟化技术的复杂性和潜在意外都要求一个全面的、整体的、并且旨在最充分利用它们的战略。IBM全球技术服务立足于虚拟化的不同环节而提供了一系列广泛的技术服务。比如，IBM IT改造和优化咨询服务将与您的IT团队一起构建虚拟化计划，以便用最直接和最合理的方式将虚拟化解决方案同您的总体业务目标联系起来。对于分布式IT架构，比如基于x86的服务器，IBM虚拟基础架构访问服务可以借助基于开放标准的模块化方法在不危及安全的情况下帮助您实现从物理到虚拟的转变。IBM 基于POWER的System p服务器具有独特的虚拟化优势，为了确保POWER 架构的这一优势能得到最大程度的发挥，使用该产品的客户可能会考虑IBM的System p实现服务。

总而言之，IBM是在企业级虚拟化领域中拥有得天独厚条件的供应商之一。IBM可以为当今的组织提供一站式指导，以帮助他们迈向完美融合和集成了与虚拟化有关的产品、最佳实践和成熟战略的将来，并借此降低成本和复杂程度，同时提高IT基础架构的利用率。

关于更多信息

如需了解有关整合及虚拟化的更多信息，请联系IBM业务代表或IBM业务合作伙伴，或访问以下网址：ibm.com/systems/optimizeit/cost_efficiency/consolidation/

“应用”在线数据照常迁移

IBM助您实现数据迁移：

- “零”宕机时间
- 任意存储厂商间
- 减少“海量”数据迁移时间
- 过程轻松管理

IBM“不间断数据迁移解决方案”为用户降低数据迁移的成本、复杂性和风险，同时实现业务连续性和客户满意度的大幅提升。

数据迁移 ≠ 应用下线

随着当今社会信息化程度的提高，企业的关键业务对信息系统的依赖性越来越大。这也意味着企业机构对信息系统的稳定性和可靠性的要求越来越高。

同时，随着科技的进步以及企业IT环境随业务需求发生的改变，企业常常面临下列需求：

- 企业需要将IT系统现有数据向新采购的存储设备或集中存储设备转移；
- 企业的数据中心需要进行搬迁；
- ……

通过下图，我们可以看出各种数据迁移需求在整个市场中所占的比例。

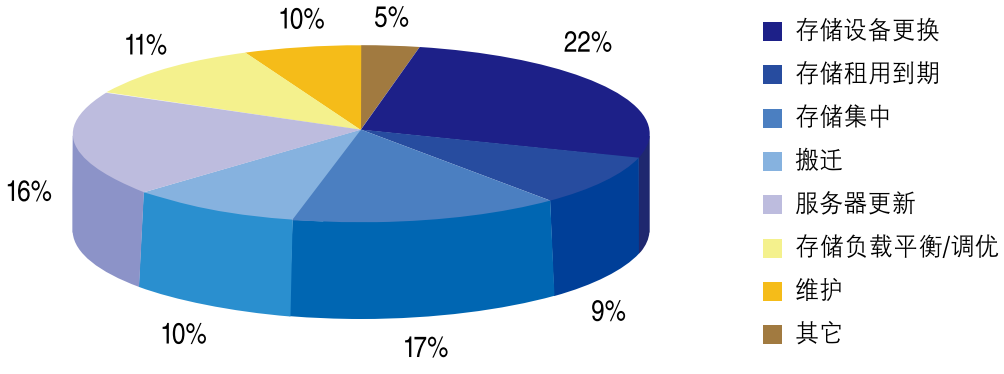


图1 数据迁移需求比例图

下面这张图形象地表达了各种数据迁移需求实施的过程。

下面这张图形象地表达了各种数据迁移需求实施的过程。

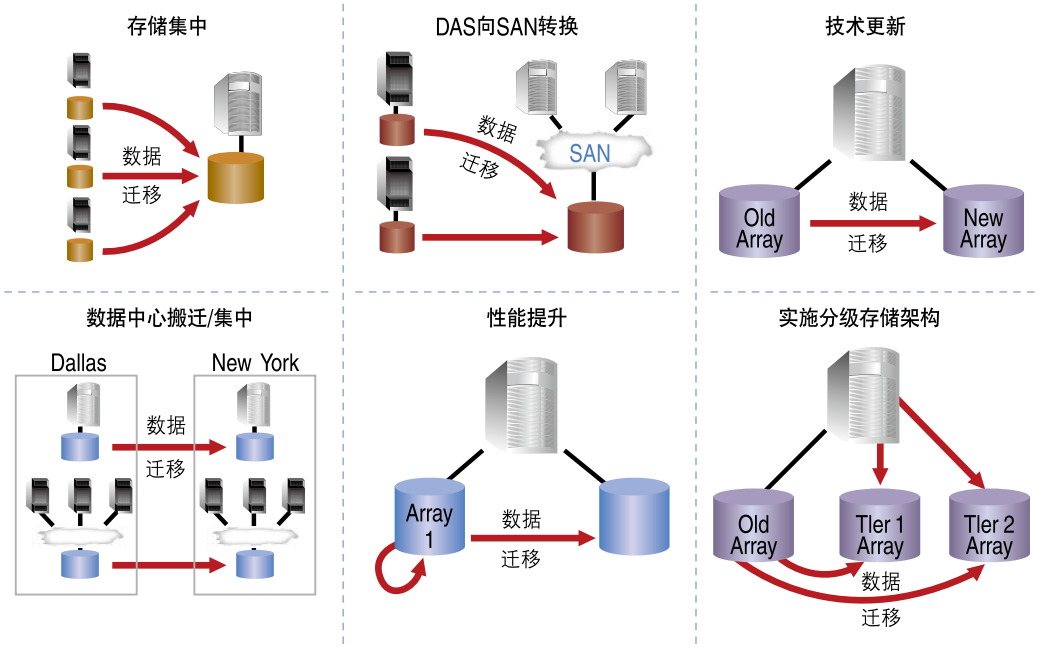


图2 数据迁移需求种类

下面这张图清楚地显示了数据迁移过程中将面临的各种风险：

下面这张图清楚地显示了数据迁移过程中将面临的各种风险：

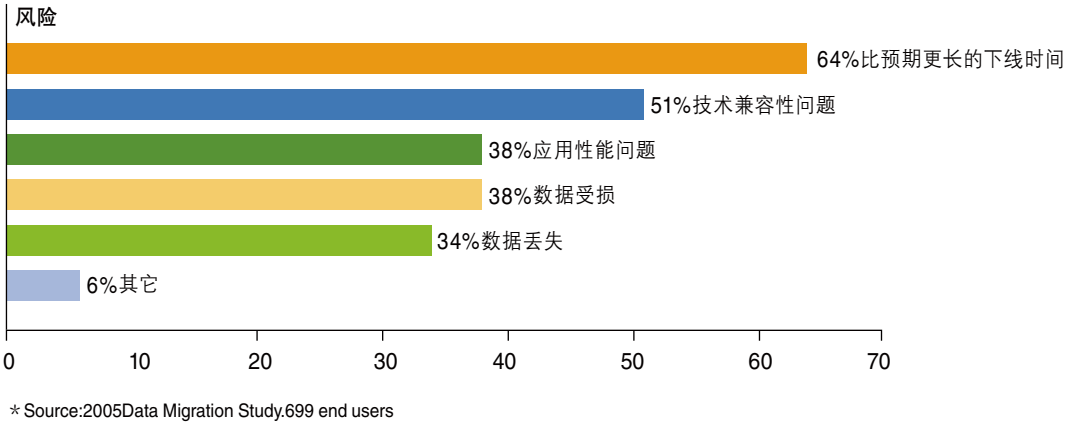


图3 数据迁移风险

在数据迁移层面，海量的业务数据为企业带来下列挑战：

- 数据迁移导致系统停顿时间过长（有时长达数天），给企业业务运营带来极大的不便；
- 数据迁移就意味着应用下线；
- 数据迁移过程中存在数据一致性风险；
- 需要迁移的数据量巨大（TB 级别）；
- 企业同时采用Z/OS、UNIX、Windows等多个平台，数据迁移要跨平台操作，环境复杂，发生错误的机率较高；
- ……

由此可见，数据迁移对企业IT部门来说是一项非常浩大的工程，稍有不慎就会造成难以换回的损失。

IBM数据迁移（Softek TDMF）解决方案能够为您排忧解难。

IBM数据迁移（Softek TDMF）解决方案：

在本方案中，IBM将通过TDMF软件，将您的重要数据从在线磁盘逻辑卷复制到离线目标逻辑卷。在这个过程中，您依然可以对数据进行读、写等应用操作，保障您的业务连续性。

TDMF软件安装非常简便，且支持所有原有文件系统，能够实现跨平台统一界面，有了TDMF软件，您可以不依赖任何存储硬件厂商，轻松实现数据的在线、动态复制。

通过IBM数据迁移（Softek TDMF）解决方案，您将获得的价值有：

- 通过逻辑卷级的数据迁移，获得较高的效率；
- 通过压缩提高传输率，降低数据迁移对网络带宽可能造成的影响；
- 具有断点续传功能，保证数据一致性；
- 数据迁移无文件数目限制。

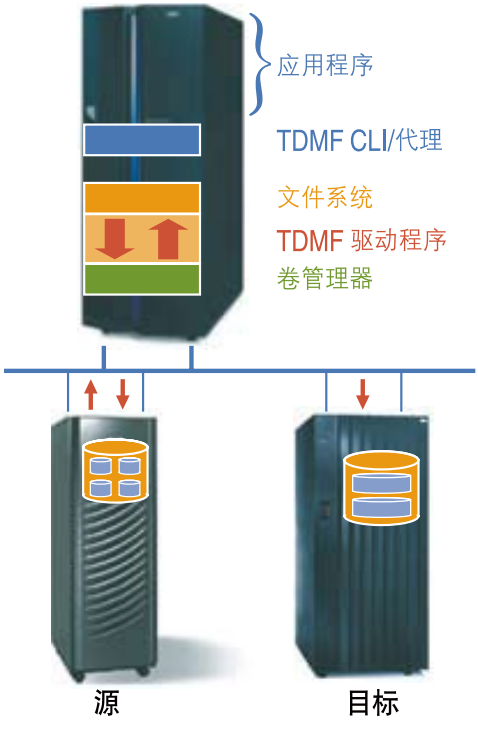


图4 IBM数据迁移（Softek TDMF）解决方案图

针对企业数据迁移过程中的常见问题，IBM——给出了解决之道，免除您的后顾之忧。

常见问题	客户的困扰	IBM数据迁移解决方案目标
间断性问题	数据迁移会造成业务停顿，企业只能选择在周末进行数据迁移。	• 当数据迁移方案实施安装、配置、使用后，应用无需停顿，即可进行数据迁移。 • 动态交换功能确保业务调用逻辑卷已经转换到新的逻辑卷上。
异构性问题	多种不同厂商、不同类型的存储设备混杂使用，在数据迁移前，需要根据其各自的特性制定相应的方案。	**IBM数据迁移方案能够提供：** • 跨不同厂商 • 不同年份存储设备的、统一的数据迁移平台。
业务性能受影响的问题	企业业务系统要求24×7的可用性，否则将会遭受业务损失。	• 在数据迁移过程中，应用继续正常运行。
迁移时间超长问题	大部分数据迁移是手工进行操作的，有时甚至需要持续几个星期。	• 每一个复制命令可以支持多达1000逻辑卷的并行复制。
复杂性问题	当企业对成百上千的逻辑卷进行复制时，存储设备上的任务设置非常复杂。	• ″组″的功能为一组逻辑卷迁移定义了同一名称，从而大大简化了迁移管理。

在数据复制层面，您的企业是否面临以下的问题：

- 企业有数据复制层容灾需求（RTO/RPO小时级）；
- 企业容灾方案预算有限；
- 企业容灾方案要求维护工作简便易行；
- 企业容灾方案涉及多种开放平台（如IBM AIX, HP-UX, Sun Solaris, Microsoft Windows NT/2000/2003,Red Hat Linux，等等）；
- ……

如果您的企业存在上述需求，IBM数据复制（Softek Replicator）解决方案一定能帮得上您的忙！IBM数据复制（Softek Replicator）解决方案具备以下特点：

- 支持服务器之间的数据复制；
- 保证数据一致性；
- BAB（异步缓存）
- Pstore（变化量位图）
- 不依赖于存储设备厂商；
- 数据通过TCP/IP网络传输；
- 支持同步、异步传输方式；
- 支持一对多和多对一的复制方式。

在本方案中，IBM通过复制软件，将应用写入主存储设备的数据同步或异步地复制到备份存储设备中，实现数据的镜像复制（其中异步复制方案可满足生产中心与容灾中心距离较远的环境）。一旦灾难发生时，您就可以通过手工或高可用性软件在备份系统上实现业务接管。

通过IBM数据复制（Softek Replicator）解决方案，您将获得的价值有：

- 业务系统运行的高可用性和业务数据的高可靠性；
- 生产中心、容灾中心两端结构简单，图形化界面易于维护；
- 支持所有开放平台环境（包括IBM AIX, HP-UX, Sun Solaris, Microsoft Windows NT/2000/2003,Red Hat Linux）的解决方案；
- 良好的系统可扩展能力，可从两节点容灾扩充到多节点容灾；
- 高性价比且满足容灾服务需求的解决方案。

IBM全球信息科技服务部（GTS）收购Softek是IBM发展过程中的一个战略性的里程碑。通过此次收购，IBM全球信息科技服务部拥有了一个高效、标准、基于软件资产的服务产品。这一举动非常符合IBM战略发展目标，即将硬件、软件和服务整合销售。

IBM数据复制（Softek Replicator）解决方案：

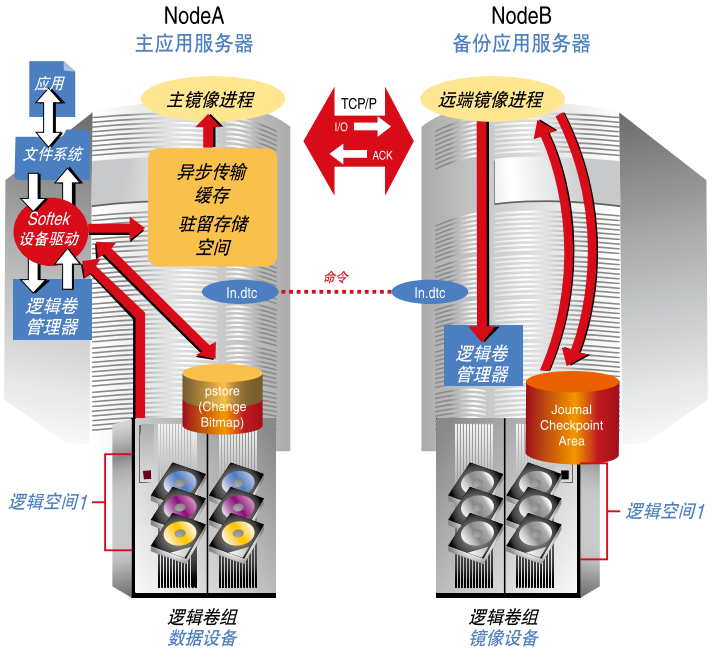


图5 IBM数据复制（Softek Replicator）解决方案图

IBM全球信息科技服务部的宗旨是为客户提供业务与技术服务，帮助用户提升业绩，包括协助用户转型，调整IT服务来满足业务需求。

在IBM收购Softek以前，用户在遇到数据迁移项目时，通常采用凌乱的工具和流程，经常会导致系统应用下线。IBM收购Softek后，将会为用户提供专业的数据迁移服务，保证用户的业务连续性。

现在IBM可以为用户提供在线数据迁移服务，此项在线迁移服务可以跨操作系统平台、厂商进行迁移，并且不受距离限制，全方位满足用户数据迁移需求。

作为存储设备厂商，IBM一直致力于深入了解用户存储的相关需求，诸如存储集中、存储搬迁、存储更新、分级存储架构和异构存储架构的数据迁移，等等。通过将Softek与IBM存储与数据服务结合，能够很好地为用户提供数据迁移相关服务。

Softek作为数据迁移专业厂商，拥有十多年为用户提供关键数据迁移的成功经验，能够为用户提供产品、咨询和支持服务。

Softek拥有成熟的数据迁移技术，包括支持开放系统的TDMF和IBM主机Data set级别的LDMF软件工具包，协助用户实现数据迁移的高投资回报。

Softek在数据迁移解决方案领域拥有多项专利，其丰富的实施经验和客户满意度赢得企业执行层的高度认可。

Softek数据迁移解决方案降低了数据迁移的风险、复杂度和成本，提高了用户应用的可用性。结合IBM方法论和管理流程，Softek统一的跨平台数据迁移解决方案将协助企业大幅提升整体IT管理水平。

IBM加Softek，将为业界提供无可匹敌的数据迁移解决方案。

提供“不间断数据迁移软件平台”，实现简便、统一的数据在线迁移。

IBM企业信息架构—信息保留方案群组

信息保留方案群组

Information Infrastructure Solution

领驭信息架构 创新存储时代

通过IBM CommonStore和DR550实现电子邮件归档

用于保护数据、管理数据并满足法规遵从要求的电子邮件归档解决方案

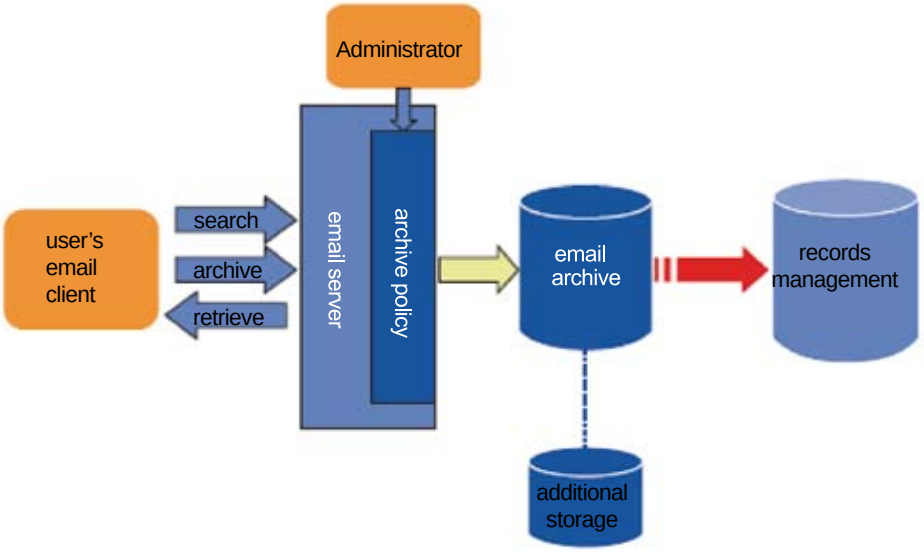
摘要

- 解决电子邮件系统不断增长的问题，包括提高用户响应和保存电子邮件，用于法规遵从、公司经营和法律取证的目的
- IBM提供端到端的解决方案来帮助公司对电子邮件进行生命周期管理

公司经营和法规遵从是电子邮件归档要求的主要驱动力，尤其是在金融服务、医疗保健、制药、公用事业和政府等受到严格管制的行业。然而，大多数电子邮件软件从设计上都不支持对日积月累的大量邮件实施选择性检索。公司日益依靠电子邮件来开展日常业务，致使需要管理和保存的信息量大幅度增加—许多电子邮件中都包含大规模的文件附件，给从未被设计成大型存储库的系统带来了巨大压力。

对于限制信息量的增加对电子邮件系统的影响，IT的做法通常是限制邮箱规模并规定系统在一段时间后自动删除电子邮件。这些做法可能导致企业不能按规章制度的要求将电子邮件保存足够长的时间，或者使用备份磁带代替活动的归档来保存信息，从而可能出现违规问题。

为了摆脱IT部门的限制，用户可能会在自己的PC上创



建本地电子邮件文件夹。当电子邮件被转移到这些本地文件夹时，其他人员便再也无法察看它们。通过这种方式保存的电子邮件在审计或诉讼期间无法使用且IT不能对它们实施终生管理或者适当地删除它们。

对于IT人手有限且预算紧张的中型企业来说，满足越来越严重的电子邮件归档问题尤其困难。

问题的根源是电子邮件数量和规模的激增

电子邮件不仅在数量上快速增加，而且还频繁携带文档、电子数据表、演示文稿、图像及音频和视频文件等附件，使电子邮件文件的规模越来越大。

公司可将这些电子讯息保存在哪里呢？如果保存在电子邮件服务器上，那么，运行、管理和磁盘存储成本都将很高。而且，让电子邮件服务器来管理所有这些电子邮件还将降低系统的响应速度并给IT带来备份和恢复问题。

归档解决方案能够最大限度地降低电子邮件数量激增带来的影响为了最大限度地降低存储成本及其对用户的性能影响，某些IT机构强制实施存储限制或用户必须将电子邮件保留到本地。

但此类策略存在任意删除宝贵信息、过量的文件复制以及难以满足法律要求等问题，这是因为信息保存时间太长或者过于分散而难以被发现。

如果不实施存储限制，则存储成本将大幅度增加。据Enterprise Strategy Group调查，IT机构常把电子邮件视为数字归档的主要驱动力。[1]

电子邮件数量的激增及新规章制度的不断颁布迫使公司实施电子邮件归档和管理战略— 不仅通过保护数据和处理过期数据来降低业务风险，而且还用于控制存储成本并提高用户响应性能。将电子邮件保存在独立于电子邮件服务器的信息库中是实现这些目标的公认方法。将很久以前的电子邮件从高速的高成本的存储设备上转移到低成本的存储设备中，能够帮助企业大幅度降低存储成本。

IBM提供全面的电子邮件归档解决方案

IBM提供卓越的内容管理和电子邮件归档软件来帮助所有机构降低电子邮件的管理成本、满足公司经营要求并简化为法律诉讼而进行电子邮件取证的流程。

IBM电子邮件归档解决方案可帮助IT管理员对电子邮件及其附件进行全生命周期管理，无论是IBM Lotus Notes®还是Microsoft® Exchange环境。这些解决方案包括IBM CommonStore for Exchange or Domino®电子邮件归档软件及IBM System Storage™ DR550系统等。

- IBM CommonStore for Lotus®Domino or Exchange Server，提供强大的电子邮件管理和检索功能
- IBM Content Manager软件，用作信息库
- IBM eMail Search for CommonStore(可选)，设计用于允许授权用户查找用户邮箱并输出结果，以供查看并在法律诉讼中使用
- IBM Records Manager (可选)软件，设计用于提供全面的电子邮件记录管理、审计和报告功能
- IBM System Storage DR550，设计用于提供安全的、可扩展的、经济高效的、基于策略的信息保存系统
- IBM全球服务部或IBM业务伙伴，提供实施服务

IBM System Storage DR550是业界公认的、获奖的存储解决方案，设计用于帮助企业迎接日益加剧的业务信息长期管理和保护的挑战，同时提高运行效率。DR550最多可扩展到224 TB的物理磁盘存储容量，如果连接磁带系统，可提供PB字节的存储容量。

DR550设计用于：

- 通过灵活的存储层级架构来降低TCO。始终将所有的归档数据都保存在近线存储器中成本很高。支持迁移和层级存储架构(磁盘、磁带和光盘)，同时能够长期高效地保存信息是DR550的一大特色。
- 迁移。DR550设计用于支持将数据从磁盘迁移到磁带或者在几代存储产品之间进行迁移，同时维护数据的完整性。迁移工作可以安排在下班时间自动实施、由客户手动实施、或者由您作为一项服务提供给客户。
- 按年代顺序保存数据或基于事件保存数据保存。DR550使用不同策略管理并保存信息，设计用于防止数据在到期前被删除。
- 不可擦除、不可重复写的档案存储器。DR550提供不可擦除、不可重复写的存储控制功能来防止删除或篡改保存在系统上的数据，除非数据已经到期。

- 通过数据加密和数据分割选项提供安全性和数据保护。DR550提供数据加密选项 (128位AES或56位DES技术)来帮助公司保护网络中传输的数据或者保存在磁盘或磁带上的数据。数据在传输前被加密并且在DR550中一直保持加密状态，包括备份拷贝。
- 集成备份。DR550提供固有的免费备份功能，允许您将整个DR550备份到外部磁带系统中。

电子邮件归档同时给IT管理员和用户创造优势

IBM CommonStore电子邮件归档软件设计用于将电子邮件从用户信箱直接转移到外部归档系统中。减少电子邮件服务器保存的信息量可帮助公司通过两种方法提高用户生产率。首先，无限的虚拟邮箱空间无需用户管理自己的电子邮箱的内容，从而加速检索已归档的邮件。同样用户将能够获得速度更快的电子邮件系统响应体验。

归档可帮助降低IT管理成本。如果不归档，电子邮件和附件数量的增加将会影响到电子邮件服务器的效率，甚至失去控制。电子邮件归档可减少必须备份的数据量，从而帮助缩短电子邮件服务器的备份和恢复时间。由于磁带在创建后基本得不到严格控制，因此，从备份磁带中发现并恢复电子邮件是极为复杂的耗时工作，很容易遭到法律诉讼。

将电子邮件归档到IBM DR550等利用不同存储介质(磁带、磁盘、光盘)的存储系统中能够降低长期的电子邮件保存成本，不仅帮助机构减轻主存储的管理 负担，而且还能帮助他们利用高成本的存储资产来更加有效地保存活动数据。

IBM应用设计用于帮助企业满足法规遵从要求并提供法律支持

IBM的三个应用均设计用于提供更多的法规遵从和法律诉讼支持：

IBM eMail Search for CommonStore for Lotus Domino and Microsoft Exchange

这个可选的软件设计用于允许法规遵从或法律人员等授权个人用户搜索用户邮箱并输出结果，用于法规遵从、公司经营和法律取证等目的。使用Web浏览器，这些用户可找出需要保存的电子邮件和附件(因故不能删除)，以便在现在或将来提供法律诉讼支持。

IBM Records Manager

这个可选的应用设计用于提供全面的记录管理以及电子邮件和附件的审计和报告功能，以满足法规遵从要求。IBM Records Manager还帮助公司基于文件记录保存规划来管理电子邮件的存储、维护和处理工作。

由IBM业务伙伴或IBM全球服务部提供

IBM或IBM业务伙伴可为您配置并安装完整的解决方案。

图1

Administrator	管理员
user´s email client	用户的电子邮件客户端
search	搜索
archive	归档
retrieve	检索
email archive	电子邮件档案
records management	记录管理
email server	电子邮件服务器
archive policy	归档策略
additional storage	其他存储器

帮助政府部门迎接归档和存储挑战

作者：Heidi Biggar
贡献作者：Brian Babineau

介绍

现在的记录保留法源自于法律界多年来一直使用的制衡体系。当政府机构制订法律时，记录自法律颁布之日起由立法人员保存。根据这个惯例，美国证券交易委员会及英国金融服务管理局等权威机构已将记录创建和保存规则写入法律中。可笑的是，虽然大多数行业权威机构的数据保存法都适用于电子记录—如电子邮件—但这个流程仍然未被许多政府机构妥善实施。这是因为现在的大多数文件都是电子文档，因此，政府机构发现他们自己也很难做到法规遵从。

数据量的增加也加重了政府机构IT人员的工作负担。随着越来越多的政府机构实现办公自动化，IT的负担也随之加重，长期的数据保存等因素进一步加重了IT负担。对于这一点，我们从为灾难恢复而备份和复制的信息中便可见一斑。

政府机构还必须处理一些特殊的数据访问问题。例如，出生证明、政治演讲稿及地方地图等政府记录有着不同的访问要求。IT机构必须在保存成本和满足数据可用性(或访问)要求间进行平衡。此外，许多政府记录还包含机密和高度机密的信息，要求在整个生命周期(即整个保存期)中始终得到保护。

当政府机构寻求解决法规遵从所带来的数据保存、数据保护和安全问题时，势必会讨论通过多级存储来归档信息(即多层存储平台)。许多私营企业都在使用磁盘和磁带系统结合的方式满足他们的存储需求。这种做法帮助他们实现长期的信息保存，同时满足适当的可访问性和成本的要求。某些情况下，客户都购买多个存储硬件和软件解决方案并且在这些资源之间来回迁移数据。

IBM System Storage DR550大幅度简化了这个流程和成本效率，允许用户根据数据增长的需求在一个系统中通过添加磁盘或磁带(甚至光学介质)来扩展容量。本文将介绍DR550的功能以及为什么说DR550是用于帮助政府机构满足法规遵从要求的理想平台。本文还将列举一些具体的法律要求并阐述政府机构如何解决将来的信息保存和安全问题。

政府规章制度

NARA的角色

几乎每个政府机构都必须创建并保存记录。实际上，这方面的规章制度实在太多，不是一篇文章就能涵盖的。因此，本文只是对它们进行举例说明，首先是美国国家档案记录管理局(NARA)颁布的规则。

NARA负责决定联邦政府工作部门必须保存哪些类型的文档。NARA的机构和规则（决定政府档案记录的生成、传输和保存）(图1)。

图1. 以下规章制度摘录自美国法典，均与NARA和联邦政府记录管理计划相关

规章制度	相关章节的标题/说明
44 美国法典(U.S.C.)第21章第2102小节[1]	**机构。** 政府必须成立独立的执行机构，取名“国家档案管理局”。管理局应该由档案学家负责监督管理。
44 U.S.C.第31章第3101小节[2] (联邦记录法)	**由政府部门主管来管理记录；通用职责。** 每个联邦政府部门的主管都应制作并保存记录，这些记录中应包含足够的、适当的文档，详细记录该部门的组织结构、职能、政策、程序和主要事务，以便提供保护受该部门直接影响的政府及个人的法律和经济权益所需的信息。
36CFRSec. 1220.1[3]	**记录管理计划的责任。** 1984年美国档案和记录管理法补充了记录管理法令，明确分配了国家档案记录管理局(NARA)和总务管理局(GSA)的职责。根据这个法律，NARA 负责提供足够的文档记录和记录处理工作，GSA负责记录管理的经济性和高效性。这个法律在本小节中修改了面向NARA的制度，在41 CFR part 102-193中修改了面向GSA的记录管理制度。联邦政府机构的记录管理计划必须同时满足NARA和GSA的要求。

当政府部门制订自己的记录管理计划时，必须考虑到不同要求。例如，国防部5015.2标准规定，国防部门同时保护和保存机密和非机密的记录。这个规则要求美国国防部的下属任何机构在实施记录管理解决方案之前都必须通过国防部的认证。如想详细了解这个法律，请访问：http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf。

由于信息系统的变化，NARA将法规扩展到电子记录领域—具体说，包括如何保存电子记录以及最终用于保存这些记录的存储介质考虑因素和设施要求等(图2)。这些规则与美国联邦政府的记录管理政策存在一些吻合。

地方政府的义务

在美国，虽然各州有自己的记录维护法规，但他们都执行着某种类型的“阳光法案”。这些法律要求政府提供特定记录供公众查看—如房地产文件及学校委员会会议纪要等。虽然有些记录还使用纸张，但越来越多的数据公布在政府网站上进行共享，以满足信息可访问性要求。将这些信息放到网站上帮助地方政府机构解决了一些运行问题(例如，通过更少的IT人员满足记录请求)。这种做法的缺点是启动并运行这些记录管理系统和相关存储设施给IT人员带来了沉重负担，尤其是人手有限的IT机构负担更大。然而，考虑到这些信息的重要性，政府机构几乎没有选择的余地：他们必须保护自己生成的数据，这是强制性要求。

图2. 联邦记录法与电子记录相关的章节

规章制度	相关章节的标题/说明
36 CFR Sec. 1234.1[4]	本节的适用范围。 本节规定了与创建、维护、使用和处理电子记录相关的基本要求。电子记录中包括数字、图形和文本信息，应记录在可从电脑读取并满足记录定义的介质中，包括但不限于磁介质，如磁带、磁盘和光盘。除非另有规定，否则，这些要求适用于所有的电子信息系统，无论是在微型计算机、迷你计算机还是在主机上，也不论是网络存储还是单独配置的存储。本节还规定了个人用户使用电子邮件创建的、维护、使用和处理要求联邦政府记录。
36 CFR Sec. 1234.10˚	**政府机构的职责。** 联邦政府部门主管应负责确保管理包含以下电子记录： (a) 分配开发和实施整个机构的管理在电子介质上创建、接收、维护、使用和保存的全部记录的记录管理流程的人员职责，将相关负责人员的姓名和职务提交给位于8601 Adelphi Rd., College Park, MD 20740-6001的国家档案记录管理局现代记录计划部(NWM)，以及位于Washington, DC 20505的总务管理局政府事务办公室 (MKB) 。 (b) 将部门的电子记录管理与其他的记录和信息资源管理计划相结合。 (c) 将电子记录管理目标、职责和权力写入相关的部门文件中并在整个部门进行分发。 (d) 制订用于满足记录管理要求的程序，包括记录保存和销毁的要求，然后才去考虑部署全新的电子信息系统或增强现有系统。 (e) 确保对电子邮件系统的用户提供记录保存需求和如何满足记录保存要求、如何区分联邦政府记录和非记录资料、如何分发联邦政府记录、以及如何在部门的记录保存系统中转移或拷贝记录的培训； (f) 确保给电子信息系统的用户提供足够的培训，教授他们如何使用、保护并处理系统中使用的设备、软件和介质。 (g) 针对所有的电子信息系统开发和维护最新的文档记录，要做到：为读取或处理记录规定所需的全部技术特征；识别系统的所有既定输入和输出；规定文件和记录的内容；规定记录的访问和使用限制；了解系统的目的和功能；描述向系统中添加信息、更改系统信息、删除系统信息的周期、条件或规则；确保根据权限及时处理记录。 (h) 规定保存电子记录的位置、方法和介质，以满足运行和归档要求；将电子信息系统的信息保有量维持在一定水平，以促进数据处理。 (i) 开发并确保NARA审批记录销毁时间表，确保实施他们的规定。 (j) 规定对国家机密、敏感和保密信息实施的控制方法，并规定通过电子方式保存和使用受保密法约束的记录的管理方法。 (k) 制订适当程序来确保将本节的要求应用到签约人创建或维护的电子记录上。 (l) 确保满足相关国家制度、程序和标准的要求，如管理和预算办公室、 美国审计总局、美国国家档案记录管理局和美国国家标准局。 (m) 定期审核电子信息系统，确保满足既定的部门程序、标准和制度，满足44 U.S.C. 3506规定的定期审核要求。审核可用于决定记录是否被适当识别和描述以及记录说明和保存期是否满足最新的信息内容保存和使用要求。如果没有满足要求或者系统结构、设计、代码、目的或使用发生的大幅度变化，请将SF 115, ´记录处理权限申请´ 提交给NARA。

图3. 乔治亚州公开记录法中的节选章节

章节	相关章节的标题/说明
§50-18-706	检查公众记录；打印国家房地产契约记录的联机索引；决定允许访问被请求的记录的时间；以电子形式访问记录。 (a) 在本章节，术语“公众记录”指公共机关或政府部门在运行期间准备、维护或接到的所有文档、证件、信函、地图、书籍、磁带、照片、基于计算机的信息或生成的信息、或者类似资料。“公众记录”还指由个人或公共机关或政府部门接收或维护的资料，目的是防止信息被披露。然而，法案规定政府机构严禁将这些资料交由个人或实体保管，以防泄露。由个人、公司或其他私有制实体出于服务或履行义务的原因代表政府机构、公众机构或公众办公室接收或维护的记录可以在一定程度上进行披露，前提是披露程度与这些政府机构、公共机构，或公职人员自己保管资料程度相同。在本文中，术语“政府机构”或"公共机构"或"公职人员"应具有相同的含义，术语“政府机构”的定义见法案第50-14-1章(a)小节第(1)段，此外，还应包括具备以下特征的任何联合会、公司或其他类似组织：(1) 这个州的合格公民或官员组成的机构或主要由县级和市级公司或学区组成的机构或任意组合；(2)机构的主要运营经费由政府拨款.... (f) 管理此类公众记录的个人应有充足的时间来决定根据这个章节的规定是否允许公众访问、查看或拷贝他们请求的记录。无论任何情况，这项工作都不能超过三个工作日。如果公众请求的记录确实存在，但负责人没能在三个工作日提供它们，则必须在这三个工作日中提供此类记录的书面说明以及允许查看和拷贝记录的时间表。然而，倘若这些记录根据本章节的规定不提供给公众查看，则负责人无需提供它们给公众查看或拷贝，或者根据法案第50-18-72章第(h)条规定，向公众说明如果负责管理此类记录的公众办公室或政府机构在这三个工作日内接到州高级法院的命令，通知他们可以根据本章节的例外条例拒绝公众对此类记录的范围请求，则可以不向公众提供此类记录进行查看或拷贝。 (g) 对于请求访问此类记录的个人、公司或其他实体，保存在计算机中的记录应通过可行的电子方式提供给他们，包括互联网访问，同时必须实施合理的安全限制，以防他们访问未请求的或者不可用的记录。

州法律适用于县级和市级政府，通常包括计算机生成的记录。这要求政府机构适当地准备好存储基础设施以便保存房地产契约和建筑图的数字图像及州政府工作人员的医疗保健记录。

国际制度

虽然其他国家的政府机构的结构可能有别于美国机构且法律颁布时间更为久远，但他们也面临同样挑战：电子信息越来越多，必须改造IT基础设施来满足全新的存储和可用性要求。例如，英国有多项法案都要求政府机构出于健康原因跟踪农产品的生产和运输流程，并要求随时提供这些信息以防流行病的爆发。

澳大利亚新南威尔市州也扩展了记录保存制度并为电子记录规定了技术指导原则—都是为了确保信息安全性和规定时段内的可访问性(图4)，包括针对记录保存和相关备案工作给政府部门提供的建议。从技术的角度看，这意味着IT解决方案需要提供审计跟踪功能并满足保存要求，与保存时间长短无关。

图4. 新南威尔市州的数字记录保存制度[7]

章节	相关章节的标题/说明
1. 州数字记录随技术的变化进行迁移。	• 对记录进行例行监视，以便识别出存在数据荒废风险的任何格式。 • 对记录迁移应做好规划、质量控制和记录工作。 • 公共机构应迁移具有长期价值的数据和档案记录为长期稳定的格式，以便在有效期过后它们也不会被荒废。开放文件格式就属于长期稳定的格式。 • 如果记录保存在特殊的或者传统格式中/且系统不支持迁移路径，则必须由公众办公室负责支持它们，直到满足所有的保存要求或者作为州卷宗被转移为止。关于如何给此类记录选择适当保存技术的指导原则，由州档案局提供。
2. 州数字记录的内容和基本特征在数据保存期间不允许更改。	• 应通过测试来检查数字记录的内容和基本特征不受保存流程的影响。 • 公众办公室应负责给不能因保存流程而更改的记录定义基本特征
3. 州数字记录必须保存在上下文中。	• 必须了解信息，并且在整个保存过程中将数字记录的使用与信息相链接或关联。 • 必须记录下数字记录的保存过程。
4. 州数字记录必须是安全的，并且在整个保存过程中必须是可以跟踪的。	• 保存者应实施安全措施来确保正被保存的记录在整个保存期间不会被破坏。 • 必须能够证明在整个保存过程中有完整的监管链。
5. 数字记录的保存流程应该是灵活的。	• 州数字档案应由州档案局保存成字节流和可以迁移的任何其他的格式，以便将来利用这些数字记录。 • 保存机构应尽量将非专用技术作为基本的数字记录保存方法，以免将来因工作变化而丧失对政府拥有的信息的控制权。
定义	• "记录"指以书面、胶片或电子等任何形式编译、记录或保存的任何文档或其他来源的信息。 • "州记录"指公众办公室工作人员在开展任何正式工作时生成并保存或者接到并保存的任何记录，或者指公众办公室出于任何目的开展活动时使用的记录，与发生时间是在本章节颁布之前还是之后无关。[8]

法规对存储的影响

存储介质的要求

新南威尔市州只是为政府机构和政府部门采用电子记录管理制度的全球诸多政府之一。虽然在规章制度中很少说明，但他们将电子记录保存在某些类型的电子介质上进行了规定。制度要求电子介质能够充分和大规模的IT基础设施，政府部门必须考虑到保存期、文件格式、访问和可用性要求及相关的IT成本等因素。

NARA还对政府部门选择存储介质提出了特定要求(图5)。虽然非常全面，但这项法律没有推荐任何类型的技术。然而，法律要求政府部门至少每10年备份一次记录并轮换一次磁带介质，看这个法律无疑从备份的角度，尤其是随着数据量的增加对IT环境产生了影响。

图5. 美国联邦记录法- 电子存储介质

规章制度	相关章节的标题/说明
36CFRSec. 1234.30[9]	**1234.30：电子记录存储介质的选择和维护。** (a) 政府部门应为在整个生命周期保存记录选择适当的介质和系统，满足以下要求： (1) 允许及时进行轻松检索； (2) 将记录与非记录资料区分开来； (3) 以可用的格式保存记录，直到到期为止； (4) 如果介质中包含永久性记录且无法按照本章节第1228.270条的规定将永久性记录传输给NARA，请将永久性记录转移到满足法规要求的介质中。 (b) 选择存储介质或者更换存储介质时应考虑以下因素： (1) 在调度期间决定的记录的保存期； (2) 记录的维护要求； (3) 保存和检索记录的成本； (4) 记录的密度； (5) 检索已保存记录的访问时间； (6) 介质的可移植性(即选择运行在多家制造商提供的设备上的介质)以及在介质间传输信息的能力(例如从光盘到磁带)； (7) 介质是否满足现行联邦信息处理标准的要求。 (c) 机构应避免将软盘作为唯一的介质来长期保存永久性数据或不定期的电子记录。 (d) 机构应对建立或采取程序的外部标记，确保所有授权用户都能识别并检索保存在磁盘、可移动磁盘或磁带上的信息。 (e) 机构在将更换存储介质以满足现有软硬件兼容性的要求时，应确保不会因为更换技术或技术降级而导致数据丢失。开始迁移到不同介质之前，机构必须确定转换之后能够依照权限处理电子记录。 (f) 机构应定期备份记录以免因设备故障或人为错误导致信息丢失。永久性或不定期的的记录副本应保存在与记录原有位置的不同的存储区。 (g) 维护计算机用磁带。 (1) 在将计算机用磁带作为介质来保存定期或不定期的长久保留的电子记录，政府部门应在6个月内检测这些磁带，以便验证磁带不存在永久性错误并且满足美国标准局颁布的标准或行业标准。 (2) 政府部门应在下面的温度和相对湿度条件下对包含永久性记录或不定期记录的计算机用磁带进行维护和检测： 恒温：62 - 68° F。 恒定的相对湿度：35% - 45% (3) 机构每年应检查一次包含永久性记录和不定期记录的所有计算机用磁带卷轴的统计样本，以便发现所有的数据丢失并且找到和排除数据丢失根源。在最多包含1800个卷轴的磁带库中，部门应抽样检查20%的数据或至少50个卷轴。在包含1800个卷轴以上的磁带库中，部门应抽样检查284个卷轴。对于至少存在10处错误的磁带应给予替换，并尽量恢复丢失的数据。对于受相同原因影响的所有其他磁带(如低质量磁带、高利用率、恶劣的环境和处理不当等)，应给予适当的了解和纠正。 (4) 在磁带使用接近10年之前，部门应将磁带上保存的永久性记录或意外生成的数据复制到经过测试和验证的新磁带上。 (5) 对于保存永久性记录或不定期的电子记录的磁带，面向它们的外部标签(或同等的自动磁带管理系统)应对每个卷轴应用独一无二的标记，包括负责这些数据的组织部门的名称、系统名称及安全级别等。此外，对于用于保存永久性或意外生成的电子记录的每个卷轴，标签都应提供以下信息(但不是强制要求)：文件名；创建日期；保存期；记录密度；内部标签的类型；卷宗的序列号；跟踪编号；字符代码/软件相关性；数据库规模；卷轴序列号；文件是否属于多卷轴文件集等等。对于数字的数据文件，还应提供记录格式和逻辑记录长度；数据集名称和顺序以及每个数据集中所含记录数量等信息。 (6) 政府部门应严禁在包含永久性记录或不定期的记录的计算机用磁带的存储间以及测试和评估区吸烟和进食。 (h) 直接存取存储介质的维护。 (1) 政府部门应发表书面规定，要求相关人员根据介质制造商的建议认真处理直接存取存储介质。 (2) 对于用于处理或临时保存永久性或不定期的记录的磁盘或可移动磁盘，它们的外部标签应包含以下信息：负责这些记录的组织单位的名称；内容的说明性标题；创建日期；安全级别及所用软硬件的名称等。

显然，存储系统在长期保存记录方面发挥关键作用。然而，许多政府规章制度都没有特别提到存储系统，导致人们误以为存储系统并不重要。虽然相对某些其他法律而言记录保存法并未得到重视，但却对长期保存信息和存储解决方案的选择提出了要求，是成功的记录管理计划中不可或缺的组成部分。

信息增长与法规遵从的交叉点

据ESG估计，主要的数据库实例年增长率高达25%，非结构化数据和电子邮件的增长率更是高达这个数字的2-3倍，这给IT部门带来了沉重压力—迫使他们在同等IT预算的情况下通过新方法来存储和保护不断增长的存储容量。

政府部门不仅需要处理这些问题，而且处境比其他市场更糟糕。在政府部门，IT经常是事后诸葛亮，尤其是当预算主要用在竞争或新培训计划时。法规遵从无疑是雪上加霜。现在，IT必须处理电子记录。例如，州的水资源部门必须查看电子邮件和电子记录才能去了解水位、水的质量、堤坝安全检查结果、降雨量预测和历史资源合同等信息。

保存这些记录是一个挑战，保护这些记录在保存期间免遭删除和篡改又是另一个挑战。此外，这些记录必须供不同用户访问，包括军人、政府工作人员和普通公民。即使IT知道如何保存和保护所有这些记录，他们仍必须满足信息安全规定。例如，联邦信息安全管理法案(FISMA)具体指出“管理联邦政府信息创建和实施等安全事务的法律、制度和条例必须得到特批并签订特殊契约。”

电子邮件的角色

尽管即时消息传递、社交网络和许多其他形式的协作和信息共享技术不断涌现，但电子邮件仍然是企业和政府机构的关键任务工具。为法规遵从和法律目的而保存、搜索和检索电子邮件仍然是各行各业和各类机构面临的主要问题—政府部门也不例外。此外，随着电子邮件数量的增加，管理员在满足服务水平要求、同时允许最终用户合理访问陈旧电子邮件消息方面面临巨大压力。

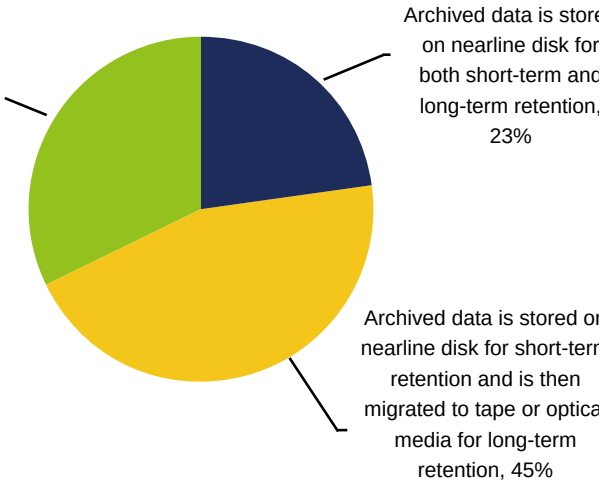
因此，越来越多的机构使用某些类型的由策略驱动的流程来管理陈旧的电子邮件消息的保存和保护工作，从灾难恢复和备份流程(例如，临时拷贝最终将被重写的消息)到消息归档流程(例如，从物理上将实际消息—不是拷贝—从一个系统转移到另一个系统中，以便在不更改或不删除信息的情况下将消息的永久性拷贝保存一段时间)。

过去，包括政府部门在内的许多机构都通过简单的备份流程来满足这些要求。然而现在，越来越多的机构发现要想满足业务优先级和法规遵从要求，他们需要更高级的、基于策略的自动流程和工具，不仅能够长期保存消息，而且还允许他们查找、访问、编制索引并对电子邮件的整个生命周期进行管理。

这个趋势将迫使依靠传统备份解决方案来处理和保存“被请求的电子邮件”的政府机构手动搜索文件，可谓是“大海捞针”。庆幸的是，许多机构都在实施技术和流程来管理长期保存的电子邮件，无论目的是开展业务、确保法规遵从、还是法律或数据/基础设施的管理。

此外，ESG调查发现，虽然许多机构最初都将电子邮件和其他内容保存在某些类型的近线磁盘平台上，77%的已经实施了层级存储战略，在一段时间后将信息从磁盘转移到磁带或光盘上(图6)。原因很简单：使公司在长期经济优势(包括系统、维护、电力和冷却成本)与数据可用性和数据检索之间找到最佳平衡点。

图6. 政府机构/部门选用的归档存储基础设施



来源：ESG调查报告：Electronic Discovery Requirements Escalate, 2007

电子取证也适用于政府部门

电子邮件是在电子取证期间最常用到的信息源。很多人都认为电子取证只限盈利性企业；然而，近期发生的情况证明信息也是政府部门调查时的关键证据来源。例如，美国对于白宫和总统办公室不适当地删除电子邮件记录一事争议颇多，有些白宫工作人员在撰写政治活动文章时提到了创建正式的电子邮件系统，因此他们不希望电子邮件消息被归档。

无论是大型联邦政府机构还是小型政府部门，电子取证都是必须满足的要求。NARA已经对法院如何使用电子记录制订了规则(图6)。电子邮件、合同、就业文件等都是潜在目标。如果再考虑要求政府机构将数据保存30年甚至更长时间的记录维护法以及信息增长等因素，我们不难想象为什么找到所需的电子证据如此困难。

图7. 美国联邦记录法案- 法院对电子记录的使用

规章制度	相关章节的标题/说明
36CFRSec. 1234.26[10]	**1234.26：法院对电子记录的使用。** 电子记录可用作联邦法院的庭审证据(联邦证据法规803(8))，前提是记录保存系统的运行以及系统负责人对其实施的控制值得信任。政府部门应实施以下程序来增强电子记录的法律可采性。 (a) 始终通过相同流程来创建用于生成或保存相似类型电子记录的文档并采用标准的检索方法。 (b) 证实安全程序能够防止非法添加、修改或删除记录并确保系统保护措施能够抵御断电等问题。 (c) 识别终生保存记录的电子介质以及记录在每个存储介质上保存的最长时间，按照NARA的规定处理全部记录。 (d) 与法律顾问、高级IRM和记录管理人员协调满足上述所有要求。

电子取证只是政府部门必须解决的问题之一。此外，他们还必须通过适当的保护措施来长时间确保数据的完整性。这意味着在保存期防止数据被滥用、篡改或删除。电子取证还要求政府部门必须将某些记录保存在更容易接入的存储介质中，如很可能需要频繁访问的记录。

归档的法规遵从和存储优势

需要采用新方法

规章制度、电子取证流程和电子邮件需求都要求政府机构换个角度去重新审视归档问题。调查活动及阳光法的颁布对信息的可访问性提出了不同要求，因此，政府部门不能再将信息全部保存在磁带上，但全部保存在磁盘上从经济上又行不通，尽管磁盘成本不断降低，但仍然非常高昂。最佳做法是基于数据类型和特定的规章制度要求采用多层存储系统。当政府部门为确保法规遵从并且提高总体存储环境的效率而选择存储产品时，还必须考虑到数据迁移和安全。

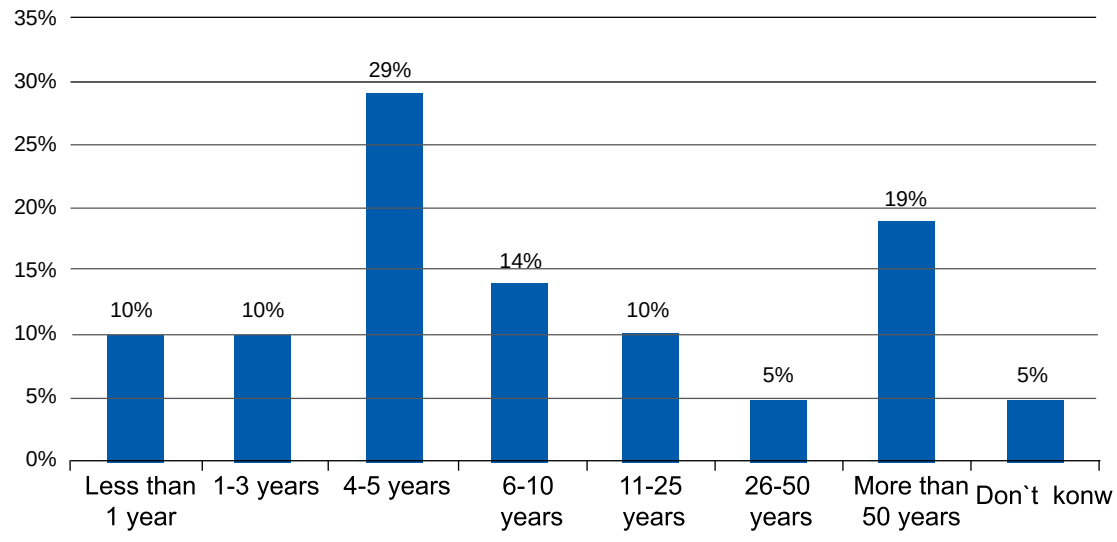
政府机构所部署的归档解决方案应该能够满足现在和将来的数据保存要求、数据真实性和灾难恢复要求、并且从应用(如电子邮件、数据库和文件)和存储(磁盘、磁带、光盘)支持的角度看应该是非常灵活的。IBM DR550允许用户创建灵活的数据归档—允许客户通过技术来满足法规遵从和IT运行要求。

IBM DR550解决主要的法规遵从问题

经济高效地长期保存大量数据

如果综合考虑信息量激增和保持周期延长的情况，我们不难理解政府部门的存储预算为什么会失控。例如，一个政府部门必须将所有的法律会议视频保存10年。另一个政府部门需要不定期地保存某些类型的数据和期间生成的其他数据(图7)。

图8. 归档内容的平均保存期– 政府部门



来源：ESG调查报告：2007年电子邮件数据库/文件归档调查, 11/2007

如何找到能够适应特定记录管理环境的归档解决方案对政府部门来说是个挑战。IBM为政府部门提供两个型号的DR550。2233 DR1是单一服务器单一机柜(25U)系统，提供超过30TB的可用容量，设计用于市县级IT部门等小型政府部门。2233 DR2设计用于英国议会或美国国土安全部等大型政府机构，容量可从8TB扩展到224TB。此外，DR2还允许政府机构实施两个服务器用于实现高可用性，并通过实施同步或异步复制选项来实现灾难恢复。

DR550支持一个档案库使用多种介质(磁盘、磁带和光盘)，可帮助降低归档成本(将数据保存在相应的介质中)并允许政府部门将档案库的容量扩展到PB级字节。数据迁移是由策略或事件驱动的自动流程。通常情况下，陈旧的数据或不常使用的数据都将被转移到磁带中，由Systems Storage Archive Manager (SSAM)负责。SSAM属于IBM TSM软件，是DR550档案库的“中枢神经”。SSAM运行在DR550的集成服务器上，负责定义并执行保存策略并启动数据迁移流程(例如，将数据从磁盘转移到磁带或从磁带转移到光盘中)。

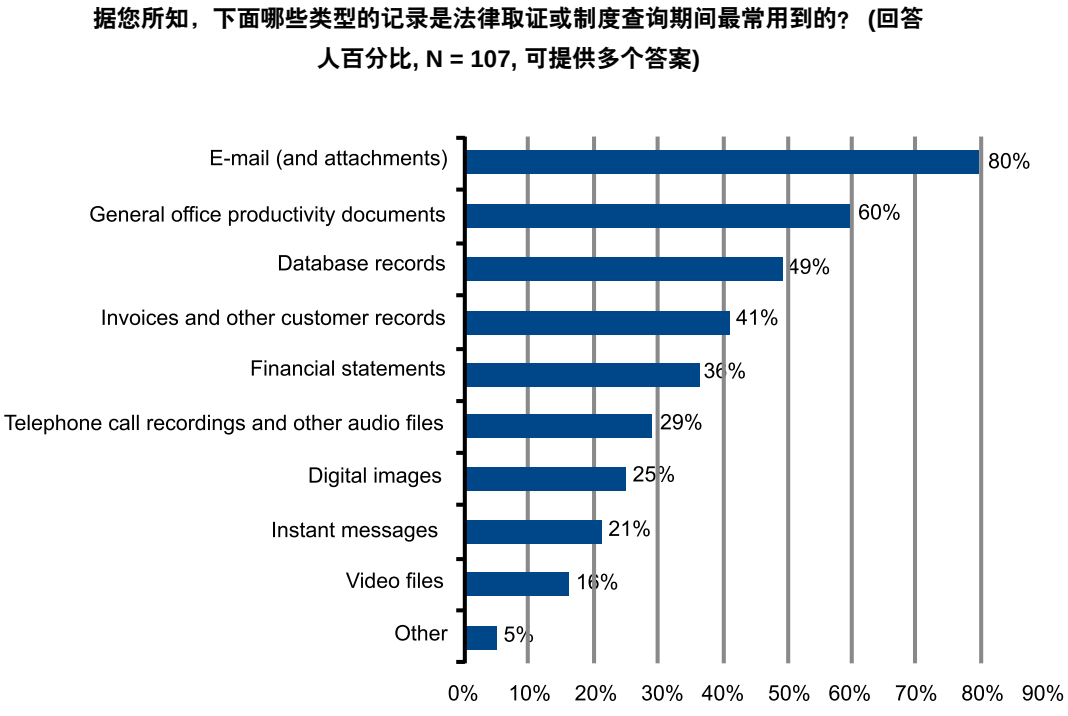
SSAM API与超过40个归档和内容管理应用相集成。其中某些应用已通过美国国防部认证，满足5015.2标准。国防部下属的政府部门可选择联合使用通过认证的软硬件来管理记录。记录的保存期由档案应用决定，由DR550负责执行。这个系统还提供网关功能，允许用户将NFS和CIFS文件放到档案库中并使用SSAM为数据分配保存策略，同时基于策略或特定事件在归档介质之间自动转移数据。

对于政府部门来说，DR550非常灵活，可确保将需要随时访问的数据保存在磁盘中，以供任何人员查询和调查使用；而将从历史的角度看非常重要但访问需求不大的数据保存在最经济高效的介质中；将不经常使用的数据长期保存在磁带中。

II. 集中保存商业记录以便实施一致的管理

政府记录中可能包括影像系统、人力资源管理和其他应用生成的电子邮件、数据库数据和文件。所有这些数据都必须是准确无误的，因为您不知道调查人员会调查哪些来源的数据(图8)。尝试为每个应用部署特定的档案存储系统将给IT带来沉重负担。IBM DR550为所有这些类型的数据创建了集中的多级存储库，从而简化了这个流程。数据迁移由DR550的SSAM自动执行和管理。

图9. 电子取证期间最常用的记录类型



III. 记录的保存和安全性

将记录归档与保留一次已存储的数据完全是两码事。自动执行这两项任务对于政府机构来说至关重要。鉴于政府部门需要保存大量数据，因此，必须自动保护关键业务数据。

DR550提供自动WORM功能，适用于所有存储层(磁盘、磁带和光盘)，能够保护数据免于重写或擦除。这意味着终生保护记录，更重要的是，能够保护在DR550多个层次之间迁移的数据。政府机构可从DR550内部制订记录保存策略，或者直接从数据库、电子邮件或归档应用制订记录保存策略。此外，DR550还支持基于WORM的磁带库。

DR550还提供固有的加密功能，允许政府机构加密数据以保护传输到磁带上的记录。安全特性可帮助政府部门满足FISMA或HIPAA等规章制度的要求，HIPAA虽然是医疗保健行业规范，但许多政府都运行着部队医院，因此也需要满足相关要求。

IV. 保护公司档案

DR550的集成介质管理功能的影响力绝不局限于归档领域。用户可使用SSAM将记录从DR550直接备份到磁带，这个功能非常重要，原因如下：1) 允许用户轻松保护归档文件；2) 无需更多的(备份)软件，因此具有经济高效性。对于小型政府部门来说，保护归档文件时无需添加软件能够缓解不小的预算压力。

对于业务连续性，DR550 DR2(企业级产品)提供可选的同步或异步数据复制功能，为用户最关键的归档数据提供了进一步的保护。这种数据分配方式对于需要转移数据保存位置的政府部门将起到帮助，例如在大使馆或领事馆之间转移数据。镜像任务包含在DR550中。通过在场外同步或异步复制数据， DR550可帮助政府部门确保在灾难时保护关键记录，从而执行业务连续性计划中重要规定。

结语

由于数据量和规章制度的适用范围有所不同，因此，不同机构应采取不同措施来满足信息保留和安全规定。然而，创建并长时间地保存和保护越来越多的电子记录是许多机构面临的共同挑战—政府部门也不例外。

NARA提供对所有政府部门都具有约束力的电子记录管理基准，许多政府部门都已开始采用这个基准。关于如何选择存储介质以及在法规遵从过程中如何依法处理存储记录，新南威尔市州的做法提醒其他政府部门数字记录时代已经到来。

IBM的信息归档和保存战略允许政府机构将信息价值与

存储介质(如磁盘或磁带)相挂钩，从而优化存储基础设施。这种做法允许用户享受到混合解决方案的成本优势。虽然磁盘和磁带的价格近几年不断拉近，但磁带的购买和长期维护成本仍比磁盘低，其供电和冷却效率也比磁盘高。

IBM DR550是归档市场上集成了磁盘和磁带的唯一产品，这意味着产品能够大幅度扩展，更重要的是，能够采用经济高效的方法。政府机构能够经济高效地将数据在线保存更长时间但不会增加运行成本，这是因为软件能够根据策略自动转移数据并备份记录。由于政府记录中常包含国家、州或县的历史信息，因此，通过复制和加密等机制来保护它们同样非常重要。IBM DR550解决方案都能提供这些功能。

欧洲国家一直根据正式法规保存政府记录。美国政府因为认识到了保护关键记录的重要性而在1934年成立了NARA。这意味着创建和保存这些记录的方法发生了巨变，但被记录的信息的重要性始终不变。随着政府部门扩展基础设施来满足现在和将来的法规遵从要求，存储系统将变得越来越重要，最终成为法规遵从计划中不可或缺的组件。政府部门对解决方案的选择将决定他们满足法规遵从要求的效率和效力。

13页的图6：

政府部门现在使用的归档存储基础设施（回答人百分比，N=21）

Archived data is stored on tape or optical media for both short-term and long-term retention, 32%：
将归档后的数据保存在磁带或光盘中，同时用于短期和长期保存，32%；

Archived data is stored on nearline disk for both short-term and long-term retention, 23%：
将归档后的数据保存在近线磁盘中，同时用于短期和长期保存，23%；

Archived data is stored on nearline disk for short-term retention and is then migrated to tape or optical media for long-term retention, 45%：
将归档后的数据保存在近线磁盘中用于短期保存；然后再将它们转移到磁盘或光盘上用于长期保存，45%。

15页的图8：

政府部门保存归档后内容的平均时长（回答人百分比，N=21）

Less than 1 year：不到1年；
1 - 3 years：1 - 3年;
4 - 5 years：4 – 5年；
6 – 10 years：6 – 10年；
11 – 25 years：11 – 25年
26 – 50 years：26 – 50年
More than 50 years：超过50年；
Don't know：不知道

18页的图9：

E-mail (and attachments)：电子邮件（和附件）；
General office productivity documents：普通的办公文档；
Database records：数据库记录；
Invoices and other customer records：发票和其他客户记录；
Financial statements：财务报表；
Telephone call recordings and other audio files：电话呼叫记录和其他音频文件；
Digital images：数字图像；
Instant messages：即时 消息；
Video files：视频文件；
Other：其他

注释

1 http://assembler.law.cornell.edu/uscode/uscode44/usc_sec_44_00002102—000-.html

2 http://assembler.law.cornell.edu/uscode/44/usc_sec_44_00003101—000-.html

3 http://www.archives.gov/about/regulations/part-1220.html

4 http://www.archives.gov/about/regulations/part-1234.html

5 http://www.archives.gov/about/regulations/part-1234.html

6 http://web.lexis-nexis.com/research/retrieve?_m=316c864163ac278a08ba35e2bd022219&csvc=

7 http://www.records.nsw.gov.au/recordkeeping/

8 http://www.austlii.edu.au/au/legis/nsw/consol_act/sra1998156/s3.html#record

9 http://www.archives.gov/about/regulations/part-1234.html

20 Asylum Street
Milford, MA 01757
电话: 508-482-0188
传真: 508-482-0218

vwww.enterprisestrategygroup.com

通过IBM FileNet Image Services和IBM System Storage DR550对影像进行归档

转变基于纸张的记录管理，降低风险和成本

内容要点

- 完全整合的影像归档解决方案不仅能够帮助企业简化了用于eDiscovery或者合规性审计的需求，同时还能实现对影像快速而高效的检索
- 灵活的带有多级存储的影像归档和保留解决方案极大地降低了对海量电子影像的管理成本
- 先进的数据保护技术能够消除数据损坏和环境变化造成的风险，确保关键业务信息在整个生命周期内的完整性

尽管在过去的几十年里我们经历了向电子文档和档案的巨大转变，然而，对许多公司来说，目前开展业务仍然在很大程度上需要涉及到纸质文件。 随着业务的不断发展，产生出了堆积如山的纸质文件，为了避免受到自然和人为的损坏，需要对这些文件进行管理、储存和保护，并且在审计或者诉讼时还要对它们进行检索。 在堆满一箱箱文件的仓库中寻找一份文件不仅耗费大量的时间，而且也是造成了极大的成本浪费。

对许多企业来说，这种纸质文件的不断增长不仅使企业的劳动力和存储成本不断上升，而且还会为企业带来内在的风险，为企业的高效决策、法规遵从和业务连续性造成不利影响。

从纸质文件、影像以及其它对象中提取内容并将它们转变为电子格式有助于帮助企业从纸质文件中获取最大的业务价值，对重要的数据加以保护并降低费用。

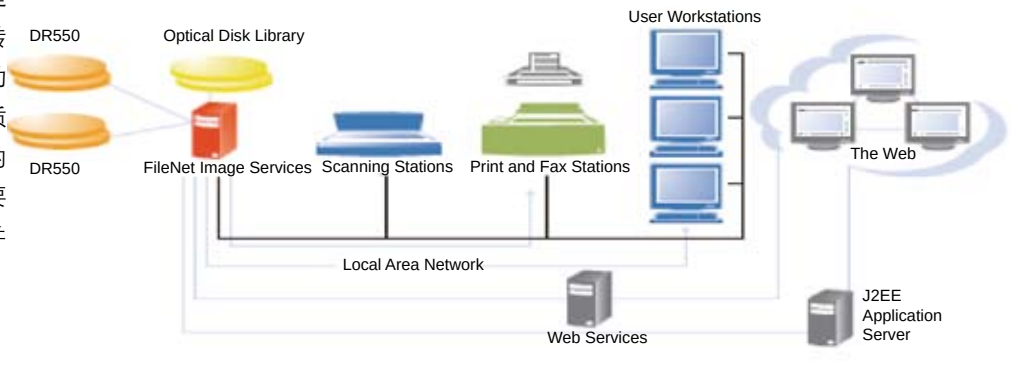
新的扫描技术(如光学字符识别技术)进一步降低了人为干预的需求，帮助企业实现业务的自动化。

分析技术的巨大进步不仅可以帮助企业降低影像获取的劳动力成本，而且还为企业提供了将影像作为业务记录进行自动化管理的新的方法。 尤其是智能的影像采集技术集成了分类技术可以对文档进行自动化分类并声明为记录。 这样就帮助企业将记录管理功能扩展至更深的采集流程，消除了影像采集、储存和记录声明与保留之间的等待时间。

然而，有效的影像归档解决方案必须能够满足州、联邦甚至国际上有关信息可访问性、存储和保留的法律要求。 类似SEC 17a-4、萨班斯-奥克斯利法案和健康保险便利及责任法案（HIPAA）这样的联邦法规以及Basel I 和 II 国际标准都要求对记录进行完整而安全地保管，不得修改。

这意味着任何敏感的资料都可能被法律机构索取或审计，包括知识产权、财务交易或者电子邮件，都必须妥善保管。

IBM FileNet Image Services with IBM DR550



通过IBM解决方案满足公司管理需求

由于未能及时提供文档可能为企业带来巨大的处罚和其它严重的后果，既便是信息的延误、丢失或者意外损坏都不例外。 为了缓解这些风险，企业需要一个完整的、全面的、具有先进记录管理功能的影像归档解决方案。

IBM开发了业内一流的解决方案，它采用一流的内容管理和影像归档软件和硬件，专门满足企业高效数据管理战略的需求。

通过IBM® FileNet® Image Services软件和IBM System Storage™ DR550系统，IBM提供完全整合的信息归档和保留解决方案，旨在帮助企业满足自己的企业管理需求，简化电子取证或法规遵从审计的需求，通过分层存储架构降低对海量影像的管理成本。 IBM全新版本（4.1.1版）的Image Services能够更紧密、更快地与DR550进行整合，实现存储保护。

IBM FileNet Image Services帮助IT管理员在高性能、高度可用而又安全的环境内对影像整个生命周期的进行全面管理。 FileNet Image Manager Active Edition为数千名用户管理大量对象（例如，文档影像、CAD图纸、数据、文本、照片、语音和视频）的同时，提供快速、高性能的检索服务。

优化数据采集，帮助快速决策

通过利用IBM ZeroClick自动化技术将符合行业或公司的标准的敏感文档和e-mail作为业务记录在业务流程前端进行采集，FileNet P8能够帮助企业对关键流程进行优化。 数据可以链接至适当的业务流程处理中，让用户更方便地获取工作所需的信息，也留下明确的审计踪迹。 通过FileNet Image Services与IBM FileNet P8平台的整合，企业可以充分利用原有的投资，轻松利用IBM FileNet Records Management和其它一流的IBM ECM解决方案（例如，业务流程管理和Web内容管理）。

IBM FileNet Capture Advanced Document Recognition (ADR)通过各种方法扩展了IBM FileNet影像解决方案（Image Services和P8）中的流程和合规性能力。 通过先进的文档识别、分类和分隔功能，极大地降低了采集过程中的劳动力成本和风险。 通过对识别、分类和分离实现自动化，可以帮助企业减少海量文档管理中对手动录入的依赖；相反，合规和流程主观可以对例外情况进行审核或接受他们定义的在采集过程中对关键文档进行分类的规则。 而且，通过IBM FileNet Capture与FileNet P8 Records Manager的整合，也可以对扫描的影像文档进行识别、分类并声明为记录，即使在采集流程的初期阶段也能做到这一点。 通过这种独特的功能可以直接对文件管理计划、记录类型和规则进行采集，在采集文档的同时进行ZeroClick的记声明。

通过这种方法，可以在文档进入存储库前作为记录加以保护，从而消除了采集和合规应用之间的延时，有助于降低记录丢失的风险。

针对企业的影像和信息需要接受相关法规法律规定进行保留的话，IBM FileNet Image Services提供了基于策略的完全自动的数据保持。 为了始终对数据进行保护，防止数据受到损坏和意外环境干扰，IBM FileNet Image Services对业务信息的完整性提供全生命周期的保护。

IBM System Storage DR550帮助企业提高运作效率

作为对FileNet Image Services软件强大的影像归档功能的补充，IBM System Storage DR550旨在提高企业运作灵活性的同时帮助企业解决业务信息进行长期管理和保护的挑战。System Storage DR550可以扩展至224 TB的物理硬盘存储容量，而且可以通过附加的磁带存储系统将容量扩展至PB级。

System Storage DR550是一个获奖的、行业公认的信息保留解决方案。 它旨在帮助企业：

- 通过灵活的存储分层来降低总拥有成本。 在整个数据保存期间把所有已归档数据保存到近线存储的成本非常高昂的。System Storage DR550可以在不同的存储级别（硬盘、磁带和光学存储设备）进行迁移分级存储，提高长期高效的数据保留。
- 迁移。System Storage DR550在保证数据安全和一致的前提下，提供了将数据从磁盘到磁带，一级到一级的迁移功能。 数据迁移可以自动进行，也可以设定在下班时间进行，可以由客户来执行，也可以作为一项服务执行。
- 根据时间顺序和事件驱动的数据保留。System Storage DR550根据用户定义的策略对信息以及信息的保留进行管理，在没有满足数据删除标准之前拒绝删除数据。
- 保护存储。System Storage DR550提供不可重写、

不可擦除的存储控制，防止存储在系统上的数据在不符合删除规定的情况下被删除或修改。

- 通过数据加密选项确保数据安全。System Storage DR550提供数据加密选项，可以在通过网络传输数据或者将数据保存至硬盘或磁带时对数据进行保护。数据在传输之前被加密，并且在System Storage DR550中仍然保持加密状态，包括备份拷贝都是被加密。

通过自动化存取来降低风险和成本

通过与System Storage DR550相结合，FileNet Image Services提供了功能强大的在记录的生命周期内的处理和检索的工具。 在完全执行预先确定的安全和版本控制策略的同时，通过自动化的流程对记录进行访问，这样就能帮助企业杜绝数据丢失和违反安全规定的风险，提高eDiscovery的速度，并帮助企业降低人工查找的成本。

作为企业级归档软件和存储硬件领域的市场领袖，IBM影像归档解决方案提供灵活且可以高度扩展的平台。此完全整合的解决方案能够帮助企业：

通过提高灾难恢复能力，更好的安全性和更加完善的存取访问，降低使用和存储纸质记录的风险。

- 通过对业务和记录保持流程进行增强，降低与物理记录存储有关的成本。
- 提高基于纸张的业务处理的可见性，提高业务决策水平。
- 提高工作效率，找回在基于纸张的业务流程中损失的工作效率。
- 最大限度地降低诉讼的风险和成本。

随着法规监管形势的不断发展以及类似照片、语音和视频等这些文档对法律诉讼变得越来越重要，企业需要功能强大的影像归档解决方案来满足相关法律法规的要求。 IBM FileNet Image Services和IBM System Storage DR550能够满足相关行业法律法规约束的、长期数据保存和保护的企业的数据保留的需求。

图1

IBM FileNet Image Services with IBM DR550	带有IBM DR550的IBM FileNet Image Services
DR550	DR550
DR550	DR550
Optical Disk Library	光盘库
FileNet Image Services	FileNet Image Services
Scanning Stations	扫描站
Local Area Network	局域网
Print and Fax Stations	打印和传真站
Web Services	Web服务
User Workstations	用户工作站
The Web	Web
J2EE Application Server	J2EE应用服务器

借助IBM的数据归档和保留解决方案管理呈指数级增长的信息和成本

信息无处不在：电子邮件、即时和文本消息、蜂窝通信、互联网和数字视频已成为我们日常生活的一部分。这些渠道已成为几乎各行各业进行商业交流所不可或缺的工具。关键业务ERP、CRM及其他事务处理应用程序也收集并积累了大量的业务信息。这些应用程序可以为新的业务计划提供强大支撑、支持日常运营并推动创收。随着企业产生越来越多的信息，必须对这些信息成功进行管理，从而满足业务目标、降低风险并推动创新。

信息关键性、信息价值和信息量的迅猛增长势不可挡，但是信息的价值对于各个应用程序并不是相等的，并且会随着时间而改变。确定不经常使用的数据（不活动数据），然后区分真正的历史数据与必须保持立即可用的数据（活动数据）对于企业来说非常重要。正确管理不活动数据将会对生产效率和运营成本产生决定性的影响。

在法规措施不断增多且对符合记录保留要求的需求越来越高的环境中，必须对业务信息进行适当的存储和保护，并在出于法规或商业目的不再需要时进行适当的处理。在诉讼或监管审计中不能及时提供文档可能会导致严重的后果，包括高额罚款，即使信息延迟、丢失或损坏仅仅是意外情况也是如此。随着信息量的增长以及所需存储时间的延长，IT部门受到了巨大的影响，因为管理、存储和保护业务信息变得越来越具有挑战性并且成本日益高昂。

评估您的需求

在应对其独特的数据保留和可访问性需求时，公司应经常进行自我评估，以便寻找合适的方法来管理信息并降低与电子信息增长相关的风险：

- 您是否对存储和管理所有信息的成本进行过评估？
- 您的基础架构是否根据您的数据保留要求进行过优化？
- 您是否对所有业务部门所需的合规等级进行过评估？
- 您是否担心自己出于法律要求进行及时搜索的能力？
- 您的服务器备份与恢复是否足够快速、可靠？
- 您目前如何满足这些要求？

归档如何有助于提高生产效率、降低成本和管理风险

随着当前的IT专家开始考虑信息增长所带来的各种复杂问题组合，归档逐渐成为围绕信息存储与可访问性的合理解决方案。归档可以帮助公司提高生产效率、控制基础架构与法律成本并管理合规与运营风险。

生产系统中信息的快速增长可能会对业务运营带来不利的影响。组织需要保留多份关键数据的备份副本以防止数据丢失。数据还被复制用于开发和测试目的－“乘法效应”－这进一步增加了存储和维护成本。以控制成本和降低风险为重心，IT部门正竭尽全力来充分利用现有的投资并降低基础架构复杂性。归档有助于实现存储优化并降低成本。通过将活动数据与历史/不活动数据分离并根据其业务价值将其移动到较低成本的存储上，可以优化利用率和控制成本，并同时仍然满足服务要求。

从数据库中归档不活动的应用程序数据可以缩减生产数据库的规模并提高应用程序的性能和可用性。归档不活动的应用程序数据还有助于组织在升级和迁移过程中最小化风险，并在服务等级要求内完成备份与恢复操作。

更好地管理风险和合规性

法规和不符合法规的风险不可小视。不符合法规要求不仅会带来法律和经济风险，还可能会危及声誉。此外，被牵涉到诉讼中的风险也越来越高，这还意味着企业需要付出更高的代价。

由于涉及业务记录创建、保留和保存的法规非常众多，因此法务官和企业法务人员通常第一个想到的便是信息归档和保留解决方案，从而改善整体合规流程并管理运营和法律风险。

IBM作为存储领域的行业领导者拥有超凡的经验、工具和服务来帮助公司克服其数据归档和保留挑战。IBM提供了各种工具和流程，可以在整个企业内实现全面的内容管理。IBM归档和保留战略支持基于策略的分层存储环境，可以混用各种存储介质－不同的存储类型或存储层，例如磁盘、磁带和光盘－从而获得成本效益。IBM解决方案可以在介质之间提供无缝的迁移，并且可以优化信息的可用性和性能。

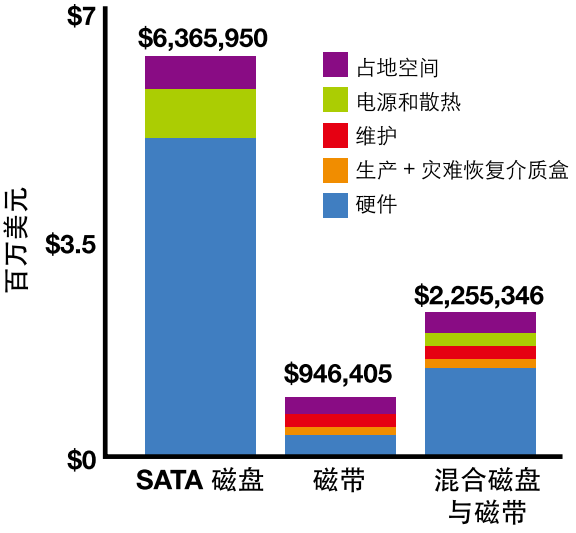
分层方式的价值

每年，组织都要对其IT基础架构进行巨额的投资以便存储宝贵的信息。许多组织正在通过扩充主存储容量来应对信息增长。但是研究发现储存在主存储中的数据有30%到50%是不活动的。1将这类信息留在第一层存储（例如高性能磁盘）上，从长期来说会给组织带来高昂的成本。

IBM信息归档和保留战略可以使信息的价值与合适的存储介质相匹配，从而帮助组织优化其存储基础架构。遵循该战略可以使用户获得混合解决方案的成本优势。不活动信息可以储存在较低成本的存储上，即磁带或光盘介质，而更加相关、关键和活动的信息可以储存在近线磁盘上，以便进行快速的检索和搜索。集成且自动化的存储备份与灾难恢复功能可以帮助提高可用性，并同时削减管理和保护已归档业务信息所需的时间和人力成本。

通过混合磁带和磁盘可以使 TCO 降低 50%*

以 10 年的 TCO 为例。假设 250 TB 存储容量，每年增长 25%



资料来源：IBM 关于 System Storage DR550 的 TCO 调研，2007 年

企业策略集团公司（ESG）在2007年进行的一次文件归档调研发现42%答复者表示其归档数据保存在近线磁盘上进行短期保留，然后再迁移到磁带或光盘介质上进行长期保留。2随着组织在长期经济考量（与系统成本、维护以及电源和散热相关）与要求归档数据即时可用和可检索以用于业务、法律或监管目的的需求之间寻求平衡，ESG相信组织将会继续对归档存储采取分层的方法。

基于策略和自动化的移动

基于策略的归档允许管理员定义各种规则来确定哪些内容应移动到哪种类型的存储以及该内容应保存多长时间。公司可以精确地确定更适合位于备用存储层上的内容并跨不同的存储层管理数据放置，从而满足服务等级要求。因此，组织可以优化存储利用率并同时保持最终用户的工作效率。

由于数据的寿命要长于介质，因此为了进行长期保留，数据需要被迁移到更新的介质和相关的技术，这也是另一个非常重要的成本因素。IBM提供的基于策略的数据归档解决方案具有内置的介质和技术迁移功能，可以帮助减轻这些成本问题。数据可以从磁盘移动到磁带以及从一代技术迁移到另一代技术，并且可以使数据保持不可删除和不可重写，直至保留策略允许删除。

保护信息

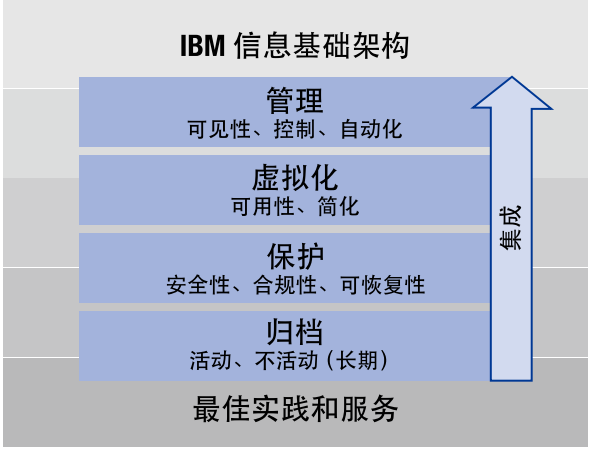
IBM基于策略的数据管理功能可以帮助组织满足各个政府和行业机构的法规要求。IBM提供了集成的解决方案，可以方便以最灵活、功能最丰富的方式来满足最严格的法规要求。许多法规要求将记录、电子邮件、设计文档和其他数据归档保留许多年的时间。此外，法规还要求数据不得更改或删除，并在其生命周期结束后正确进行处理。IBM解决方案包含不可擦除、不可重写（NENR）和一次写入只读（WORM）技术，以确保信息完整性。

作为对归档解决方案的增强，IBM可以通过对分层环境中的磁带、磁盘或两者进行加密，从而帮助公司提供更高的信息安全性。对数据进行加密有助于避免关键信息泄露的商业风险。无论数据是在通过网络传输之前或者是在保存到磁盘或磁带时进行加密，加密功能都可以为企业提供增强的安全性。未加密磁带在今天是一个巨大的安全风险。根据ESG的调查，在参与调查的227位答复者中，有47% 的人认为其组织的数据至少一半可以被视为机密。平均来说，数据库包含了最高比例的机密数据（54%），之后分别是电子文档（40%）、电子邮

件/附件（31%）和其他非结构化数据（24%）。在保护机密数据方面，ESG的研究表明用户更加担心违反法规要求。实际上，超过四分之三（81%） 的用户表示政府法规是其保护机密信息的最大动力。[2]

对于加密而言，密钥管理至关重要。没有正确的密钥，加密的数据便无法读取，因此组织需要实施合适的密钥管理解决方案，不仅要能够保护整个组织内的各种加密密钥，还要能够帮助确保密钥对于需要访问数据的系统和应用程序高度可用。随着机密数据的量继续增长，有效的密钥管理变得更加重要，尤其是对于关键业务信息和出于合规目的必须归档和保护的信息。IBM提供了灵活、透明的系统管理、应用程序管理或磁带库管理的加密选项。IBM加密磁带解决方案包括驱动器级的加密和基于软件的密钥管理器，它可以在各种服务器平台上运行并且能够透明地检测支持加密的介质。这些选项为公司合适地保护其环境中的数据提供了巨大的灵活性。

支持高效归档和保留的信息基础架构



IBM 全面的归档和保留解决方案包括各种技术和流程以支持保存、发现、保留和处理所有类型的信息，包括结构化的数据（例如数据库数据）和非结构化的数据（例如电子邮件、用户文件、医学影像、即时消息和文档）。

IBM 解决方案可以通过下述方式帮助管理与信息相关的业务和法律风险：

- 通过保护业务信息，促进符合记录保留要求和企业保留策略。
  - 通过灵活的密钥管理对磁带和磁盘进行加密
  - 充分利用NENR 和WORM 技术
- 通过下述方式控制成本并优化利用率：
  - 充分利用混合的存储介质层（磁盘、磁带、光盘）。
  - 提供基于策略的自动化数据迁移功能。
- 通过下述方式提高最终用户工作效率：
  - 自动化的数据管理流程和工具。
  - 提高关键生产系统的性能和可用性。

来自IBM 的端到端归档和保留解决方案

IBM久经考验的优良记录以及广泛的产品组合及服务可以帮助公司更好地管理、储存、保护和共享整个企业内的信息。IBM解决方案包含集成的硬件和软件以便管理各种内容，包括文档、数据库和非结构化数据（例如电子邮件），从满足广泛的性能和预算需求。IBM可以为需要最高灵活性和简易性的客户提供“交钥匙式”或有针对性的解决方案，并且订购和部署均非常简单。

IBM围绕归档和保留提供灵活的服务以满足各种要求，从“告诉我做什么”、“帮助我做”到“为我做”无所不包。从评估IT环境和业务需求、构建业务案例和准备归档战略一直到开发和部署体系架构，IBM全球服务团队拥有丰富的技能和工具在各个方面提供帮助。

IBM全球归档解决方案中心是世界上第一个专门为了帮助全球的组织开发和实施长期计划来管理和归档海量业务信息而设计的中心。IBM的海法研究实验室在新兴归档技术方面（例如长期数字保存）遥遥领先。

无论您是在当前的信息爆炸中的面对存储危机，还是需要用于长期数字保存的归档技术，又或是仅仅想要使您的信息资产更加有条理和安全，IBM都可随时提供帮助。

注释:

[1] 100 年归档要求调查。100 年归档特别工作组，存储网络行业协会（SNIA）。2007 年1 月。www.snia.org/forums/dmf/programs/ltacsi/100_year

[2] 2007 File Archiving Survey. 企业策略集团公司（ESG）。2008 年1 月24 日。www.enterprisestrategygroup.com/ESGPublications/ReportDetail.asp?ReportID=932

IBM企业信息架构—信息安全方案群组

Information Infrastructure Solution
领驭信息架构 创新存储时代

信息安全方案群组

IBM Proventia Network Intrusion Prevention System GX4002

为网络边界提供前瞻性地防护

IBM Proventia® 网络入侵防护系统GX4002延续了业界领先的Proventia技术持续为用户的网络边界提供防护，在这些外部安全威胁影响到用户业务之前提供了阻断防护。通过1个物理网段的200M检测吞吐率的防护能力，Proventia网络入侵防护系统GX4002可以为用户提供安全的、高性能的、高可靠性的全面的解决方案，同时还可以非常简单的进行部署和管理。

作为先进的串接式入侵防护系统，Proventia® GX系列硬件设备能够实时阻隔已知和未知的攻击，包括分布式拒绝服务（DDoS），后门以及混合威胁等，而无需工作繁忙的系统管理人员的参与。Proventia® GX系列可以和IBM ISS的其他网络防护系统协同工作，并能够通过SiteProtector™管理平台进行集中管理。

Proventia® GX系列IPS优势

- 动态阻断功能
- 即时、可靠地拦截不需要的流量
- 可防止混合型威胁（如Sasser、MS Blaster、SQL Slammer、Nimda 和Code Red）传播
- 精确检测和防护超过190种协议
- 允许合法流量顺畅通过，而不影响网络性能
- 立即对已知和未知的攻击进行防护，而不必手动应用未计划的更新程序或热修复程序

成熟的入侵防护技术不会出现误报

- 深层次的协议分析功能提供精确而高效的防护，以预防已知和未知攻击
- 能够分析190多种网络协议，并包含2,600多个业界独一无二的威胁检查项
- Proventia® GX入侵防护设备采用的技术在NSS Group 举行的IPS Group Test (IPS产品组测试)中获得了NSS Approved (推荐产品)奖项。Proventia® GX成功证实了自己100%的反识别成功率

通过SiteProtector进行集中式管理

- 以最少的人员的运营成本进行控制、监视和分析
- 可从小型企业到大型乃至全球性企业轻松扩展
- 利用SiteProtector SecurityFusion™模块进行高级数据关联、影响分析以及攻击模式识别

可灵活部署的集成防护设备

- 使用单一设备即可监视多个网段
- 只需进行简单配置即可快速启动和运行，实现即时防护
- 在检测功能与防护功能之间轻松切换，无需中断或妨碍合法的网络流量
- 三种工作模式包括：主动模式（串接，阻断功能），被动模式(非串接，无阻断功能），模拟模式（串接，无阻断功能）
- 支持非对称路由网络
- 虚拟入侵防护系统，可基于端口、网段、IP、VLAN设置策略
- 本地Web管理界面

技术参数	型号 GX4002
性能指标	
检测吞吐率	200Mbps
延迟	< 150微秒
并发会话数	1,200,000
每秒新建连接数	21,000
工作模式	
主动防御	是
旁路监控	是
在线模拟	是
检测端口	
防护网段	1
监控端口	2*10/100/1,000 电口

技术参数	型号 GX4002
高可用性	
主－主	否
主－备	是
硬件级Bypass	内置Bypass
冗余电源	否
冗余存储	否
规格	
机柜单元	1-U
高度（英寸/毫米）	1.73/44
宽度（英寸/毫米）	16.9/429
深度（英寸/毫米）	15/382
重量（磅/公斤）	24.5/11.1
功耗	
单位	AC
电流（A）	4.96/2.48
电压（V）	115/220
输入电压范围（V）	100-127/200-240
工作温度	50°F-90°F(10°C-35°C)
非工作温度	-4°F-158°F(-20°C-70°C)
相对湿度（非工作）	90%@86°F(30°C)
电磁辐射	• FCC Class A • EN 55022 • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • VCCI Class A
安全认证	• UL • EN 60950-1

IBM Proventia Network Intrusion Prevention System GX4004

为网络边界提供前瞻性地防护

IBM Proventia®网络入侵防护系统GX4004延续了业界领先的Proventia技术持续为用户的网络边界提供防护，在这些外部安全威胁影响到用户业务之前提供了阻断防护。通过2个物理网段的200M检测吞吐率的防护能力，Proventia网络入侵防护系统GX4004可以为用户提供安全的、高性能的、高可靠性的全面的解决方案，同时还可以非常简单的进行部署和管理。

作为先进的串接式入侵防护系统，Proventia® GX系列硬件设备能够实时阻隔已知和未知的攻击，包括分布式拒绝服务（DDoS），后门以及混合威胁等，而无需工作繁忙的系统管理人员的参与。Proventia® GX系列可以和IBM ISS的其他网络防护系统协同工作，并能够通过SiteProtector™管理平台进行集中管理。

Proventia® GX系列IPS优势

- 动态阻断功能
- 即时、可靠地拦截不需要的流量
- 可防止混合型威胁（如Sasser、MS Blaster、SQL Slammer、Nimda 和Code Red）传播
- 精确检测和防护超过190种协议
- 允许合法流量顺畅通过，而不影响网络性能
- 立即对已知和未知的攻击进行防护，而不必手动应用未计划的更新程序或热修复程序

成熟的入侵防护技术不会出现误报

- 深层次的协议分析功能提供精确而高效的防护，以预防已知和未知攻击
- 能够分析190多种网络协议，并包含2,600多个业界独一无二的威胁检查项
- Proventia® GX入侵防护设备采用的技术在NSS Group 举行的IPS Group Test (IPS产品组测试)中获得了NSS Approved (推荐产品)奖项。Proventia® GX成功证实了自己100%的反识别成功率

通过SiteProtector进行集中式管理

- 以最少的人员的运营成本进行控制、监视和分析
- 可从小型企业到大型乃至全球性企业轻松扩展
- 利用SiteProtector SecurityFusion™模块进行高级数据关联、影响分析以及攻击模式识别

可灵活部署的集成防护设备

- 使用单一设备即可监视多个网段
- 只需进行简单配置即可快速启动和运行，实现即时防护
- 在检测功能与防护功能之间轻松切换，无需中断或妨碍合法的网络流量
- 三种工作模式包括：主动模式（串接，阻断功能），被动模式(非串接，无阻断功能），模拟模式（串接，无阻断功能）
- 支持非对称路由网络
- 虚拟入侵防护系统，可基于端口、网段、IP、VLAN设置策略
- 本地Web 管理界面

技术参数	型号 GX4004
性能指标	
检测吞吐率	200Mbps
延迟	< 150微秒
并发会话数	1,200,000
每秒新建连接数	21,000
工作模式	
主动防御	是
旁路监控	是
在线模拟	是
检测端口	
防护网段	2
监控端口	4*10/100/1,000 电口

技术参数	型号 GX4004
高可用性	
主－主	否
主－备	是
硬件级Bypass	内置Bypass
冗余电源	否
冗余存储	否
规格	
机柜单元	1-U
高度（英寸/毫米）	1.73/44
宽度（英寸/毫米）	16.9/429
深度（英寸/毫米）	15/382
重量（磅/公斤）	24.5/11.1
功耗	
单位	AC
电流（A）	4.96/2.48
电压（V）	115/220
输入电压范围（V）	100-127/200-240
工作温度	50°F-90°F(10°C-35°C)
非工作温度	-4°F-158°F(-20°C-70°C)
相对湿度（非工作）	90%@86°F(30°C)
电磁辐射	• FCC Class A • EN 55022 • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • VCCI Class A
安全认证	• UL • EN 60950-1

IBM Proventia Network Intrusion Prevention System GX5008

为网络边界提供前瞻性地防护

IBM Proventia®网络入侵防护系统GX5008延续了业界领先的Proventia技术持续为用户的网络边界提供防护，在这些外部安全威胁影响到用户业务之前提供了阻断防护。通过4个物理网段的400M检测吞吐率的防护能力，Proventia网络入侵防护系统GX5008可以为用户提供安全的、高性能的、高可靠性的全面的解决方案，同时还可以非常简单的进行部署和管理。

作为先进的串接式入侵防护系统，Proventia® GX系列硬件设备能够实时阻隔已知和未知的攻击，包括分布式拒绝服务（DDoS），后门以及混合威胁等，而无需工作繁忙的系统管理人员的参与。Proventia® GX系列可以和IBM ISS的其他网络防护系统协同工作，并能够通过SiteProtector™管理平台进行集中管理。

Proventia® GX系列IPS优势

- 动态阻断功能
- 即时、可靠地拦截不需要的流量
- 可防止混合型威胁（如Sasser、MS Blaster、SQL Slammer、Nimda 和Code Red）传播
- 精确检测和防护超过190种协议
- 允许合法流量顺畅通过，而不影响网络性能
- 立即对已知和未知的攻击进行防护，而不必手动应用未计划的更新程序或热修复程序

成熟的入侵防护技术不会出现误报

- 深层次的协议分析功能提供精确而高效的防护，以预防已知和未知攻击
- 能够分析190多种网络协议，并包含2,600多个业界独一无二的威胁检查项
- Proventia® GX入侵防护设备采用的技术在NSS Group 举行的IPS Group Test (IPS产品组测试)中获得了NSS Approved (推荐产品)奖项。Proventia® GX成功证实了自己100%的反识别成功率

通过SiteProtector进行集中式管理

- 以最少的人员的运营成本进行控制、监视和分析
- 可从小型企业到大型乃至全球性企业轻松扩展
- 利用SiteProtector SecurityFusion™模块进行高级数据关联、影响分析以及攻击模式识别

可灵活部署的集成防护设备

- 使用单一设备即可监视多个网段
- 只需进行简单配置即可快速启动和运行，实现即时防护
- 在检测功能与防护功能之间轻松切换，无需中断或妨碍合法的网络流量
- 三种工作模式包括：主动模式（串接，阻断功能），被动模式(非串接，无阻断功能），模拟模式（串接，无阻断功能）
- 支持非对称路由网络
- 虚拟入侵防护系统，可基于端口、网段、IP、VLAN设置策略
- 本地Web 管理界面

技术参数	型号 GX5008
性能指标	
检测吞吐率	400Mbps
延迟	< 200微秒
并发会话数	1,200,000
每秒新建连接数	35,000
工作模式	
主动防御	是
旁路监控	是
在线模拟	是
检测端口	
防护网段	4
监控端口	1) 8*10/100/1,000 TX 2) 8*SFP/mini-GBIC 3) 4*10/100/1,000 TX+4* SFP/mini-GBIC

技术参数	型号 GX5008
高可用性	
主－主	是
主－备	是
硬件级Bypass	内置Bypass（可选）
冗余电源	是
冗余存储	是
规格	
机柜单元	2-U
高度（英寸/毫米）	3.5/88
宽度（英寸/毫米）	16.9/429
深度（英寸/毫米）	20.5/520
重量（磅/公斤）	40/18
功耗	
单位	AC
电流（A）	8.4/4.2
电压（V）	115/220
输入电压范围（V）	100-127/200-240
工作温度	50°F-90°F(10°C-35°C)
非工作温度	-4°F-158°F(-20°C-70°C)
相对湿度（非工作）	90%@86°F(30°C)
电磁辐射	• FCC Class A • EN 55022 • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • VCCI Class A
安全认证	• UL • EN 60950-1

IBM Proventia Network Intrusion Prevention System GX5108

为网络边界提供前瞻性地防护

IBM Proventia®网络入侵防护系统GX5108延续了业界领先的Proventia技术持续为用户的网络边界提供防护，在这些外部安全威胁影响到用户业务之前提供了阻断防护。通过4 个物理网段的1.2G检测吞吐率的防护能力，Proventia网络入侵防护系统GX5108可以为用户提供安全的、高性能的、高可靠性的全面的解决方案，同时还可以非常简单的进行部署和管理。

作为先进的串接式入侵防护系统，Proventia® GX系列硬件设备能够实时阻隔已知和未知的攻击，包括分布式拒绝服务（DDoS），后门以及混合威胁等，而无需工作繁忙的系统管理人员的参与。Proventia® GX系列可以和IBM ISS的其他网络防护系统协同工作，并能够通过SiteProtector™管理平台进行集中管理。

Proventia® GX系列IPS优势

- 动态阻断功能
- 即时、可靠地拦截不需要的流量
- 可防止混合型威胁（如Sasser、MS Blaster、SQL Slammer、Nimda 和Code Red）传播
- 精确检测和防护超过190种协议
- 允许合法流量顺畅通过，而不影响网络性能
- 立即对已知和未知的攻击进行防护，而不必手动应用未计划的更新程序或热修复程序

成熟的入侵防护技术不会出现误报

- 深层次的协议分析功能提供精确而高效的防护，以预防已知和未知攻击
- 能够分析190多种网络协议，并包含2,600多个业界独一无二的威胁检查项
- Proventia® GX入侵防护设备采用的技术在NSS Group 举行的IPS Group Test (IPS产品组测试)中获得了NSS Approved (推荐产品)奖项。Proventia® GX成功证实了自己100%的反识别成功率

通过SiteProtector进行集中式管理

- 以最少的人员的运营成本进行控制、监视和分析
- 可从小型企业到大型乃至全球性企业轻松扩展
- 利用SiteProtector SecurityFusion™模块进行高级数据关联、影响分析以及攻击模式识别

可灵活部署的集成防护设备

- 使用单一设备即可监视多个网段
- 只需进行简单配置即可快速启动和运行，实现即时防护
- 在检测功能与防护功能之间轻松切换，无需中断或妨碍合法的网络流量
- 三种工作模式包括：主动模式（串接，阻断功能），被动模式(非串接，无阻断功能），模拟模式（串接，无阻断功能）
- 支持非对称路由网络
- 虚拟入侵防护系统，可基于端口、网段、IP、VLAN设置策略
- 本地Web 管理界面

技术参数	型号 GX5108
性能指标	
检测吞吐率	1.2Gbps
延迟	< 200微秒
并发会话数	1,450,000
每秒新建连接数	40,000
工作模式	
主动防御	是
旁路监控	是
在线模拟	是
检测端口	
防护网段	4
监控端口	1) 8*10/100/1,000 TX 2) 8*SFP/mini-GBIC 3) 4*10/100/1,000 TX+4* SFP/mini-GBIC

技术参数	型号 GX5108
高可用性	
主－主	是
主－备	是
硬件级Bypass	内置Bypass（可选）
冗余电源	是
冗余存储	是
规格	
机柜单元	2-U
高度（英寸/毫米）	3.5/88
宽度（英寸/毫米）	16.9/429
深度（英寸/毫米）	20.5/520
重量（磅/公斤）	40/18
功耗	
单位	AC
电流（A）	8.4/4.2
电压（V）	115/220
输入电压范围（V）	100-127/200-240
工作温度	50°F-90°F(10°C-35°C)
非工作温度	-4°F-158°F(-20°C-70°C)
相对湿度（非工作）	90%@86°F(30°C)
电磁辐射	• FCC Class A • EN 55022 • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • VCCI Class A
安全认证	• UL • EN 60950-1

IBM Proventia Network Intrusion Prevention System GX5208

为网络边界提供前瞻性地防护

IBM Proventia®网络入侵防护系统GX5208延续了业界领先的Proventia技术持续为用户的网络边界提供防护，在这些外部安全威胁影响到用户业务之前提供了阻断防护。通过4个物理网段的2G检测吞吐率的防护能力，Proventia网络入侵防护系统GX5208可以为用户提供安全的、高性能的、高可靠性的全面的解决方案，同时还可以非常简单的进行部署和管理。

作为先进的串接式入侵防护系统，Proventia® GX系列硬件设备能够实时阻隔已知和未知的攻击，包括分布式拒绝服务（DDoS），后门以及混合威胁等，而无需工作繁忙的系统管理人员的参与。Proventia® GX系列可以和IBM ISS的其他网络防护系统协同工作，并能够通过SiteProtector™管理平台进行集中管理。

Proventia® GX系列IPS优势

- 动态阻断功能
- 即时、可靠地拦截不需要的流量
- 可防止混合型威胁（如Sasser、MS Blaster、SQL Slammer、Nimda 和Code Red）传播
- 精确检测和防护超过190种协议
- 允许合法流量顺畅通过，而不影响网络性能
- 立即对已知和未知的攻击进行防护，而不必手动应用未计划的更新程序或热修复程序

成熟的入侵防护技术不会出现误报

- 深层次的协议分析功能提供精确而高效的防护，以预防已知和未知攻击
- 能够分析190多种网络协议，并包含2,600多个业界独一无二的威胁检查项
- Proventia® GX入侵防护设备采用的技术在NSS Group 举行的IPS Group Test (IPS产品组测试)中获得了NSS Approved (推荐产品)奖项。Proventia® GX成功证实了自己100%的反识别成功率

通过SiteProtector进行集中式管理

- 以最少的人员的运营成本进行控制、监视和分析
- 可从小型企业到大型乃至全球性企业轻松扩展
- 利用SiteProtector SecurityFusion™模块进行高级数据关联、影响分析以及攻击模式识别

可灵活部署的集成防护设备

- 使用单一设备即可监视多个网段
- 只需进行简单配置即可快速启动和运行，实现即时防护
- 在检测功能与防护功能之间轻松切换，无需中断或妨碍合法的网络流量
- 三种工作模式包括：主动模式（串接，阻断功能），被动模式(非串接，无阻断功能），模拟模式（串接，无阻断功能）
- 支持非对称路由网络
- 虚拟入侵防护系统，可基于端口、网段、IP、VLAN设置策略
- 本地Web 管理界面

技术参数	型号 GX5208
性能指标	
检测吞吐率	2Gbps
延迟	< 200微秒
并发会话数	1,800,000
每秒新建连接数	60,000
工作模式	
主动防御	是
旁路监控	是
在线模拟	是
检测端口	
防护网段	4
监控端口	1) 8*10/100/1,000 TX 2) 8*SFP/mini-GBIC

技术参数	型号 GX5208
高可用性	
主－主	是
主－备	是
硬件级Bypass	内置Bypass（可选）
冗余电源	是
冗余存储	是
规格	
机柜单元	2-U
高度（英寸/毫米）	3.5/88
宽度（英寸/毫米）	16.9/429
深度（英寸/毫米）	21.5/546
重量（磅/公斤）	37.5/17
功耗	
单位	AC
电流（A）	8.4/4.2
电压（V）	115/220
输入电压范围（V）	100-127/200-240
工作温度	50°F-90°F(10°C-35°C)
非工作温度	-4°F-158°F(-20°C-70°C)
相对湿度（非工作）	90%@86°F(30°C)
电磁辐射	• FCC Class A • EN 55022 • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • VCCI Class A
安全认证	• UL • EN 60950-1

IBM Internet Security Systems Datasheet

IBM Proventia® Network

GX3002

为企业网络提供前瞻性安全防护

Proventia®网络入侵防系统（NIPS）GX3002产品将业界领先的前瞻性安全防护延伸到远端网络及中小企业使用，保护远端设备及网络安全免受攻击。

GX3002提供价格低廉、安全可靠、易于安装管理以及高效能的功能给中小企业分支机构使用。既减少安全专业人员的投资以达到保障信息的效果。

Proventia GX3002网络入侵防护系统，可在不影响网络运行效能的同时，实时分析数据包内容，并自动阻断网络上恶意的攻击活动与拒绝服务攻击的行为。与目前市面上的防火墙、入侵检测系统、入侵防护系统比较，Proventia GX3002具备最先进、准确率最高的检测技术，提供其他产品望尘莫及的防护能力。

Proventia GX3002可能阻挡已知与未知的攻击行为，包括Dos、DDos、后门程序以及混合型攻击手法。其主动防御的特性，可以有效地节省管理者投入的资金与人力。通过SiteProtector的中央控管平台，Proventia GX3002可与其它安全产品进行集中管理。共同提供企业网络、服务器以及个人电脑的安全。

PM-IPSGX6116DS-0107

规格指标	
吞吐量	10Mbps
保护网段	1
检测接口	2 x 10/100 TX
时延	< 1 毫秒
并发会话	220,000
每秒连接数	3,750
操作模式	
主动保护	支持
被动检测	支持
串联仿真	支持
高可用性	
硬件级旁路能力	内置旁路
冗余电源	否
冗余存储	否
尺寸	
设备高度	桌面型
高(英寸/ 公分)	1.97/5
宽(英寸/ 公分)	8.86/22.5
深(英寸/ 公分)	8.07/20.5
重量(磅/ 公斤)	2.6/1.2
功耗	
单位	AC
电流	1.5/1.0
电压(V)	115/220
输入范围(V)	100-127/200-240
工作温度	67˚F-130˚F (5˚C -40˚C)
非工作温度	58˚F-184˚F (0˚C -70˚C)
相对湿度(非工作环境)	90%@86˚ F(30˚C)
安全认证	
	- UL - EN 60950-1
电磁辐射认证	
	- FCC Class B - EN 55022 Class B - EN 55024 - EN 61000-3-2 - EN 61000-3-3 - AS/NZS CISPR 22 - VCCI Class A
环境认证	
	RoHS

了解更多!

关于ProventiaR Network IPS Gx3002如何为您的网络提供强大的防护，更多信息访问www.iss.net，或请您就近咨询IBM Internet Security Systems 办公室。

关于IBM Internet Security Systems

IBM Internet Security Systems是全球五百家企业及政府单位信赖的网络安全供应商。ISS提供前瞻性的安全系列产品来保护客户宝贵的数字资产。IBM Internet Security Systems成立于1994年，总部在美国的亚特兰大，并在纳斯达克上市（ISSX）。IBM Internet Security Systems全球有超过11,000个客户。目前在27个国设有分支机构，并拥有1,200名员工。

IBM Internet Security Systems Datasheet

IBM Proventia Network Intrusion Prevention System (IPS) GX6116

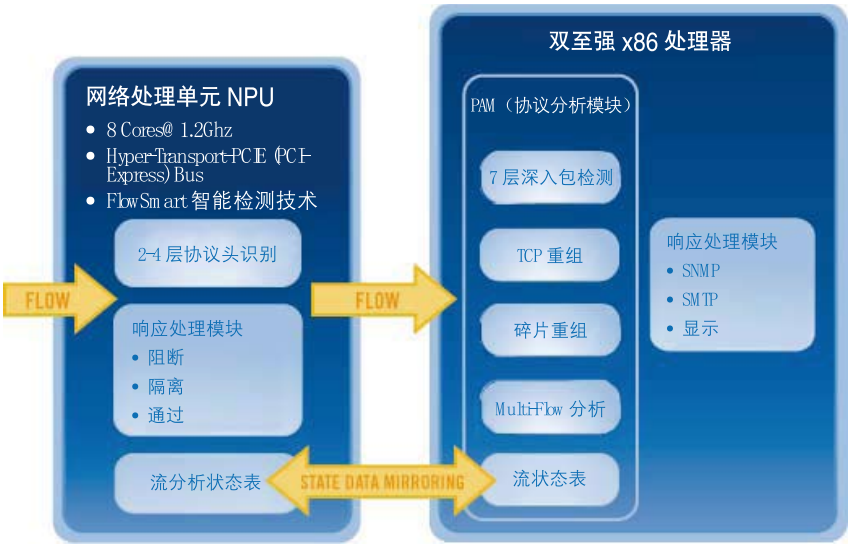
固若金汤的核心网络防护

Proventia®网络入侵防护系统GX6116将ISS全球领先的前瞻性防护技术延伸到网络核心层，

阻断来自外部和内部的威胁，保护您的核心业务。在核心层的高性能应用程序如VoIP等需要高吞吐量、高扩展性和低时延的安全解决方案，Proventia GX6116系统可以满足这三个要求，并且提供多达8 个防护网段、高达6Gbps的检测吞吐能力以及可配置的时延阈值。

为了满足网络核心层的防护需求，Proventia GX6116在入侵防护技术领域引入了两种革命性的先进技术：

- 定制的NPU，高速处理网络数据包。
- FlowSmart 技术，基于网络流数据的状态统计进行数据包智能检测。



Proventia GX6116定制NPU 和FlowSmart技术是网络安全领域的突破

性能指标	
吞吐量	15 Gbps
检测吞吐量	6 Gbps
操作模式	
主动保护	支持
被动检测	支持
串联仿真	支持
扩展性	
保护网段	8
检测接口	16×SFP/Mini-GBIC (1000 TX/SX/LX)
高可用性	
Active-Active	支持
Active-Passive	支持
硬件级旁路能力	外接旁路（可选）
冗余电源	支持
冗余存储	支持
尺寸	
设备高度	2-RU
高(英寸/ 公分)	3.5 /88
宽(英寸/ 公分)	16.9/429
深(英寸/ 公分)	20.5/520
安全认证	
	- UL - cUL - EN 60950-1
电磁辐射认证	
	- FCC Class A - EN 55022 Class A - EN 55024 - EN 61000-3-2 - EN 61000-3-3 - EN 60950-1 - VCCI Class A
环境认证	
	RoHS

Proventia GX116 方便部署，易于管理，功能全面，性能出众、安全可靠，可为用户打造固若金汤的核心层网络安全解决方案。

了解更多!

关于 Proventia Network IPS GX6116 如何为网络核心提供保护的详细信息，请访问：www.iss.net或联系IBM公司。

PM-IPSGX6116DS-0107

IBM Proventia Network Intrusion Prevention System

Delivering uncompromising protection for every layer of the network

Preemptive protection for your network

With a comprehensive line of models, the IBM Proventia® Network Intrusion Prevention System (IPS) is designed to deliver uncompromising protection for every layer of the network, protecting your business from both internal and external threats.

Model	GX3002	GX4002	GX4004	GX5008	GX5108	G2000	GX6116
Typical deployment	Remote office	Remote office	Network perimeter	Network perimeter	Network core	Network core	Network core
Performance characteristics							
Throughput	10 Mbps	200 Mbps	200 Mbps	400 Mbps	1.2 Gbps	2 Gbps	15 Gbps
Inspected throughput	10 Mbps	200 Mbps	200 Mbps	400 Mbps	1.2 Gbps	2 Gbps	15 Gbps
Latency	< 1 millisecond	< 150 microseconds	< 150 microseconds	< 200 microseconds	< 200 microseconds	< 200 microseconds	< 150 microseconds
Connections per second	3,750	21,000	21,000	35,000	40,000	40,000	160,000
Concurrent sessions (rated max)	220,000	1,200,000	1,200,000	1,200,000	F1,450,000	1,300,000	4,600,000
Physical characteristics							
Form factor	Desktop	1 rack unit	1 rack unit	2 rack units	2 rack units	2 rack units	2 rack units
Dimensions							
Height (in/mm) Width (in/mm) Depth (in/mm) Weight (lb/kg)	1.97/50 8.86/225 8.07/205 2.6/1.2	1.73/44 16.9/429 15/382 24.5/11.1	1.73/44 16.9/429 15/382 24.5/11.1	3.5/88 16.9/429 20.5/520 40/18	3.5/88 16.9/429 20.5/520 40/18	3.40/87.5 16.93/430 26.4/672 60/27	3.5/88 16.9/429 20.5/520 56/25.45
Monitoring interfaces	2x10/100 copper	2x10/100/1,000 copper only	4x10/100/1,000 copper only	8x10/100/1,000 copper or 4x10/100/1,000 copper + 4x SFP/mini-GBIC ports (TX/SX/LX transceivers supported) or 8x SFP/mini-GBIC ports (1,000 TX/SX/LX)	8x10/100/1,000 copper or 4x10/100/1,000 copper + 4x SFP/mini-GBIC ports (TX/SX/LX transceivers supported) or 8x SFP/mini-GBIC ports (1,000 TX/SX/LX)	8x10/100/1,000 copper and/or SX Fiber (LC)	16x SFP/mini-GBIC ports (1,000 TX/SX/LX)
Inline protected segments	1 network segment	1 network segment	2 network segments	4 network segments	4 network segments	4 network segments	8 network segments
Redundant power supplies	No	No	No	Yes	Yes	Yes	Yes
Redundant storage	No	No	No	Yes	Yes	Yes	Yes

Model	GX3002	GX4002	GX4004	GX5008	GX5108	G2000	GX6116
High availability	Active-active: no Active-passive: yes Hardware-level bypass: integrated bypass	Active-active: no Active-passive: yes Hardware-level bypass: integrated bypass	Active-active: no Active-passive: yes Hardware-level bypass: integrated bypass	Active-active: yes Active-passive: yes Hardware-level bypass: external bypass (optional)	Active-active: yes Active-passive: yes Hardware-level bypass: external bypass (optional)	Active-active: yes Active-passive: yes Hardware-level bypass: requires optional integrated copper bypass External fiber bypass (optional)	Active-active: yes Active-passive: yes Hardware-level bypass: requires optional integrated copper bypass External fiber bypass (optional)
Power requirements							
Units Amps Input range (V)	AC 1.5/1.0 100-127/200-240	AC 4.96/2.48 100-127/200-240	AC 4.96/2.48 100-127/200-240	AC 8.4/4.2 100-127/200-240	AC 8.4/4.2 100-127/200-240	AC 8.9/5.4 100-127/200-240	AC 10/5 100-240
Operating temperature	41˚F–104˚F (5˚C–40˚C)	50˚F–95˚F (10˚C–35˚C)	50˚F–95˚F (10˚C–35˚C)	50˚F–95˚F (10˚C–35˚C)	50˚F–95˚F (10˚C–35˚C)	50˚F–95˚F (10˚C–35˚C)	50˚F–104˚F (10˚C–40˚C)
Nonoperating temperature	32˚F–158˚F (0˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)	-4˚F–158˚F (-20˚C–70˚C)
Relative humidity (nonoperating)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)	90% @ 86˚F (30˚C)
Safety certification	UL EN 60950-01	UL EN 60950-01	UL EN 60950-01	UL EN 60950-01	UL EN 60950-01	UL EN 60950-01 IEC 60950-1 AS/NZS 60950	UL EN 60950-01
Emissions	FCC Class B EN 55022 Class B EN 55024 EN 61000-3-2 EN 61000-3-3 AS/NZS CISPR 22 VCCI Class A	FCC Class B EN 55022 Class B EN 55024 EN 61000-3-2 EN 61000-3-3 AS/NZS CISPR 22 VCCI Class A	FCC Class A EN 55022 EN 55024 EN 61000-3-2 EN 61000-3-3 VCCI Class A	FCC Class A EN 55022 Class A EN 55024 EN 61000-3-2 EN 61000-3-3 VCCI Class A	FCC Class A EN 55022 Class A EN 55024 EN 61000-3-2 EN 61000-3-3 VCCI Class A	FCC Class A EN 55022 EN 55024 EN 61000-3-2 EN 61000-3-3 ICES-003 Issue 4 CISPR 22 VCCI Class A	FCC Class A EN 55022 Class A EN 55011 Class A AS/NZS CISPR 2004 Class A EN 6100-6-4 EN 61000-3-2 EN 61000-3-3 EN 55024 VCCI Class A
Environmental certification	RoHS	RoHS	RoHS	RoHS	RoHS	RoHS	RoHS

For more information

To learn more about IBM Proventia Network IPS and other IBM Global Services capabilities, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/services/us/iss

IBM Proventia Server Intrusion Prevention System for Linux

概述

IBM Proventia® Server Intrusion Prevention System（IPS）for Linux软件可为法规遵从提供支持，满足有关可能损害服务器和敏感数据的恶意威胁的安全性法规要求。通过Proventia Server IPS，企业能够保护数据安全不受破坏，并受益于其简化和支持法规遵从要求的能力。

Proventia Server IPS for Linux作为企业数据丢失防护（DLP）战略中的一个关键组件，其优势不只在于法规遵从支持。在根据每次受损的成本记录与停机时间对服务器安全破坏成本进行衡量的趋势下，使用 Proventia Server IPS的全面DLP战略将：

- 实现有关数据和应用的实时报告
- 提供防止数据丢失和前瞻性的保护，同时，还针对服务器实施企业安全策略
- 检查进入服务器的流量，阻止试图入侵和提取敏感数据的恶意代码

Proventia Server IPS for Linux可无缝接合到企业的IT基础设施，由IBM SiteProtector™系统进行集中管理。

优势

Proventia Server IPS for Linux提供了多种功能，可满足法规遵从和必要的安全技术要求，支持全面的DLP战略。

Proventia Server IPS for Linux能够主动支持法规遵从要求，将企业作为一个整体进行保护。安全专家可获得完整的有关登录、权限升级和与其他应用相关的、对于衡量法规遵从极为重要的事件活动视图。

Proventia Server IPS for Linux能够主动保护您的服务器免受恶意攻击，同时还支持法规遵从需求。Proventia Server IPS可以在内部服务器攻击和威胁造成损害之前将其阻止。Proventia Server IPS可以在防火墙和IPS阻止攻击之后提供最后一道防护，它还包括缓冲溢出漏洞防护（BOEP）。

- 通过跟踪和报告工具保持合规。接收有关权限升级和未经授权的配置变更的活动警告。
- 无需补丁，即可保护服务器免受已知和未知攻击。无需中断服务器和服务器应用来安装紧急补丁。Proventia Server IPS可以提供以漏洞为中心的入侵防护，阻止网络蠕虫和其他漏洞，同时，缓冲区溢出漏洞防护还能够阻止未知的缓冲区溢出漏洞的攻击。
- 实施网络访问策略。为入站和出站流量设置端口和IP限制，以避免服务器的受到攻击。
- 管理应用级入侵检测和审计。通过操作系统和应用活动的日志监控来检测和响应应用级攻击或未经授权的活动，保持系统完整性和合规性。
- 旨在优化资源利用率。
  最大限度地减少内存和CPU的占用空间。
- Web应用保护。通过检查安全套接层 （SSL）加密流量，防止恶意活动，从而保护Web应用。
- 与活动目录相集成。使用活动目录组织结构，以管理策略，监控事件并创建报表。

前瞻性防护

有些主机保护解决方案除了提供一个本地防火墙之外，还会提供入侵防护签名。基于签名的入侵防护与防病毒签名极为相似，只能有效地抵御已知威胁－但是对于未知漏洞则一筹莫展。前瞻性的保护将以漏洞为中心的入侵防护与其他保护技术相结合，保护重要服务器不受恶意攻击。

缓冲溢出漏洞防护

缓冲区溢出漏洞防护（BOEP）是一种很少使用签名的技术，可以在内存缓冲区溢出过程中主动寻找恶意代

码。BOEP技术即使在不知道存在特殊漏洞的情况下也能够提供保护。该技术旨在阻止蠕虫传播，并防止攻击者利用缓冲区溢出漏洞在您的系统上运行任何代码。BOEP技术可以挂起系统调用（不仅是API等级），并对此类漏洞进行防护而不会出现复杂的窗口。

防火墙

Proventia Server IPS for Linux的防火墙功能可阻止对端口和IP地址的未经授权的访问，防止IP欺骗和终端劫持，从而缩小受攻击范围。

支持的平台

Red Hat Enterprise Linux 4.0 AS Update 4 & 5 Red Hat Enterprise Linux 4.0 ES Update 4 & 5 Red Hat Enterprise Linux 3.0 AS Update 8 &9 Red Hat Enterprise Linux 3.0 ES Update 8 & 9 SuSE Linux Enterprise Server 9 SP3

更多信息

如需了解有关Proventia Server IPS for Linux的更多信息，请联系IBM ISS销售代表，或者访问：**www.ibm.com/services/us/iss。**

关于IBM互联网安全系统公司

IBM互联网安全系统（ISS）是广受信赖的安全专家，为全球企业与政府提供网络安全产品和服务，保护他们免受互联网威胁的侵扰。IBM ISS成立于1994年，是IT安全领域的全球领导者，其解决方案的成本效益经过实践的检验，能够降低整个企业的法规与业务风险。IBM ISS产品与服务基于IBM网络安全系统X-Force®研发团队的主动安全智能，该团队是网络安全漏洞与威胁研究领域的全球权威。如需更多信息，请访问：www.ibm.com/ services/us/iss或致电：1 800 776-2362。

IBM Proventia Server Intrusion Prevention System for Windows

概述

IBM Proventia® Server Intrusion Prevention System（IPS）for Windows可为法规遵从提供支持，满足有关可能损害服务器和敏感数据的恶意威胁的安全性法规要求。通过Proventia Server IPS，企业能够保护数据安全不受破坏，并受益于简化和支持法规遵从要求的能力。

Proventia Server IPS作为企业数据丢失防护（DLP）战略中的一个关键组件，其优势不只在于法规遵从支持。在根据每次受损的成本记录与停机时间对服务器安全破坏成本进行衡量的趋势下，使用Proventia Server IPS的全面DLP战略将：

- 实现有关数据安全性和应用保护的实时报告
- 有助于数据丢失的防止战略和前瞻性的保护，同时，还针对服务器实施企业安全策略
- 检查进入服务器的流量，阻止试图入侵和提取关键数据的恶意代码

Proventia Server IPS for Windows可无缝接入到您的IT基础设施，它由IBM SiteProtector™系统集中管理。

收益

Proventia Server IPS提供多种功能，可满足法规遵从和必要的安全技术要求，支持全面的DLP战略。

Proventia Server IPS可以保护您的服务器免受恶意攻击，同时还满足法规遵从需求。该系统可以提供实时监控，针对指定文件和文件夹中的变更发出警告。这些优势能够帮助各企业保持对于数据接入点的控制，并监控机密数据的变更。此外，应用控制还可以锁定可用于控制服务器的程序的访问。

Proventia Server IPS能够防止数据丢失。可以阻止内部/外部服务器攻击，在威胁对系统造成破坏和导致数据丢失或被窃之前将其阻止。Proventia Server IPS可以在防火墙和IPS阻止攻击之后再提供一层防护，它还包括缓冲溢出漏洞防护（BOEP）功能。

- 通过跟踪和报告工具保持合规性。接收有关权限升级、机密文件访问/修改和未经授权的配置变更的活动警告。
- 无需补丁即可保护服务器免受已知和未知攻击。无需中断服务器和应用服务器来安装紧急补丁。Proventia Server IPS可以提供以漏洞为中心的入侵防护，阻止利用已知漏洞的网络蠕虫和其他漏洞，同时，还能够阻止来自未知的缓冲区溢出漏洞的攻击。
- 审计服务器应用。在制订应用或网络锁定策略之前，对运行和访问网络的应用进行快速审计。
- 检测和响应式攻击和/或未经授权的活动。通过操作系统和应用活动日志监控来保持系统完整性和合规性。
- 实施服务器和应用策略。确定服务器上只运行获得授权的服务和应用。防止安装未经授权的程序。
- 实施网络访问策略。确定只有获得授权的应用可以访问网络，并为入站和出站流量设置端口和IP限制。
- 确定关键文件的完整性。将实时文件完整性监控与文件系统基线相结合，检查敏感文件、关键系统二进制和配置文件的完整性，跟踪未经授权的用户所进行的更改。
- 阻止未经授权的用户进行安全更改。防止任何软件工具和任何人停止或禁用 Proventia Server IPS，无论是使用本地还是远程管理权限。
- 提供本地用户接口。本地用户接口可以提供对于安全策略配置的即时访问。策略优先级可以集中控制、本地控制或共享控制（通过集中管理优先级）
- 与活动目录相集成。使用 活动目录组织结构来管理策略，监控事件并创建报表。

- 实施防病毒法规遵从。确定服务器可以接收最新的防病毒更新，并报告不符合法规遵从要求的服务器。

前瞻性的保护

有些主机保护解决方案除了提供一个本地防火墙之外，还会提供入侵防护签名。基于签名的入侵防护与防病毒签名极为相似，只能有效地阻止已知威胁－但是对于未知漏洞则一筹莫展。前瞻性的保护将以漏洞为中心的入侵防护与其他保护技术相结合，保护重要服务器不受恶意攻击。

前瞻性的威胁防护

IBM Internet Security Systems™（ISS） 通过其网络、服务器和桌面安全性产品，可以提供前瞻性的保护，其中即包括 Proventia Server IPS for Windows。 多年来，IBM ISS以漏洞为中心的入侵防护始终在保护s免受蠕虫、病毒和黑客攻击等网络威胁。

支持的平台

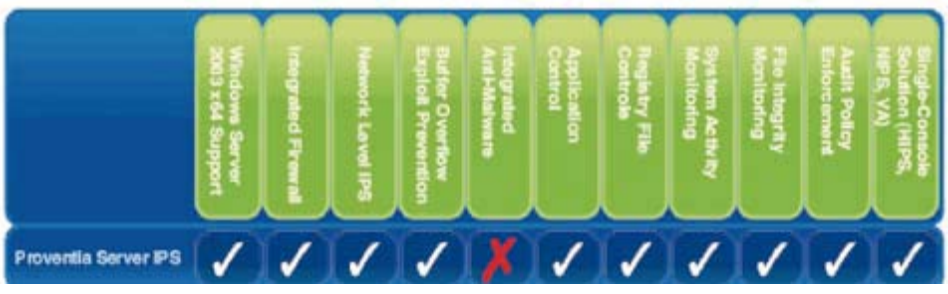
- Windows Server 2003 x64 SP2, Standard Edition
- x64 SP2, Enterprise Edition
- x64 R2, Standard Edition
- x64 R2, Enterprise Edition
- x64 SP1, Standard Edition
- x64 SP1, Enterprise Edition
- SP2, Standard Edition
- SP2, Web Edition
- SP2, Enterprise Edition
- R2, Standard Edition
- R2, Enterprise Edition
- SP1, Standard Edition
- SPI, Web Edition
- SP1, Enterprise Edition
- Windows 2000 Server SP4 andAdvanced Server SP4
- VMware ESX 2.5 & 3.0 (guest OS)

更多信息

如需有关Proventia Server IPS for Windows的更多信息，请联系IBM ISS销售代表，或者访问：www.ibm.com/services/us/iss。

关于IBM互联网安全系统公司

IBM互联网安全系统（ISS）是广受信赖的安全专家，为全球企业与政府提供网络安全产品和服务，保护他们免受互联网威胁的侵扰。IBM ISS成立于1994年，是安全领域的全球领导者，其解决方案的成本效益经过实践的检验，能够降低整个企业的法规与业务风险。IBM ISS产品与服务基于IBM网络安全系统X－Force®研发团队的主动安全智能，该团队是网络安全漏洞与威胁研究领域的全球权威。如需更多信息，请访问:www.ibm.com/services/us/iss或致电:1 800 776-2362。



RealSecure ® Server Sensor

Internet Security Systems, an IBM Company

前瞻性安全防护

企业通常依赖于关键服务器来运行应用程序和存放数据。其服务的任何中断都可能引起客户满意度的下降（收入降低和成本增加）。现在每天都能发现新的入侵、攻击和漏洞，它们持续不断地威胁着这些关键服务器的正常运转，关键服务器是攻击的焦点。因此，企业在确保服务器维护数据和应用程序正常运转的同时，还需要保护服务器环境的安全，这项任务始终是一个重大挑战。

解决方案

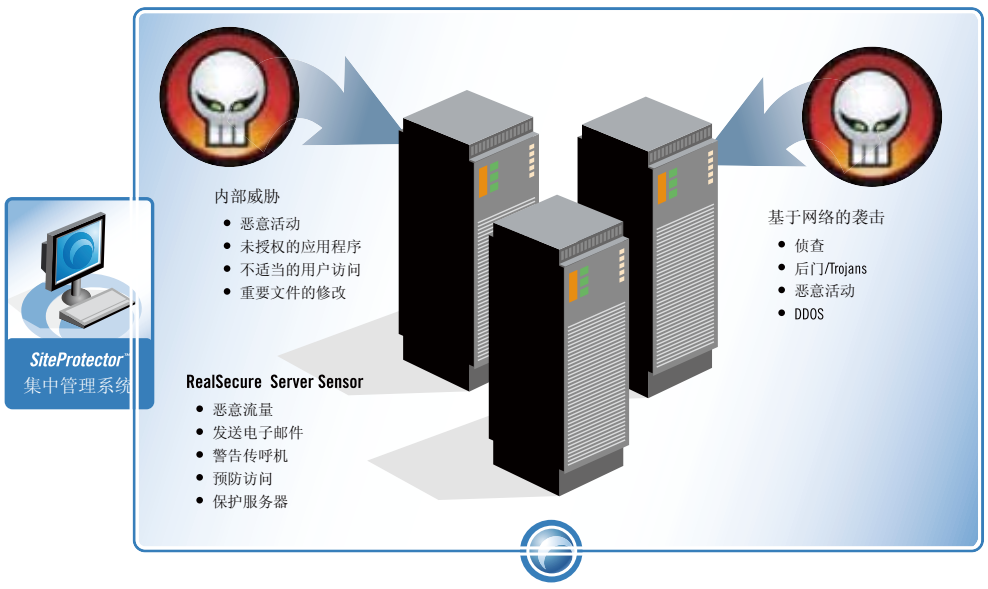
RealSecure Server Sensor可以保护关键服务器免受不断演变和发展的各种威胁的攻击，同时使服务器能够保持数据和应用程序的可靠性、可用性和机密性。RealSecure Server Sensor是业界第一个智能型、自配型和集中化管理的企业防护代理软件，它融合了强大的防火墙功能、先进的入侵防护系统功能，从而保护关键服务器。该软件持续不断地对操作系统、应用程序和网络活动进行实时监控和分析，从而保护关键服务器环境免受滥用和入侵的威胁，而对系统性能几乎不造成任何影响。

特点和优势

RealSecure Server Sensor - 通过分析关键服务器上的事件、主机日志、进出网络的活动以及阻止破坏重要资产的恶意活动，提供自动实时的入侵检测和防护功能。RealSecure Server Sensor应用复杂的协议分析、行为模式集和自动事件关联，同时预防已知和未知的攻击，大幅降低安全维护成本并且减少宕机时间。

Web 应用保护- RealSecure Server Sensor通过对恶意活动的检测来保护Web应用程序，并且通过检测SSL加密为Apache和IIS Web服务器上运行的应用程序增加额外的保护。

REALSECURE SERVER SENSOR



高级入侵防护/ 阻断 – 监控所有出入流量以便检测和预防已知和未知的袭击。这包括缓冲溢出、特洛依、暴力攻击、未授权的访问和网络蠕虫以及其他各种类型的攻击。

本地和基于网络的保护 – 通过日志监控提供灵活的检测和保护本地以及网络免受攻击。这可预防授权的用户攻击该系统，同时也预防了对系统资源的暴力攻击和未授权的使用。否则，这将危及数据机密性、完整性和可用性。

审计策略– 集中化的OS审计策略能确保所有关键服务器都有唯一统一有效的审计策略，这个策略可允许真正核心级审计的管理。

缓冲区溢出攻击防护（仅用于windows）–缓冲区溢出在高风险漏洞中所占的比重很大。IPS阻断已知的缓冲区溢出漏洞，但缓冲区溢出防护提供了更高的保护级别，这种技术能保护主机免受攻击者和网络蠕虫使用已知或未知的缓冲区溢出来攻击系统式传播。

集中管理–RealSecure server sensor能通过ISS的SiteProtector™统一安全管理平台进行管理。这种管理控制台统一管理网络、服务器和桌面等，能显著减少对员工和其他操作资源的需求。

SiteProtector™ SecurityFusion™模块–在减少错误警告的同时，这一SiteProtector插件模块通过内置安全智能也可以更精确地定位威胁安全事件。这种模块能迅速与多种原始资料中的安全资料相关联，以便增强各种威胁的分析，如对存在漏洞资产的袭击、转换和分步式袭击。

由X-Force研发组织支持–ISS的X-Force由业内最受尊敬的安全专家组成。X-Force成员研究最前沿的安全方向，通过ISS全球威胁处理中心跟踪威胁变化并确保ISS产品包含最新威胁防护技术。X-Force拥有安全管理策略方面的广泛专业知识。对分配计算、全球网络化、编程和辩论方面的深刻理解使X-Force站在最新安全发展的前列。

系统要求

支持的操作系统

- Microsoft Windows Server 2003
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Sun Solaris
- RedHat Linux
- IBM AIX
- Hewlett-Packard HP-UX

Microsoft Windows Server 2003和Windows 2000 Server认证

RealSecure Server Sensor 由VeriTest 在下列平台的基础上认证VeriTest 为微软公司的 ″Certified for Windows″ 项目进行企业测试

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server

这种严格的测试被分析者和企业认可，因为它验证了该应用程序更强大更具管理的特性和功能。

VeriTest 证书报告网址：

http://cert.veritest.com/CfWreports/server/SearchResults.asp?co=1391&1o=0&bs=Search&pr=0&pc=0

MC-RSSSDS-0305

通过IBM Proventia Management SiteProtector管理、监控和评估企业安全

集中的安全管理

IBM Proventia® Management SiteProtector™通过一个安全管理平台将策略、产品和内容更新应用于大量安全代理程序和设备。SiteProtector统一了对网关、网络、服务器和桌面以及第三方安全解决方案的管理。

SiteProtector承担起集中管理、监控和评估企业安全的任务－从而使企业不堪重负的IT人员能够集中精力关注其他关键项目。使用该产品可根据网络、网关、主机代理和设备的发现创建Helpdesk ticket和指派IT人员。或者通过同一个控制台进行信息资产发现和漏洞评估；命令和控制邮件安全和异常检测系统；分析安全性事件并报告安全流程和状态。通过集成工作流和系统管理、网络以及数据库管理工具，SiteProtector可以融入IT流程，而不只是一个安全组件。

Proventia Management SiteProtector是一个独立安全管理设备，您只需购买一个单一设备即可获得最高稳定性的安全管理能力。

IBM帮助您降低安全复杂度，并优化价值

通过使用SiteProtector的单一控制台简化安全部署和管理，IBM网络安全系统（ISS）统一了对不同安全技术的管理。这一创新的安全管理系统为以下类型的安全设备提供集中管理的命令和控制功能，可以逐个消除安全管理的复杂度：

- 高性能网络安全
- 端点或桌面安全（包括防病毒）
- 关键服务器安全
- 漏洞管理系统
- 远程办公室/分支办公室安全
- 内部安全
- 邮件安全

利用现有的基础设施

将SiteProtector整合到您现有的基础设施－包括Microsoft® Active Directory、Remedy Help Desk和SQL Server 2005，使安全修补工作成为IT工作流中更轻松的一部分。

优先防范最高风险

该系统使用关联分析来创建优先顺序和可行修补指令。通过在事件数据与特定网络漏洞之间建立关联，您可以集中精力首先使用资源来应对等级最高的风险。SiteProtector还能够忽略对企业风险很小的安性事件。

保持集中管理的安全性策略

SiteProtector系统旨在通过一个集中管理的、可对企业进行扩展的控制台来配置和实施保护策略，24x7全天候监控安全性状态，评估策略状态以及查找网络漏洞。该系统根据所有代理和应用所设置的规则或限定值进行集中响应。其全面的报告选项可以帮助您使用单一系统按照您的安全策略来评估安全合规性。

集中管理的更多优势

SiteProtector为你提供“发展空间”

一个集中管理系统必须要能够提供足够的灵活性，随着时间的推移，能够部署更多的安全控制工具。事实上，证明安全合规性还需要始终关注相关标准的修订。SiteProtector可以帮助您提供一个灵活的安全部署路线图，随着时间的推移，为您安全性功能提供发展空间。绝大多数其他同类产品都不能像SiteProtector这样，通过单一系统提供多种不同类型的安全命令和控制。通过为您的安全性基础设施添加 SiteProtector，也将带来企业安全设计的可扩展性。

SiteProtector设施合规性

SiteProtector通过全面的信息资产数据库、风险降低和补救工作记录以及集中管理的安全性策略帮助您证明安全管理合规性。由于能够提供有关资产、威胁和趋势安全状态的实时报告，该系统还能够提供商业智能，从而帮助您做出成本得当有关网络的决策。SiteProtector可以帮助您的企业采取以下措施满足法规遵从要求：

- 获得深入了解所有IT资产的可视性
- 建立一个全面的资产数据库
- 评估风险并分配补救工作
- 对被阻止的安全攻击和补救工作进行备案
- 实施集中管理的安全策略
- 针对既有安全策略的基准测试
- 推进策略管理、漏洞管理、事件响应策略和程序
- 跟踪配置和策略变更

Proventia Management SiteProtector如何能够与众不同?

对于您的所有安全技术的全面管理SiteProtector可以管理IBM保护平台，包括主机和网络入侵检测与防护、异常检测、漏洞管理、防火墙/虚拟专用网（VPN）和内容安全。

集成其他系统，优化您的投资

SiteProtector可以利用活动目录等现有基础设施进行资产识别与分类，并通过现有的域证书管理访问控制。SiteProtector还与Remedy Help Desk系统相集成，并提供一个本地帮助功能。它可以管理 Checkpoint、Cisco Pix和其它厂商的安全产品；管理网络产品，如Netcool；以及使用SQL DB集群管理数据库。

可扩展性推动部署和发展

Proventia Management SiteProtector可以支持数十万个安全设备和具有 1,000,000多个节点的网络。它使用了“建立代理”技术，能够轻松部署预配置的产品设计。凭借这种可扩展性，此系统成为政府机构、大型商业企业和金融机构的首选的解决方案。

智能关联提供更强大的安全性

Proventia Management SiteProtector系统的分析功能范围涵盖从基线视图到自定义的资产分组。通过使用IBM SecurityFusion™模块，该产品还可以通过在实时漏洞和威胁信息之间建立关联从而迅速辨别安全威胁。因此，它使您的员工可以集中精力应对实际的安全威胁。它可以通过丢弃未成功的攻击来提高警告的优先级，并减少控制台和数据库集群。

功能强大的报表进一步降低风险

Proventia Management SiteProtector可以提供灵活且功能强大的企业级报表。它提供数十个预定义报表和自定义报表，支持企业提供：

- 策略和合规性管理报表
- 审计和管理报表
- 漏洞和配置管理报表
- 事件和事件管理报表
- 用于业务管理的报表，包括整个合规性等级、决议、当前的威胁和企业范围趋势
- 为技术经理提供的粒度报告，在资产、操作系统和业务部门层面上详细说明合规性

SiteProtector系统的报表功能可以证明合规性，并进行攻击分析。它根据法规遵从标准分类IT资产。此外，其关于漏洞和威胁补救的报告还可以让您直观了解企业的安全状况。SiteProtector以最完善的安全智能的丰富经验，向客户提供最佳的保护。

IBM ISS提供全面的安全管理功能

IBM ISS可以为企业提供端到端的安全保护。Proventia Management SiteProtector是一个集中管理平台，将网络、服务器、桌面与漏洞管理与保护合为一体的完整的解决方案。

更多信息

有关更多Proventia Management SiteProtector信息，请就近联系IBM办事处或访问：ibm.com/services/us/iss。

IBM Proventia Network Mail Security System

- 保护邮件用户免受垃圾邮件的困扰
- 正确识别并阻止各种零日病毒
- 阻止超过120,000种已知病毒
- 提供可定制的事件报告
- 提供7×24小时的技术支持

持续地抵御垃圾邮件、病毒邮件以及其他的恶意流量

IBM ISS的Proventia Network Mail Security系统针对企业的信息平台提供了前瞻性的防护和垃圾邮件的控制。Proventia Network Mail Security系统包含了可定制的分析模块使得系统可以非常方便地适应企业的需求并强制设备来接受这些策略。IBM ISS有着业界领先的端到端安全解决方案，覆盖包括了对于终端、服务器、网络和网关的安全防护，其中Proventia Network Mail Security是整个安全解决方案中非常重要的组成部分。

Proventia Network Mail Security系统针对于不同规模的企业设计提供了两种解决方案：硬件设备；虚拟平台。任何形式的Proventia Network Mail Security系统会均会进行自动更新并作为邮件安全网关来持续抵御垃圾邮件、病毒邮件以及其他恶意流量，为企业用户提供了业界领先的前瞻性的防护。

特点及优势	
安全威胁管理	
入侵防护	• 保护设备以及邮件服务器不会受到攻击，例如：拒绝服务（Denial of Service）攻击、帐户收集（directory harvest）攻击、缓存区溢出（buffer overflow）攻击 • 由IBM ISS的X-Force研发团队来进行安全漏洞的研发 • 提供IBM ISS虚拟补丁技术
Patented virus prevention system (VPS)	• 利用了基于行为的防病毒检测技术 • 提供了前瞻性的防护而不是单纯的基于病毒特征检测 • 阻止各种零日病毒 • 检测并分析Spyware
基于特征的防病毒系统（可选）	• 可识别并阻止超过120,000的已知病毒 • 对于进出的邮件均进行检测 • 可检测邮件的附件内容（包括已压缩文件）
垃圾邮件控制	• 垃圾邮件检测命中率（包括带附件的）超过98% • 误报率低于0.01%（1 in 10,000） • 超过20种可定制的分析模块 • 被识别的垃圾邮件可以被隔离/阻止/标识 • 嵌入式的URL过滤 • 可基于Global/Group/User进行不同的设置 • 支持多国语言 • 超过10种不同的操作类型
垃圾邮件分析模块	• Spam real-time blackhole list (RBL)检测 • Spam指纹检测 • Spam特征库 • Spam Bayesian classifier • Spam架构检测 • Spam流检测 • Spam URL检测 • Spam关键字检测 • Spam启发式检测 • 网络钓鱼检测
附加的分析模块	• 消息字段检测 • URL检测 • 附件检测 • 语言检测 • 关键字搜索 • 黑白名单

	• 组合分析 • 病毒检测 • 发件者策略架构 • 信用卡号码/身份证件号码识别
内容过滤	• 私有内容分析引擎 • 过滤进出的流量 • 可基于Global/Group/User进行不同的设置
IBM Proventia Network Mail过滤库	• 全球最大也是更新最快的过滤库 • 通过对62亿个URL、Image、垃圾邮件的分析而建立起来的超过8000万个过滤条目
管理选项	
IBM Proventia Management SiteProtector	集中进行策略管理、配置、更新、报告和告警
本地管理接口（LMI）	• 初始化网络配置 • 关机 • 重启
集成LDAP	支持IBM Lotus Notes/Domino，Microsoft Active Directory，Novell eDirectory，Netscape，SUN and OpenLDAP
设备健康监控	• SiteProtector接口 • 本地管理接口 • 支持SNMP、Syslog、通过SiteProtector Management console实现基于邮件的告警
集群/高可用性	通过主设备可访问到被隔离的邮件以及跟踪信息 注：Clustering仅限于MS3004
全球级别的技术支持	提供7×24的技术支持，包括平台升级
MS3004技术参数	
型号	MS3004
机架高度	2U
可测量性	最高支持到10,000个用户，支持集群环境
最高吞吐率	
原始邮件	750,000邮件/小时
实际环境流量	36,000邮件/小时（实现全部的分析和隔离操作）
平台	基于Linux
存储	4×80GB＋2×250（RAID1）
冗余	硬盘、电源、风扇
尺寸	
高度（英寸/毫米）	3.40/87.5
宽度（英寸/毫米）	16.93/43
深度（英寸/毫米）	26.46/67.20
重量（磅/千克）	60/27
功耗	
单位	AC
电流	8.9/5.4
电压(V)	115/220
输入范围(V)	110-128/200-240
工作温度	+50ºF to +95ºF (+10ºC to +35ºC)
非工作温度	-40ºF to 158ºF (-40ºC to +70ºC)
湿度	95% @ 30ºC (90ºF)
电磁辐射	FCC Class A
MS1002-VM技术参数	
可测量性	理论上适用于不超过1,000用户的中小型企业，也可以基于硬件进行相应扩展
平台	基于下列平台上安装的VMware Workstation： Windows 2000、XP、2003 RedHat Enterprise Linux 2.4或者2.6
系统需求	以下为安装Proventia Network Mail VMware virtual installations的最小硬件需求软件需求： • VMware GSX Server 1.0.2 or later • VMware Workstation 5.5 or later • VMware Player 1.0.3 or later 主机硬件需求： • 2GB RAM(每个虚拟机至少需要512M RAM) • 100GB Hard disk space(每个虚拟机至少需要30G硬盘空间) • 2 Network Interface(1 Host Only Interface/1 Bridge Network Interface) 虚拟主机硬件需求 • 512MB RAM • 30GB disk space

IBM Internet Security Systems
IBM Proventia
企业扫描器

IBM Proventia 企业扫描器 (Enterprise Scanner) 能分辨危险所在位置，提出优先顺序保护行动，并对结果产生报表说明。企业扫描器可有效地保护关键业务的可用性，保护企业数据。

优点

- 降低网络在线时的风险，能有效保护重要资产，提高带宽使用效率
- 自动扫描过程帮助企业减轻资源
- 利用企业现有基础架构，与活动目录、资产管理数据库、工作流程系统无缝结合
- 信息只需存储一次，即可在各系统分享，避免重复作业
- 避免紧急补丁操作，按正常更改控制流程：ISS 虚拟补丁技术能有效弥制造商提供正式补丁前的安全防护措施
- 满足符合性要求，提供强大审计功能

功能特点

- 能缺省有效识别2,691种资产类别，包含桌面机、服务器、路由器、交换机、应用程序和操作系统
- 能有效辨别新近连接上的设备以及之前在网络上未发现的资产
- 可追踪被指定的特定资产状况并记录
- 能和 IBM Proventia ADS设备整合做资产管理

多重来源发现

- 主动式发现扫描
- 活动目录导入
- 基于IPS 的发现
- 基于 ADS 的发现
- 资产数据库导入
- 手册输入
- 定制服务发现

资产辨别技术

- Ping sweep
- UDP 探查
- 资产指纹识别
- 快速发现
- 基于NetBIOS 的发现
- TCP 的发现
- UDP 端口发现
- 操作系统指纹识别
- 应用程序指纹识别
- 集成 NMAP 4.0数据库

网络服务识别

- 2,691种

资产分类

- 阶层式的分组架构可对应至公司的组织，以利于扫描及报表的内容对应关系
- 活动目录导入和对应
- 资产资料库导入
- 区域、组织、拓扑或系统级的分类管理

漏洞评估

- 基于发现的评估
  - 高效能的漏洞评估
- 脚本评估
  - 允许无需程序更新即可加入新内容
  - 提供少量资料内容更新(XPU更新)。
  - 更快的提供安全内容
- 攻击模拟
  - 执行特定测试(不影响网络)，以分析真实攻击可能造成的影响
- 利用著名的ISS X-Force数据库识别可能导致危害
  - 资产的漏洞或程序错误

- Frost & Sullivan 2005 年评选ISS 漏洞评估产品为市场领导产品
- 对主机优先顺序扫描评估

虚拟补丁技术提供安全内容更新

- 前瞻性的威胁防护技术，由著名的IBM ISS -Force 研究机构所主导

间谍软件扫描

- 检测间谍软件

“信任X-Force ”选项

- 根据X- Force 专家的建议自动检测新的漏洞

扫描视图

- 打开扫描视图时自动扫描
- 自动中断/ 自动恢复 - 关闭扫描视图时自动暂停，开启扫描视图开启时自动恢复
- 扫描视图配置简单轻松
- 在视图扫描开启期间可定时自动新数据，确保最新的弱点信息
- 分组扫描视图

工作流程

- 漏洞分级
- 内部工单系统
- 集成Remedy
- 开放API 支持其他工单系统
- 所有者指派和追踪
- 行动日志和追踪
- 传统 〝补丁并保护 〝补救法
- 虚拟补丁技术和ISS 入侵防护系统可整合使用
- 自动解析功能
- 单工单多漏洞
- 状态监控和追踪（8 级）

扫描及阻断保护

- 结合IBM Proventia IPS形成漏洞弱点防护系统，无部署商补丁
- 和Proventia SiteProtector 管理平台无逢整合
- 检测漏洞并辨识在IPS 中相应的阻断方法
- 和IPS 系统可通过同一平台管理和互动

报表

- 提供报告来描绘组织内的信息
  - –针对组织内的分组风险状况作报告
  - – 根据地区、网路、业务系统或其他的资产组合形成分组报告
  - – 在正确的时间提供风险报告给正确的人，快速针对不同地区业务系统或位置提供比较报告
- 灵活定制视图，分析报告共有超过1,800 种之多
- 企业级多重扫描报表分析
- 扫描前可先预设报表
- 报表可输出成PDFTM, CSV, HTML 格式
- 可依时间计划排定报表输出
- 网站浏览式报表
- 快速分析报表
- 强大的过滤功能

自动化

- 减少人工作业，省钱省时
- 自动和连续性扫描
- 扫描优先顺序排列
- 团队扫描
- 通过xpu更新漏洞信息
- 资产分类及群组

基于Linux® 易于安装的设备

管理

- 由 SiteProtector 进行管理，SiteProtector 是屡获大奖的集中平台可提供安全业界唯一同时可以管理保护网络，服务器和桌面型电脑的系统
- 紧急扫描服务，依据需求提供快速的网络扫描服务
- 根据最新的威胁自动更新安全智能数据库
  - – 由XPU是全球知名的IBM X Press研发组织提供的安全更新

用户介面选项

- Proventia SiteProtector 集中式管理平台
- 基于Web 的 Proventia Manager 本地管理界面

Proventia SiteProtector 管理平台

- 集中命令、报表、分析
- 用户审计
- 强大的事件分析

Proventia Manager

- 基于Web 的本地管理界面(LMI)
- 设备配置和 SiteProtector 建立通讯连接

设备健康监视

- SiteProtector 集中式管理界面
- 基于浏览器的本地管理界面

基于资产的管理

- 以资产为中心的评估策略
- 分组资产扫描策略
- 刷新评估周期
- 扫描视图
- 用于Windows和SSH评估凭据
- 评估策略
- 发现策略/ 自定义扫描目标

相关性

- 支持 Security Fusion TM 模块
- SiteProtector快速分析和集中关联分析

独立发现与评估

- 单独策略
- 单独扫描视图
- 单独刷新间隔

世界级支持

- 7天24小时支持，包含平台更新

规格

扫描接口

- 5个千兆以太网络接口(1 个使用，4个备用)

管理接口

- 1个千兆以太网络接口

Console口

- 1个串接口

USB接口

- 2个前置USB2.0 接口

LCD显示

- LED面板
- 4个按钮

LED标识电源状态与数据访问

- LEDS

电源

- 全范围250W ATX PSU
- 自动切换

尺寸

- 42.9 公分长 × 38.2 公分宽 × 4.4 公分高

重量

- 6.5 公斤净重

工作环境

- 温度: 5℃ -35℃
- 湿度: 20%-90% RH

存储环境

- 温度 -20C-70C

认证

- CE/FCC/UL/cUL

实体特征

- 机架高度，1-RU
- 安规标准，FCC A 类

性能

高可用性/ 高效能配置

- 多个扫描器可连接形成自动负载均衡功能

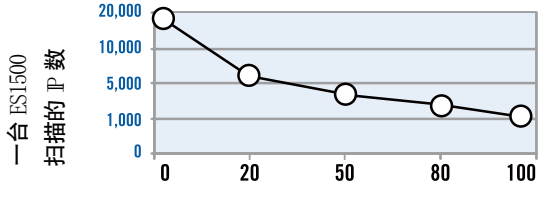
部置位置

- 网络核心
- 网络边界
- 网络外围

使用Pinger 的发现扫描性能

- 于0% IP空间(0% Populated IP Space)
  - 每小时19,794 个IP

使用 Pinger程序发现需要的时间



- 于20%IP空间
  - 每小时6,621个IP
- 于50%IP空间
  - 每小时 2,590个IP
- 于80% IP空间
  - 每小时2,008个IP
- 于100% IP空间
  - 每小时1,605个IP

未使用Pinger 的发现扫描性能

- 于0% IP 空间
  - 每小时2,289 个IP
- 于 20% IP 空间
  - 每小时2,713 个IP
- 发现 50% IP 空间
  - 每小时 2,580 个IP
- 发现 80% IP 空间
  - 每小时 1,953 个IP
- 发现 100% IP 空间
  - 每小时 1,648 个IP

性能特点

- 动态可检查项分派可用于辨别及执行和操作系统相对应的检查
- 多个扫描器之间的负载均衡

扫描时间工作分派

- 可在增加一个扫描器后自动透明的进行负载均衡功能
- 透明的负载均衡

分布式扫描

- 在网络内不同地区增加多个扫描器，达到最佳化效果
- 多个扫描器以代管方式做负载均衡

性能特点:

全面评估(启用所有非 DOS 选项)*

- 每小时803个设备

注：评估并无数量限制，只是评估是以发现主机设备为主

扫描团队效能分析

（使用多个扫描器来改善性能）

扫描团队	减少百分比		
	发现	评估	时间
1个扫描器	0%	0%	(基础) 1小时
2个扫描器	45%	45%	35分钟
3个扫描器	60%	60%	24分钟
4个扫描器	70%	70%	18分钟
5个扫描器	75%	75%	15分钟
6个扫描器	80%	80%	12分钟

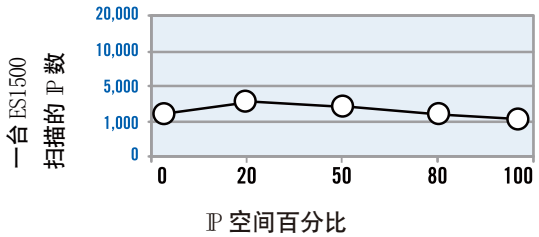
请即联系IBM，评估Proventia网络企业扫描器系统!

Proventia网络企业扫描器也是IBM Internet Security Systems安全服务的重要部分。IBM安全服务提供7天24小时全年无休的专家监控及保护。请您就近咨询IBM Internet Security Systems办公室。即可发现企业扫描器如何保护您的资产，杜绝各种威胁。关于ISS办公地点及产品信息，请访问www.iss.net。

并于IBM Internet Security Systems

IBM Internet Security Systems是全球五百家企业及政府单位信赖的网络安全供应商。ISS提供前瞻性的安全系列产品来保护客户宝贵的数字资产。IBM Internet Security Systems成立于 1994年，总部在美国亚特兰大，并在纳斯达克上市(ISSX)。IBM Internet Security Systems全球有超过 11,000个客户。目前在27个国家设有分支机构，并拥有1,200名员工。

使用 Pinger 程序发现需要的时间



Internet Scanner® 漏洞评估系统

Internet Security Systems, an IBM Company
前瞻性安全防护

智能扫描代理

通过使用动态检查项分配（Dynamic Check Assignment），InternetScanner与其他产品相比都能以更高的准确度和更快的速度来识别更多资产并找出更多漏洞。

策略管理

用户可以自定义用来扫描的策略；内含预置的20条标准扫描策略。特点包括:

- 20条默认扫描策略
- 自定义扫描策略
- 生成新模板功能
- 编辑/更改策略
- FlexCheck自定义项实现的自定义检查（用户定制）
- 可搜索的策略系统（通过CVE、通配符、漏洞名称）

管理、访问和控制

可使用授权管理进入到终端系统进行深层扫描；可识别特权管理账户以获得更多关于网络设备的信息。功能包括:

- 域帐户注册与支持
- 支持访问终端系统
- 已知帐户模糊化管理
- 数据库管理
- 增强的命令行界面
- 程序文件位置定义
- 扫描器DSN修改
- 本地记录

资产识别

使用协议栈指纹识别技术并从您公司已存在资产数据库中导入信息。可识别超过1300种资产类型（操作系统和网络设备）:

- 集成NMAP指纹识别
- 使用自定义指纹识别
- 扫描时间Ping资产识别
- 主机文件导入
- 主机列表生成器
- 主机文件导出
- 范围列举
- DNS名称
- IP地址识别
- NetBIOS名称
- NetBIOS域
- 操作系统类型
- MAC地址
- IP 协议栈指纹识别
- 开放端口旗标识别

实时显示选项

在屏幕上显示出漏洞识别和易受攻击主机的快速识别信息。屏幕显示功能包括:

- 主机视图
- 漏洞视图
- 服务视图
- 帐户视图
- 包含检查进程功能的实时活动监控
- 主动会话监控
- 扫描状态窗口
- 敏感内容窗口

本地扫描控制

通过使用自动化执行任务工具，如合并扫描会话等来使扫描操作人员能够对扫描器进行准确控制。节省扫描操作人员的时间。此功能特点包括:

- 立即扫描
- 停止扫描
- 暂停/ 恢复扫描

- 多扫描线程支持
- 合并扫描会话
- 编辑传感器属性
- 拒绝服务检查隔离
- X-Press UpdateTM产品更新

全面的漏洞类目

用来指导用户了解漏洞的根本原因，漏洞的详细描述。消除漏洞的补救步骤，以及连接到相关链接以获得更多信息。提供专业化安全防护信息，包括:

- 本地帮助
- 补救信息
- 基于漏洞的信息报告

报告

使您可以在整个公司层面实现快速方便的信息共享。超过74种预先定义报告的全套组合包括:

- 管理层报告
- 各级管理报告
- 技术报告
- 趋势报告
- 操作系统报告
- 支持多种语言
- 导入自定义报告

Internet Scanner可识别以下一些漏洞类型/ 类目:

Brute Force密码穷举暴力攻击
后门
浏览器
CGI-Bin
Daemons
DCOM
拒绝服务（DOS）
DNS
电子邮件
防火墙
FTP
信息搜集
即时信息（IM）
LDAP
NetBIOS
网络
Network Sniffer
NFS 系统需求
NIS
协议欺骗
路由交换
RPC
共享
SNMP
Web 扫描
Window 关键问题
Windows 组
Windows Networking
Windows 密码检查
Windows 密码策略
Windows 补丁
Windows 策略问题
Windows 注册表
Windows 服务
Windows 用户
X-Windows

Internet Scanner 可识别超过1300 多种不同资产类型上所存在的风险，包括以下操作系统:

AIX
BeOS
BSD generic
Caldera OpenLinux
Caldera UnixWare
Cisco IOS
Fedora Core
FreeBSD
HP Apollo Domain/OS
HP-UX
IBM AS/400
Immunix
NEC UP-UX/V
NEC UX/4800
NetBSD
NeXTSTEP
Novell NetWare
OpenBSD
Slackware Linux
Solaris
SunOS
SuSE Linux
Trustix Secure Linux
Turbolinux
Compaq True64
Conectiva Linux
Convex OS
Debian Linux
DG/UX
EnGarde Secure Linux
IRIX
Linux
Mac OS
Mandrake Linux
Microsoft Windows 所有版本
NEC EWS-UX/V
OpenVMS
OS/2
OS-9
QNX
RedHat Linux
SCO Open Server
Ultrix
UNICOS
UnitedLinux
VxWork

SiteProtector 所能提供的附加功能

企业级可扩展性

SiteProtector控制和操作着数百个远程扫描代理，能够快速地对结果生成报告。通过这种大型企业的可升级能力，SiteProtector提供了以下漏洞管理功能:

- 多扫描器控制
- 多层体系结构
- 分布式漏洞收集
- 企业数据库支持
- 多站点支持
- 具有漏洞关联功能的企业级仪表板
- 多窗口视图
- 集中式服务器

漏洞管理

ISS 的SiteProtector™ 集中管理平台控制多个Internet Scanner，提供一个全面的企业漏洞管理系统。

企业级报告

能够进行多扫描器/ 多线程的扫描企业关联、汇总与报告。包括所有独立扫描器报告功能，以及:

- 企业多次扫描报告
- 预扫描默认报告
- 以pdf、csv以及html格式导出报告
- 以组为基础生成报告
- 定时报告
- 可Web 访问报告
- 快速分析报告
- 全面过滤功能

远程扫描能力

可控制和操作位于远程办公点或防火墙后的扫描代理。远程操作包括:

- 立即扫描
- 编辑策略
- 停止扫描
- 暂停/ 恢复扫描

自动化可定时命令

消除了对手动运行循环扫描的需要。任务计划器消除了繁琐步骤并节省了您的时间:

- 立即扫描
- 停止扫描
- 生成报告
- 应用X-Press更新

用户管理

授权多个用户以不同权限登录控制漏洞管理进程。功能包括:

- 使用域帐户角色管理(可选）
- 使用本地帐户管理
- 多用户角色
- 以组为基础的用户访问控制

资产管理

通过以下功能使您能够方便并准确地识别、分组、并管理信息资产:

- 活动目录集成
- 自动资产分组
- 手动资产分组
- 整合防护视图
- 定制组名称
- 以组为基础报告
- 多层次资产分组
- 以组为基础的用户访问控制
- 未分组资产识别

发现和评估

包括以ISS安全架构上的流量分析为基础进行自动（被动）信息资产发现；在新资产被增加到网络或组中时，系统按用户自定义的类别或保留在“未分组资产”中来帮助识别新资产。

更新

接受定期安全防护内容更新以增强扫描和漏洞管理功能。更新包括:

- X-Press更新产品增强与服务包
- 自动内容更新
- 按需更新
- 定时更新
- 通过Web更新
- 离线更新
- 集中更新服务器
- 更新镜像

数据和漏洞分析视图

实时显示安全防护信息；灵活的显示提供了对事件具体情况或概要信息的视图；在创建了分析视图之后，可以保存、调用或与其他用户共享。显示项包括:

- 基于组的分析视图
- 17种默认分析视图
- 右键点击数据导航（快速分析）
- 自定义视图
- 漏洞清除
- 漏洞事件创建
- 异常漏洞创建
- 连结到事件具体细节
- 查看漏洞信息
- 目标分析模式
- 传感器/ 扫描器分析模式数据

导出到打印机

- 含有漏洞信息的数据导出
- 定时数据的导出
- 图形化分析视图
- 基线和比较视图
- 返回基线
- 组过滤
- 分析视图过滤
- 自定义分析显示
- 综合漏洞视图

管理功能

- 支持Internet代理
- SSL加密通讯
- 可信证书支持（SSL）
- 可选本地文档
- Web 文档
- 管理跟踪（本地日志）
- 用户审核

数据维护

- 提供定时备案
- 立即清除数据
- 按计划清除数据
- 数据备份
- 整理碎片

MC-ISVAADS-0405

整体分析业务驱动的安全性

摘要

“所有企业都在不停地寻求通过新方法在风险与最佳回报之间实现最佳均衡。对于IT安全专家来说，在业务目标和投资回报上客观地分析风险是最艰巨的工作。虽然看似违反常理，但企业的最终目标不是零风险— 把自己封闭起来是实现零风险的最佳方法，就像交换机抵御安全攻击最保险的做法是根本不开机一样－ 而是在公司能够容忍的‘风险极限’范围内实现最大经营绩效。每个业务决策都有风险，在风险适度的条件下实现最大回报才是最明智的IT决策。”[1]

网络安全工业联盟(Cyber Security Industry Alliance)日前开展的个人用户调查显示：

- 44%的回答人认为自己在开展电子商务时信息是安全的。
- 50%的回答人拒绝在线采购，因为他们害怕金融信息被盗。
- 94%的回答人认为身份盗用属于严重问题。
- 只有24%的回答人相信企业会采取适当措施来保护信息系统和网络。[2]

由于新兴威胁是有组织的攻击并且通过渗透公司网络使公司蒙受巨大经济损失，因此，企业需要识别和抵御快速增长的新兴威胁。

IBM提供全面而深入的解决方案和服务来帮助企业采用业务驱动的全局方法基于IT管理框架调整安全措施。

概述

现在的企业领导人面临多重挑战：在竞争极为激烈的商业环境中进行创新；迎接高度动态的法规合规挑战；加速实现投资回报以便解决IT预算紧缩问题；保护企业免遭不断发展的、手段越来越高明的威胁。然而，不同于其他业务挑战，企业通常采取技术驱动的方法来保护基础设施，在现实中业务驱动的方法必要的。

业务驱动方法指的是由业务目标决定企业保护要求，这种安全保护方法有别于技术中心方法。企业常采用从下到上的方法来保护安全性，这是因为安全解决方案供应商通常为客户推荐这种方法。为了解决既定的安全问题，企业通过不断增加安全投资的做法来扩展防御范围并提高防御能力。这个技术中心方法论常促进企业构建过度复杂和脱节的安全基础设施，很难管理且易于出现不可预测的安全漏洞。此外，企业还要承担不断增加的IT成本压力，最终引发运行效率低下问题，阻碍而不是促进业务增长。

公司应了解对公司最有意义的安全风险管理活动，并为它们分配优先级，而不是试图抵御所有能够预见的安全威胁。通过了解公司能够承受的风险级别，IT部门可以更轻松地集中精力去牵制不容忽略的风险。过分强调某些风险将造成资源浪费，同时对其他风险重视不够，产生严重后果。

企业发现自己很难找到端到端的战略性安全方法来支持驱动创新和降低运行成本等业务目标并满足采取法规合规措施及抵御内外部威胁等运行要求。本文将介绍公司应采取哪些措施从业务和运行的角度提高安全工作的成效，并讨论IBM如何凭借领先的安全优势帮助企业取得成功。

优化并保护业务流程

通过部署广泛的功能来抵御最常见的威胁是盈利性企业心中根深蒂固的常见安全保护模式。这种安全保护方法致使企业部署了大量孤立的安全工具。这些工具不仅缺乏通过协作来抵御手段最高明的有组织攻击的能力，而且还存在许多缺陷，包括阻碍企业提高运行效率、产生多余成本、带来IT复杂性、运行孤立性以及无法提供适当的评估标准来帮助重视业务的安全执行官决定业务效率等。

脱离了企业中的其他业务活动，安全性将无从谈起。企业应从业务的角度去审视安全问题— 将安全性作为手段来保护并增强业务流程。对于这一点，大多数企业都选择了80/20规则：少数几个业务流程的业务风险至少是80%，其他多个业务流程的业务风险不到20%。为了根据业务优先级安排安全保护工作，企业应重点保护业务风险极高的那几个流程。此外，企业还必须基于风险和安全漏洞对公司最关键业务流程的中断影响为它们分配优先级。

这个战略需要企业开展适当的规划和评估工作以便找出主要业务领域的风险，包括整条业务链中的人员、流程、数据和技术。此类规划能够促进设计并构建业务驱动的蓝图和战略以便有效保护整个企业— 满足业务需求并优化经营业绩。

跨越所有风险领域保护业务流程

IT决策与业务决策一样，都是为了在能够容忍的风险级别条件下最大限度地提高投资回报。企业需要在五个主要安全区域实施潜在的风险及影响力检查。企业必须在这些区域中定义并管理可接受的最大风险级别，这一点至关重要。没有任何企业能够牵制全部风险(或者说从成本的角度出发不应该去牵制全部风险)，但他们必须在业务目标上客观地分析风险。

- 人员和身份 — 企业需要确保公司内部及供应链上的人员能够在需要时访问所需数据和工具，同时阻止不当访问和非法访问。在这个领域，企业必须解决的业务问题是有效管理入职或离职的动态工作量，增强客户、供应商及业务伙伴之间的安全协作。此外，IT法规合规仍然是企业必须考虑的问题，也是驱动企业实施全面的用户配置流程的主要作用力。企业应采取适当的安全控制措施来跨越多个技术系统，安全地管理用户权限，确保最终用户根据既定策略访问适当的IT资源。

- 数据和信息— 企业需要支持广泛的电子协作，同时保护关键数据— 无论是传输中的数据还是闲置数据。企业需要了解关键数据的保存位置并应用适当的方法论来管理与数据分类、优先级分配和保护相关的所有流程。有效的信息安全性要从适当的风险评估方法开始，在风险与数据的可用性和保密性之间达成最佳均衡。企业在实施这种方法时应考虑到保护整个企业中所有数据的价值，防止它们被滥用和误用。对许多企业来说，他们最关心在人手和能力有限的情况下，如何实施如此全面的数据安全解决方案。企业可通过评估并报告企业的IT法规合规状态来保护数据。此外，识别、划分优先级并保护敏感数据以及采用有效的安全控制措施都是实现并保护企业信息价值的主要手段。

- 应用 — 企业需要在整个生命周期中主动保护关键业务应用和流程，免遭内外部威胁的攻击— 从设计到实施直到生产。实现这个目标通常需要集中验证、访问和审计策略管理、Web应用安全漏洞扫描和入侵防御等功能。无论应用是面向内部的应用－如通过服务导向架构(SOA)提供的客户关系管理－还是全新客户门户等面向外部的应用，明确定义的安全策略和流程对于确保新应用支持业务而不是带来更多风险都将发挥至关重要的作用。

- 网络、服务器和端点— 对公司的网络、服务器和端点主动实施威胁和安全漏洞的监视和管理对于公司钳制新兴威胁，防止它们对系统组件以及相关人员和业务流程产生负面影响至关重要。由于新兴威胁是有组织　的攻击并且通过渗透公司网络使公司蒙受巨大经济损失，因此，企业越来越重视识别和抵御快速增长的新兴威胁。例如，企业利用虚拟技术来实现更快速、更灵活地交付服务的目标。通过在这个环境中构建安全控制架构，企业可实现虚拟化目标— 如提高物理资源利用率、提高硬件效率并降低电力成本等 — 同时坚信虚拟系统能够像物理系统一样得到严格保护。

- 物理基础设施— 保护公司的基础设施还意味着确保物理资产免遭安全威胁的攻击。要想有效地保护物理资产的安全性，企业需要通过集中管理系统来监控公司财产、员工、客户和普通大众。例如，通过摄像机和集中监视产品来保护数据中心外围对于管理公司IT资产的访问至关重要。因此，对于银行、零售商店或公众代理机构等担心盗用和欺诈的公司来说，应定义并实施集成物理安全监管战略－包括监视、分析和集中控制功能－这一点至关重要。这种方法使企业能够从多个来源提取智能数据、比手动监视环境更加快速地响应威胁并降低成本和信息丢失风险。

每个公司都应了解这五个领域的风险并管理风险。遗憾的是，大多数安全解决方案供应商都只是关注一个或两个领域，更糟糕的是，他们只关心去保护一个领域中的一项技术。因此，他们提供的点解决方案无法保护整个企业中的所有业务流程，还创建了安全孤岛来加剧了复杂性、留下安全漏洞并最终导致公司无法满足总体业务需求。

利用业务驱动的方法来提高IT安全性

现在的企业执行官都希望如同CFO一样管理自己责任领域的风险，他们需要将安全风险及其IT影响通知给企业中的其他业务执行官。此外，他们还需要调节IT安全控制措施，以便与业务流程保持一致，同时从业务的角度监视并量化IT风险，大幅度提高执行官级别的业务水平洞察力。他们需要管理风险并调节安全运行工作，同时确保法规合规并优化经营绩效。

在企业保护业务流程时，业务驱动的方法将成为通过互相促进的全局方法来保护所有安全领域并确保与公司总体业务目标相一致的主导方法。否则，公司将因为IT与业务战略脱节而易于遭受安全风险。

通过业务驱动的方法来保护IT安全性还能帮助公司通过独特的业务目标来决定法规合规目标，而不是让法规合规目标来决定业务。太多的公司投入大量精力和物力来确保满足行业和政府的规章制度，但他们最终只是发现主要业务流程仍然易于遭到攻击，可惜为时已晚。从业务驱动的角度利用安全管理解决方案将使公司能够成功保护这些业务流程，同时提供必要的证据来证明自己遵纪守法。

通过IBM解决方案最大限度地取得业务成功

作为行业分析家公认的顶级安全解决方案供应商，IBM提供全面而深入的解决方案和服务来帮助企业采用业务驱动的全局方法基于IT管理框架调整安全措施。IBM允许企业动态监视并量化安全风险，以便更好地了解威胁和安全漏洞的业务影响，通过安全控制来更好地响应安全事件以便优化经营绩效，更好地量化安全投资并为它们分配优先级。IBM可帮助企业简化并自动化业务控制流程，从而大幅度节省成本，同时做出明智的资金和资源分配决策，以便管理安全风险并帮助企业创造更高的商业价值。

IBM凭借无与伦比的能力来驱动业务创新并跨越所有风险领域保护运行流程。IBM全面的解决方案和服务包括身份识别和访问管理、信息和数据安全性、应用安全性、威胁和安全漏洞管理及物理安全性等组件，可帮助企业降低安全管理的复杂性并实施全局安全管理战略来优化经营绩效。

更多信息

如想详细了解IBM安全服务和解决方案如何帮助公司从全局的高度协调并实施企业级安全措施以便最大限度地取得业务成功，请与当地的IBM业务代表或IBM业务伙伴联系，或者访问：ibm. com/itsolutions/security。

关于IBM服务管理解决方案

IBM服务管理解决方案能够帮助企业始终给用户、客户及合作伙伴提供允许有效管理的、安全的、高质量的服务。无论规模大小，企业都能利用IBM服务、软件和硬件来规划、执行并管理他们的服务和资产管理以及IT开发和IT运行计划，提供全面的客户体验、最佳业务实践和基于开放标准的技术。作为战略合作伙伴，IBM可帮助客户实施适当解决方案来快速实现经营绩效并加速业务增长。

企业磁带加密

Jon Oltsik
Enterprise Strategy Group
08/2006

概述

几乎每一天，您都会在各大报纸的醒目位置看到公开披露数据违规行为的新闻。有些事件是笔记本电脑丢失所致，其他事件则是恶意攻击所致。但是，在这些事件中，影响最恶劣的事件都是因为备份磁带被盗或丢失。因此，磁带加密理所当然地成为现在最炙手可热的话题。

ESG认为，磁带加密应该尽早考虑，并很快将会得到普及。然而，大多数企业在考虑磁带加密时仍然只是围绕着眼前的需求考虑，这种目光短浅的策略已经不能适应时代的发展。本文将要得出的结论是：

- 磁带加密必须同时支持业务和IT的发展。企业不能只将磁带加密视为基本保障措施，而是应该通过磁带加密来实现安全的业务流程，如涉及到磁带的数据共享和记录保存等。此外，磁带加密在满足此类要求时不能给IT增加任何不必要的运行负担或安全风险。
- 企业级磁带加密(ETE)架构是关键。大型机构应追求包含加密服务的磁带加密架构，而不是单纯地部署磁带加密产品。磁带加密架构将帮助确保磁带加密足够灵活，能够适应配置变化并满足可扩展性要求。
- 用户必须解决短期安全漏洞，同时为满足长期需求做好规划。由于磁带加密已经是企业必须满足的要求，因此，CIO不能坐等供应商开发下一代ETE架构，而是应该明智地即刻购买能够进行集成并适应未来发展变化的开放式磁带加密解决方案。

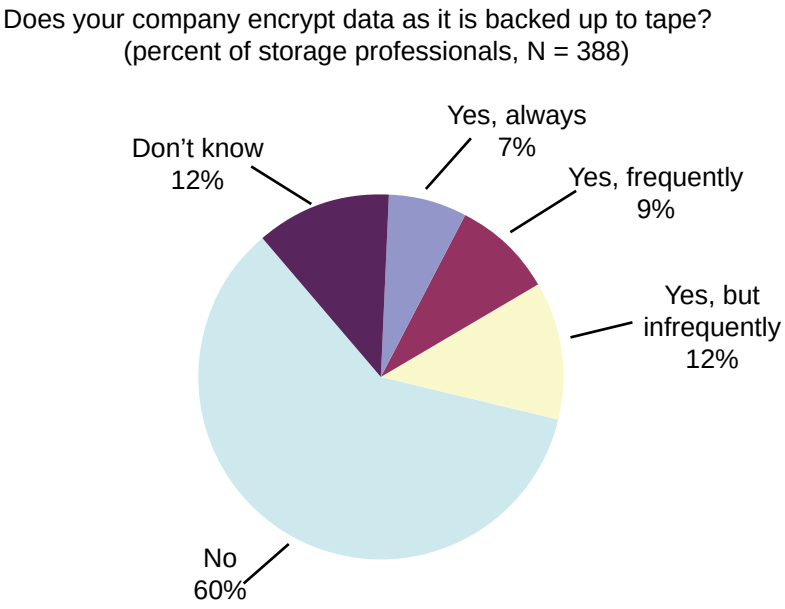
磁带加密成为越来越迫切的需求

备份供应商多年来一直将加密功能嵌入在其产品中，但很少有客户买账。为什么呢？因为IT经理始终认为基于磁带的数据保存相对比较安全。毕竟，磁带是由IT专家使用的，且磁带设备能够得到IP网络的保护。此外，加密技术有导致性能降低、加重IT运行负载以及提高前期购置成本等缺点。由于想当然地认为磁带风险很低，因此，大多数CIO都不假思索地拒绝磁带加密技术的应用。据ESG统计，大多数存储专家称他们的公司从未对磁带进行加密(见图1)。

这种局面到2006年开始出现明显变化。从这一年开始，市场对磁带加密的关注迅速升温，原因如下：

- 逐渐规范的保密数据管理。遵循全球保密法规，涉密数据长期的保存在基于磁带介质的存储设备上，如欧洲隐私权与电子通信指令(2002)及日本保护私人数据法案(2001)等。保密制度在全球范围内继续保持发展势头。到2006年初，已有23个国家制订了自己的保密制度，在2005年，仅美国国会就颁布了13个相关法案。但这些法案对企业采用最佳业务实践的要求不是很严格。例如，维萨/万事达卡PCI标准和日本银行协会的数据保护支持标准都对数据保密技术和控制方法进行了详细说明。磁带加密的发展速度明显超过了这些规章制度和业务计划。
- 公开披露数据违规行为。加利福尼亚州数据库违规法案(即California SB1386, 2003)等规章制度明文规定必须公开披露涉及到加州公民保密数据的所有数据违规行为。2005年2月到2006年8月间，因备份磁带丢失/被盗而公开披露的数据违规事件总共17起，造成900多万美国人的保密数据被泄漏(来源：Privacyrights.org)。数据违规事件发生后，责任人需要通知客户、监视信用等级并控制损失，无形中增加数百万美元的意外成本。
- 多项可供选择的新技术。IT市场对磁带加密的渴望与日俱增。首先，加密处理器技术大幅度提高了产品性能并降低了成本，并驱动生成了基于硬件的全新密码加速和加密产品。随着需求的增长，市场很快便将涌现出五花八门的加密技术供IT专家选择使用。

图1. 磁带加密的使用情况



在制度遵从的压力下，ESG看到市场对磁带加密技术的需求始终呈现增长态势。经最新统计，42%的存储专家报告说，受到公开披露的与磁带丢失/被盗相关的数据违规事件的影响，他们正在调查、评估或实施磁带加密解决方案(见图2)。

磁带加密必须支持业务发展

为了避免因数据违规而影响公众形象，许多公司匆匆加入到备份磁盘加密的行列。在这个例示中，您可将磁带加密视为保险单- 仅仅加密备份磁带便会使磁带丢失/被盗、数据维护和意外成本等威胁消失殆尽。这种思维虽然合乎逻辑，但却目光短浅。的确，磁带加密能够在磁带丢失或被盗情况下防止数据泄漏，但您还应将磁带加密集成到基于磁带的业务流程的安全程序中(见图1)，如：

- 数据共享。磁带仍是业务伙伴之间交换数据时常用的介质，但这个过程的磁带丢失和被盗风险与数据异地解决方案相同。

图2. 害怕数据违规驱动市场日益关注磁带加密技术

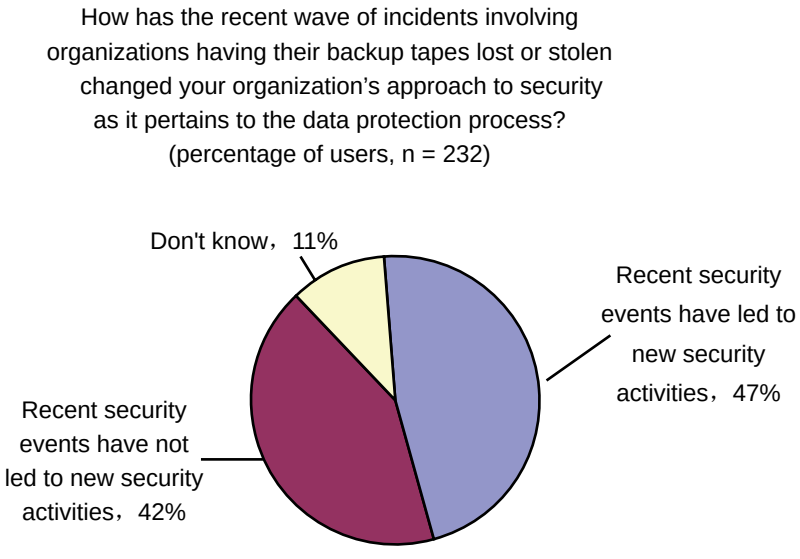


表1. 业务流程需要磁带加密

活动	业务要求	技术要求
通过磁带介质分配与业务伙伴共享数据	为数据共享流程添加安全保护，但不中断现有流程	加密、密钥管理、验证及合作伙伴间的密钥共享
数据归档	通过安全的方式多年保存记录，以确保制度遵从和知识产权管理	长期密钥管理。能够适应技术变化，同时维护可管理性和安全性

磁带加密解决方案还必须支持业务伙伴之间共享加密密钥。

- 数据归档。HIPAA和SEC 17a-4等政府规章制度要求将历史记录至少保存20年。由于磁带介质是常用的数据归档方法，因此，企业可利用磁带加密来保护数据的保密性并防止数据被篡改。在归档应用中，磁带加密必须支持密钥生命周期管理功能以便长期保存加密的数据。

这些功能不仅能够给磁带加密解决方案增添商业价值，而且还不会加重IT运行负担，因此非常重要。为了支持IT和业务的发展，磁带加密解决方案必须能够：

- 与现有技术和流程互操作。磁带加密解决方案应能够轻松集成可被备份软件、存储管理系统、设备驱动器、磁带库和磁带驱动器调用的一系列服务。除了对安全团队提出新的磁带管理要求外(如密钥管理和审计等)，磁带加密解决方案不应给日常的备份、恢复和归档工作添加任何不必要的负担或造成性能降级。

- 集成到灾难恢复规划中。鉴于加密的数据在使用前必须解密，因此，磁带加密必须是灾难规划/业务连续性流程中的一个环节。这要求公司紧密控制密钥管理、密钥备份和冗余密钥恢复设备，且公司在执行所有这些任务时都不应影响关键业务的RTO和RPO。

- 为未来发展提供灵活的选项。磁带加密解决方案必须在持续变化的环境中始终保持完整性。例如，如果文件被保存10年，磁带驱动器、服务器和应用技术在此期间肯定会发生巨大变化。因此，磁带加密解决方案必须足够灵活以便适应不可避免的技术变化，同时长期维护加密密钥和管理策略的完整性。

如果以能否同时满足业务和IT要求来权衡现在的磁带加密解决方案的话，这些解决方案简直是糟糕得令人可怕。

大型机构需要企业级磁带加密解决方案

现在，提供“防拷贝”功能的磁带加密解决方案受到普遍欢迎，但很快便将无法满足大型机构的需求。ESG认为，老练的CIO将会关注被ESG称为“企业级磁带加密(ETE)”的新型安全解决方案，而不是实施多个磁带加密解决方案。不同于大多数的独立点产品，ETE被构建成一系列加密服务。因此，ETE能够：

- 分隔加密和管理功能。密码处理及密钥管理和控制等ETE服务都是单独运行的对象。通过分隔这些服务，您可在高速安全处理器上执行密码处理任务，同时集中执行密钥管理和控制任务以便提高运行效率和安全性。随着越来越的数据被加密，这种基于对象的模式将能够提供规模和性能优势，因此从长远的角度看非常重要。为了避免将来可扩展性出现问题，现在基于服务器的万能解决方案可逐渐迁移到分布式模式中(即，跨越多个产品实施加密并集中管理多个服务器)。

- 提供易于集成性。ETE服务可供需要加密数据的系统(如应用、操作系统和安全管理系统)及实际执行加密任务的产品(如密码处理器、加密软件和产品等)轻松访问。换句话说，ETE是加密中间件，提供开放的API用于请求或执行加密服务。

- 虚拟化密钥管理工作。为了维护关键密钥管理服务的可用性，企业必须成对配置许多加密产品以实现故障切换。ETE不是将多个产品群集在一起，而是使用基于多个分布式系统构建的分布式数据库，类似于全球DNS基础设施。此类架构能够定位ETE服务请求，从而最大限度地缩短时延，藉此提高性能，同时还能消除任何单一故障点。当本地ETE系统脱机时，ETE服务可简单地调用另一个系统。

- 满足密钥共享需求。ETE知道企业数据中心和业务伙伴之间需要共享密钥。为了满足这个需求，ETE提供多个技术解决方案，包括PKI、Kerberos、共享加密密钥和安全解密工具等。

- 利用磁带压缩技术。企业级磁带加密解决方案能够将吞吐量提高300%、降低介质成本并减少IT运行人员需要处理的物理磁带的数量。为了同时利用压缩技术的运行优势以及加密技术的安全优势，您必须在加密之前先压缩磁带。为了实现运行和安全目标，ETE可在允许在磁带压缩后实施加密图形处理的地方分配加密服务。

与其他主要服务相同(如网络目录和DNS等)，ETE更改了磁带加密的方法。ETE根据需要为单独的系统、应用和设备提供服务，以便用户能够获得集中加密管理提供的运行和安全优势，同时利用分布式加密处理带来的性能优势。

ETE架构

如上所述，ETE基于一系列可通过安全的开放式API调用的分布式服务。最简单的ETE架构包括三个离散层(见图3)：

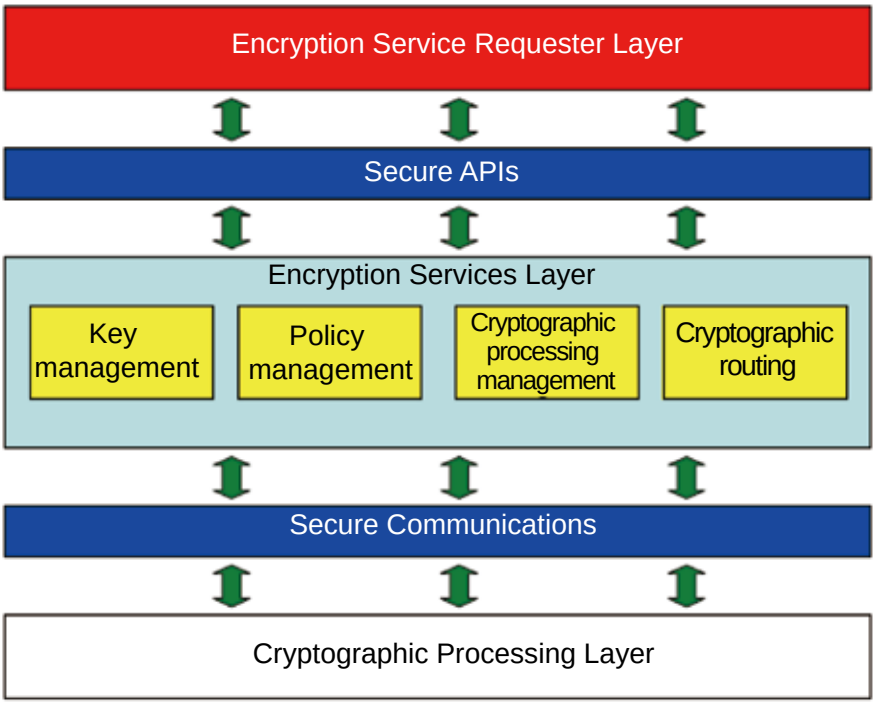
- 加密服务申请层。需要加密数据的不同系统(如文件系统)和应用(备份应用)都可呼叫加密服务层并告知需要加密什么数据。除这个呼叫之外，整个磁带加密流程对申请层的系统和应用是完全透明的。当备份应用希望恢复加密后的数据时，加密服务层将拦截这个申请，执行适当的操作以解密数据，然后继续向前传递数据。申请层还能与现有的数据管理和系统管理产品进行适当集成以便最大限度地避免更改客户的业务流程。

- 加密服务层。ETE服务层是整个架构的引擎，对应用和设备隐藏企业级磁带加密的复杂性。为了实现这个目标，ETE加密服务层作为中间件将加密申请人与密码处理器桥接在一起，为密钥生命周期管理(如密钥生成、密钥保护和管理等)、策略管理、日志记录/报告和实际的密码处理提供服务。服务层还能与现有的安全软件相集成，用于访问控制、制度遵从和审计等目的。

- 密码处理层。您可在整个基础设施的任何位置执行实际的加密任务。当密码处理器接到数据加密申请后，它将呼叫密钥管理服务器，请求生成加密密钥。接到密钥管理器提供的加密密钥后，密码处理器将根据申请开展适当的加密操作。通过这种方式，密码处理层还可作为服务使用，但多数时间都处在休眠状态。当受命加密数据时，密码处理层将会苏醒过来并与加密服务层协作，基于特定的策略执行加密任务。

考虑到ETE基于服务的架构以及典型企业环境中系统和产品的分散性质，ETE的目标是为满足日常的磁带加密要求提供灵活性。例如，备份系统可在包含多个磁带库的磁带群集中从任何可用驱动请求加密服务。

图3. ETE架构



同样，归档系统能够在安全的位置加密一系列远程磁带驱动中的大量文件。随着新型服务器、备份应用和磁带驱动逐渐被添加到企业中，由于它们受ETE服务层的控制比连接到特定系统中更合适，它们也可参与到ETE流程中。

IBM加密解决方案：现有的ETE机型

IBM现在提供的ETE解决方案虽然涵盖ETE架构的某些组件，但完整的ETE解决方案还只是个构想。也就是说，IBM通过为客户提供两款互补的加密产品而奠定了早期ETE领袖的地位：Encryption Facility for z/OS和近期推出的提供板载加密功能的T1120磁带驱动器。这两个产品都基于公共密钥基础设施，使用相同的密钥分配和保护机制，都能利用System z提供的硬件加密特征。特别是，System z提供防篡改加密单元，确保不在系统内存中提供任何未经加密的密钥信息。此类加密技术称为安全密钥加密技术，是许多企业迫切需要的主要密钥管理技术。

Encryption Facility for z/OS – 业务伙伴数据交换

Encryption Facility for z/OS是基于主机的程序，使用主机密码硬件加速技术来加密数据。您可通过添加步骤来调用这个加密功能。加密后的数据可直接写入目前支持的任何磁带存储产品中。Encryption Facility还能在数据加密之前选择性地压缩数据。Encryption Facility提供免费客户端，以便数据接收方能够轻松解密或重新加密数据，无需购买全新加密产品。由于支持客户端并能够使用传统的存储设备，Encryption Facility成为大多数业务伙伴用于交换数据的理想选择。

基于IBM TS1120磁带驱动器的数据加密- 数据归档

2006年8月，IBM宣布推出全新版本的TS1120磁带驱动器，藉此增强了其加密解决方案(注：现有的TS1120可现场升级)。TS1120驱动器不是在主机上加密数据，而是在压缩完数据后在磁带产品上以接近标准磁带驱动器的速度加密数据。主机和开放系统都支持TS1120磁带驱动器，因此，磁带驱动器的加密功能能够实现：

- 高性能和介质利用率。经IBM测试，TS1120的写性能可维持在100MB/秒的水平，即使打开密码处理功能也不例外。TS1120加密不会干扰现有的压缩功能，因此，用户仍可通过压缩数据将介质利用率提高3倍。
- 密钥管理集成。您可在与TS1120相连接的、基于Java的任何服务器上集中管理TS1120密钥，以便利用密钥管理服务器提供的特殊的安全特性。在z/OS环境中，集中密钥管理将利用ICSF、 RACF和安全密钥加密硬件，以便TS1120加密仍集中在高性能密码处理上并利用现有的主机密钥管理系统提供的安全性、高可用性和运行效率。
- 策略灵活性。您也可将TS1120加密功能集成到各类策略管理应用中。例如，您可通过DFDSM等工具来管理主机磁带加密策略，而对UNIX、Linux、System i 5/OS和Windows应用基于磁带驱动器、磁带介质序列号或磁带库的加密策略，这与ETE产品支持大量用户共享的设计初衷不谋而合。

TS1120磁带驱动器提供卓越性能，可满足将大量数据加密保存到磁带上的归档要求。此外，由于集中密钥管理工具可利用安全的密钥库，如z/OS上的ICSF，因此，您可将归档后的数据安全地保存多年时间。

ETE工作原理

无论是Encryption Facility for z/OS还是主机外加密，TS1120都与上面定义的ETE要求相对应(见表2)。IBM还计划扩展加密技术，以便实现磁盘子系统内的加密，同时继续利用主机硬件和软件的集中密钥管理技术。

展望：ETE的意义

关于加密，今后几年势必出现两种情况：第一，越来越多的加密技术用于保护保密数据。第二，实施不同的加密技术最终将对IT运行和灾难恢复准备工作产生深远影响。

ESG认为，依据战略性的架构方案来实施加密技术是通过加密实现数据保密目标同时不造成运行问题的唯一方法。为了根据计划将加密技术应用到IT和业务流程中，明智的CIO会选择：

- 从一开始就做好集中密钥管理的规划工作。即便实施严格的控制与管理，运行多个密钥管理服务器也会不可避免地带来重复工作、安全漏洞和复杂的灾难恢复等问题。为避免出现这些问题，IT执行官应将规划工作的重点放在集中密钥管理服务上。如果必须要使用多个密钥管理系统，CIO应确保这些服务器在未来能够轻松集成或合并。
- 为密码处理做好长短期规划。考虑到密码处理器和存储供应商的发展方向，将来的产品无疑将包括基于集成线路板的加密功能，但这项功能只有在现有产

表2.与ETE要求相对应的IBM解决方案

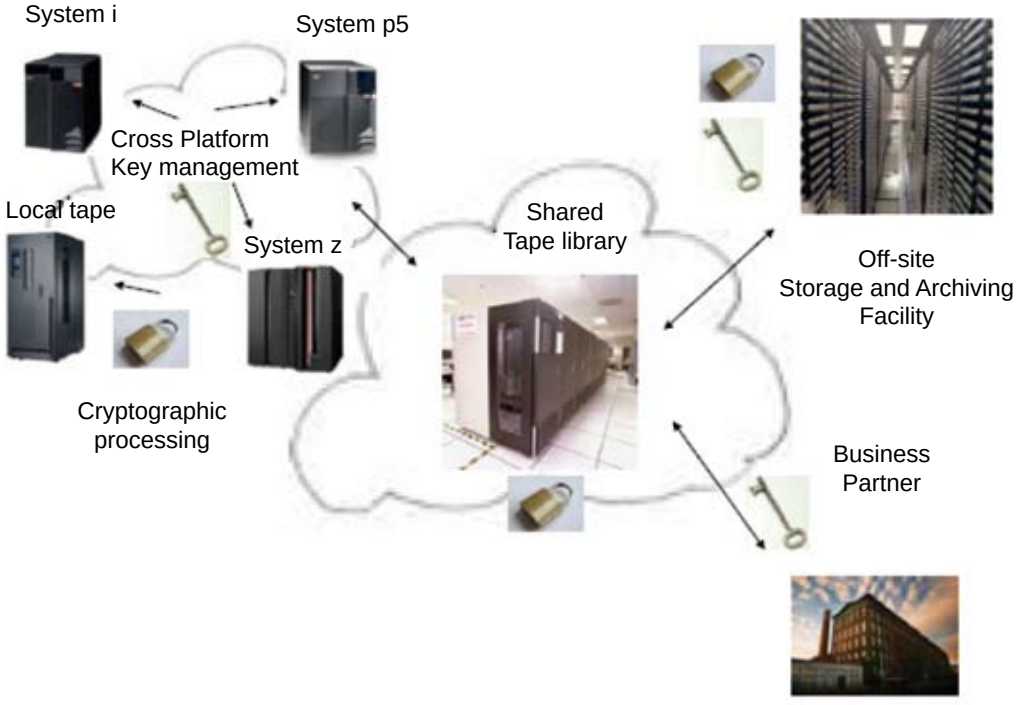
ETE要求	业务伙伴数据交换：Encryption Facility for z/OS	数据归档：TS1120板外加密
分隔加密和管理功能	利用硬件密码加速技术在服务器内加密数据。密钥管理和控制集中在z/OS环境中完成。面向合作伙伴的公共密钥和企业专用密钥可在极为安全的数据库中管理。	在磁带驱动器中以线速实施压缩和加密。面向企业的磁带密钥管理可在z/OS环境中集中实施。面向合作伙伴的公共密钥和企业专用密钥可在极为安全的数据库中管理。
易于集成性	您可以通过添加作业步将产品轻松集成到现有流程中。客户可使用现有的磁带交换产品和策略。 为不运行主机或Encryption Facility for z/OS的业务伙伴提供基于Java的客户端。 可使用主机中现有的验证、授权和审计服务(RACF)。	与现有的数据管理流程相集成。可在z/OS系统管理的存储器中定义策略驱动的加密。对于非z/OS系统，可基于介质容量的序列号范围提出加密请求。对于z/OS集中密钥管理，可使用主机中现有的验证、授权和审计服务(RACF)。
虚拟化密钥管理工作	z/OS上高可用的密钥库。设计用于不带单一故障点，并行系统配置允许z/OS的多个实例访问密钥库。	z/OS上高可用的密钥库。设计用于不带单一故障点，并行系统配置允许z/OS的多个实例访问密钥库。每个z/OS映像都带有自己的本地密钥管理器以便最大限度地提高可用性和性能。客户在远程访问这些密钥管理器时，产品将使用虚拟IP寻址(VIPA)功能将其自动路由到适当的密钥管理器中，用于实现高可用性。
满足密钥共享要求	合作伙伴之间可使用密码或公共密钥安全地交换数据。可利用业界标准的公共密钥管理流程和现有的主机数字证书服务。	合作伙伴之间可使用密码或公共密钥安全地交换数据。可利用业界标准的公共密钥管理流程和现有的主机数字证书服务。
利用磁带压缩技术	可在加密前利用基于主机的压缩技术。	可在加密前利用基于TS1120驱动器的压缩技术。

品被替换后才能得到应用，将是一个漫长过程。为了避免出现单一机型锁定问题，请您使用标准加密算法并确定加密密钥能够输出，同时寻找能够与集中密钥管理服务器互操作的开放式密钥管理功能。

- 分析供应商的开放标准、互操作性和平台支持承诺。由于加密和密钥管理解决方案相对不成熟，因此，许多解决方案都存在各自为政，相互不兼容的问题。不要忘记，企业需要长期而灵活的通过更多应用加密数据并使用更多产品来提供加密功能。CIO应确定供应商满足开放标准以便实现将来的ETE集成。平台支持同样重要。许多企业应用都分散在Windows、UNIX、Linux、System i5/OS和主机等多个层次中。因此，最佳的ETE解决方案应能够支持所有这些标准企业平台。
- 考虑记录保存期 – 而不是产品使用期。技术产品的有效期通常是3-5年，一旦失去价值，企业可通过新产品来替换它们。这种情况不适用于记录保存，因为有些规章制度要求企业将某些数据保存几十年。对于磁带加密，我们需要考虑一个基本问题“这项技术(或供应商)能否延续20年？”对于任何存在疑问的解决方案，我们都要毫不犹豫地淘汰掉。

IBM磁带加密解决方案再次与这些重要标准不谋而合。鉴于z/OS的长期和严格的密钥管理服务，主机客户可考虑在z/OS服务器上集中管理密钥。

图4. ESG绘制的IBM ETE架构图



优势总结

部署磁带加密技术的驱动力是什么？很简单 – 制度遵从以及对数据违规披露的恐慌。虽然安全保护对于避免违反规章制度功不可没，但这绝对不能体现它们的全部价值。只有在保护业务流程，同时能够与未来的IT运行无缝衔接的情况下，加密等安全技术才能实现最大价值。

这也正是企业级磁带加密架构的设计初衷。ETE可从以下几方面提供磁带加密优势：

1. 业务要求。ETE为业务应用提供加密服务以便保护磁带上的数据。由于这些数据常被传送给业务伙伴，因此，ETE提供多种方法来帮助业务伙伴自己识别数据、开展真实性验证、解密保密数据、最终保障数据的安全和可用。

2. 战术需求和战略规划。由于ETE提供独立的加密服务，因此，大型机构可基于现有的基础设施和业务需求混合匹配这些服务，从而避免对供应商的依赖，从长远规划上实现IT架构的灵活性。

3. 集成到现有IT基础设施中。磁带加密不会增加IT运行负担或带来灾难恢复风险。除了标准的磁带管理流程外，ETE几乎不给安全团队增加任何工作负担，尽量做到完全透明。

紧急情况下，ETE可调用提供典型企业级功能的架构，如高可用性、可扩展性、可靠性和严格安全控制等。此外，ETE还必须经得住时间考验。尽管技术跨度长达20年，ETE也能够找到2006年前的密钥并解密数据。

基于IBM System Storage TS112的Encryption Facility for z/OS和加密解决方案能够满足上述全部要求。因此，每位CIO在为满足现在的生产需求或执行未来战略计划而寻找磁带加密解决方案时，IBM产品都是值得考虑的。

图1

Does your company encrypt data as it is backed up to tape?：您的公司是否加密备份到磁带上的数据？

(percent of storage professionals, N = 388)：(存储专家的百分比，N = 388)

Don´ t know：不知道
Yes, always：是的，始终加密
Yes, frequently：是的，经常加密
Yes, but infrequently：是的，但不经常
No：否。

图2

How has the recent wave of incidents involving organizations having their backup tapes lost or stolen changed your organization´ s approach to security as it pertains to the data protection process? (percentage of users, n = 232):

近期，备份磁带丢失/被盗的事故频繁发生，您的公司是否受此影响而改变了数据安全保护方法？(用户百分比, n = 232)；

Don't know：不知道

Recent security events have not led to new security activities：近期安全事故并未导致我们公司改变安全保护措施；

Recent security events have led to new security activities：近期安全事故驱动我们公司改变了安全保护措施。

图3

Encryption Service Requester Layer：加密服务申请层；

Secure APIs：安全的API；
Encryption Services Layer：加密服务层；
Key management：密钥管理；
Policy management：策略管理；
Cryptographic processing management：密码处理管理；
Cryptographic routing：密码路由；

Secure Communications：安全的通信；
Cryptographic Processing Layer：密码处理层；

图4

Cross Platform Key management：跨平台的密钥管理；

Local tape：本地磁带；
Cryptographic processing：密码处理；
Shared Tape library：共享磁带库；
Off-site Storage and Archiving Facility：场外存储和归档设施；
Business Partner：业务伙伴

了解如何通过10份报告来帮助您解决最紧迫的特权用户监视和审计难题

大多数组织所采取的网络安全计划都集中在压制外部的黑客和入侵者方面，但事实上，来自内部的威胁可能代表了一种更重要的损失来源。

尽管拒绝特权用户的访问是不实际的，但监视他们的操作却至关重要——因为由“内部人员”所进行的偶然或者恶意的破坏可能对您的企业造成相当大的损失。IBM Tivoli® Compliance Insight Manager包含用于防御内部威胁的强大工具，包括监视和审计企业内特权用户行为的10大最佳实践报告。

通过提供对内部威胁行为的敏锐的可见性，Tivoli Compliance Insight Manager用于审计和遵从性目的报告引擎将成为维护网络安全的一项宝贵资产。

谁对您的网络的危害更大呢？——外部黑客、授权员工、客户、合作伙伴还是外包商？答案可能令人惊讶：后者。法规和审计要求表明，现有安全技术将重点放在网络级别、外来威胁上的做法是错误的。公司内部的特权用户才更应该受到怀疑——他们每天都在您的网络上，可能会蓄意或者偶然地引起损失。

此外，Payment Card Industry Data Security Standard (PCI DSS)、Sarbanes-Oxley (SOX)、Gramm-Leach-Bliley Act (GLBA)和Health Insurance Portability and Accountability Act (HIPAA)审计表明，特权用户（比如管理员和网络管理员）的活动是法律关心的一个问题。

监管人员和审计师都可能提出以下问题，对于这些问题，您必须拥有现成的答案：

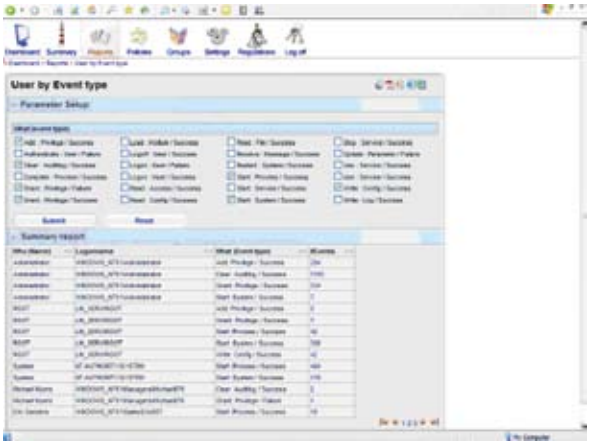
- 系统管理员、数据库管理员和根用户都对您的网络做了什么？
- 系统变更经过授权了吗？
- 特权访问是否违反了职责分开原则？
- 不满的管理员是否会尝试盗窃身份？
- 系统管理员是否看到了机密的或者管制的数据？

继续阅读，了解Tivoli Compliance Insight Manager中的10大特权用户活动监视报告如何帮助确保您对所有这些问题（以及更多问题）都拥有了快速且适当的答案。

企业仪表板使您可以深入了解系统中的所有活动。在本例中，某个划分为管理员的人正在审计日志，同时，一些管理员正在访问数据——二者都明显违反了可接受的使用指南。

1. 企业仪表板

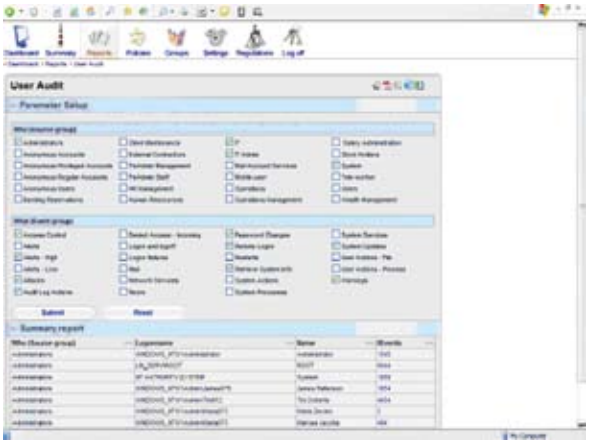
Tivoli Compliance Insight Manager企业仪表板允许您查看系统中的所有活动，包括人员、活动及对象。每个圆的大小与它所代表的活动数量相关，而颜色则表示遵从性级别。红色的圆代表特定的风险区域——在这种情况下，您可接受的使用策略正在受到侵犯。屏幕的下部并排显示了人员和活动，突出显示了潜在的非法活动。



按事件类型显示用户的报告使您能够快速、全面地了解整个企业的管理活动及其执行人员。在这里，您可以迅速确定是否有非管理员对系统进行了特权更改——您的审计员肯定对这个话题感兴趣。

2.按事件类型显示用户

能够追踪企业中所有的管理活动并了解其执行者是非常重要的。Tivoli Compliance Insight Manager的按事件类型显示用户的报告通过显示执行活动的每个人及其执行的活动类型来实现这个目标。只需一次但就就可以了解可疑活动的更多细节。



用户审计报告显示了管理活动的执行者及执行频率。

3. 用户及其活动选择概述

Tivoli Compliance Insight Manager的用户审计报告是用于PCI、HIPAA或者ISO遵从性审计的理想报告。此报告允许您选择管理员，然后选择最受关注的特定活动。

按类型显示事件的报告使您可以检查发生了多少事件，多少事件违反了您的安全策略，有多少非法意图警告，以及有多少操作失败。

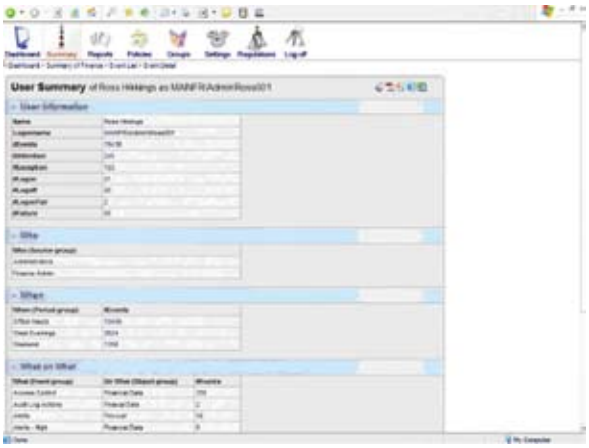
4. 按类型显示事件

Tivoli Compliance Insight Manager按类型显示事件报告对您网络上的活动提供了一个集中视图，并且有助于向审计员表明您对这些活动有足够的了解。

事件细节报告允许您“放大”事件的每个细节，通过追踪将其升级至一个工作流系统，并且继续进行更详细的调查。

5. 详细事故调查

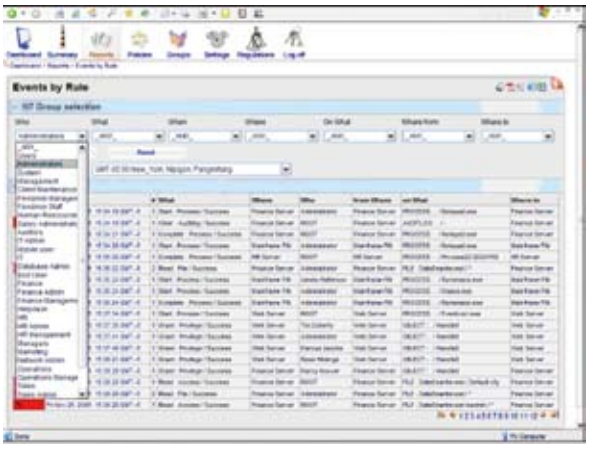
Tivoli Compliance Insight Manager的事件细节报告提供了关于任何事故的所有可用文件，甚至包括事故的时间和起源等细节。事实上，详细的事故调查报告以字段级别提供了所有细节，以及策略组。



用户汇总报告允许您进行“放大”来分析一个可疑用户及其最近的操作。

6. 用户调查

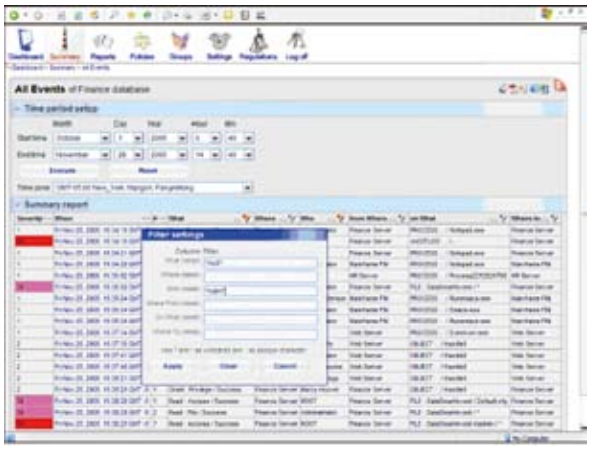
当发生了一个事故并且一个特权用户的活动值得怀疑时，能够查看该用户最近操作的详情非常重要。Tivoli Compliance Insight Manager用户汇总报告使您可以密切关注该用户创建了多少事件，这些事件何时发生，多少事件违反了策略，多少事件受到注意警告或失败，以及该用户属于哪个组。



借助按规则显示事件的报告，您只需选择您要查看的用户组，从而使调查效率更高且更简单。例如：要调查一个特权用户，您只需选择“管理员”组，然后开始调查。

7. 按规则显示事件

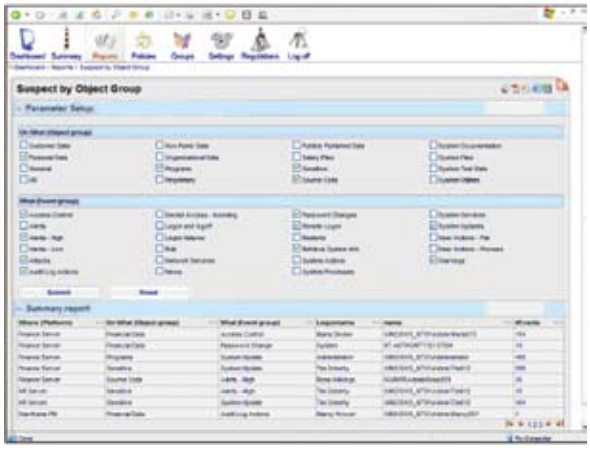
任何优秀的报告都能够快速筛选复杂信息。通过允许您选择您所要查看的群组，Tivoli Compliance Insight Manager按规则显示事件的报告促进了对特定事件的快速理解，允许您仅选择想要查看的用户组。



带搜索筛选器的全部事件报告允许使将搜索范围缩小为非法事件。此处，对篡改审计日志的管理员的搜索发现了一个删除审计日志的实例——这显然违背了策略。

8.带筛选器的所有事件

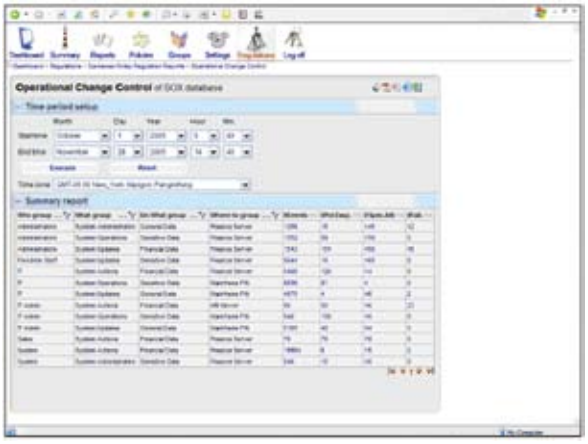
当您调查特权用户活动时，Tivoli Compliance Insight Manager中包含的此报告使您可以真正缩小搜索范围。所有事件报告中的搜索筛选器使用Boolean搜索功能来从您的视图中移除数百万个事件，仅保留您所关心的事件。



谁在篡改您受保护的数据？对象组报告提供的可疑人员将回答这个问题，并促进进一步的调查。

9. 敏感数据篡改

Tivoli Compliance Insight Manager中对象组报告的怀疑提供了关于谁可能篡改受保护数据（例如与SOX、PCI、HIPAA或者GLBA相关联的数据）的信息。只需选择您想要调查的数据，然后将搜索范围缩小至特权活动，您可以发现发生在金融、信贷、病人或者客户数据上的此类活动。



运营变更控制报告监视跨平台的管理变更，对管理活动进行报告，同时允许进行“点击行为”调查。

10. 运营变更管理

监视管理变更至关重要，而运营变更控制报告能够详细了解这类变更。Tivoli Compliance Insight Manager的这部分功能遵循ISO的最佳实践建议，提供所做更改的一个总体概述。它还允许您和您的审计员验证这些变更是否遵守策略。

采用这10种方法实现网络安全

Tivoli Compliance Insight Manager及其关于特权用户活动监视的10大报告使您能够更好地了解用户在您的企业网络中做什么。通过使用Tivoli Compliance Insight Manager来监视和消除网络内部的威胁，您能够帮助显著增强网络安全性，同时能够有信心满足审计员的要求。

更多信息

要了解更多关于Tivoli Compliance Insight Manager如何帮助您的组织监视和审计特权用户活动的信息，请联系您的IBM代表或IBM业务合作合作伙伴，或者访问ibm.com/tivoli。

关于IBM的Tivoli软件

Tivoli软件提供一系列产品和功能来支持IBM服务管理，运用可伸缩的模块化方法为您的业务提供更加有效和高效的服务。Tivoli软件有助于满足任何规模业务的需求，通过流程、工作流及任务的集成和自动化，使您能够提供卓越的服务来支持您的业务目标。具有丰富的安全行、基于开放标准的Tivoli服务管理平台是通过前瞻性的运营管理解决方案来实现的，这些解决方案提供了端到端的可视性和控制能力。它同时也受到世界级的IBM Services、IBM Support及活跃的IBM业务合作伙伴生态系统的支持。通过参加在全球独立运行的IBM Tivoli用户组，Tivoli客户和业务合作伙伴也可以互相利用彼此的最佳实践——访问www.tivoli-ug.org。

选择正确的身份和访问管理解决方案，消除创新障碍

全球各地的商业领袖都在更新他们对于尖端增长的关注——他们将创新视为达成此目标的手段。创新应如何出现？通过消除协作式工作环境的阻碍，使员工、客户和合作伙伴随时可访问关键资源，并有效地加以利用。

但在力所能及的范围内推动创新的访问同样也会给组织带来严峻的考验。每一天，组织都要面临着多重内部和外部的安全隐患。除了这些真正的隐患之外，还存在一个更大的挑战：需要保护业务系统的使用，并避免敏感业务数据的泄漏，以符合企业和政府要求。如果没有严格的控制，商业价值就会因客户缺乏信心、业务中断和企业或客户数据被窃导致的无法创新而迅速蒸发。为了保护业务完整性并促进遵从性，组织必须：

- 验证访问资源的所有用户的真实性。
- 根据恰当的使用策略以及遵从法规的要求监控这些访问。
- 在出现违规时，采取合理措施。

急需一种安全性管理解决方案，帮助保护资产免受未经授权的访问，在不降低生产力的前提下完成此任务。这就是企业求助于身份和访问管理解决方案的原因。

身份和访问管理可以回答两个关键问题：您是谁？您可以访问什么？组织应该能够有效地跨多个领域回答这两个问题：数据、流程、应用程序、网络和其他端点以及物理基础设施。但组织往往有着耗时、低效的手动流程，用于定义、实现、维护和审计身份和访问策略，例如：

- 在各应用程序和数据库内构建安全性。
- 在无数目录、数据库和文件中管理各种格式的用户信息。
- 为数百个位置的众多相同用户管理安全性规则。
- 需要多个密码。
- 通过电子表格和其他文件手动检索和创建关键（但难以彼此关联的）遵从性和审计信息。

这份买方指南帮助您选择正确的解决方案，帮助管理和控制企业内部和跨企业的访问。文中从CSO、IT操作人员、业务线经理和企业架构师的视角列举了组织所面临的最常见的身份和访问管理挑战。随后还概述了直接应对各挑战的组件，帮您评估特定厂商的解决方案是否能够最好地应对您的优先挑战。

身份和访问管理入门

在选择身份和访问管理解决方案时，应注意以下这些主要类别：

1. 在整个生命周期内管理用户和用户信息
2. 确保高效访问有效的资源，最大化用户生产力
3. 跨所有应用程序、数据源、操作系统和企业边界一致地管理和实施访问控制策略
4. 通过身份治理监控和验证谁有权访问什么
5. 加速价值实现进程
6. 选择正确的安全性提供商

对于每一个类别，您都会看到一份一览表，可在评估厂商及其产品时使用。

1. 在整个生命周期内管理用户和用户信息

IT员工要付出大量时间管理用户特权和策略，这些内容可能存在于数百个不同的位置。以来一个处理一个的方式添加用户权限可能要耗费几个小时乃至几周的时间。删除用户权限也要耗费同样长的时间，还会带来遗漏本应停止访问的应用程序的风险。

为了消除无效的访问路径，IT团队必须始终手动审计所有生产服务器和应用程序。每当有人更改作业、角色或就职状态时，其所有现有的用户账户都必须得到合理的更改或删除——跨所有应用程序、操作系统和其他系统。

集中、自动化的解决方案使您能够更有效地掌控管理用户身份、凭据、账户、访问权限和审计的任务。自动化能够降低IT员工完成重复任务的成本，同时能够确保安全性得到了一致的管理。IT员工将从为所有应用程序构建安全性的繁琐任务中解放出来，指派解决方案来管理安全性——从而以最低的成本实现高度有效的安全性。

杰出解决方案的特征：	IBM	其他厂商
提供单一、安全的身份存储库	√	
提供基于Web的集成化界面，包含简单的向导和丰富的配置编辑器，使您能够轻松创建、修改和查看配置对象及其关系	√	
交付灵活的账户采用方法，这是安全有效地将账户映射到用户所必需的	√	
支持基于角色、基于规则和基于请求的供应用例	√	
提供核心角色管理和责任划分能力，提供与连续业务控制系统集成的开放接口	√	
支持工具使用基于简单向导的导航和用于较高级业务流程的拖放式GUI来构建用户供应工作流——均通过一个通用的Web界面完成	√	
跨异构数据存储库同步身份数据，这些存储库根据需求接收不同的授权信息	√	
将从权威源接收到的身份数据修改复制到其他需要利用这些数据的数据库和目录中	√	
管理分布式用户集合，包括为这些用户分配一种或几种角色的能力	√	
以随需应变的方法自动协调账户，从而迅速、可靠地发现“孤儿”（无效）账户，并启动自动或手动的补救流程	√	
自动化用户的登记，从入职到离职	√	
利用身份集成功能来建立规则，确定哪些组和个人有权更改哪些数据字段	√	
维护准确的配置和用户访问权限更改记录，以便用于审计	√	
提供对操作工作流的访问，允许定制供应活动	√	
支持供应内部网和外部网位置文件	√	
支持开箱即用的手动服务，使您可以快速轻松地自动化业务流程，治理目标，同时依然手动执行实际的供应任务	√	
支持开箱即用的手动服务，使您可以快速轻松地自动化以电话订购和其他手动管理项为中心的业务流程	√	
提供可定制、基于角色的用户GUI，具有经理、最终用户、审计人员、帮助台等角色的视图	√	

2. 确保高效访问有效的资源，最大化用户生产力

为员工提供及时、直接的有效信息、应用程序和服务访问能够提高员工生产力。承诺新价值和增长机遇，向客户和合作伙伴敞开门户。合法用户数量的不断增加带来了严峻的安全性和实用性挑战。如果安全控件阻塞用户访问所需资源，或者要求经过多次登录和身份验证，用户就不会满意，不能获得较高的生产力。

输入、更改和重设密码占用了员工和IT管理员的更多时间。跨本地、基于Web和远程系统的单点登录（SSO）功能以及身份和访问控制解决方案可最小化密码相关问题的数量：

- 多个密码造成的混淆
- 在人们写下密码时造成的安全性泄漏
- 最终用户无法登录账户时所体验到的宕机时间
- IT员工耗费在密码管理方面的时间

联邦SSO功能使用户能够使用SSO无缝地跨域边界的Web站点导航。联邦SSO功能减少了挫折和用户管理成本，促进了与合作伙伴组织之间的无缝协作环境。

自助服务功能可进一步改进用户体验，允许用户管理自己的账户、重置密码。利用这些功能，用户即可迅速准备好重新运行，而无需为呼叫IT帮助台而付出额外的时间和成本。

解决方案应提高生产力。 确保您选择的解决方案有以下特征：	IBM	其他厂商
提供直观、可定制的管理GUI，即指即点的功能允许您轻松创建新的用户GUI视图	✓	
管理GUI内包含多重作业特性，允许您启动一个作业、打开第二个作业，然后切换回初始作业并完成它	✓	
提供一种应用架构，使用一种GUI，可在其中执行所有管理职能	✓	
允许您在一个GUI内提交和跟踪状态请求，监控工作流作业	✓	
交付了向导和模板，可迅速轻松地进行配置，轻松访问为细粒度定制而生成的脚本	✓	
使用用于多种身份验证解决方案的归档集成路径提供开箱即用的身份验证集成	✓	
提供完整、集成化的联邦和信任管理解决方案，包含通用的安全令牌服务，用于Web服务/SOA环境内基于标准的身份传播	✓	
提供与IBM WebSphere® Enterprise Service Bus的强大集成，促进和保护ESB的安全联邦访问	✓	
包含健壮的目录、目录集成和同步成本——无任何附加费用	✓	
通过工作流扩展自动化登录、密码更改和注销流程，推进自动化超越简单的SSO	✓	
提供同一共向工作站上的快速用户切换，使一名用户注销、另一名用户登录，而宕机时间最短	✓	
提供广泛的身份验证因素选择，包括用户ID和密码、USB智能卡、一次性密码、主动RFID和生物测定	✓	
支持指派访问受保护资源所需的授权级别、在用户必须提供下一级别的身份验证时实施逐步完成的策略	✓	
提供完全可配置的身份验证机制，附带外部身份验证界面，支持以任何语言编写的Web应用程序	✓	
提供对本地和远程的全面端点覆盖；使用会话管理扩展SSO，包括对个人、共享（信息亭）、私有（信息亭与多重会话）、终端客户端、拨号会话、普适设备和漫游桌面的支持	✓	
与身份服务器、应用程序、中间件、操作系统和平台广泛集成	✓	

解决方案应提供对有效资源的高效访问。确保您选择的解决方案有以下特征：	IBM	其他厂商
跨Web应用程序等内容为用户交付SSO，包括IBM WebSphere、Microsoft®、Oracle和众多其他门户与应用程序环境	✓	
为.NET环境应用程序提供直接的SSO支持，例如Microsoft SharePoint® 和 Exchange servers	✓	
为Active Directory®（AD）实现密码更改、支持使用AD替代性userPrincipalName (UPN)电子邮件地址来验证，并将Active Directory Application Mode (ADAM) 作为用户注册库，从而简化Microsoft用户登录	✓	
为跨站点身份验证支持多种标准，包括Security Assurance Markup Language (SAML)、Liberty Alliance and Web Services Federation Language (WS-Federation)令牌传递协议	✓	
支持Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) 协议，允许用户通过一次登录访问多个Web资源	✓	
在解决方案中实现容错，而无需依赖可选的第三方工具	✓	
为密码重置、密码同步和用户账户更新提供自助服务界面	✓	
复制策略（而不是仅缓存）来提供高可用性，使策略在策略服务器宕机时依然能够正常实施	✓	
利用Web授权方法，提供高性能，扩展到数千万应用程序的用户实现中	✓	
提供灵活的Java™ EE基于Web的架构，可使用加固的反转代理或现有Web服务器的插件模块来保护资源（在某些情况下，专用代理可提供更高的安全性级别）	✓	
提供久经考验的反转代理技术，经过超过1,000次客户安装的验证，从变更和配置管理的角度来看，非常出色	✓	
包括会话管理服务，可限制各领域创建的会话数量、消除服务器重启、允许多个服务器实例共享用户会话，从而提高性能	✓	
提供邮政功能，聚合如电子邮件、待办事项等，可根据您的选择进行配置	✓	
支持轻量级联邦解决方案，允许较小的组织迅速与大型企业建立联邦	✓	
支持企业到消费者（B2C）的联邦，使用新兴的用户中心身份，包括OpenID和Information Card Profile，使用Microsoft CardSpace或Higgins身份框架等身份选择机制	✓	

解决方案应提供企业单点登录（ESSO）。确保您选择的解决方案有以下特征：	IBM	其他厂商
包括一个ESSO解决方案，其与多种不同应用程序协作的高级功能、与强大的身份验证的集成、会话管理的灵活方法、记录和审计最终用户活动的能力都使它在市场中卓尔出群	✓	
包含领先的ESSO解决方案，它应该全面集成，由提供整个身份和访问管理套件的同一家厂商开发并支持	✓	
提供一个ESSO解决方案，构建于Java EE架构之上，可轻松与身份、Web访问、联邦、强大的身份验证和其他安全性组件集成	✓	
提供一个ESSO解决方案，包含多种会话管理功能，包括共享桌面、私有桌面和漫游桌面，促进迅速的用户切换集成广泛的第三方强力身份验证因素	✓	
提供一个ESSO解决方案，与Web、桌面、电传和大型机应用程序以及Microsoft Windows® CE和Windows Xpe等客户端设备平台相集成，包容最广泛的应用程序	✓	
提供一个ESSO解决方案，支持桌面密码重置功能	✓	
支持ESSO，无需给目录基础设施带来额外的负载或影响目录模式	✓	

3. 跨所有应用程序、数据源、操作系统和企业边界一致地管理和实施访问控制策略

为了满足法规要求，组织需要保护数据和应用程序，确保访问此策略和数据泄漏规则跨所有应用程序、数据源和操作系统一致地实现和实施。有了这些功能之后，您就应该能够开展审计，证明和报告IT安全控制的有效性，同时准备好回答以下问题：

- 谁能够进入我的应用程序或数据库？
- 哪里有哪些数据？因此我们应建立哪些访问控制？
- 谁需要访问这些数据？
- 我能否轻松证明用户仅访问了自己应该访问的内容？
- 我能否有效地审计服务器上被访问的关键数据？

正确的身份和访问控制解决方案会应用相同的业务策略来在整个组织内控制访问，包括针对跟踪系统管理员的高级审计跟踪。它提供了谁访问了哪些内容、为什么获得了相应的访问权限、这样的访问权限使用户能够做什么的闭环视图。这种可见性必须扩展到特权和受信任的用户，因为超级用户账户常会被滥用——往往对这些账户的访问权限没有任何控制，也无法审计使用这些账户的人们采取的操作。

理想情况下，您选择的身份和访问管理解决方案应处理使用正确的基于角色的访问权限注册新用户的完整生命周期，实施这些访问控制策略并检测和纠正任何尝试修改安全策略或用户权限的企图。

应选择具有以下特征的解决方案：	IBM	其他厂商
提供灵活、迅速配置、可扩展的身份提供方法，推送来自单一权威源的身份数据或从多个源拉取并聚合数据		
为业务经理和审计人员提供业务友好的描述，说明用户利用其访问权限能够做什么，从而帮助在新的访问批准请求、重新认证和审计评审中制订更好的决策		
允许管理员为细粒度资源应用有意义的描述，为快速引用和搜索进行分类，为它分配一个所有者，定义独特的批准和重新认证工作流，提供关于这些资源的详细报告		
具备无缝地与SAP和Oracle ERP集成的工作流，细粒度的责任划分检查与灵活的异常处理方法		
提供集中管理GUI进行控制和修改，消除手动更新各适配器以反映身份验证和授权方法更改的需要		
包含“what-if”策略更改模拟分析，可在做出更改之前确认哪些用户和权利将受到影响		
将业务规则整合到访问控制决策之中，在运行时评估这些规则		
在应用程序代码之外管理访问控制业务规则，允许您更改影响访问的策略参数，而无需重新和重新编译应用程序		
扫描应用程序漏洞，如跨站点脚本，在检测到漏洞之后帮助修复		
跨多个并发会话跟踪用户的行动，用户在一处注销之后，解决方案即可使其全面注销，以避免并发登录		
实施访问策略，用于不活动超时、三振出局规则和其他跨多个实施点的选项		
提供统一的策略管理，集中管理和控制访问，从操作系统 资源到基于Web的应用程序SSO		
定义基于策略的规则，允许您轻松设置可用于不同系统、用户、存储或信息的安全策略		
设置访问策略，自动实时检测和纠正故意和无意造成的违规事件		
具有一个工作流，能够在提示的操作未完成时自动将工作流处理累加和重定向到另一参与者		
扩展到数千万用户，进行身份验证和授权，还可伸缩以满足内部网、外部网、Internet用户群的需求		
通过支持非标准、安全的IP负载均衡程序、通过复制服务器进行的智能化负载均衡和所含的集群支持提供可伸缩性和可用性		
利用SSL加速卡技术，保护硬件密钥存储，提供故障转移功能，允许自动切换到备份Web服务器		

4. 通过身份治理监控和验证谁有权访问什么内容

最有效的身份和访问管理解决方案采用集中、可伸缩的方法，跨所有应用程序交付久经考验的特性和健壮的安全性，以符合SOA设计目标。集中管理能够提供跟踪所有访问过系统的用户、协调根据业务优先事项和需求授予的访问程度的可见性，从而改进安全性工作的一致性。

为了跨复合业务应用程序和业务单元管理用户身份，企业架构师应能够创建通用的身份代理服务或“作为服务的受信任的身份管理”。这样做能够提高业务灵活性，可在业务需求变化时添加新服务或连接现有服务，而无需重新编写身份处理的代码。它允许业务线专家关注交付应用程序内需要的业务逻辑——而不必担忧应用程序本身的安全性。

企业架构师还应能够通过高效有效地跨SOA管理和供应用户身份的能力扩展企业服务总线（ESB）的功能。这种方法创建了一种“身份感知”的ESB，使企业架构师能够确保用户能根据其安全性凭据和访问级别获得对应用程序、数据和信息的访问权限——无论他们所访问的应用程序是什么。

应选择具有以下特征的解决方案：	IBM	其他厂商
提供真正的闭环策略遵从性实施，检测和补救在供应流程之外授予的访问权限，而不必完成可能存在多个故障点的复杂、多步骤的系列流程		
包括开箱即用的自动化、可配置、高级的证明/重新证明处理，帮助满足需求，例如Sarbanes-Oxley (SOX) 404访问重新证明要求		
利用单一、安全的身份存储库，从中可跟踪和审计所有身份事件		
提供单一身份GUI，通过它可执行所有管理功能，跟踪和审计身份事件		
自动提供所有活动的审计日志——包括管理活动（如策略修改），以开箱即用的方式提供		
包括工作流，作为解决方案的完整组成部分，使整个生命周期和供应事件都能被解决方案管理和监控，解决方案还可记录下所有事务数据，以便在依法审计和报告时使用		
建立中心框架，治理和保护您的SOA环境		
为各服务应用程序实施和治理恰当的访问控制		
跨不同的服务转换和映射一组不同的用户身份		
跨组织筒仓和防火墙管理特定于应用程序的身份		
建立身份信任管理框架，确保事务得到安全执行		
端到端地传播所需凭据——从联系点（如XML网关）通过ESB传递到后台（如ERP或大型机应用程序）		
跟踪和比较所有登录事件，允许您审计应用程序访问		
提供广泛的审计和细节报告，可将其提交给管理机构、外部和企业审计人员		
跨广泛的安全设备周边集中收集、简化和关联与安全性有关的事件和警告		
提供审计跟踪记录，说明谁有权访问什么、谁批准了相应的访问权限		
提供特权用户监控和报告		
为跨所有解决方案组件调度、分发、查看和定制报告提供一个通用的报告系统		

5. 加速价值实现进程

在评估不同的身份和访问管理解决方案时，有必要选择一种提供快速的价值实现进程的产品。成本效益高的解决方案包含多种旨在提供轻松配置、集成和维护的关键特性。

应选择具有以下特征的解决方案：	IBM	其他厂商
所有必要的基础设施适配器，领先的中间件和软件组件商业版本，包括必要的数据库、LDAP服务器和Web与应用服务器		
功能全面、开箱即用的功能，无限制的组件版本，如工作流必须升级，这样才能使用所需的全部丰富特性		
同类最佳的目录和数据集成与同步工具，与解决方案绑定，可很好地应对任何集成挑战		
成熟、久经考验的功能，经过数百次全球客户安装的考验		
经验丰富的服务团队，可在实现过程中确保高生产力		
专门设计用于加速实现的工具		
提供教育和培训课程，使您的员工能够更快地获得高生产力		
解决所有异构目标需求的能力		
嵌入式集成业界领先的IBM WebSphere Application Server		
定制身份验证，可将现有基于Web的身份验证应用迅速集成到针对所有用户的身份验证流程之后，而无需借助第三方开发		
支持在一台服务器上完成安装，支持轻松配置，包括所有底层中间件		

应选择具有以下特征的解决方案：	IBM	其他厂商
与最新应用程序的广泛集成（包括PeopleSoft和Siebel），支持使用多个目录/用户存储库和异构中间件（包括Oracle Application Server）		
明确而直观的定价和许可费用，并非根据使用类型和其他额外收费的自选服务器、应用程序等定价		
支持本地语言，整合动态语言支持，显示特定内容的部署，如以各用户的首选语言显示的密码加密/响应问题或电子邮件通知		
策略、配置和框架的导入/导出功能，可加速QA和生产之间的系统推广，也适用于策略定义的版本控制		
平台支持的广度，包括Windows、UNIX、Linux on distributed、Linux® on IBM System z™ and IBM z/OS®		
定制自助服务UI的品牌形象（外观和感觉）以及布局的能力，在修订和升级之后保持定制效果，从而保护投资		
Evaluation Assurance Level 3或更高版本的通用标准认证		
标准配置和编程语言，而不是专用脚本或工作流定义语言		
用于监控身份和访问管理解决方案健康状况和可用性的工具		
自助服务密码重置，与服务台（帮助台）系统相集成，包括事故单的生成和结束		

6. 选择正确的安全性提供商

您选择的提供商应该能够为您的身份和访问管理解决方案提供全面支持。理想情况下，您还希望提供商能够在您实现解决方案的整个过程中为您提供支持。在选择提供商之前，请务必提出以下问题：

厂商的安全性愿景是否与您的愿景一致？

理想的厂商应该与您一样重视安全性，也理解不够可靠的安全性基础设施会给您的组织造成怎样的影响。

厂商是否关注真正的企业安全性需求？

对于关注点过于狭窄，仅关注针对特定环境的一种解决方案的厂商，您可能会遭遇“安全性孤岛”问题。应该选择能够应对全局的厂商。

厂商是否通过其技术为您的业务目标提供支持？

理想厂商的解决方案应与您的业务目标一致。他们的解决方案是否提高了效率、缩短了业务服务部署时间、降低了成本、加速了推向市场的进程？

厂商提供整体解决方案的一部分还是完整的解决方案？

如果需要涉及多家厂商，解决方案的成本和管理多家厂商所需的时间会大大增加。理想的厂商应该拥有身份和访问管理的完整产品组合，包括UNIX®和大型机访问控制、Web服务安全性和联邦。

厂商的产品是否为提供无缝的功能而紧密集成？

解决方案集成得越好，手动集成技术所需的工作就越少。

厂商的客户支持情况如何？

厂商应该提供快速响应、高度有效的迅速客户支持。务必理解其逐级上报的过程，务必确保他们有能力将您的业务放在第一位，以这样的方式为您提供支持。

厂商的全球形象属于哪种类型？

如果您的组织有国际分支机构，就应该寻找有全球影响力、久经考验的国际业务经验的厂商。应确保厂商能够通过其当地资源为您的国外分支机构提供支持。

在您需要时，是否有可信赖、拥有足够的专业经验和带宽的成熟支持组织为解决方案提供支持？

理想的厂商应该有着久经考验的支持组织，可帮助您最大化软件投资的价值。

厂商的解决方案是否一贯受到分析家的好评？

理想的解决方案应该经过领先分析家开展的多维度独立分析和考察，且得到认可。

您对厂商的稳定性及其在当今激烈的经济环境中保持力量的能力是否有信心？

在当今的经济环境中，一个重大的问题就是厂商的稳定性和生存能力。理想的厂商应该有着在该行业中的长期发展史，有着可靠、长远的战略和安全度过经济艰难时期的资源。

厂商能否交付有着战略设计、技术超群的产品？

比较各种安全性解决方案时，应关注技术优越性——设计良好的功能性、智能化的架构设计以及对行业标准的广泛支持，例如Security Assertion Markup Language (SAML)、Liberty Alliance、WS-Federation、Service Provisioning Markup Language (SPML) 和 eXtensible Access Control Markup Language (XACML)。

携手IBM，满足您的身份和访问管理需求

开始评估身份和访问管理厂商时，您会发现，IBM不仅提供了同类最佳的解决方案，其安全性解决方案的广度和集成也是无与伦比的。只有IBM使您能够通过灵活、自适应的方法跨整个IT安全风险领域降低保护企业的复杂度，从而集中精力促进业务创新。在您准备好扩展到其他安全性管理领域时，IBM可随时支持您的长期安全性目标。

对于身份和访问管理周期的每一个阶段，IBM都提供了能达到杰出解决方案的所有标准的软件：

- IBM Tivoli® Identity Manager软件使您能够快速供应用户身份，并在整个生命周期内管理身份及其访问权限，支持用户自助服务（例如密码重置）——完全向您的安全性策略看齐。
- IBM Tivoli Access Manager for e-business提供了企业范围内的端到端应用程序安全性，包括SSO、URL和应用程序级授权、基于分布式Web的管理和策略驱动的安全性。
- IBM Tivoli Access Manager for Operating Systems保护非结构化数据文件以及应用程序和操作系统资源，它能够建立规则来调优对所有UNIX和Linux账户的访问，包括特权用户账户，如超级用户和根账户。

- IBM Tivoli Federated Identity Manager在SOA和Web服务环境中交付了跨域或联邦SSO以及身份传播，支持可靠、便利、可审计的合作伙伴交互，解决了与其他域的合作伙伴访问相关的关键遵从性问题。
- IBM Tivoli Access Manager for Enterprise Single Sign-On帮助简化、扩展和保护最终用户对于Web和非Web应用程序的ESSO，使您能够优化生产力、降低与密码相关的帮助台成本并简化最终用户的密码管理工作。
- IBM Tivoli zSecure Suite联合IBM z/OS Resource Access Control Facility(RACF®)的管理、审计、警告和监控功能。设计用于帮助最小化安全性泄漏，流线化遵从性工作。

这种广泛的身份和访问管理产品组合能提供支持当今需求所必需的基础设施。除了管理用户身份和资源访问之外，建立来自IBM的集中、自动化的身份和访问控制基础设施终将成为业务驱动因素，帮助您：

最小化响应多种内部和外部控制和法规的复杂度。

- 通过捕捉、创建和自动化可重复工作的最佳实践来优化生产力和成本。
- 使IT员工能够转而关注价值更高的活动。
- 消除创新障碍，提供借助新业务机遇取得领先地位所必需的敏捷性。
- 促进业务流程的完整性和机密性。

更多信息

进一步了解适合您的企业的身份和访问管理解决方案，讨论IBM服务管理软件为您的组织带来的收益，请联系您的IBM销售代表或IBM业务合作伙伴，也可访问ibm.com/tivoli/solutions/security

关于IBM Tivoli服务管理软件

Tivoli软件为组织提供了一个服务管理平台，通过提供可见性、控制和自动化来交付优质服务——查看和理解其业务运作的可见性；有效管理其业务、最小化风险、保护品牌的控制；优化业务、降低运营成本、更快速地交付新服务的自动化。与IT中心的服务管理不同，Tivoli软件交付了管理、集成和协调业务与技术需求的通用平台。Tivoli软件设计用于快速处理组织内最紧迫的服务管理需求，帮助前瞻性地响应不断变化的业务需求。Tivoli产品组合由世界级的IBM Services、IBM Support和IBM业务合作伙伴的活跃生态系统提供支持。Tivoli客户和业务合作伙伴还可参与全球各地独立运作的IBM Tivoli User Groups（请访问www.tivoli-ug.org），利用彼此的最佳实践。