网管天下

系统与服务监控技术实践

SYSTEMS AND SERVERS MONITORING TECHNOLORY IN PRACTICE

主　编　王淑江
副主编　刘晓辉　张喜平　岳　明

- Windows Server 2003/2008系统性能监控
- Active Directory和Exchange Server 2003以及SQL Server服务状态监控
- 使用MOM 2005对Windows服务器的监控
- Windows系统管理命令行和Windows系统故障的诊断与恢复

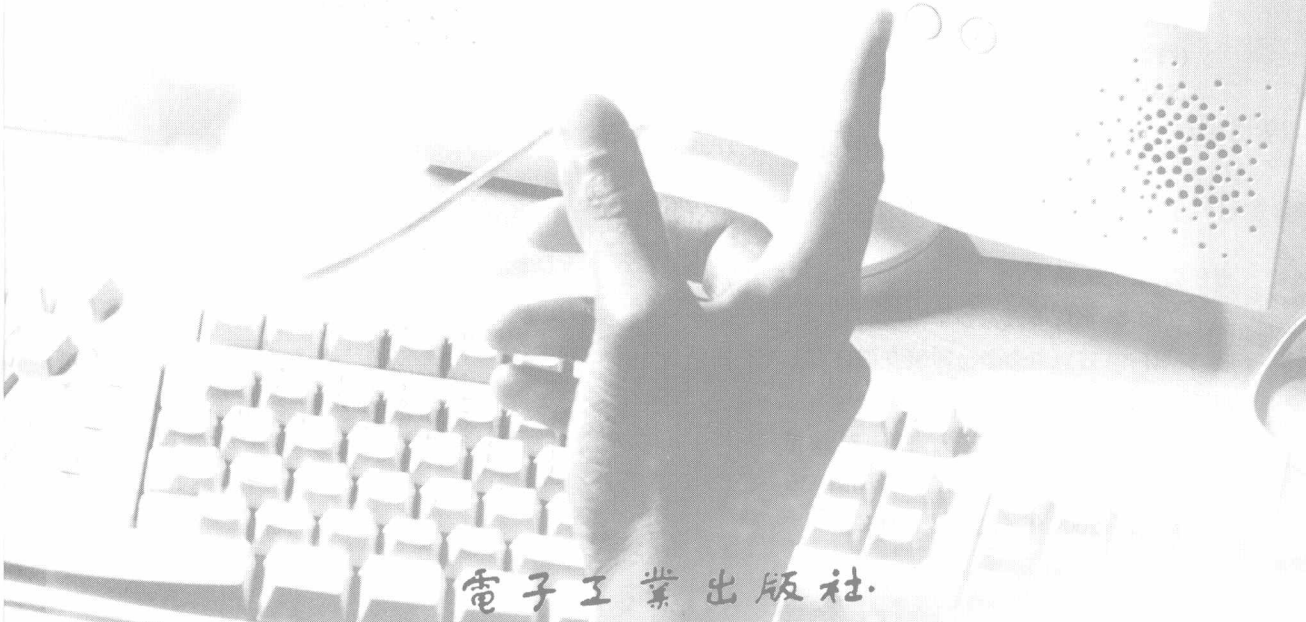
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网管天下

系统与服务监控技术实践

主　编　王淑江

副主编　刘晓辉　张喜平　岳　明



電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书围绕 Windows Server 2003/2008 系统性能和网络服务状态监控为主题，全面介绍了如何借助操作系统内置系统监控和日志管理工具，以及专业管理软件 MCOM 2007 的 Spotlight 系列产品，实现对 Windows Server 2003/2008 系统性能，以及 Active Directory、Exchange Server 2003 和 SQL Server 服务状态的监控。同时，还简单介绍了使用 MOM 2005 对 Windows 服务器的监控方法，以及 Windows 系统管理命令行和 Windows 系统故障的诊断与恢复。最后，介绍了 SQL 代码性能优化和 SQL 日志监控和管理数据库。本书无疑是监控和优化 Windows 服务器操作系统的得力帮手，是系统管理员和网络管理员及时了解服务器运行状态的有力工具。

本书内容具有很强的实践性和指导性，要求读者具有一定的网络基础知识、一定的系统管理水平和一定的计算机操作能力，既可以作为企事业、各单位信息部门参考用书，也可以作为高级网络培训班的参考教材，或者作为计算机网络专业毕业生在即将走向工作岗位以前的实习参考书。

图书在版编目(CIP)数据

系统与服务监控技术实践 / 王淑江主编.—北京：电子工业出版社，2009.6
(网管天下)
ISBN 978-7-121-08954-1

Ⅰ. 系… Ⅱ.王… Ⅲ.计算机网络－管理 Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字（2009）第 089196 号

责任编辑： 郭鹏飞
印　　刷： 北京市天竺颖华印刷厂
装　　订： 三河市鑫金马印装有限公司
出版发行： 电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本： 787×1092　1/16　印张：36　字数：922 千字
印　　次： 2009 年 6 月第 1 次印刷
定　　价： 65.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

在部署 Windows 系统的网络中，任何一个服务器操作系统使用者都能够遇到同样一个问题，就是随着数据量的增加，累计运行时间越来越多时，系统速度越来越慢，对客户端用户的响应时间越来越迟钝，用户抱怨声四起。甚至 Windows 服务器还可能会突然停止服务，从而使整个网络的运行陷于停顿。面对类似状况时，由于系统管理员和网络管理员往往缺乏必要的分析和诊断工具，因此，很难迅速判断到底是服务器、存储、网络、数据库、软件（操作系统和应用系统）中哪个部分出现了问题，是病毒感染而需要设置访问列表，还是由于硬件配置较低而需要进行硬件设备升级。

本书以 Windows Server 2008 服务器操作系统为基础，兼顾 Windows Server 2003，通过对操作系统的监控，使读者知道服务器需要监控的内容，通过对 CPU、内存、磁盘等性能计数器的理解，通晓制作系统稳定性基线的方法，这个基线可以作为衡量系统是否稳定的标准。当系统出现问题后，如何使用内置工具分析和调整系统性能，而不要听信别人善意的“谎言”——出现性能问题就要升级硬件设施。

其他部分以 Microsoft System Center Operations Manager 2007（SCOM）和 Quest 的 Spolight 系列产品为基础，监控在网络环境中应用广泛的 Active Directory、SQL Server 数据库和 Exchange Server，由于 Windows 产品存在许多共性，本书介绍的方法读者可以部署其他版本的 Windows Server 服务器操作系统中。其中，重点介绍了对 SQL Server 数据库的监控和调整，以及如何借助日志监控了解数据库中数据的变化，借助 SQL 代码性能优化大幅度提高 SQL Server 的性能。需要注意的是，由于 SQL Server 是运行在 Windows Server 操作系统之上的，因此，在监控 SQL Server 数据库的同时，一定要监控其操作系统平台。

SCOM 中引入了对分布式操作系统的监控方法，对 Active Directory 的监控就是一个很好的例子。本书通过对一个分布式应用程序实例的部署，让读者掌握自定义部署监控分布式应用程序的方法，了解 SCOM 监控应用程序的过程，以及监控部件之间的逻辑关系，将操作系统监控、端口监控、数据库监控、数据源监控集成到一个监控控制台的方法，读者可以根据自己网络状况，定制监控平台。

本书共分 19 章，内容涵盖 Windows Server 操作系统监控和常用应用系统监控，内容概要介绍如下。

第 1 章系统监控概述，概要介绍为什么要监控系统，以及介绍根据监控的结果如何判断系统是否存在性能问题。第 2 章监控系统资源，介绍 Windows Server 2008 中任务管理器和资源管理器的使用，资源管理器使用评估模式对当前系统进行综合评估，可以直观地了解当前系统状态。第 3 章可靠性和性能监视器，介绍 Windows Server 2003/2008 中的性能监视器、可靠性监视器和数据收集器的使用，使用上述三种监视器，可以创建性能基线，作为评估系统的基础依据。第 4 章系统事件日志管理，介绍在 Windows Server 2003/2008 中事件、事件关联任务，以及如何基于操作系统收集其他系统事件。第 5 章系统资源管理器，介绍如何为

应用程序或者服务分配系统资源，将有限的资源充分使用。第 6 章监控安全审核策略，审核与事件相对应，如果不开启审核策略在系统中将不能产生日志，本章介绍如何启用审核策略。第 7 章监控和调整 Windows Server，介绍使用 Spotlight on Windows 监控 Windows Server 2008 操作系统，和最基本的性能调整。第 8 章部署 SCOM，介绍如何在网络环境中部署 Microsoft System Center Operations Manager 2007，该软件是微软公司专业的监控系统性能软件，可以和微软知识库结合，为管理员提供对应的故障解决方案。第 9 章监控 Active Directory，引导读者通过 SCOM 和 Spotlight on Active Directory 软件监控 Active Directory。第 10 章监控 Exchange Server 2003，介绍网络中如何部署 SCOM 监控 Exchange Server。第 11 章 SQL Server 数据库监控，引导读者通过 SCOM 和 Spotlight on SQL Server 软件监控 SQL Server 数据库。第 12 章事件统一监控，介绍使用 SCOM 的收集审核服务收集服务器日志，统一管理。第 13 章 SCOM 自定义监控任务，介绍使用 SCOM 部署端口监控、数据源监控、分布式应用程序监控、警报通知等常见任务，引导读者学会根据网络状况自定义部署监控任务。第 14 章 Windows 服务器管理，介绍如何借助 MOM 2005 实现对 Windows Server 2003 网络服务的监控与管理。第 15 章系统与服务状态监视工具，重点介绍了几款常用、实用、管用的第三方 Windows 系统和网络服务状态监控工具。第 16 章系统和服务管理命令行，详细介绍了有关 Windows 系统和服务命令行的格式、参数和示例。第 17 章 SQL Server 代码优化，主要介绍通过 SQL Server 2005 数据库引擎优化顾问和 Toad 工具优化 SQL 代码，提高代码的执行效率，从而提高数据库系统的性能。第 18 章 SQL Server 日志监控与管理，介绍使用 Log Explorer 工具监控和管理 SQL Server 数据库日志。第 19 章 Windows 系统故障修复，详细介绍了导致系统故障的原因，以及系统故障的的诊断与修复。

本书主编为王淑江，副主编为刘晓辉、张喜平、岳明。在这个日新月异的信息化时代，网络新技术、新应用不断涌现。为此，我们也将密切关注网络技术的发展和读者的需要，将更新、更实用的技术介绍给读者，将更好的产品和应用推荐给大家。有关本书的意见和建议，可以发邮件到 ytdaily@gmail.com 联系作者。

笔者

2009 年 5 月

目录

CONTENTS

第 1 章　系统监控概述

计算机网络中的监控是一个广义的概念。本书中的监控，指的是 Windows Server 系统性能监控和常用网络服务监控，着重介绍如何使用监控和调整系统性能和应用程序性能。本章简介系统性能监控的目标和监控的内容。

1.1　监 控 概 述

网络中的服务器系统部署完成后，随着时间的推移，系统中的数据量和用户数量不断增加，系统压力越来越重，系统运行速度越来越慢，客户端用户等待的时间相应越来越长，用户的不满程度越来越高，甚至影响网络的正常运行。客户端用户从等待时间长，逐渐演变成长时间的抱怨，甚至到集体罢工的程度。如何监控和解决系统性能问题，成为管理员急需解决的棘手难题。

1.1.1　系统状态

系统越来越慢，是每个网络管理员都会遇到的问题。系统为什么慢，造成慢的原因是什么，如何解决慢的问题，如何调整服务器性能，都是管理员关心的问题。

应用系统一般包括服务器、存储、网络、数据库、软件（操作系统和应用系统），在系统建设时还需要集成商参与，当出现系统慢的问题时，将不同的供应商召集到一起，共同研究慢的问题，得出的结论基本是“设备正常，没有问题”。

由于网络中使用不同的产品，针对不同的产品均有各自的性能监控工具，通过性能监控工具的诊断分析报告，才能判断产生系统瓶颈的真正原因所在。性能监控工具是彻底解决性问题必备的利器。既然性能的瓶颈来自服务器、存储、网络、数据库、软件等不同的产品，所以监控软件必须综合不同资源的性能进行监控。系统缓慢是因为数据量增加后，长时间累积出来的现象，性能监控手段还要包含长期性能增长的趋势预测分析。

最常见的提高性能的方法就是升级。将现有产品升级到更高性能指标的产品来提升性能、降低运行压力，不同的厂商将会提供不同的产品升级方法。产品升级后，管理员可能会发现系统性能并没有根本改变，无论是采购更高性能指标的设备，还是从软件方面进行系统优化改造，多方面付出努力和投入，但收效仍然不明显。

1.1.2　监控目标

在进行性能调整前，首先要知道要调整什么，系统的瓶颈到底在什么地方，只有监控工具才能完成此任务。

1. 监控目标

监控目标主要分为四部分：硬件资源（处理器、内存、存储和网络），操作系统，数据库和应用软件。每一部分都必须同时监控，监控内容包含吞吐量、反应时间和使用率，任何一部分都有可能是造成瓶颈的原因。

2. 日志采集

日志是监控的重要内容，管理员要收集不同目标的性能日志，日志可以用来描述系统工作状态和即将出现的问题。经过历史数据的统计，可以判断哪些是正常运行的平均值和正常值，也可以判断那些是超过正常值的合理范围，甚至统计出目前资源设备可以承载的最大极限值，任何的性能隐患都可以提出告警。通过历史数据的对比分析，看到随着时间变化的性能发展趋势，这个发展趋势是递增还是持平的？有没有时间上的规律，如每日、每周、每月、或是每年，依据这些趋势和规律分析，判断和预测未来需求。

1.1.3 性能监控工具

要分析造成系统慢的真正瓶颈，首先需要性能监控工具。经由这些工具来诊断分析由应用软件、数据库、操作系统、处理器性能、内存性能、I/O 存储和网络性能等方面可能带来的瓶颈。

管理员使用性能监控工具时，既可以使用专业的性能监控工具，例如 Quest 公司的 Spotlight 系列产品，也可以使用 Microsoft 公司的 Microsoft System Center Operations Manager 2007（SCOM）产品，更方便的是使用 Windows Server 本身集成的性能监视器，当然也可以使用更加专业的监控系统。本书将分别介绍 Spotlight、SCOM 以及性能监视器在网络管理中的应用。

1.2 系统性能监控

本书中的系统性能监控，监控目标计算机使用的操作系统为 Windows Server 2008，监控中的方法同样适用于其他版本的 Windows 服务器操作系统。在操作系统监控中，主要监控三方面的性能，分别为：CPU、内存和磁盘，书中其他部分将详细阐述监控实现的方法。

1.2.1 监控 CPU 性能

CPU 全称 Centre Process Unit（中央处理器），CPU 是系统性能的最重要指标，也是计算机的基础组件，主要完成数据运算功能，可以将 CPU 形象比喻为“大脑”。CPU 的性能从根本上决定着服务器的性能。如果 CPU 出现瓶颈将影响计算机的性能。在 Windows Server 操作系统中，提供了针对 CPU 的性能计数器，通过计数器即可了解 CPU 的利用率。

1. CPU 性能计数器

Windows Server2008 操作系统中提供的“Processor”对象，详细提供 CPU 的使用时间、

空闲时间、传输性能等参数。

“Processor”性能计数器

“Processor”性能计数器是能够监控处理器活动方面的计数器。处理器是计算机进行算数和逻辑计算、在附属件起始操作及运行处理线程的部分。一台计算机可以有多台处理器。处理器对象将每台处理器作为对象的实例，如图 1-1 所示。

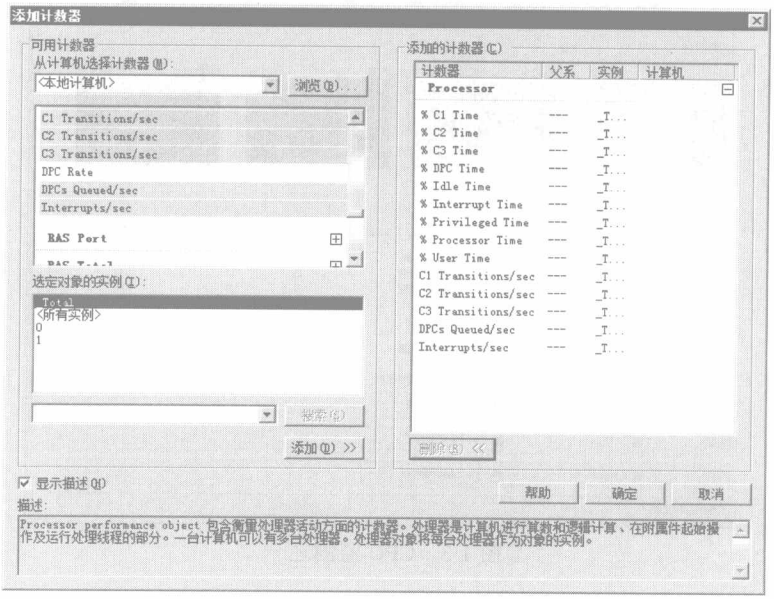


图 1-1　CPU 性能计数器之一

正在监控的“Processor”性能指标如图 1-2 所示。从该指标中，可以分析出当前计算机 CPU 的使用状态。

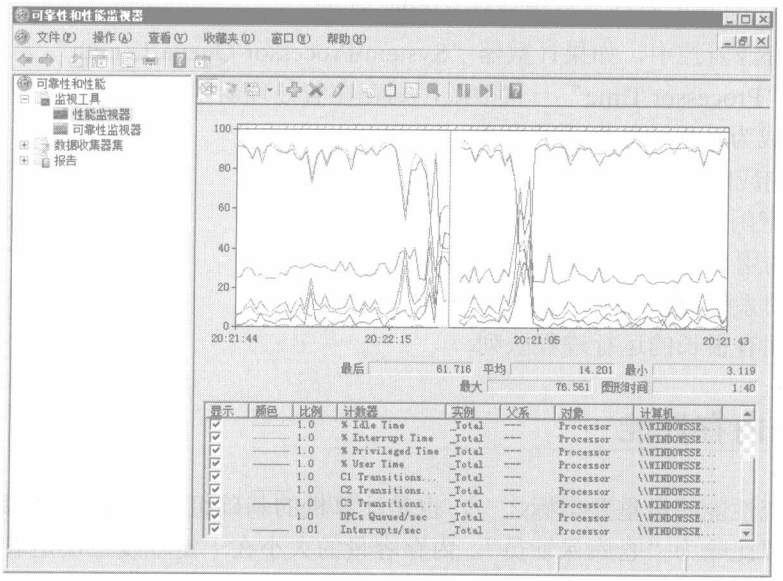


图 1-2　CPU 性能计数器之二

2. 资源监视器-CPU 监测

资源监视器提供 CPU 监测功能，通过图表和文本信息可以详细了解正在使用的 CPU 基本状态，能够显示正在运行的应用程序 CPU 的利用率、线程数以及 CPU 的平均利用率，如图 1-3 所示。

图 1-3 CPU 监测之一

3. CPU 性能计数器分析

CPU 利用率值如果持续超过 95%，表明 CPU 存在瓶颈，可以考虑增加一个处理器或更换一个更快的处理器。如果服务器专用于 SQL Server 数据库，可接受的最大上限是 80%~85%，通常情况下 CPU 的利用率合理使用范围在 60%~70%。

Windows 资源监控中，如果计数器“System\Processor Queue Length”大于 2，而处理器利用率计数器“Processor Time”一直很低，则存在着处理器阻塞情况。

CPU 资源成为系统性能瓶颈的预兆：

- 系统响应时间很慢
- CPU 空闲时间为零
- 过高的用户占用 CPU 时间
- 过高的系统占用 CPU 时间
- 长时间有很长的运行进程队列

1.2.2 监控内存性能

内存是系统性能的最重要指标之一，也是计算机的基础组件，主要完成数据转储功能，可以将内存形象比喻为“仓库保管员”。内存容量的大小在一定程度上决定着服务器的性能。如果内存分配完毕将使用虚拟内存调用文件，内存瓶颈将影响计算机的性能。在 Windows Server 操作系统中，提供了针对内存的性能计数器，通过计数器即可了解内存的使用状态。