

IBM Guardium Data Protection 12.1

Course Table of Contents

Duration: 3 Days / 24 Hours

Format: Instructor-led with hands-on labs (21 modules, 29 labs)

Day 1 — Guardium Fundamentals, Administration and Data Discovery

Module 1: Introduction to IBM Guardium Data Protection

- IBM Guardium Data Protection Overview
- Data Security and Database Protection
- Database Activity Monitoring
- Guardium Use Cases
- Guardium Data Protection 12.1 Architecture
- Guardium Components and Data Flow

Module 2: Guardium Architecture

- Guardium Collector
- Guardium Aggregator
- Central Manager
- S-TAP
- Guardium Installation Manager (GIM)
- Inspection Engine
- Guardium Data Flow
- Managed Units

Module 3: Guardium Administration

- Guardium User Interface
- System Administration
- User Management
- Roles and Privileges
- Access Management
- Groups and Group Management
- System Configuration
- Data Management

Module 4: Guardium Groups

- Group Builder
- Group Types
- Static Groups
- Dynamic Groups
- Database Groups
- User Groups
- Object Groups
- Groups in Security Policies

Module 5: Database Environment and S-TAP

- Guardium Data Sources
- Database Connectivity

- S-TAP Architecture
- Guardium Installation Manager
- S-TAP Installation
- S-TAP Configuration
- S-TAP Communication
- S-TAP Status and Monitoring
- Inspection Engine

Module 6: Data Discovery and Classification

- Database Discovery
- Data Source Discovery
- Sensitive Data Discovery
- Data Classification
- Classification Rules
- Sensitive Data Identification
- Classification Results
- Discovery Results

Hands-on Labs — Day 1

1. Access and Explore Guardium 12.1
2. Explore Guardium Architecture and Data Flow
3. Create Guardium Users and Roles
4. Create and Manage Guardium Groups
5. Configure the Database Environment
6. Install and Configure GIM/S-TAP
7. Verify S-TAP Connectivity
8. Register and Verify a Database Data Source
9. Discover Sensitive Data
10. Review Data Classification Results

Day 2 — Database Activity Monitoring, Policies, Queries and Reports

Module 7: Database Activity Monitoring

- Database Activity Monitoring Overview
- Database Sessions
- Database Users
- Client Information
- SQL Activity
- Database Objects
- Application Information
- Activity Monitoring
- S-TAP Monitoring

Module 8: Guardium Security Policies

- Policy Architecture
- Policy Builder
- Policy Rules
- Rule Conditions
- Rule Actions
- Database Rules
- User Rules
- Object Rules
- Group-Based Rules
- Policy Installation
- Policy Management

Module 9: Policy Monitoring and Enforcement

- Monitoring Rules
- Violation Detection
- Policy Violations
- Exception Rules
- Blocking Concepts
- Policy Enforcement
- Reviewing Policy Results

Module 10: Alerts and Notifications

- Guardium Alerts
- Real-Time Alerts
- Alert Conditions
- Alert Actions
- Alert Messages
- Notification Configuration
- Policy-Based Alerts

Module 11: Guardium Queries

- Query Overview
- Query Builder
- Query Conditions
- Query Fields
- Filtering

- Database Activity Queries
- User Activity Queries
- Policy Violation Queries
- Custom Queries

Module 12: Reports and Dashboards

- Guardium Reports
- Predefined Reports
- Custom Reports
- Report Filters
- Report Scheduling
- Report Distribution
- Dashboards
- Security Monitoring Dashboards

Hands-on Labs — Day 2

11. Generate and Monitor Database Activity
12. Investigate Database Sessions
13. Create a Database Monitoring Policy
14. Create a Sensitive-Table Monitoring Policy
15. Create a Privileged-User Monitoring Policy
16. Configure a Real-Time Alert
17. Generate and Investigate a Policy Violation
18. Build a Custom Guardium Query
19. Create a Custom Security Report
20. Build a Security Monitoring Dashboard

Day 3 — Auditing, Vulnerability Assessment, Compliance and Operations

Module 13: Guardium Auditing

- Guardium Audit Overview
- Audit Requirements
- Audit Process Builder
- Audit Tasks
- Audit Reports
- Audit Data
- Audit Review
- Audit Sign-Off
- Audit Scheduling
- Audit Distribution

Module 14: Vulnerability Assessment

- Vulnerability Assessment Overview
- Database Security Assessment
- Vulnerability Assessment Tests
- Security Assessment Configuration
- Assessment Results
- Security Findings
- Vulnerability Analysis
- Assessment Exceptions
- Assessment Tuning

Module 15: Sensitive Data and Threat Detection

- Sensitive Data Monitoring
- Privileged User Monitoring
- Suspicious Database Activity
- Unauthorized Access
- Security Violations
- Threat Detection
- Investigation of Suspicious Activity

Module 16: Compliance and Data Security

- Data Security Compliance
- PCI DSS
- HIPAA
- SOX
- GDPR
- Compliance Monitoring
- Compliance Reports
- Audit Evidence
- Security Policies for Compliance

Module 17: Guardium Data Management

- Data Management Overview
- Data Retention
- Data Purging
- Data Archiving

- Storage Management
- Repository Management

Module 18: Backup and Restore

- Guardium Backup Overview
- Configuration Backup
- Data Backup
- Backup Scheduling
- Restore Concepts
- Restore Requirements
- Disaster Recovery Considerations

Module 19: Guardium Troubleshooting

- S-TAP Troubleshooting
- Database Connectivity Issues
- Collector Connectivity
- Policy Troubleshooting
- Monitoring Issues
- Guardium Logs
- System Diagnostics

Module 20: Guardium REST API

- Guardium REST API Overview
- API Authentication
- Guardium API Architecture
- REST API Requests
- GET Operations
- POST Operations
- API-Based Administration
- API-Based Monitoring

Module 21: End-to-End Guardium Scenario

- Database Activity Generation
- S-TAP Monitoring
- Policy Configuration
- Policy Violation
- Alert Generation
- Query Analysis
- Report Generation
- Audit Process
- Vulnerability Assessment
- Compliance Evidence

Hands-on Labs — Day 3

21. Create a Guardium Audit Process
22. Schedule and Distribute Audit Results
23. Run a Vulnerability Assessment
24. Tune a Vulnerability Assessment
25. Generate Compliance Evidence
26. Perform Guardium Backup and Restore Operations
27. Troubleshoot an S-TAP/Database Monitoring Issue

- 28. Use Guardium REST APIs
- 29. Complete an End-to-End Database Security Monitoring Scenario