学校编码：10384

学号：X2009230282

厦门大学

硕士学位论文

数据中心网络安全服务管理系统的设计与实现

Design and Implementation of Network Security Service Management System in Data Center

杨兵照

指导教师：吴清锋

专业名称：工程硕士(软件工程)

答辩日期：2012年5月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文(包括纸质版和电子版)，允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于:

(　　)1.经厦门大学保密委员会审查核定的保密学位论文，于　年　月　日解密，解密后适用上述授权。

(　　)2.不保密，适用上述授权。

(请在以上相应括号内打“✓”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。)

声明人(签名):

年　　月　　日

摘 要

随着我国企业信息化的深入，企业对信息系统高度依赖。由于企业规模不断扩大，越来越多的大型跨区域企业、集团都建立了自己的业务网络和数据中心用于运行和支撑企业核心业务。与此同时，各种信息安全威胁层出不穷，对企业的网络安全防护提出了新的挑战。这在充分体现网络安全支撑重要性的同时，对网络安全管理的稳定和高效均带来了巨大的压力。很多企业都基于数据中心构建了企业网络安全防护体系，其中包括管理和技术两个层面，正如信息安全领域中经常提到的，信息安全“三分靠技术，七分靠管理”。仅仅靠在信息安全防护设备方面进行投入，并不能保障企业的信息安全，缺乏有效的信息安全管理才是目前企业信息安全体系运行保障的瓶颈。

本文尝试使用目前国际上流行的基于ITIL (Information Technology Infrastructure Library，IT基础架构库) 的IT 服务管理理念来解决数据中心面临的网络安全管理难题，并探讨国内企业如何成功实施应用ITIL。

本文首先介绍了 IT 服务管理的概念，对 IT 服务管理的研究背景、发展历程与现状进行阐述，然后结合国内某集团的实际，对该集团的数据中心网络安全服务管理系统进行了总体框架设计，并详细设计和实现网络安全监控、服务台管理等模块功能。在信息系统实现的过程中，论文针对如何提高故障诊断效率和现有用户管理策略的缺陷，提出了基于因果图剪枝的网络故障诊断机制和基于角色和流程的用户授权机制。这显著地提高了故障诊断效率，增强了系统的安全性。

通过本文的研究得出以下结论：基于 ITIL 的 IT 服务管理理论可以很好的指导企业的网络安全管理。基于该理论建立的网络安全服务管理系统，大大的提高了企业的网络安全服务管理水平，降低了管理人员培训成本和运维成本。通过配置管理和服务台管理确保了系统故障的有效跟踪和用户操作的合规和可审计。

关键词：IT 服务管理；IT基础架构库；网络安全

Abstract

With the development of the enterprise informationization, enterprises depend heavily on Information System in our country. With the continuous expansion of the scale of enterprises, more and more large multinational enterprises and groups have constructed their own business network and information-processing centre for operating and supporting their core business. At the same time, various threats of information security emerge endlessly and have become a new challenge to the security protection of Enterprise network; this completely shows the importance of supporting the network security and exerts great pressure on the stability & high efficiency of the secure management of network. A lot of enterprises construct the Enterprise Network Security Defense System based on the information centre, including the two ways of management and technology. As the saying goes in the information security field: three points depend on technology and seven points depend on management to obtain the information security. The huge investment in the information security construction does not mean realizing the information security. The absence of efficient security management is the bottleneck of supporting the enterprise information security system running at present.

The dissertation is attempting to resolve the conundrum of network security management confronting information centers with the internationally popular idea of IT Service Management based on the ITIL (Information Technology Infrastructure Library), and to discuss how the domestic enterprises should implement the ITIL successfully.

This dissertation firstly introduces the concept of ITSM (Information Technology System Management) and then elaborates the background of its research, the history of its development and its status quo. And finally taking one domestic enterprise group as a practical example, the dissertation presents the integrate

frame work design and in detail designs the network security service management system of the enterprise group information and data centre, and realizes the network security monitoring, desk management , block model function etc. Aiming at how to enhance fault diagnosis efficiency and the fault of current user management policy during the information system realization, the dissertation proposes the network fault diagnosis mechanism based on Causality Diagram Pruned and User Authorization Mechanism based on Access Control and Process, which observably enhances the fault diagnosis efficiency and the system security.

The following conclusion can be made from the research: The IT Service Management Theory based on ITIL can guide the enterprise network security management very well; A Group Network Security Service Management System constructed based on this theory greatly enhances the network security service management level and reduces the management personnel training cost and running and maintaining expense; It insures the effectively tracing the system breakdown, user operation compliance and audit.

Keywords: ITSM; ITIL; Network Security

参考资料

[1]左天祖,刘伟.中国 IT 服务管理指南[M].北京:北京大学出版社,2005.
[2]孙强,左天祖,刘伟.IT 服务管理、概念、理解与实施〔M〕.北京:机械 I 业出版社,2003.
[3] IT 服务管理论坛官方网站 http://WWW.ITSMF.com.
[4] OGC.The Official Introduction to the ITILService Lifecycle.
[5]翰纬 IT 管理研究咨询中心 http://www.sinoseviceone.com/.
[6] Jan van Bon 著,章斌译.IT 服务管理—基于 ITIL 的全球最佳实践[M].北京:清华大学出版社,2006:128-139.
[7]中国 IT 治理研究中心 http://www.itgov.org.cn.
[8]中国惠普有限公司.惠普之道—— IT 服务管理篇.北京:清华大学出版社.2006.
[9] IT 服务管理门户站 http://www.itsmportal.com.
[10]徐宏涛.面向知识管理的运维服务管理系统[D].天津:天津大学,2009 .
[11] Steinder M,Sethi A S. Probabilistic Fault Diagnosis in Communication Systems through Incremental Hypothesis Updating [J].Computer Networks. 2004: 45(4):537-562.
[12] 刘培奇, 李增智,赵银亮. Study on Natural Language Interface of Network Fault Diagnosis Expert System [J]. Academic Journal of Xi ’ an Jiaotong University. 2006(2).
[13] Bouloutas A T, Calo S, Finkel A. Alarm Correlation and Fault Identification in Communication Networks[J] IEEE Transactions on Communications, 1994, 42(234): 523-533.
[14]吴光成,时云峰.基于 RBAC 的权限管理系统的实现[J].电子测试,2008,05.
[15] 沈磊,张媛,蒋平.基于 RBAC 的权限管理在 Web 中的设计与实现[J].电子测试,20082009,03.
[16] Pierangela Samarati and Sabrina De Capitani di Vimercati. Access Control：Policy,models and Mechanisms.
[17] David F.Ferraiolo,R.S.Sandhu,Serban avrila,et al.Proposed NIST Standard forRole-Based Access Control.ACM Transactions on Information and SystemsSecurity(TISSEC),Volume 4,Number 3,August 2001.
[18]陈宏峰,《翰纬 IT 服务台白皮书》,翰纬 TI 管理文库,2005.8.
[19]BMC 公司,BMC Remedy Action Request System 7.5.00 概念指南.
[20] BMC 公司,http://www.bmc.com.