

数据加密-数据中心的新措施

背景资料

安全一直都是数据中心经理最关心，也是最棘手的问题。

当今的数据中心安全措施都关注在网络和用户的访问控制领域，比如有网络的 VLAN 技术，防火墙技术，防止外部的未被授权的客户端访问数据中心网络，防止正在传输的数据被克隆、复制。在用户管理方面，数据中心有完善的权限管理，密码管理等措施，防止未被授权的用户访问数据中心系统。

但是这些措施是远远不够的，自 2005 年以来，我们经常听到这样的新闻，某某银行丢失了几千个用户的资料；某某信用卡公司客户资料丢失几万个；某某金融公司的数据资料被丢失。究其原因，这些全部都是由于介质丢失造成的。如果网络被攻破，丢失的只是少部分的数据，如果介质丢失，往往都是成千上万的数据资料丢失。

虽然数据中心介质的资料丢失都是小概率事件，但往往这些事件造成的损失都是致命的，就像地震、火灾对数据中心的容灾解决方案一样，数据加密可以保证数据的安全。

正是由于数据丢失事件经常发生对客户的隐私造成不可挽回的损失，造成了企业信誉的下降，许多国家和地区都已经开始着手立法解决这个问题，比如美国、欧盟、日本包括我国的香港都已经立法，要求数据中心解决数据加密的问题。

加密方法

根据数据保存的过程，加密可以在服务器上、SAN Fabric 网络中和存储上进行。

1、服务器加密

数据在服务器上加密，也就是应用系统在产生出数据后，在服务器端通过加密软件，在送出服务器前生成加密的数据。这种方法确保了端到端的隐私性，一般应用在备份系统中，较好地解决了磁带的加密问题。

然而这种方法也存在一些缺点。因为是在主机上加密数据，所以必须在服务器上进行重复数据删除操作。加密操作向服务器增加了负载，延长了备份窗口等待时间，这可能会影响到整体性能水平。而且，用户可能无法从随机数据中辨别出加密数据，这样就可能导致磁带驱动器压缩是完全没有用处的。因为大多数磁带驱动器的硬件压缩率至少在 2:1 左右，所有服务器层级的加密轻易就使你的磁带消耗翻一番。

2、存储端加密

存储端加密就是利用磁盘阵列或磁带驱动器的加密功能进行数据加密。比如现有的磁带驱动器都普遍植入了加密的硬件，可以解决服务器加密中对磁带的过量消耗的问题。现在的 EMC 的 Power Path 和 NetApp 的 Decru 加密方案可以和相关的磁盘解决方案相配合，将数据写入磁盘缓存之后进行加密，然后再写入物理磁盘中。

这些方法一定程度上解决了服务器加密的不足，但是它们由于和相应的寄生与服务器上的软件相配合，扩展性较差，应用的局限性非常明显，不能做到对操作系统和业务系统完全透明。

3、SAN Fabric 网络中加密

现在数据中心的业务系统都构建在 SAN Fabric 基础之上，通过 SAN Fabric 实现了异构平台、多业务系统的存储共享和数据集中，数据都是通过 SAN Fabric 进行传输的，这样为数据的集中加密提供了条件。

通过 SAN Fabric 网络加密就是在 Fabric 网络中接入可以进行数据加密的专用硬件设备，业务系统产生的数据通过 Fabric 时，自动重定向到加密的设备进行加密，然后再送到相应的存储设备端口保存。

这种方式的突出优点是对业务系统和存储系统透明。所有的存储系统和操作系统都可以

使用，而且不增加服务器的负载。它可以实现集中管理，对密钥的管理进行集中控制，扩展性较好。它可以和多种加密解决方案，也就是密钥管理方案相配合，比如 EMC 的 RSA Key Manager 等。

Fabric 加密方法

在 Brocade 产品家族中有一款数据加密的产品 Brocade BES (Brocade Encryption Switch), 它利用的交换机中的数据帧重定向(Frame Redirection)功能，将原本送到存储的数据送到 BES 上。

在 BES 内部有一个数据加密引擎 (Encryption Engine)，在配置完成后，数据加密的密钥会保存到数据加密的引擎中，密钥和加密引擎一起对数据进行加密。

为保证没有单点故障，在一个 Fabric 中通常需要两台 BES 进行冗余，互为备份，以便数据加密和解密的过程可以顺畅地进行。

加密过程的关键是密钥的管理。BES 并不进行密钥管理，密钥管理是通过专业的加密算法厂商，比如 EMC RSA、NetApp 或 HP SKM 等来完成的。由于 BES 是相对独立的解决方案，所以理论上可以兼容几乎所有的密钥管理方案。

通过 Fabric 方式，不仅可以对当前生成的数据进行加密，也可以对已经保存在磁盘上的为加密的数据进行加密；同时也解决了密钥的定期更换问题，可以将原来加密过的数据进行解密，并且使用新的密钥进行重新加密，为管理员进行数据管理提供了更多的灵活性。

总结

由于通过 SAN Fabric 进行加密有应用广泛、使用灵活、扩展性好等特点，未来必将称为加密方式的主流解决方案。