科研成果

堡垒机跨数据中心双活部署的原理与实现

车濡均 卢伟开

（南方电网数字电网研究院有限公司 510000）

摘要：信息化进程的不断推进，让企业信息系统变得更加复杂。在企业信息管理管理，由于部分工作人员存在着信息安全意识不充分、实际工作能力不突出的问题，给企业的信息安全保障工作的开展带来了极大的阻碍。针对这一问题，在企业的信息安全管理工作中，采用堡垒机作为企业信息安全防护的手段成为了很多企业在信息安全管理工作中的首选。对此，本次研究中，对针对企业信息安全管理工作中堡垒机的实际应用开展深入的研究，论述有关堡垒机跨数据中心部署的具体原理以及具体存在的困难、探讨堡垒机跨数据中心部署的实现方式，并详细说明双活堡垒机在日常工作中的运行维护管理，为企业在信息安全管理工作中更好的使用堡垒机设备提供可靠的参考依据。

关键词：堡垒机；跨数据中心部署；运行维护管理

作为一种对特定区域网络内的网络信息进行方位系统设备，堡垒机的防护主要是两个层面，一个是外部的用户访问入侵和恶意破坏，另一个是防护内部用户对网络信息资源的访问入侵和恶意破坏。堡垒机的应用为企业信息的安全方醍醐提供了切实的保障，但是在堡垒机实际应用的过程中，也遇到了一定的阻碍。这些具体问题给堡垒机在企业信息安全防护带来了很大的消极影响，如何有效解决堡垒机实际应用过程中出现的各种难题，真正实现企业信息安全管理中堡垒机设备的跨数据中心双活部署，是很多企业都十分关心的一项问题。正是基于这一点，本次研究中，将对相关的问题开展深入的研究。

1. 堡垒机在实际应用中跨数据中心部署的原理与主要难点

在企业信息安全管理中，堡垒机设备在实际应用的过程中，进行跨数据中心的双活部署，需要具体解决两项问题。其一是网络引流的问题，即堡垒机运行维户会话的负载分发，对此可以通过采用适合的负载配置将运行维护会话请求分配到适合的堡垒机节点上，由堡垒机节点完成连接服务器的后续操作。其二是在堡垒机设备的实际应用过程中，要保障两台堡垒机之间的数据能够保持一致，无论是在哪一个数据中心，企业中的系统中运行维护工作人员都能够使用同一个系统运行维护的界面，开展完全相同的工作。只有实现这两点，堡垒机的应用才能发挥出其应有的效果，才能为设备的用户提供跨数据中心运行维护的正确访问授权以及数据审计服务[1]。

在堡垒机的实际应用过程中，关于具体设备网络引流的实现，需要借助 LVS-SH 调度算法，LVS-SH 调度算法在应用中，能够对访问堡垒机的源地址进行 Hash，并通过 Hash 找出对应的堡垒机节点。这样，系统用户在使用同一个 IP 对堡垒机集群进行访问时，会话保活期内用户进行访问，访问的都是同一台节点，而之后所有的设备运行数据都会通过这一节点与用户端进行互联，不需要经过系统中的调度节点进行相关信息的转发，因而能够实现系统信息处理效率的进一步提升，更重要的是，这一算法不存在单点瓶颈，当调度节点出现故障之后，也不会对系统中其他部分的正常运行造成影响[2]。

而为了保证系统设备数据的一致性，堡垒机将配置数据保存在 Postgre SQL 数据库中，并采用 Postgre SQL Replication 技术来实现数据同步。在数据的集群内部，PG 主节点是重要的节点，系统中的各项命令都通过这一节点发布与执行。而其他的节点作为从节点，会根据主节点的数据变化情况，进行数据内容的备份。这种部署形式既能够保证系统数据高度的可用性，也能够最大程度上保证系统数据集群的实际性能。除此之外，堡垒机跨数据部署的过程中，即使是出现了一些极端的情况，例如系统主服务器宕机等，系统数据也能够通过实现的备份，各项工作得以正常的运行[3]。

2. 堡垒机在实际应用中跨数据中心部署的实现

在充分明确堡垒机跨数据部署中的基本原理以及主要的难点之后，对于企业信息安全管理中，进行堡垒机跨数据的双活部署时，在部署思路以及方法上就能够得到更充分的明确。企业信息安全管理中，在实现堡垒机跨数据双活数据中心构建的基础上，可以搭建一个虚拟堡垒机数据库服务器，部署 Postgre SQL 数据库。将两台堡垒机与两个数据中心进行对应的布置,在为两台堡垒机配置相应的 IP 地址后,可以借助 VRRP 协议得出具体的 IP 地址,相关的工作人员就可以通过这个虚拟 IP 连接相应的堡垒机，开展具体的运营维护工作。在两台设备部署全部完成之后,相关的企业可以针对此进行堡垒机切换测试以及堡垒机故障演练,具体方法为：工作人员将其中一台堡垒机的电源切断，这时再查看另外一台堡垒机对于这台堡垒机工作的实际接管情况,以此方式来检验堡垒机双活部署的具体数据处理效果[4]。通过具体的检验过程,验证得到了本次研究中想要得到的结果，双活堡垒机在部署过程中的数据切换完全正常。本次研究中的堡垒机跨数据双活部署具体如下图所示:

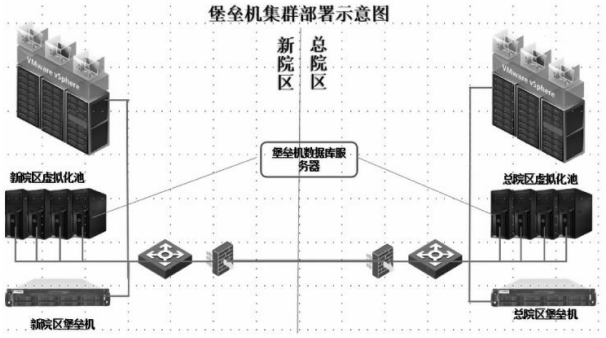

图 1.堡垒机跨数据双活部署结构

堡垒机设备在实际部署的过程中，会遇到很多的困难。在企业信息安全管理中，堡垒机应用中会存在内存使用率过高的问题，这一问题是目前堡垒机实际应用中最常遇到的问题。本次研究中针对这一问题的原因进行了深入的分析,对于这一问题产生的原因有了充分的认知。在双活部署模式下,相关的工作人员数量众多,所产生的数据体量十分巨大,而数据体量的庞大，会造成堡垒机数据处理模块的工作效率出现下降，系统在每分钟处理数据量要远远低于每分钟产生的数据量，导致堡垒机内部的数据缓存不断的增多，很多数据信息都被积压在系统当中。使得系统中的数据存储空间不断被占用，最终使系统内部的数据存储空间被消耗殆尽。在本次研究中，为解决这一问题，专门与系统研发与实施的工程人员进行反复研究,并结合相关的研究资料，对这一问题的根本成因有了进一步的认知。具体的成因是：在双活部署环境下，堡垒机数据库的分区表插件工作效率严重下降导致,通过研发工程师重写分区表插件解决了这个问题。部署过程中还遇到用户在多次使用堡垒机的过程中,造成很多业务无法正常使用或需要频繁登录。通过 LVS 会话持久化配置,使登录用户在一定时间段内连接的会话均分发至同一堡垒机,从而解决用户某些需要会话保持的功能,无法正常使用的问题[5]。

3. 堡垒机在实际应用中跨数据中心部署的实际运维管理

在企业信息安全管理工作中，堡垒机设备在其中发挥着极为重要的作用。而在堡垒机设备的跨数据中心部署中,通过这一过程，能够有效保证系统中在发生情况下,服务器仍然能够正常开展各项运营维护工作,使用习惯不改变,维护效率不降低,能够展现出极为突出的效果。但是，很多事情都有正反两个方面,要想保证系统的高度可用性以及安全性需要更强大的技术支撑,需要更加复杂的系统结构组成,这就对系统的运营维护工作提出了更高的要求。

3.1 建立起完善的数据运营维护管理制度

在堡垒机实际应用的过程中，在开展堡垒机运营维护管理的实际过程中，首先需要对工作制度进行进一步的完善，充分明确在企业的数据运营维护管理工作中的具体责任义务。首先在堡垒机用户账号的办理过程中,企业内部的工作人员以及企业内的驻场人员,都需要在办理账号之前，要事先签署系统使用的保密协议，并且要有使用服务器的实际需要，不符合以上两个条件的人员一律不得办理系统的账号，也不得借用他人账号使用该系统。在账号办理的过程中，必须要仰恩按照企业规定的流程进行审核批准,在审核通过之后进行账号的办理。另外，账号管理工作中要采取分级管理的制度,根据用户的系统使用需求,设置系统使用的不同级别权限，以便对系统的实际应用加以更合理的统筹管理[6]。

3.2 积极借助堡垒机执行技术管控工作

在堡垒机的实际应用中，需要通过堡垒机对系统用户进行身份认证与 SSO ,这就需要将服务器其他的使用通道与端口进行封闭，以避免其他用户对这项工作实际

开展的干扰。对此，系统要进一步加强防火墙防护性能的完善，真正有效执行 ACL 策略,对远程桌面方式访问 Windows 系统以及 SSH 协议或 telnet 协议访问 Centos 等 Linux 系统加以充分的远程控制。除此之外,还要对访问系统服务器的 IP 地址加以进一步的限制,只允许系统认定的 IP 地址，也就是堡垒机的 IP 地址对服务器进行访问,以便对系统在实际使用过程中，所有的运维及访问入口均通过堡垒机设备管控,真正实现全流程监管[7]。

3.3 进一步细化堡垒机自身的安全策略

在堡垒机设备的实际应用过程中，登录堡垒机的账户在进行登陆操作时，除了要输入由用户自行设置，并报系统监控人员核准认定的账户密码外，还要在系统登录界面输入由系统主机提供的随机验证码,这一登录方式，能够很大程度上降低系统遭受外部攻击的可能性。另外，系统在实际运行的过程中，还要开启防暴力破解功能,以此对外部的攻击做到更有效的预防，进一步避免系统中各项信息的外泄[8]。

3.4 定期开展设备的检查工作

堡垒机双活部署虽然能够有效保证系统运营维护极高的可用性,但是，如果系统的日常运维工作没有及时的跟进,也会导致系统的高度可用性出现流失，给系统的正常运营维护工作带来不利的影响,因此就需要相关工作人员对双活堡垒机进行定期的巡检。对此，相关的工作人员需要每天的特定时段，登陆主备堡垒机以及堡垒机数据的主服务器，对系统中数据库服务器的运行状态进行系统查看,第一时间发现其中存在的问题，并对这些问题采取针对性的处理措施,让两台堡垒机能够始终保持一个良好的运行状态,避免信息管理工作中各种损失的出现[9]。

结束语：在很多企业的信息安全管理工作中，堡垒机发挥着至关重要的作用。在本次研究中，就堡垒机跨数据双活部署的有关内容进行了深入的研究。通过本次研究内容，进一步明确了双活部署中的具体难点，以及双活部署的具体实现，在此基础上，本次研究中对堡垒机跨数据双活部署的具体运维管理内容也进行了一定的论述。希望通过本次研究，能够让企业对堡垒机的实际应用有更深入的了解，为企业信息安全建设提供一定的帮助。

参考文献：

[1]林志达,张华兵,曹小明,卢伟开.基于堡垒机技术的企业信息网络安全防护模型[J].电子设计工程,2022,30(18):179-183.

[2]王璐璐,王致君.电力监控仿真系统堡垒机培训探析[J].山东电力高等专科学校学报,2022,25(02):49-51+59.

[3]纪亚亮,郑阳.医院网络安全运维架构设计与应用[J].中国新通信,2022,24(01):29-31.

[4]韩百然.运维变更自动化安全审计在企业中的应用[J].网络空间安全,2021,12(Z6):32-35.

[5]朱成祥. 远程办公爆发下数据安全挑战凸显 企业如何握住“数据命脉”？ [N]. 每日经济新闻,2021-11-30(004).

[6]匡石磊.基于堡垒机的屏幕录像系统的运维操作审计研究与实践[J].网络安全技术与应用,2021(06):7-10.

[7]孙保峰,谭健,程铭.医院外联业务集成平台数据安全防护方案设计[J].网络安全技术与应用,2021(03):108-110.

[8]张喆.堡垒机及 VPN 技术在人行远程处置突发信息系统故障中的应用[J].黑龙江金融,2021(02):48-50.

[9]陶文伟,陈刚,郑伟文,石灿彬.一种可实时审计与阻断运维指令的变电站移动堡垒机的设计[J].网络安全技术与应用,2021(02):112-115.

张鸿（1978.5），男 汉族 山西临汾人 学历：博士 职称：副教授，从事航空发动机结构强度、振动及可靠研究