

Course Guide

Guardium Data Protection: Fundamentals



Table of Contents

Introduction	1
Unit 1: Guardium overview	2
Guardium data security.....	4
Introduction to Guardium Data Protection	10
Summary.....	15
Unit 2: Guardium architecture	16
Guardium data sources.....	18
Capturing data traffic	28
Aggregation and central managers	37
Summary.....	44
Unit 3: Guardium user interfaces	45
Navigating the user interface.....	47
Command line interface introduction	61
Summary.....	84
Unit 4: Access Management	85
Managing users	87
Managing roles	96
Summary.....	104
Unit 5: Guardium Groups	105
Building groups.....	107
Populating groups	112
Hierarchical groups	121
Summary.....	125
Unit 6: System Management	126
System view and configuration.....	128
GIM and S-TAP	133
Guardium deployment health monitoring tools	141
Summary.....	146
Unit 7: Data Management	147
Aggregating data	149
Archiving data	152
Backing up and restoring data.....	158
Summary.....	161

Unit 8: Guardium discovery & vulnerability assessment	162
Data discovery and classification	164
Vulnerability assessment.....	174
Summary.....	181
Unit 9: Audit process automation.....	182
Creating an audit process	184
Managing audit results.....	196
Summary.....	202
Unit 10: Policy design.....	203
Introduction to policies.....	205
Create and install policies.....	214
Guardium policy rule order and logic.....	226
Policy actions.....	232
Summary.....	237
Unit 11: Policy configuration.....	238
Access rules.....	240
Extrusion rules.....	244
Exception rules.....	250
Selective audit trail policy.....	255
Session level policy	259
Summary.....	262
Unit 12: Guardium reports.....	263
Domains and entities	265
Building a query report.....	276
Customizing query-reports	287
Summary.....	296
Unit 13: Guardium alerts	297
Introduction to Guardium alerts.....	299
Real-time alerts.....	305
Correlation alerts.....	313
Configuring alerts	316
Alerter	327
Summary.....	332
Summary	333

Introduction

Data security and privacy challenges are never-ending. IBM Guardium® Data Protection (Guardium) provides a broad range of data security and protection capabilities that can protect sensitive and regulated data across environments and platforms. It discovers and classifies sensitive data from across an enterprise, providing real-time data activity monitoring and advanced user behavior analytics to help discover unusual data activity.

This course prepares the student to administer Guardium appliances, discover unusual data activity, locate vulnerable data, automate compliance processes, and monitor and protect sensitive data. To practice using Guardium, students complete hands-on lab exercises.

In this course, you learn to:

- Identify the primary functions of Guardium Data Protection
- Describe key Guardium architecture components
- Navigate the Guardium user interface and use the command line interface
- Manage user access to Guardium
- Build and populate Guardium groups
- Use system settings and management tools to manage, configure, and monitor Guardium resources
- Archive, backup, and restore Guardium data
- Discover sensitive data and perform vulnerability assessments
- Use Guardium audit process tools to streamline the compliance process
- Describe how to apply rule order, logic, and actions to Guardium policies
- Configure policy rules that process the information that is gathered from database and file servers
- Create Guardium queries and reports to examine trends and gather data
- Use Guardium alerts to monitor a data environment

This course is based on Guardium Data Protection version 12.1.