

# Contents

- 1 Introduction . . . . . 1**
  - 1.1 Introduction . . . . . 1
  - 1.2 Computer System Life Cycle . . . . . 2
  - 1.3 Shared Hosting Data Center (SHDC) . . . . . 5
  - 1.4 Large Enterprise . . . . . 7
  - 1.5 Network Service Provider . . . . . 9
  - 1.6 History of Systems Management . . . . . 12
  - 1.7 Summary . . . . . 14
  - 1.8 Review Questions . . . . . 14
  - References . . . . . 15
  
- 2 Planning and Implementation . . . . . 17**
  - 2.1 Requirements . . . . . 18
    - 2.1.1 Performance Requirements . . . . . 18
    - 2.1.2 Resiliency and Availability Requirements . . . . . 19
    - 2.1.3 Power and Thermal Requirements . . . . . 20
    - 2.1.4 Security Requirements . . . . . 21
    - 2.1.5 Manageability Requirements . . . . . 22
    - 2.1.6 Backward Compatibility . . . . . 22
    - 2.1.7 Other Requirements . . . . . 23
  - 2.2 Evaluating Computer Systems . . . . . 24
    - 2.2.1 Evaluating Computer Systems Performance . . . . . 26
    - 2.2.2 Evaluating Resiliency and Availability . . . . . 37
    - 2.2.3 Power and Thermal Analysis . . . . . 43
    - 2.2.4 Computer System Security Analysis . . . . . 47
  - 2.3 Planning to Satisfy Requirements . . . . . 49
    - 2.3.1 Systems Planning Process . . . . . 50
  - 2.4 Implementation . . . . . 59
  - 2.5 Summary . . . . . 59
  - 2.6 Review Questions . . . . . 60
  - References . . . . . 61

<b>3</b>	<b>Operations Management</b>	63
3.1	Operations Center	63
3.2	Management Data	66
3.3	Manager Agent Protocols	69
3.3.1	Remote Consoles	69
3.3.2	Simple Network Management Protocol (SNMP)	70
3.3.3	Common Object Repository Broker Architecture (CORBA)	71
3.3.4	Web-Based Enterprise Management (WBEM)	72
3.3.5	Web Services	72
3.3.6	NetConf	73
3.3.7	Comparison of the Different Management Protocols	74
3.4	Management Information Structure	74
3.4.1	Management Information Base	75
3.4.2	Common Information Model	77
3.4.3	Issues with Standard Representation	78
3.5	Device Agent Structure	80
3.6	Management Application Structure	81
3.7	Operations Center Function	83
3.8	Summary	86
3.9	Review Questions	86
	References	87
<b>4</b>	<b>Discovery</b>	89
4.1	Discovery Approaches	90
4.1.1	Manual Inventory	90
4.1.2	Dictionary/Directory Queries	91
4.1.3	Self-Advertisement	91
4.1.4	Passive Observation	92
4.1.5	Agent-Based Discovery	92
4.1.6	Active Probing	93
4.2	Discovery of Specific Types of IT Infrastructure	94
4.2.1	Discovering Servers	94
4.2.2	Discovering Client Machines	97
4.2.3	Discovering Applications on Servers and Clients	98
4.2.4	Discovering Layer-3 Network Devices	100
4.2.5	Discovering Layer-2 Network Devices	101
4.3	Storing Discovered Information	102
4.3.1	Representing Hierarchical Relationships	103
4.3.2	Representing General Graphs	106
4.3.3	Representing Generic Relationships	107
4.3.4	Other Types of Databases	108
4.4	Summary	109
4.5	Review Questions	109
	References	110

<b>5</b>	<b>Monitoring</b>	111
5.1	Monitored Information	111
5.2	Generic Model for Monitoring	112
5.3	Data Collection	114
5.3.1	Passive Monitoring	114
5.3.2	Active Monitoring	119
5.4	Pre-DB Data Processing	123
5.4.1	Data Reduction	123
5.4.2	Data Cleansing	124
5.4.3	Data Format Conversion	127
5.5	Management Database	129
5.5.1	Partitioned Databases	130
5.5.2	Rolling Databases	131
5.5.3	Load-Balanced Databases	131
5.5.4	Hierarchical Database Federation	132
5.5.5	Round-Robin Databases	134
5.6	Summary	134
5.7	Review Questions	134
<b>6</b>	<b>Fault Management</b>	137
6.1	Fault Management Architecture	137
6.1.1	Common Types of Symptoms	139
6.1.2	Common Types of Root Causes	141
6.2	Fault Diagnosis Algorithms	143
6.2.1	Topology Analysis Methods	144
6.2.2	Rule-Based Methods	147
6.2.3	Decision Trees	148
6.2.4	Dependency Graphs	149
6.2.5	Code Book	151
6.2.6	Knowledge Bases	152
6.2.7	Case-Based Reasoning	153
6.2.8	Other Techniques	154
6.3	Self-Healing Systems	155
6.3.1	Autonomic Computing Architecture and Variations	155
6.3.2	An Example of a Self Healing System	157
6.4	Avoiding Failures	158
6.4.1	Redundancy	158
6.4.2	Independent Monitor	159
6.4.3	Collaborative Monitoring	160
6.4.4	Aged Restarts	160
6.5	Summary	161
6.6	Review Questions	161
	References	162

- 7 Configuration Management . . . . . 165**
  - 7.1 Configuration Management Overview . . . . . 165
  - 7.2 Configuration Setting . . . . . 167
    - 7.2.1 Reusing Configuration Settings . . . . . 168
    - 7.2.2 Script-Based Configuration Management . . . . . 170
    - 7.2.3 Model-Based Configuration Management . . . . . 171
    - 7.2.4 Configuration Workflows . . . . . 173
    - 7.2.5 Simplifying Configuration Through Higher Abstractions . . . . . 174
    - 7.2.6 Policy-Based Configuration Management . . . . . 175
  - 7.3 Configuration Discovery and Change Control . . . . . 176
    - 7.3.1 Structure of the CMDB . . . . . 177
    - 7.3.2 Federated CMDB . . . . . 178
    - 7.3.3 Dependency Discovery . . . . . 178
  - 7.4 Configuration Management Applications . . . . . 181
    - 7.4.1 Configuration Validation . . . . . 181
    - 7.4.2 What-If Analysis . . . . . 182
    - 7.4.3 Configuration Cloning . . . . . 183
  - 7.5 Patch Management . . . . . 183
    - 7.5.1 Patch Identification . . . . . 183
    - 7.5.2 Patch Assessment . . . . . 184
    - 7.5.3 Patch Testing . . . . . 185
    - 7.5.4 Patch Installation . . . . . 186
  - 7.6 Summary . . . . . 187
  - 7.7 Review Questions . . . . . 188
  - References . . . . . 188
  
- 8 Performance and Accounting Management . . . . . 191**
  - 8.1 Need for Operation Time Performance Management . . . . . 192
  - 8.2 Approaches for Performance Management . . . . . 192
  - 8.3 Performance Monitoring and Reporting . . . . . 194
    - 8.3.1 Performance Metrics . . . . . 195
    - 8.3.2 Addressing Scalability Issues . . . . . 196
    - 8.3.3 Error Handling and Data Cleansing . . . . . 198
    - 8.3.4 Metric Composition . . . . . 200
    - 8.3.5 Performance Monitoring Approaches . . . . . 202
    - 8.3.6 Performance Reporting and Visualization . . . . . 205
  - 8.4 Performance Troubleshooting . . . . . 209
    - 8.4.1 Detecting Performance Problems . . . . . 209
    - 8.4.2 Correcting Performance Problems . . . . . 211
  - 8.5 Capacity Planning . . . . . 213
    - 8.5.1 Simple Estimation . . . . . 214
    - 8.5.2 ARIMA Models . . . . . 215
    - 8.5.3 Seasonal Decomposition . . . . . 216
  - 8.6 Accounting Management . . . . . 217

8.7	Summary . . . . .	219
8.8	Review Questions . . . . .	219
	References . . . . .	220
<b>9</b>	<b>Security Management . . . . .</b>	<b>221</b>
9.1	General Techniques . . . . .	222
9.1.1	Cryptography and Key Management . . . . .	222
9.1.2	Authentication . . . . .	226
9.1.3	Confidentiality/Access Control . . . . .	228
9.1.4	Integrity . . . . .	229
9.1.5	Non-Repudiation . . . . .	231
9.1.6	Availability . . . . .	231
9.2	Security Management for Personal Computers . . . . .	232
9.2.1	Data Protection . . . . .	233
9.2.2	Malware Protection . . . . .	234
9.2.3	Patch Management . . . . .	235
9.2.4	Data Backup and Recovery . . . . .	236
9.3	Security Management for Computer Servers . . . . .	237
9.3.1	Password Management . . . . .	238
9.3.2	Single Sign-On . . . . .	239
9.3.3	Secure Access Protocols . . . . .	240
9.4	Security Management for Computer Networks . . . . .	241
9.4.1	Firewalls . . . . .	242
9.4.2	Intrusion Detection/Prevention Systems . . . . .	243
9.4.3	Honeypots . . . . .	245
9.5	Operational Issues . . . . .	245
9.5.1	Physical Security . . . . .	246
9.5.2	Security Policies . . . . .	246
9.5.3	Auditing . . . . .	248
9.6	Summary . . . . .	248
9.7	Review Questions . . . . .	249
	References . . . . .	250
<b>10</b>	<b>Advanced Topics . . . . .</b>	<b>251</b>
10.1	Process Management . . . . .	251
10.2	Helpdesk Systems . . . . .	252
10.3	Web, Web 2.0, and Management . . . . .	254
10.4	Summary . . . . .	255
10.5	Review Questions . . . . .	255
	References . . . . .	255
	<b>Index . . . . .</b>	<b>257</b>



<http://www.springer.com/978-0-387-89008-1>

Principles of Computer Systems and Network  
Management

Verma, D.C.

2009, XV, 260 p., Hardcover

ISBN: 978-0-387-89008-1