

安徽定远供电公司数据灾备系统

项目背景

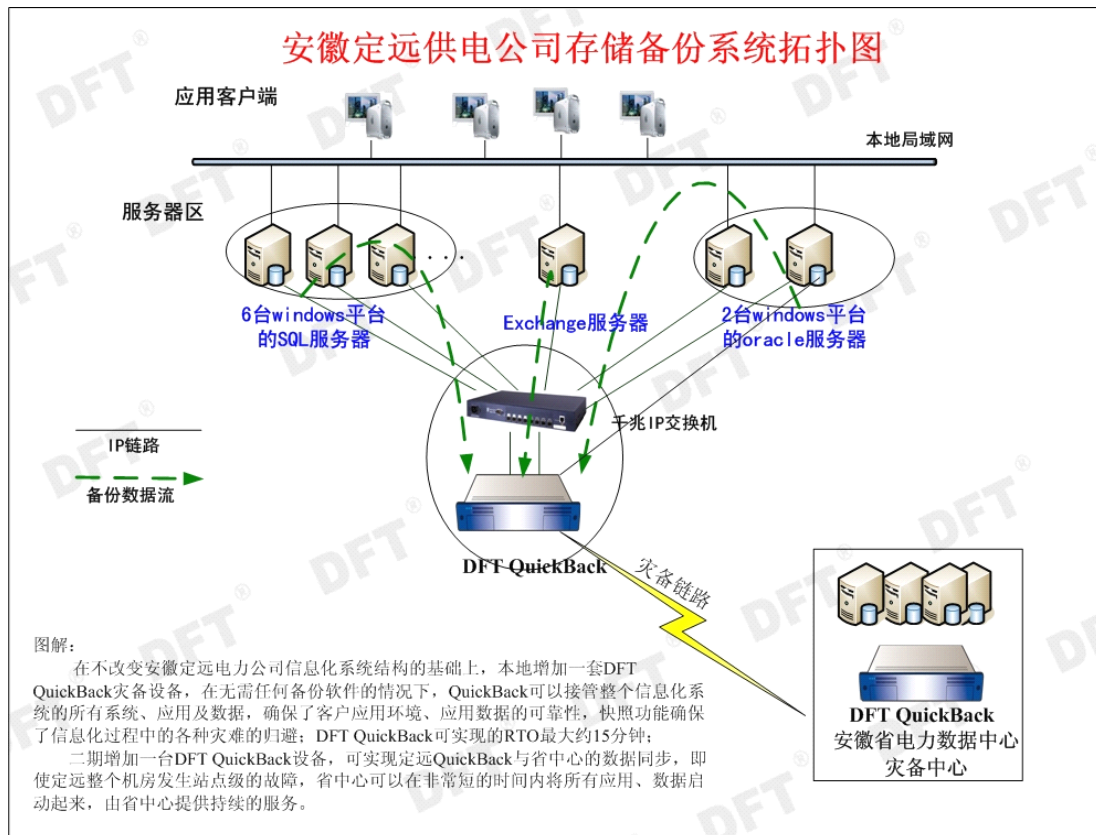
随着电力系统信息化建设的不断推进，业务的快速发展，各种应用系统已陆续建成并投入使用，这些应用系统为电力行业的发展起着重要的作用。如何保证这些系统更加稳定可靠的长时间运行，是信息建设进程中的重中之重，而其中，维系整个业务系统生存的就是在系统中不断产生、交换、变更地业务数据。保证业务系统的稳定也就成了保证业务系统中数据的安全和可靠。

在电力企业中，应用业务系统数量不多，主要有 MIS 系统、OA 系统，计费系统等核心系统。MIS 系统包括业务管理子系统、电费管理子系统、用电检查子系统、计量管理子系统、用户管理子系统；以上系统数据必须得到最安全的保证，一旦数据发生损坏或丢失，造成的后果将是不可估量。

需求分析

安徽定远供电公司的服务器系统主要有 9 台数据服务组成（6 台 windows 平台的 SQL 服务器，2 台 windows 平台的 oracle 服务器和一台 exchange 服务器），目前对服务器的数据都未进行专业的数据备份保护，重要的数据也只是人工的备份操作，如定期刻光盘、拷贝到移动硬盘上等，一旦系统或者某一硬盘出现故障，将无法及时、可靠的恢复数据，甚至造成数据丢失，直接影响供电公司业务的正常运行，基于这种环境下，信息中心决定建设一套针对服务器数据的存储备份恢复系统，来保证数据的安全和业务的持续运行。

DFT 解决方案



如拓扑图所示，定远供电公司总计有 9 台数据服务器需要进行数据备份保护，从数据的安全高效备份和未来扩展的角度考虑，DFT 本次数据备份采用千兆 IP 网络进行服务器群和备份设备之间的连通，做好了数据保护，就能够及时的恢复业务系统，减少数据中心之间切换带来的风险。

在不改变安徽定远供电公司信息化系统结构的基础上，本地增加一套DFT QuickBack灾备设备，在无需购买额外备份软件的情况下，QuickBack可以为整个信息化系统的所有系统、应用及数据提供全方位的灾难备份恢复，确保了客户应用环境、应用数据的可靠性，快照功能确保了信息化过程中的各种灾难的规避；DFT QuickBack可实现的RTO最大不超过15分钟；

二期在省电力信息数据中心增加一台DFT QuickBack设备，可实现定远QuickBack与省中心的数据同步，即使定远整个机房发生站点级的故障（如发生地震、火灾等），省中心可以在短时间内为定远县供电公司提供远程数据恢复，或者直接在灾备中心将所有应用、数据启动起来，由省中心提供持续的业务服务。

一期可实现功能如下：

在数据中心使用的存储系统本身能提供 RAID 保护机制，在一定程度上保证数据不丢失，但是这是在物理层面上，如果业务系统上出现逻辑错误造成数据丢失，则 RAID 保护机制就没有办法恢复这些数据。为此，我们在 QuickBack 配置了内部卷快照软件——Snapshot，使用该软件实现数据本地的数据保护，尤其是产生逻辑错误时，可以随时对本地盘上的数据进行快速恢复。对于每个虚拟的逻辑卷，提供高达 255 个快照版本。随时可以 Mount 出来进行数据读写。此外，还有 Copy 功能，将 Snapshot 拷贝出来，形成一个逻辑卷，进行读写。然后直接将 Snapshot 或者 Snapshot 拷贝出来的 LUN 通过 iSCSI HBA 卡或者 FC HBA 卡，派给业务服务器。这样通过 iSCSI/FC

HBA 卡直接读取 QuickBack 中备份的系统盘及数据盘，启动服务。

■ 关于业务回迁

如果存储/服务器发生灾难，停止服务，在修复好服务器/存储之后，我们可以立刻调用 DFT QuickBack 中的镜像磁盘通过 LAN 直接进行数据恢复，由于镜像磁盘与生产磁盘的数据是时时同步的，所以差异数据可以接近 0，保证恢复出来的服务器是接近 0 数据丢失的。Recovery CD 的 Microscan 功能可以保证恢复的有效性。因为 Recovery CD 自身具有一套操作系统(Linux 或 Windows)，所以不需要先在损坏的服务器中安装任何系统，直接可以启动 Recovery CD，调用系统备份磁盘进行恢复。

■ 关于磁盘的恢复

在数据盘发生故障无法使用的情况下，可以即刻将 DFT QuickBack 中的备份卷派给主机使用，首先恢复业务，这一操作，大大减小了 RTO 与 RPO，由于数据之前是时时备份的，故 DFT QuickBack 中备份卷的数据影像与主机是接近一致的，数据丢失接近于零，而业务恢复的时间也就是短短的手动换卷的时间。如果不幸的破损的数据同时同步到了 DFT QuickBack 中备份卷，使得备份卷也无法使用，这时候我们就可以启动快照，Mount 出快照到主机上，先恢复业务，在硬盘修复好之后，再恢复数据。

■ 关于系统和应用的恢复

在灾难来临之后，系统也可能受到致命的错误，从而无法启动，这时我们就可以使用 Recovery CD 来通过本地以太网恢复系统。Recovery CD 本身内部装有一套 Linux/Windows 操作系统和 iSCSI 驱动，通过光驱启动服务器后，可以读取 Recovery CD 中的系统，再为系统配置 IP 地址后就能够通过 iSCSI 协议调取 DFT QuickBack 中备份的系统盘影像及其快照。Recovery CD 使用了 MicroScan 技术，使得系统恢复的速度大大提高。快照的备份使得即使在备份影像都原盘系统的影像的情况下，调用若干天前的较好的备份影像来恢复。

实施效果

■ 24x7 持续保护应用服务器

透过应用服务器端的磁盘保护工具，定远供电公司所有系统和资料将得到及时监听，在几乎不影响应用程序运作的情况下记录磁盘区块新增异动，并依照管理者设定的保护原则，将差异的磁盘区块持续或定时排程的复制到 QuickBack 储存服务器，接着运用 Snapshot 快照技术，保存多达 255 个不同时间点的磁盘复本，无论应用服务器的系统当机、资料损毁或是硬体故障，都可以利用磁盘复本在最短的时间内复原至正常状态。

■ 立即检视、随时验证的备份还原

传统备份机制只能从备份纪录中确认工作执行完毕，却不代表资料已被正确保护，且回复失败的可能性很高。DFT QuickBack 在应用服务器端就能快速转换快照磁盘复本并检视内容，透过 iSCSI 及或 Fibre Channel 与应用服务器连结，1 分钟内就能直接载入档案系统进行资料比对和还原验证，完全不需长时间的资料回复，或占用服务器本身的磁盘空间，影响系统运作。

■ 100%保证资料库回复一致性

应用服务器的资料库在执行快照时为了确保回复资料一致性，必须暂时停止运作。DFT QuickBack 特别针对所有主流的资料库、应用程序，提供应用感知（Application-aware）的资料库代理程序（DB agent），当资料库接收到快照通知时，代理程序会自动执行记忆体资料写入磁盘，快照后重启资料库等动作，不需撰写 Script，就能 100% 确保快照备份时资料库的一致性，而且执行时资料库只会暂停一瞬间，完全不影响日常营运。

■ 5 分钟复原作业系统，关键应用不中断

恶意程序破坏、更新程序冲突、硬盘故障等状况都可能导致作业系统不稳或当机，传统备份机制需要冗长的程序才能回复正常运作。透过 DFT QuickBack 的 Remote Boot 远端启动机制，可以在意外发生后，指定最后或特定时间点的快照复本磁盘，在应用伺服器重新开机后接手本机硬盘，5 分钟内就能恢复系统正常运作，完全不需重新安装作业系统和回存资料，将停机造成的损失降至最低。

■ 10 分钟复原服务器/储存设备，节省硬件支出

应用服务器随时可能因某个硬件组件故障造成停机，传统的空机备援方式不仅耗时费力，更有兼容性的疑虑；建置高可用性丛集（HA/Cluster）不仅成本昂贵，管理更是一大负担。DFT QuickBack 结合虚拟服务器（如 VMware、Hyper-V）作为应用伺服器的复原平台，透过 P2V 复原机制（physical to virtual recovery），将快照磁盘复本直接指派给虚拟机器（virtual machine）使用，不需冗长的档案系统转换程序，不需考虑硬件与驱动程序兼容性，不用准备相同型号的备援服务器，10 分钟内就能在虚拟服务器上启动虚拟的备援服务器，快速恢复服务。相较于传统备援机制，可节省硬件的采购与维护成本。