政府边防管制机关

Bloombase® Spitfire StoreSafe™ 安全存储服务器

Bloombase® Spitfire KeyCastle™ 密钥管理服务器

政府部门有效利用 Bloombase® Spitfire StoreSafe™ 企业级安全存储加密及 Bloombase® Spitfire KeyCastle™ 密钥管理安全方案，成功实现了数据仓库系统中个人出入境管制敏感信息的加密保护。

项目背景

客户背景

- 该政府机关负责人员入境管制并签发个人身份证明及相关旅行文件
- 员工：12,000 人以上

项目简介

遵从本地个人信息保护法，为现有商业智能及报告系统中的个人敏感信息提供加密保护

主要挑战

- 不改变最终用户、管理员及操作员使用流程
- 系统生产力及响应速度不能有明显降低
- 不改变现有数据仓库系统
- 无需编码
- 无硬件、系统或应用变动
- 可分步进行部署及数据迁移
- 支持 SCSI 磁盘、磁带及虚拟磁带库 VTL 等各种存储介质
- 一个方案同时保护处理过的以及未经处理的/原始的文件系统

项目目标

- 对存储在存储区域网 (SAN) 及备份磁盘上的动态数据库数据进行加密
- 保护文件系统对象，关联数据库，未处理的 RAW 原始盘符及备份介质
- 兼容现有数据生命周期管理 (ILM) 系统，实现自动化的数据存留

方案与服务

- Spitfire KeyCastle™ 密钥管理服务器
- Spitfire StoreSafe™ 企业安全存储服务器

选择 BLOOMBASE 的理由

- 充分利用现有软硬件资源
- 提供全面的核心存储加密管理
- 中立的平台及应用解决方案
- 可升级及可扩展能力
- 支持客户自定的加密算法

项目实施特点

首个公共机构使用 Bloombase Spitfire 企业级信息安全服务器在数据读取、转换及载入(ETL)、数据仓库、数据报告、备份及存档中部署端对端的连续数据保护

主要优点

- 立即达到信息保护法规要求
- 透明的部署
- 高性能的加密保护
- 不影响系统响应
- 高可用性及容错能力

现有环境

- 没有现成的数据加密
- 数据中心的系统硬件在物理上彼此分离

硬件

- IBM p-Series 服务器
- EMC Symmetrix SAN 存储区域网
- Brocade FC SAN 交换机
- IBM 磁带库
- HP Integrity 服务器

操作系统

- IBM AIX 5.3
- Red Hat Enterprise Linux 4

软件

- IBM OnDemand Content Manager 内容管理
- IBM DB2 Universal Database 通用数据库

概述

负责边防管制的政府机关通过智能系统来追踪人员出入境记录，进行入境流动信息的采集和习惯分析。

个人信息保护法规定，此类信息需要严格控制并进行严谨的加密保护，包括存储在硬盘、光盘、磁带盒等各种介质上的所有数据。

客户需要在短短的三个月内，为已经运营5年的系统部署有效的数据保护。此外，还要求不改变系统结构及用户/操作员使用流程，并保持同等服务水平（包括系统响应率、可用性、性能等）。最终，客户选择了 Bloombase® Spitfire StoreSafe™ 企业安全存储服务器，为敏感数据提供动态加密，并通过 Bloombase® Spitfire KeyCastle™ 密钥管理服务器实现整个信息生命周期的密钥管理。

雄心勃勃的试验项目

该智能业务系统已经运营五年以上。和客户IT架构中的其它核心业务运营系统一样，这是一个关键任务处理系统。

作为数据保护的领头项目，该加密解决方案需要具备容错性、高可用性及随时可用的灾难恢复能力。

BLOOMBASE® 博隆兴中

边境出入人员的信息全天候实时提交至智能业务系统，其中包括人员姓名、身份证、签证及护照等个人身份证明文件的号码、出入境日期及时间等敏感信息。这些信息来自区内的各个边防检查单位，并暂时保存在系统的临时存储区。负责读取-转换-载入 (ETL) 的人员对进入系统的信息进行处理，启动内容过滤器进行潜在威胁扫描。带病毒的内容和有威胁的内容将被拒绝载入，并转移至信息驻留区等待检查或丢弃处理。干净的文件经过解析、内容读取处理后载入 IBM DB2 Universal Database 通用数据库系统上的关联数据库系统。

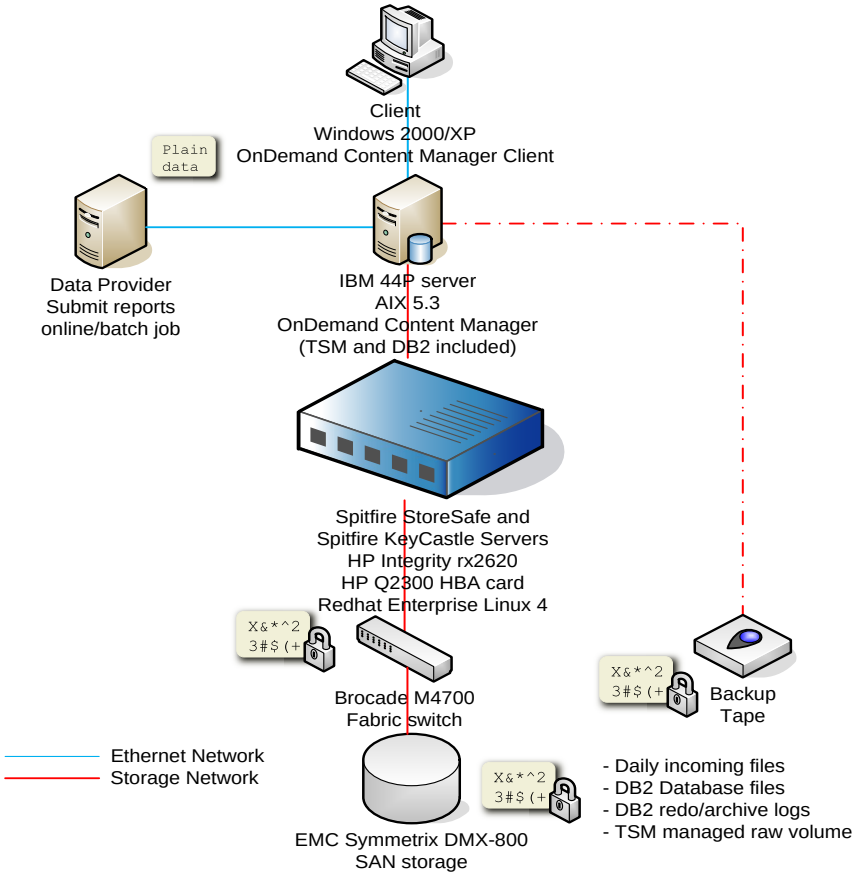
通过 IBM OnDemand Content Manager 内容管理工具的管理控制台，系统的最终用户可定义需要生成的报告及生成时间。当系统运行分析任务时，就会生成一个报告文件，存储在 IBM Tivoli Storage Manager (TSM) 存储管理系统的原始存储区。IBM OnDemand Content Manager 将分析任务连接到存储输出报告的物理地址。当用户检索分析结果时，IBM OnDemand Content Manager 就会读取物理EMC存储区域网 (SAN) 磁盘，并向用户显示可阅读的结果信息，或输出文件以供未来分析或报告之用。

IBM TSM 管理存储区的信息生命周期，自动将过期或很少访问的报告卸载到磁带库存档，为新的和经常访问的报告准备可迅速存储的空间。另一方面，当用户检索的报告属于存档报告时，IBM TSM 会从备份磁带库将报告内容恢复到 SAN 磁盘。

“Bloombase Spitfire™ 企业安全解决方案提供低总体拥有成本的整体性解决方案，实现密钥管理、文件保护、数据库保护、原始磁盘加密及备份数据加密”

在 IBM OnDemand Content Manager，DB2 UDB 及 TSM 的强大支持下，智能业务系统实现了无缝的运行，达到了配备 EMC Symmetrix SAN 的 IBM Power 平台的最高性能指标。但在数据保护方面却碰到了第一个挑战。现有的应用全部部署在非定制化的产品上，无法进行修改，因此根本无法在应用层面实施数据加密。

客户面临的第二个挑战是加密数据库。数据库的加密不仅部署困难，并且需要加密配置大量的数据库对象，而数据库加密产品根本不能解决敏感的临时存储和报告仓库中的数据私密问题。



传统文件系统加密产品的概念证明测试失败了，这让客户倍感挫折。传统文件系统加密可以处理数据临时存储区、数据库文件以及目录文件，但无法对文件系统还未经过处理的报告仓库进行加密，也就是原始文件系统或者没有文件系统的区域。

考虑到服务器容量和审计要求，客户不希望在现有 AIX 应用服务器上额外增加软件。同时，客户要求报告生成的平均处理时间必须控制在 30 秒以内。

挑战变成机遇

除了客户考虑到的各种加密产品的兼容性外，还存在很多待解决的问题：全面的密钥管理系统，系统需求增长所需的可以轻松升级的加密平台，可支持各种密码组合乃至客户特有密码算法的密码平台，还有可支持未来平台改动的平台独立性和应用独立性等等。

客户最终选择在 HP Integrity 服务器上安装 Bloombase® Spitfire™ 企业安全解决方案，以满足其严格的数据保护要求。

Spitfire StoreSafe™ 将进入系统的数据临时存储 DB2 数据文件库及 OnDemand Content Manager 报告仓库，虚拟成基于 Spitfire StoreSafe™ 文件和经过防护的虚拟存储，不需要改动任何最终用户流程、应用或硬件平台。

Spitfire StoreSafe™ 虚拟存储提供安全的、可更新的虚拟加密内容副本，通过物理方式存储在磁盘上。因此，不用修改原有的系统及应用，即可轻松访问受 Spitfire StoreSafe™ 保护的存储内容，就像访问普通的文件和磁盘一样，而实际上敏感数据都已经过了严格的加密。只有当 OnDemand Content Manager 及 DB2 UDB 要求检索存储内容时，才会触发 Spitfire StoreSafe™ 对敏感内容进行解密处理，当数据由Content Manager 进行存储，或数据库记录提交至 DB2 时，将会触发 Spitfire StoreSafe™ 对敏感数据进行加密，然后再物理存储到 EMC SAN 磁盘上。

有了 Spitfire StoreSafe™，客户可以分阶段迁移整个数据存储，从而最大程度减少窗口分割，保证服务的可用性。TSM 就像管理正常盘符一样管理加密的原始盘符，因此，保存在备份磁带盒上的存档数据可以保持原始的安全加密形式。

最终客户通过 Bloombase Spitfire™ 安全平台实现了端到端的数据私密保护，以低总体拥有成本 (TCO) 达到了国家数据安全的严格要求。

4AA0-0696EEP 09/2006

BLOOMBASE®
博隆兴中