任奥科技关于针对企业客户
云存储云计算方案

目录

一.现状

存储是用户、数字化系统保存数据，共享数据的主要形式。目前常用的存储方式是将数据放置在在计算机的硬盘、U 盘、移动硬盘等设备中；需要数据共享的时候，采用邮件、QQ 文件传输等方式。这些方式的使用起来方便，容易被用户掌握。但这些常规的方式中，也存在以下问题：

1) 不便于携带。在任何需要数据的地方，用户都必须随身携带这些存储设备，电脑之类的设备体积庞大，不便于携带。

2) 数据容易丢失。这些信息都存储在用户自己的硬盘、U 盘中，这些设备没有做任何的存储冗余机制，在硬件设备损坏的情况下，数据就会丢失。

3) 数据不安全。数据存储在个人设备中，任何使用过这些设备的人，都可能获取这些数据，从而导致不必要的损失。

4) 容量有限。通过邮件等方式传输的数据，一般都存在附件大小的限制，过大的文件则无法传递。

5) 无法与数字化系统集成。信息化的管理系统均需要对文件进行统一的调用，这就需要存储系统能够提供一个高度共享的存储池，满足用户各系统相互之间的资源共享及数据统一进行访问。

二.什么是云存储

云存储是在云计算概念上延伸和发展出来的一个新的概念，是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统。当云计算系统运算和处理的核心是大量数据的存储和管理时，云计算系统中就需要配置大量的存储设备，那么云计算系统就转变成为一个云存储系统，所以云存储是一个以数据存储和管理为核心的云计算系统。

简单来说，云存储就是将储存资源放到网络上供人存取的一种新兴方案。使用者可以在任何时间、任何地方，透过任何可连网的装置方便地存取数据。

然而在方便使用的同时，云存储还具有安全性、兼容性、可扩展性等特点：

1) 作为存储最重要的就是安全性，尤其是在云时代，数据中心存储着众多用户的数据，如果存储系统出现问题，其所带来的影响远超分散存储的时代，因此存储系统的安全性就显得愈发重要。

2) 在云数据中心所使用的存储必须具有良好的兼容性。在云时代，计算资源都被收归到数据中心之中，再连同配套的存储空间一起分发给用户，因此站在用户的角度

上是不需要关心兼容性的问题的，但是站在数据中心的角度，兼容性却是一个非常重要的问题。众多的用户带来了各种各样的需求，Windows、Linux、Unix、Mac OS,存储需要面对各种不同的操作系统，如果给每种操作系统更够配备专门的存储的话，无疑与云计算的精神背道而驰，因此，云计算环境中，首先要解决的就是兼容性问题。

3) 存储容量的扩展能力。由于要面对数量众多的用户，存储系统需要存储的文件将呈指数级增长态势，这就要求存储系统的容量扩展能够跟得上数据量的增长，做到无限扩容，同时在扩展过程中最好还要做到简便易行，不能影响到数据中心的整体运行，如果容量的扩展需要复杂的操作，甚至停机，这无疑会极大地降低数据中心的运营效率。

4) 云时代的存储系统需要的不仅仅是容量的提升，对于性能的要求同样迫切，与以往只面向有限的用户不同，在云时代，存储系统将面向更为广阔的用户群体，用户数量级的增加使得存储系统也必须在吞吐性能上有飞速的提升，只有这样才能对请求作出快速的反应，这就要求存储系统能够随着容量的增加而拥有线性增长的吞吐性能，这显然是传统的存储架构无法达成的目标，传统的存储系统由于没有采用分布式的文件系统，无法将所有访问压力平均分配到多个存储节点，因而在存储系统与计算系统之间存在着明显的传输瓶颈，由此而带来单点故障等多种后续问题，而集群存储正是解决这一问题，满足新时代要求的千金良方。

三.云存储的优势

作为最新的存储技术，与传统存储相比，云存储具有以下优点：

1) 管理方便。其实这一项也可以归纳为成本上的优势。因为将大部分数据迁移到云存储上去后，所有的升级维护任务都是由云存储服务提供商来完成，节约了学校存储系统管理员上的成本压力。还有就是云存储服务强大的可扩展性，随着学校信息化的发展，用户会发现先前的存储空间不足，就必须要考虑增加存储服务器来满足现有的存储需求。而云存储服务则可以很方便的在原有基础上扩展服务空间，满足需求；

2) 成本低。就目前来说，用户在数据存储上所付出的成本是相当大的，而且这个成本还在随着数据的暴增而不断增加。为了减少这一成本压力，许多用户将大部分数据转移到云存储上，让云存储服务提供商来为他们解决数据存储的问题。这样就能花很少的价钱获得最优的数据存储服务；

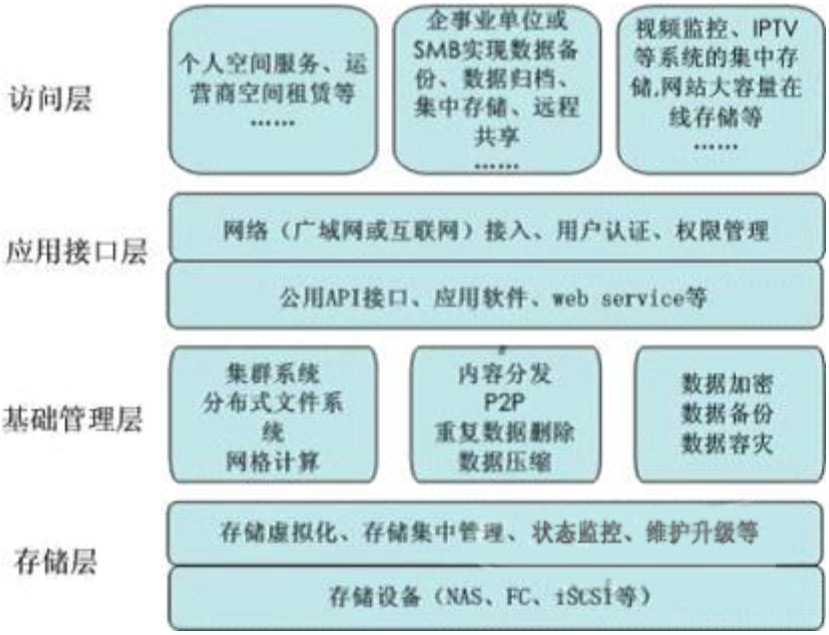
3) 量身定制。这个主要是针对于私有云。云服务提供商专门为单一的企业客户提供一个量身定制的云存储服务方案，或者可以是企业自己的 IT 机构来部署一套私有云服务架构。私有云不但能为企业用户提供最优质的贴身服务，而且还能在一定程度

上降低安全风险。

四.云存储架构

传统的存储模式已经不再适应当代数据暴增的现实问题，如何让新兴的云存储发挥它应有的能力，在解决安全、兼容等问题上，我们还需要不断的努力，就目前而言，云计算时代已经到来，作为其核心的云存储必将成为未来存储技术的必然趋势。

从架构的层面来看，云存储系统的结构模型由 4 层组成。



1) 存储层

存储层是云存储最基础的部分。存储设备可以是 FC 光纤通道存储设备，可以是 NAS 和 iSCSI 等 IP 存储设备，也可以是 SCSI 或 SAS 等 DAS 存储设备。云存储中的存储设备往往数量庞大且分布多不同地域，彼此之间通过广域网、互联网或者 FC 光纤通道网络连接在一起。

存储设备之上是一个统一存储设备管理系统，可以实现存储设备的逻辑虚拟化管理、多链路冗余管理，以及硬件设备的状态监控和故障维护。

2) 基础管理层

基础管理层是云存储最核心的部分，也是云存储中最难以实现的部分。基础管理层通过集群、分布式文件系统和网格计算等技术，实现云存储中多个存储设备之间的协同工作，使多个的存储设备可以对外提供同一种服务，并提供更大更强更好的数据访问性能。

CDN 内容分发系统、数据加密技术保证云存储中的数据不会被未授权的用户所访问，同时，通过各种数据备份和容灾技术和措施可以保证云存储中的数据不会丢失，保证云存储自身的安全和稳定。

3) 应用接口层

应用接口层是云存储最灵活多变的部分。不同的云存储运营单位可以根据实际业务类型，开发不同的应用服务接口，提供不同的应用服务。比如视频监控应用平台、IPTV 和视频点播应用平台、网络硬盘引用平台，远程数据备份应用平台等。

4) 访问层

任何一个授权用户都可以通过标准的公用应用接口来登录云存储系统，享受云存储服务。云存储运营单位不同，云存储提供的访问类型和访问手段也不同。

五.云存储方案的技术特点

该套方案中的管理系统主要管理着方案中的核心资源，包括帐号、权限、云存储门户、服务器监控及报警、服务器软硬件资产信息、服务器软件负载供应、存储等。

5.1 云存储帐号及权限管理

活动目录是 Windows Server 网络体系结构中一个基础且不可分割的部分。它提供了一套为分布式网络环境设计的目录服务，使得组织机构可以有效地对有关网络资源和用户的信息进行共享和管理。另外，目录服务在网络安全方面也扮演着中心授权机构的角色，从而使操作系统可以轻松地验证用户身份并控制其对网络资源的访问。

基于 Windows Server 2008 构建的活动目录融合了全新的技术特点，具有以下的功能：

- DNS 集成

活动目录使用域名系统（ Domain Name System ，简称 DNS ）。这使得运行在 TCP/IP 网络上的计算机可以识别和连接另一台计算机。 DNS 域和 Windows Server 2008 R2 的域自然而有机的结合在一起，使得整个目录结构成树型分布，具有了 DNS 的层次感觉，也使得 Windows Server 2008 R2 系统能够支撑庞大的目录结构，是的目录对象涵盖了整个网络元素：用户，计算机，打印机，共享文件夹，应用程序，管理策略等。

- 目录定位服务

通过 DNS 服务中的 Service Resource Record （ SRV RR ）记录公布提供目录服务的服务器地址， SRV RR 中的附加信息指出了服务器的优先权及重要度，使得客户可以选择他们所需要的最好的服务器。 DNS 记录也可以集成到目录中，随着目录复制而达到 DNS 复制的目的。

- 全局唯一的用户名

在域内一个用户对象只能有一个用户主名，而这个用户名是可以用 username@domainname 表示的，就好比一个用户的 mail 地址一样。正是具有了这个特性，才能够实现在企业内只要一套用户认证系统就可以实现所有应用系统的单一认证问题。

- 可扩展性

活动目录是可扩展的，就是说管理员可以向模式中添加新的对象类，也可以向已经存在的对象类添加新的属性。模式包括每一个对象类和对象类属性的定义，它们可以存储在目录中。

- 灵活的查询

用户和管理员可以使用 " 开始 " 菜单上的 " 查询 " 命令、桌面上的 " 我的网络 " 图标

或者 " 活动目录用户和计算机连接 " 插件来根据对象的属性快速的查找网络上的对象。

- 身份联合

ADFS （活动目录身份联合）提供了基于 Web 的 extranet 验证/授权、单一签名登陆 (SSO) 和针对 Windows Server 环境的联合的身份服务，从而提高了在涉及 B2C extranet、intracompany (多森林的) 联盟和 B2B internet 联盟的场景中、现有活动目录部署的价值。

- 基于策略的管理

组策略是在初始化时对计算机或者用户进行的配置。所有的小组策略设置都包含在组策略对象（ Group Policy Object ，简称 GPO ）中，它可以应用与活动目录站点、域或组织单元中。GPO 设置确定对目录对象和域资源的访问、哪些资源域是用户可以访问的以及这些资源域应该如何使用。

在利用企业网的目录管理服务提供单一的用户身份验证方面，总的来说，存在两方面的应用连接方式：

- C/S 应用的连接方式
- WEB 应用的连接方式

其中，WEB 应用的连接方式 比较统一，解决方法也比较成熟，而 C/S 应用的连接方式就比较复杂，需要根据特定的应用具体分析，举例来说， Domino/Notes 系统就是典型的 C/S 应用。

在综合了所有解决方案之后，通过对安全性，用户使用的方便性，管理要求，实现技术的成熟性几方面的比较，最后推荐使用登录信息代理方式解决单一用户登录，统一认证(SSO)的问题。

这种方式的实现原理是：应用的登录信息存储在目录数据库（ AD ）中，通过 AD 的用户认证得到保护。在应用系统登录时从 AD 中获得相关信息进行登录。这个过程通过 SSO 插件透明进行，从而实现 SSO 。

- UNIX 身份管理

通过将 AD 域控制器作为主 NIS 服务器，并同步 Unix 和 Windows 环境中的用户密码，UNIX 集成有助于在操作系统间建立不间断的用户访问和有效的网络资源管理。

5.2 云存储服务器运维及监控

该部分内容提供对整个业务系统及管理系统自身的监控及报警，包括定义监控内容、数据采集、监控告警等。

5.2.1 数据采集及监控

针对业务系统及各项软硬件的数据采集，我们将使用 System Center Operations Manager（SCOM）对整个系统进行监控并收集数据、汇总、生成报告。SCOM 可以对如下的基础 IT 设施进行数据采集：

- 主机数据采集，主要包括：Windows 服务器和 UNIX/Linux 服务器；
- 数据库数据采集，主要包括：Oralce、Sybase、MS Sql Server 等；
- 存储设备数据采集，包括 HP、IBM、EMC 等厂家的设备；
- 中间件数据采集，包括：Microsoft.Nnet、Adobe JRun、Bea Weblogic、IBM Websphere

等中间件；

该系统支持异构环境的综合数据采集及监测，能对 Windows 系统平台服务器、大部分主流的 UNIX/Linux 系统平台服务器、主流数据库、应用服务器、存储设备以及支持 SNMP 协议的路由器、交换机、防火墙等网络设备进行全面的深入的数据采集管理。系统使系统管理人员能在日趋复杂的 IT 环境中即时快速方便的了解整个系统的运行状况，从而能从应用层对 IT 系统的关键资源、应用进行全方位的实时监控管理。对于详细的数据采集（及监控）要求如下所述：

- **主机**数据采集（**及监控**）

系统可以从多个方面对 Windows、UNIX、Linux 服务器的硬件设备、操作系统进行监控管理。通过采集相应服务器的 CPU、内存、磁盘、网卡等硬件的关键运行参数，软件和应用程序的进程、服务、端口的运行状况，系统能够及时对影响企业服务器运行性能的故障事件发送报警，并采取相应的故障处理措施，保证服务器的正常安全运行。系统中提供的与服务器相关监控指标主要包括 CPU、内存、磁盘空间、服务、进程、网卡、错误日志、Windows 事件日志、UNIX LOG 文件、文件和目录内文件数等。系统对主机的监控采用两种方式：代理方式和无代理方式。

对于使用无代理方式进行监测服务器时，系统使用 TELNET、SSH 和 WMI 协议来获取远程服务器的系统资源。具体流程如下图所示：

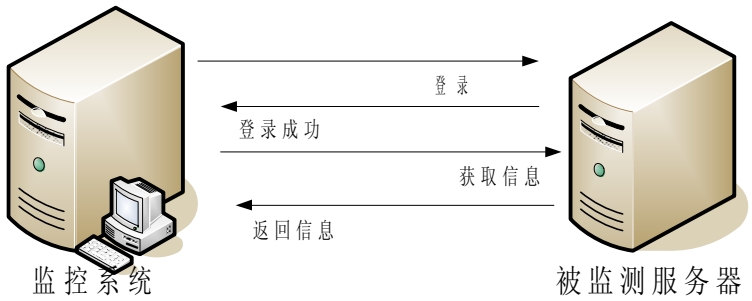


图 系统无代理监测方式

对于使用代理方式进行监测的服务器，系统使用 TCP 协议来传输经过加密的数据的方式来获取远程服务器的系统资源。具体流程如下图所示：

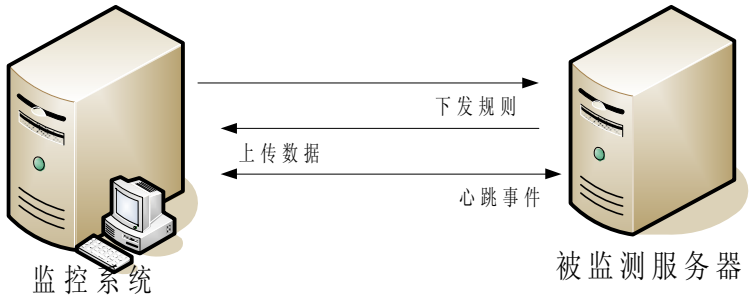


图 系统使用代理监测方式

对 Windows 主机的监测主要包括如下性能指标：

处理器	系统处理器性能通过以下性能指标在系统范围内衡量其性能： · CPU 利用率 · 中断时间百分率 · DPC 时间 处理器能够在可选性地单个处理器级别通过以下关键性能指标被监控： · CPU 利用率 · 中断时间百分率 · DPC 时间百分率 性能数据通过以下处理器性能指标被收集： · 系统处理器队列长度 · 每秒钟的系统内容交换 · 总的中断时间 · 总的 DPC 时间 · 总的 CPU 利用率
内存	包括物理存储器、虚拟存储器（即页面文件）在内的存储器通过以下性能指标被监控： · 可用存储空间（MB）； · 每秒钟的页面交换； · 页面文件利用百分率。 性能数据通过以下存储指标来收集： · 确认使用的字节百分比； · 可用的 MB · 每秒页面交换； · 非页面字节存储池（默认被禁用）； · 存储池页面字节（默认被禁用） · 页面文件使用的百分率。
逻辑磁盘	逻辑磁盘的监控和性能数据收集以平均单次读取磁盘时间、平均单次写入磁盘时间以及单次传输磁盘时间来衡量。
物理磁盘	物理磁盘的监控与性能数据以平均单次读取磁盘时间、平均单次写入磁盘时间以及单次传输磁盘时间来衡量。
网络适配器	网络适配器通过每秒钟接受的字节数、每秒钟发送到字节数、每秒钟的总字节数来被监控。同时，网络适配器的健康状态被评估而且如果连接则被设为“运行良好”如果连接中断则显示“受限制的连接或无连接”
关键进程	进程占用资源情况包括：CPU、内存、IO 的使用情况，以及进程使用句柄数、线程数等

对 UNIX/Linux 主机的监测包括如下性能指标：

处理器	CPU 利用率
内存	内存使用率 内存剩余空间
逻辑磁盘	逻辑磁盘剩余空间 逻辑磁盘使用率

磁盘 IO	传输速率 每秒读取字节数 每秒写入字节数
网络适配器	输入错误数据包数 输入总的数据包数 输出错误数据包数 输出总的数据包数
进程	系统中关键进程数量
目录	系统中特定目录下文件数量
错误日志	系统中指定日志中的错误条数
进程排名	系统中 CPU 使用率第一的进程名 系统中 CPU 使用率第二的进程名 系统中 CPU 使用率第三的进程名

■ **数据库数据采集（及监控）**

系统的数据库监测模块可以全面智能的监测企业数据库以及与数据库应用相关的服务。系统对 Oracle、SQL Server、DB2、Informix、Sybase、MySQL 等主流数据库从可用性、系统资源占用和数据库性能指标三个方面提供全面的监测管理，确保数据库的正常运行。系统的数据库性能监测模块能够连续地监控企业数据库的关键参数。例如：数据库系统设计的文件存储空间、系统资源的使用率、配置情况、数据库当前的各种锁资源情况、监控数据库进程的状态、进程所占内存空间、可用性等。系统可以在服务中断时捕获问题信息，并且自动发送到告警控制台，使系统管理员能够及时采取措施，避免灾难性的事故。 系统的数据库监测模块是通过 ODBC 和 OLE DB 协议进行监测和采集数据的，具体原理如下图所示。

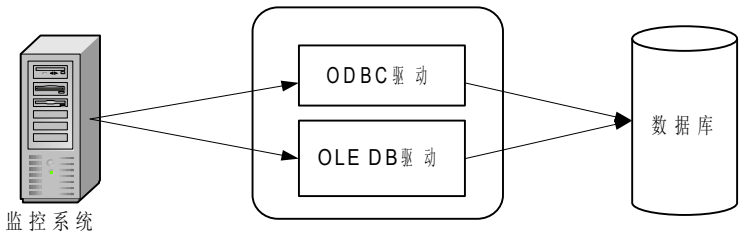


图 系统数据库监测模块原理

系统对数据库监测提供了多层面立体矩阵式的解决方案，使监测更加准确，对数据库的监控包括如下指标：

数据库性能	CPU、内存使用状况 数据库缓冲池或者数据操作状况 游标使用状况 线程状况 打开的表数量 输入输出状况 。。。

表空间	表空间总大小 保留表空间大小 数据库使用大小 剩余表空间大小 。。。
死锁状况	死锁数量 总的锁数 独占锁数量 。。。
连接数	当前连接数 最大连接数 失败连接数 。。。

- **存储设备数据采集（及监控）**

系统可以对存储设备进行监控，主要包括：IMB、HP、EMC、NetAPP 等厂商的设备，监控方式主要是采用 SNMP 协议，监测的具体指标如下：

设备基本信息，包括处理器、磁盘、设备使用的端口信息等；

设备性能信息，包括磁盘的读写速率以及字节数，磁盘缓存性能，处理器状态、磁盘状态等数据；

其他方面，包括：设备温度，风扇状态等。

本系统目前不支持 HDS 存储设备，但是可以根据用户要求定制开发。

- **中间件数据采集（及监控）**

系统可以对中间件进行监控，主要包括：Microsoft.Net、Bea Weblogic、IBMWebsphere 等，监控方式可以采用 HTTP、SNMP 或者 WMI 协议，监测的具体指标如下：

中间件服务器 JMS 状态信息，包括：创建、发送、接收、读取等；

中间件连接状态信息，包括：当前连接数、最大连接数、失败连接数等；

中间件队列以及线程状态信息，包括：空闲线程数、队列中的请求数、队列中已处理请求数等；

中间件会话状态信息，包括：当前打开的会话数、最高会话数、总的会话数等；

中间件事务状态信息，包括：全局事务数、本地开始事务数、持续全局事务数、提交全局事务数等；

- **其他数据采集（及监控）**

系统还包括其他一些监测模块如网络设备、防火墙、大型主机、打印机等设备以及其他一些常规监测模块。

1）网络设备

系统可以从各个方面对网络设备进行监测和管理，内容包括网络设备的可用性、设备性能、接口流量管理和业务分析等等。系统的网络设备管理系统支持的网络设备主要有各种类型的路由器、交换机、防火墙、以及其他启用了 SNMP 协议的相关设备。

SNMP 协议是对网络设备进行监测和管理的标准协议，系统的网络监测模块的技术核心集中在使用 SNMP 协议对网络设备进行监测的实现，并且支持 SNMP 协议的 V1、V2、V3 三个版本。通过 SNMP 协议系统中的网络设备监管模块提供的了极为广泛的监测范围。系统不但提供了多种基于 SNMP 协议的监测模块，而且还提供了基于 SNMP 协议进行监测的标准接口模

块，以满足网络设备的不同层次的监测需求。

通过该模块，管理员可以全面监测整个网络体系，例如网络的连通性及其网络设备的状态，如接口状态、接口流量、接口丢包率、路由器的 CPU 负载、内存使用率等。该监测模块需要被监测的网络设备启用 SNMP 协议，系统通过发送 Get 请求并接收来自被监测的网络设备的响应，或者主动监听 Trap 消息接收端口并对 Trap 消息进行分析过滤。下图为系统网络监测模块的工作原理。

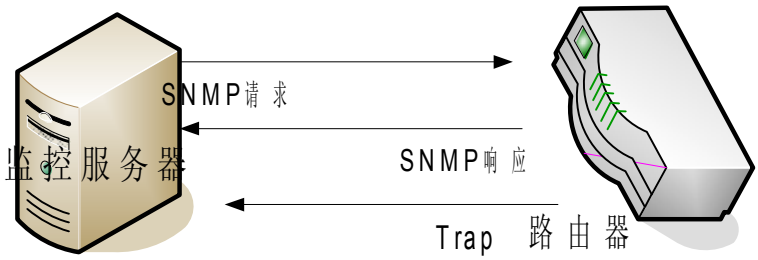


图 系统网络设备监测示意图

目前系统中可以监测的网络设备包括：Cisco 路由器、交换机，Cisco Pix 防火墙，Checkpoint 防火墙，NetScreen 防火墙，华为 3Com 路由器、交换机，Alteon 路由器、交换机，Foundry 路由器、交换机等等一些知名网络厂商的产品。

2）UPS、打印机以及大型机

系统还拥有 APC、Libert UPS、HP 打印机、AS400 主机的监测模块。

5.2.2 事件及警告管理

SCOM 系统可以实现非常灵活的事件及警告管理功能。在 SCOM 平台中对于事件告警管理采用如下流程：事件收集－－事件分析－－事件处理（警告）。

- **事件收集**

系统可以收集 CSV 格式的日志文件、文本文件格式的日志、NT 事件日志、SNMP 事件、SNMP Trap 消息、Syslog、WMI 事件，并且提供了基于 SNMP、Socket、WMI 等标准协议的采集接口，为用户提供了灵活的、可扩展的事件采集方式。通过这些接口用户可以采集自定义事件而不需要进行二次开发。

- **事件分析**

系统对采集到的事件数据提供了分析规则，规则主要分为两种：预定义规则、自定义规则。预定义规则是指和管理包一起发布的，已经定义好的规则，自定义规则是指在预定义规则不能满足用户分析过滤的需求时，所提供的接口，通过使用自定义规则用户可以定制自己的事件分析规则。事件分析规则主要由事件源、过滤条件、报警信息组成。

- **事件处理（警告）**

系统根据事件过滤表达式对事件进行过滤后，生成统一的事件格式并保存在系统的数据库中。事件数据主要包括：事件范围、级别、事件数据、消息、编号、事件参数等字段。其中事件级别包括：成功、信息、警告、错误、认证成功、认证失败六个级别，事件参数用于保存用户自定义的字段，并且支持多个自定义属性，事件数据展示时将以 XML 格式展现。

系统中的事件数据分别存储在运行时数据库和报表数据库，运行时数据库中的事件数据供实时查看使用，报表数据库中的事件数据为历史数据供生长报表以及分析时使用。事件在处理

过程中不进行事件压缩，而是只针对该事件产生的报警进行压缩和抑制。当被监测对象和监测服务器之间的通信中断时，如果是采用代理方式监测，则产生的事件数据会保存在代理端，通信恢复时会自动上。由于本系统支持 Fail-Over（故障转移）功能，因此当主服务器发生故障时，系统所采集的事件数据会自动被提交到备份服务器中。

5.3 云存储服务器软硬件资产及补丁管理

5.3.1 软硬件资产变更管理

对于服务器的目前硬件配置现状的准确的收集以及展现，是服务器管理的重要方面，只有准确了解服务器的硬件配置状况，才能根据运维采集的性能趋势数据，准确制定硬件配置升级计划，通过硬件配置的记录，可以清晰地帮助 IT 管理员掌握全面的服务器硬件资产信息。此外，对于服务器目前的软件配置状况，同样需要管理员通过自动化手段进行自动统计和配置记录。以便与管理员了解服务器的具体应用部署情况，清晰的了解服务器目前所处的服务应用角色等信息。

此功能，可以通过 System Center Configuration Manager 的资产管理功能来实现。

SCCM 的软硬件资产管理功能是基于标准的硬件清单，即通过利用 Windows Management Instrumentation (WMI)，SCCM 提高了清单扫描过程中客户端的性能并提供了一组更丰富的清单数据，其中包括 BIOS 和机架外壳数据。目前可以支持超过 130 种 WMI 的类型，可以获取丰富和准确地信息。而且 SCCM 可以提供灵活细致的清单。尽管 SCCM 使企业能跟踪其服务器系统上几乎全部的软件资产，但通常企业会有特别重要或感兴趣的一组核心应用程序和文件。通过使用通配符、环境变量和文件属性之类的功能来提供实施智能清单搜索的功能，SCCM 使企业可以专注于他们所需的信息。通过跳过压缩和加密的文件，还可以减少系统资源的消耗。为确保丰富的清单和使用情况跟踪信息易于访问且与业务相关。

5.3.2 客户端资产管理

基于 System Center Configuration Manager(SCCM)及微软终端自动化部署解决方案，可以非常方便地帮助统计所有在网内的终端的详细软硬件配置信息，包括对于每个终端具体硬件配置信息，软件安装信息的自动化统计，并且可以通过报表方式进行灵活展现，并且对于终端的软硬件配置信息的变动进行跟踪。便于对终端的有关信息的统计和管理。

5.3.3 客户端软件部署及补丁管理

- 客户端自动化安装(BDD)管理

商业桌面自动化安装 / 恢复技术

微软提供了整体商业桌面标准化自动恢复解决方案，提供了***部署标准办公终端桌面标准化配置，以及对于发生硬件损坏以后，如果快速进行完全恢复的解决方案。

商业桌面自动恢复技术包含如下几个方面：

桌面标准化镜像打包技术（Imaging）

微软终端管理平台提供了业界标准的 Windows 镜像打包技术。微软终端管理平台提供了对一个参考计算机的配置情况进行完整的镜像打包，形成一个标准的 Windows Image Format 的文件（WIM），此文件是基于扇区的对操作系统进行完整的打包，将所有的系统配置和所需要安装的软件都组合在一个文件中。并且可以支持动态地增加驱动程序，以能够支持各种不同的硬件设备。

通过 WIM 镜像进行操作系统的恢复，可以大大加快部署的效率，并且有很多灵活的配置可以通过此技术实现。

一个企业可以根据他们终端类型的不同，制定包含不同类型应用软件的镜像文件版本，或者包含不同硬件抽象层的终端设备类型的镜像文件以便灵活使用，或者可以进行动态地配置加载不同的应用程序。

统一部署架构

通过镜像打包可以生成了企业需要的标准配置镜像文件，在微软终端管理平台的统一架构上，可以实现统一管理，统一制定部署策略，可以通过局域网进行网络部署，也可以通过光盘部署。

自动策略判断区别安装技术

微软的商业桌面自动恢复技术，包含了管理信息数据库，这个数据库可以定制灵活的部署策略，例如，根据不同用户名（通过用户交互提示，输入的信息）或者计算机网卡的 MAC 地址，自动判断其需要安装镜像文件，需要加入的域名，需要属于的组织单位，使用的操作系统的产品密钥,所需要安装的应用软件等。并且可以将计算机的本地管理员的权限集中收管。

远程镜像安装技术或者光盘镜像安装技术

最后，自动部署还需要依靠计算机网卡支持网络远程启动，然后可以从网络将镜像文件进行恢复。当然，考虑到对网络的影响，对一些网络带宽资源不是很充裕的支行，也可以采用光盘镜像安装技术实现部署和恢复。

整个商业桌面自动部署实现流程如下：

按照不同的业务需求，安装需要作镜像的参考对象桌面系统。

使用桌面管理系统终端管理平台，通过终端管理平台的镜像打包向导，对参考对象桌面系统进行镜像打包。

配置自动部署策略，定制管理信息数据库，将用户名、产品密钥、域信息、硬件网卡 MAC 地址信息进行配置。

将镜像文件存放在远程安装服务器上，将计算机作为网卡启动，进行远程安装；或者将镜像文件通过光盘在每个桌面计算机上安装。

■ 客户端补丁管理

通过安全桌面管理解决方案，可以实现对终端 PC 的自动更新本地系统的操作系统（Service Pack、补丁、第三方防病毒）、应用系统等。

终端管理平台的补丁管理机制可以帮助系统管理员审计，部署和跟踪在整个企业中所有桌面操作系统的应用软件补丁。终端管理平台不光能够完成对操作系统的补丁管理，还可以实现对 Office, IE 浏览器，SQL Server, Exchange 等应用软件的补丁，以及第三方软件或者企业自开发的软件的补丁管理能力。

将通过终端管理平台应用分发将扫描工具安装到每个客户端，终端管理平台依靠本地的扫描引擎，对客户端的补丁情况进行扫描，它比对最新的补丁信息库，查找出每个客户端上需要安装的补丁信息，将这些信息存储在本地的 WMI，然后将所有信息发送给终端管理平台服

务器。

在终端管理平台控制台上，管理员可以看到每台客户端的补丁安装状况，也可以通过 Web 报表了解企业内部所有补丁安装状况。

补丁安装引擎，将完成补丁的本地安装，它将比较授权批准安装的补丁和本机需要安装的补丁列表，决定在本地需要安装补丁列表。

- 客户端软件部署管理

基于终端管理平台可以灵活地实现对于终端的各种新业务应用需要进行推广的快速部署能力。

终端管理平台提供了强大的软件分发能力，可以实现自动化的软件集中分发的能力，并且可以针对不同的终端分组，例如：不同地市公司，不同业务终端进行定制不同的软件分发策略。并且提供了部署的整体数据统计，以便于统计部署的效率以及成功率。对于软件分发，由于主要的性能在 IO 处理上，建议可以单独利用一台现有的文件服务器作为软件分发的奋发点角色，在省公司以及每个地市公司级别都可以放置这样一个角色，以提高对于软件分发的效率。

最新的终端管理平台提供了对于关键终端软件部署管理，需要考虑服务级别管理，需要设置维护窗口期。例如，在平常业务时段，是不可以对终端进行系统补丁或者软件升级安装维护工作，只有在规定的维护时间段才可以。可以灵活针对不同组合的终端设置不同的维护窗口期。

此外，终端管理平台的软件部署管理还整合了网络唤醒能力，可以将休眠或者关机的计算机进行集中唤醒然后进行软件部署管理。

- 客户端远程维护管理

基于终端管理平台，还可以实现终端的远程维护管理，管理人员可以在接受到员工遇到的桌面问题，可以利用远程维护的功能，帮助对方快速的解决问题完成维护任务。

5.4 数据备份及保护

对于服务器的全面备份／恢复管理也是服务器管理中的重要组成部分，服务器备份应该包括两个层面，应用层面的数据备份／恢复，系统状态的备份／恢复。

基于 System Center Data Protection Manager（SCDPM）可以全面的实现应用层面以及系统状态层面的备份／恢复。

对于应用层面，SCDPM 可以实现如下应用的备份／恢复：

SQL 2000, SQL 2005

Exchange 2003/2007

Microsoft SharePoint Portal Server 2003, Microsoft Office SharePoint Server 2007 (MOSS 2007)

Windows Server 文件服务器。

SCDPM 结合了 Windows Server 内置的 VSS (Volume Shadow Copy Service) writer 服务，可以实现 512 个瞬时通过 VSS writer 产生的卷拷贝，SCDPM 可以对此 VSS 卷进行磁盘到磁盘的备份。并且还可以每 15 分钟进行一个基于磁盘块级的差量数据备份恢复点，最多可以产生超过 33 万个备份恢复点。基本上保证了对于应用层面的完整备份。而且具有非常简单的管理

界面进行数据备份和恢复操作。

对于 DPM 结合 VSS writer 技术，SQL 数据库，Exchange 邮件服务器，以及 SharePoint 服务器都具备了相应的 VSS writer 服务，既可进行非常快速的在线备份。是目前 Windows 平台上，SQL, Exchange, SharePoint 最佳的备份和恢复工具。

此外，SCDPM 还可以对服务器的整体系统状态实现硬件裸设备级别的备份 / 恢复管理。

通过 SCDPM 可以实现对服务器的整体系统状态的全备份，通过此备份产生一个可以启动的 ISO 文件，即使发生硬件崩溃，可以通过次备份进行裸设备级别的恢复，快速恢复整个系统。