Information Management

IBM

Data Management

# Enterprise Database Security & Monitoring

**Gerald Tan**
**IBM Singapore**

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

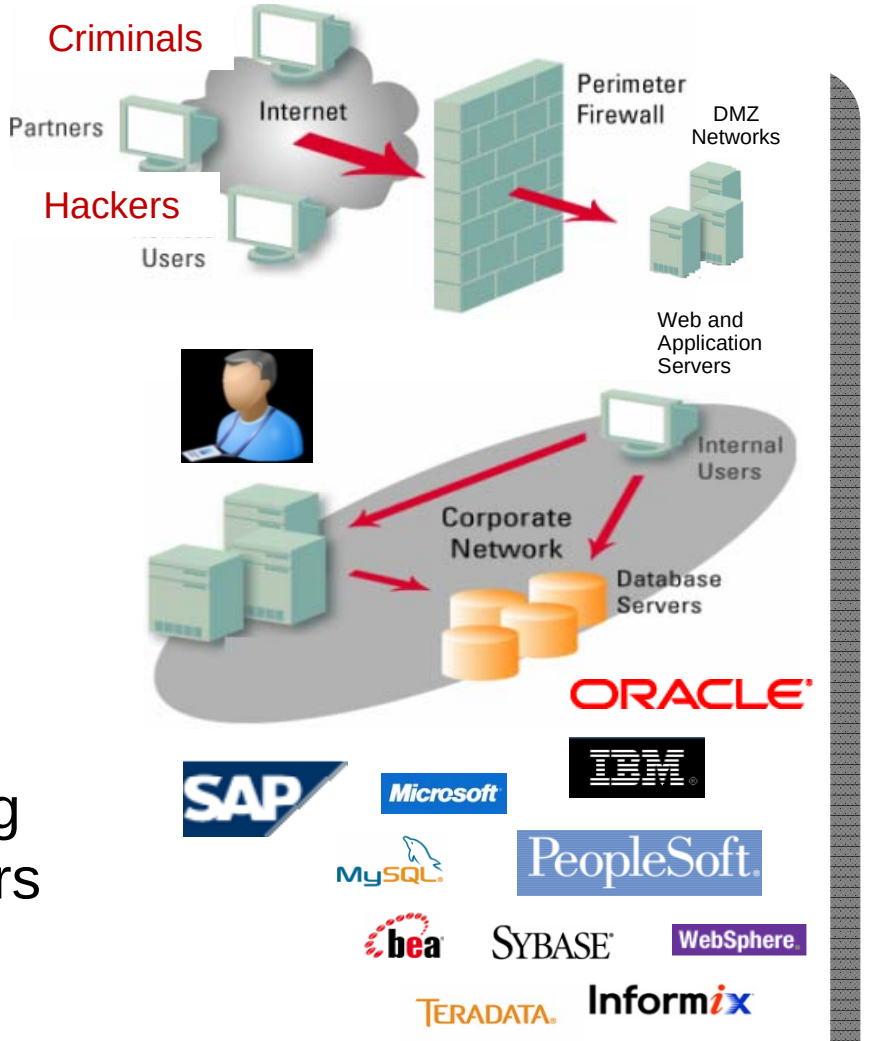
# Database Monitoring: 3 Key Business Drivers

1. **Internal threats**
   - Identify unauthorized changes (governance)
   - Prevent data leakage
2. **External threats**
   - Prevent theft
3. **Compliance**
   - Simplify processes
   - Reduce costs

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# The Complexity & Visibility Challenge

- Heterogeneous & distributed
- Multiple access paths
- Firewalls can't prevent traffic that appears to be legitimate
- Most organizations have formal data security policies but ...
- No practical enforcement mechanisms
- No visibility into what's really going on - especially with privileged users



# Top Data Protection Challenges

Where is my sensitive data - and who's accessing it (including privileged users)?

How can I enforce access control & change control policies for databases?

How do I check for vulnerabilities and lock-down database configurations?

How do I reduce costs by automating & centralizing compliance controls?

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# The Compliance Mandate

| Audit Requirements | COBIT (SOX) | PCI-DSS | ISO 27002 | Data Privacy & Protection Laws | NIST SP 800-53 (FISMA) |
|---|---|---|---|---|---|
| 1. Access to Sensitive Data (Successful/Failed SELECTs) | | ✓ | ✓ | ✓ | ✓ |
| 2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.) | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3. Data Changes (DML) (Insert, Update, Delete) | ✓ | | ✓ | | |
| 4. Security Exceptions (Failed logins, SQL errors, etc.) | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE) | ✓ | ✓ | ✓ | ✓ | ✓ |

**DDL = Data Definition Language (aka schema changes)**
**DML = Data Manipulation Language (data value changes)**
**DCL = Data Control Language**

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Addressing Key Stakeholders


- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated controls

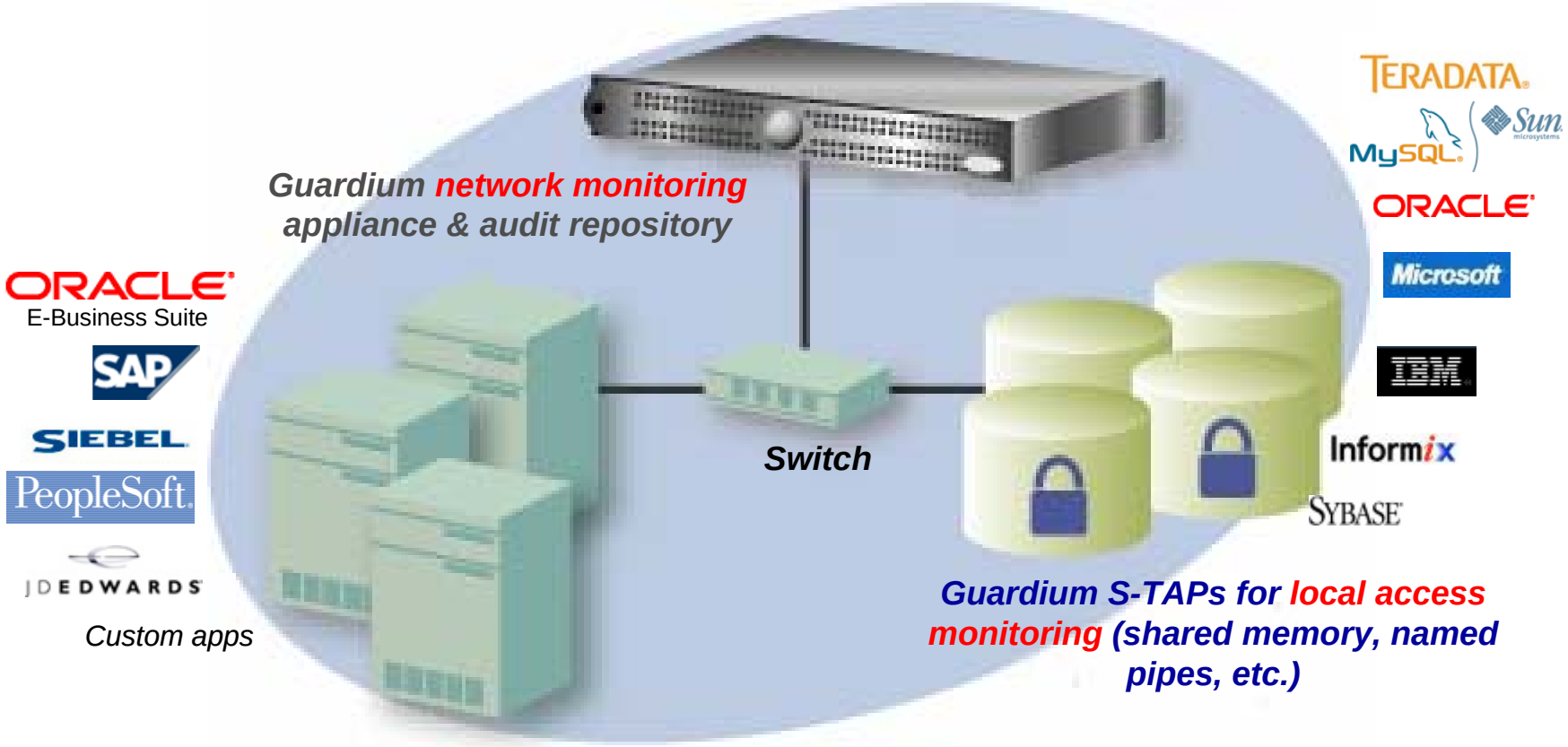

- ✓ Real-time policies
- ✓ Secure audit trail
- ✓ Data mining & forensics


- ✓ Minimal impact
- ✓ Change management
- ✓ Performance optimization

**Guardium: 100% Visibility & Unified View**

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Guardium Solution

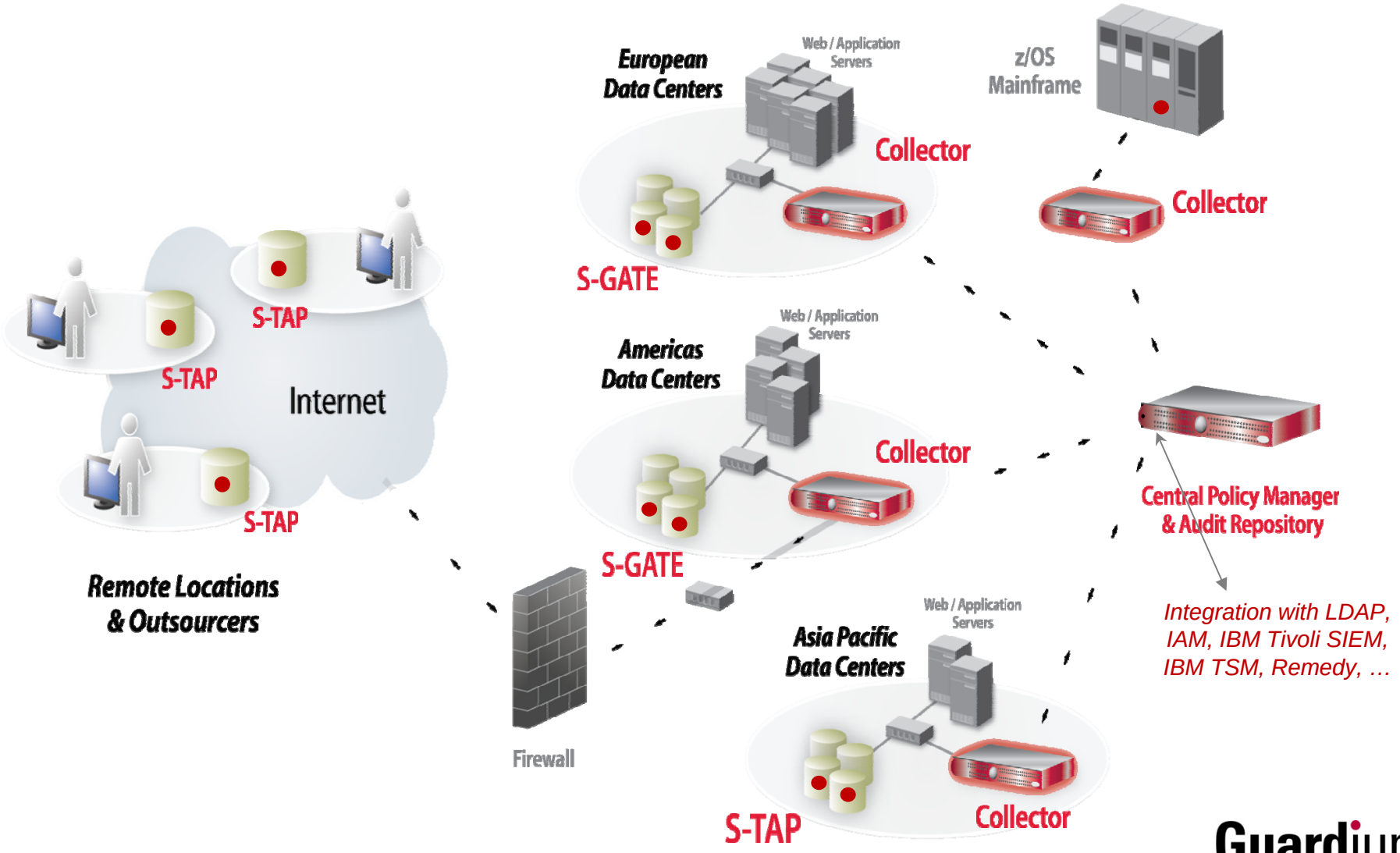



- Non-invasive
- No DBMS changes
- Minimal impact
- Does not rely on traditional DBMS-resident logs that can easily be disabled by DBAs

- Granular policies & monitoring
  - *Who, what, when, how*
- Real-time alerting
- Monitors all activities including local access by privileged users

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

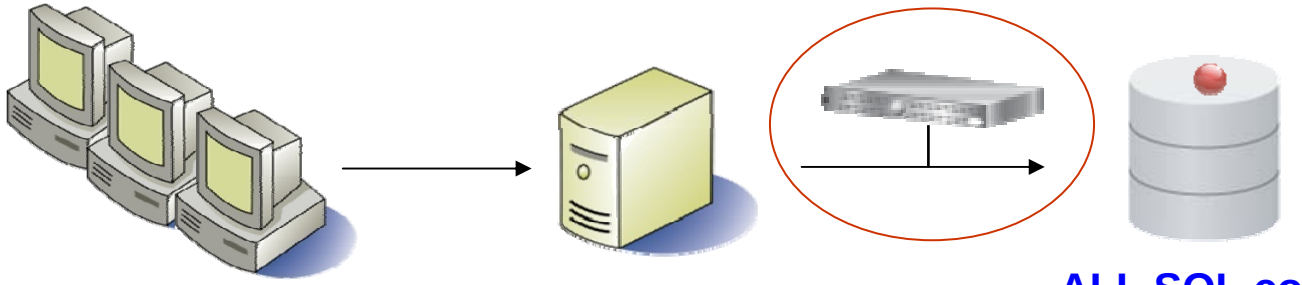
# Scalable Enterprise-wide Multi-Tier Architecture




Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Continuous Fine-grained Auditing and Security

*All SQL traffic contextually analyzed & filtered in real-time to provide specific information required by auditors*



**Client IP**
**Client host name**
**Domain login**
**Client OS**
**MAC**
**TTL**
**Origin**
**Failed logins**

**Server IP**
**Server port**
**Server name**
**Session**
**SQL patterns**
**Network protocol**
**Server OS**
**Timestamp**
**Access programs**
**App User ID**

**ALL SQL commands**
**Fields**
**Objects**
**Verbs**
**DDL**
**DML**
**DCL**
**DB user name**
**DB version**
**DB type**
**DB protocol**
**Origin**
**DB errors**
**SELECTs**

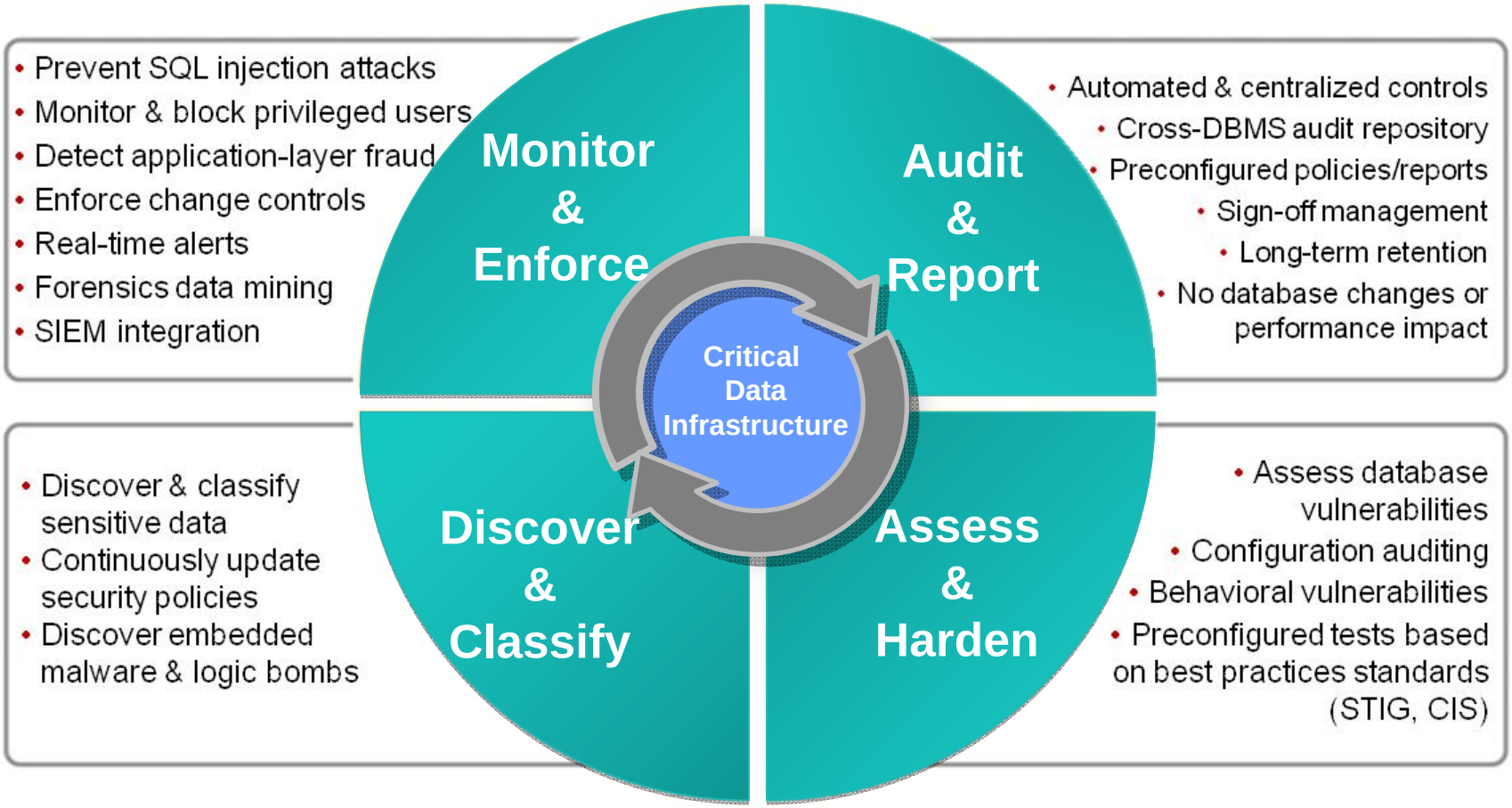
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Provide insight such as . . .

- Who is changing database schemas or dropping tables?
- When there are any unauthorized source programs changing data?
- What are DBAs or outsourced staff doing to the databases?
- How many failed login attempts have occurred?
- Who is extracting credit card data?
- What data is being accessed from which network node?
- What data is being accessed by which application?
- What are the access patterns based on time of day?
- What database errors are being generated?
- What is the exposure to sensitive objects?

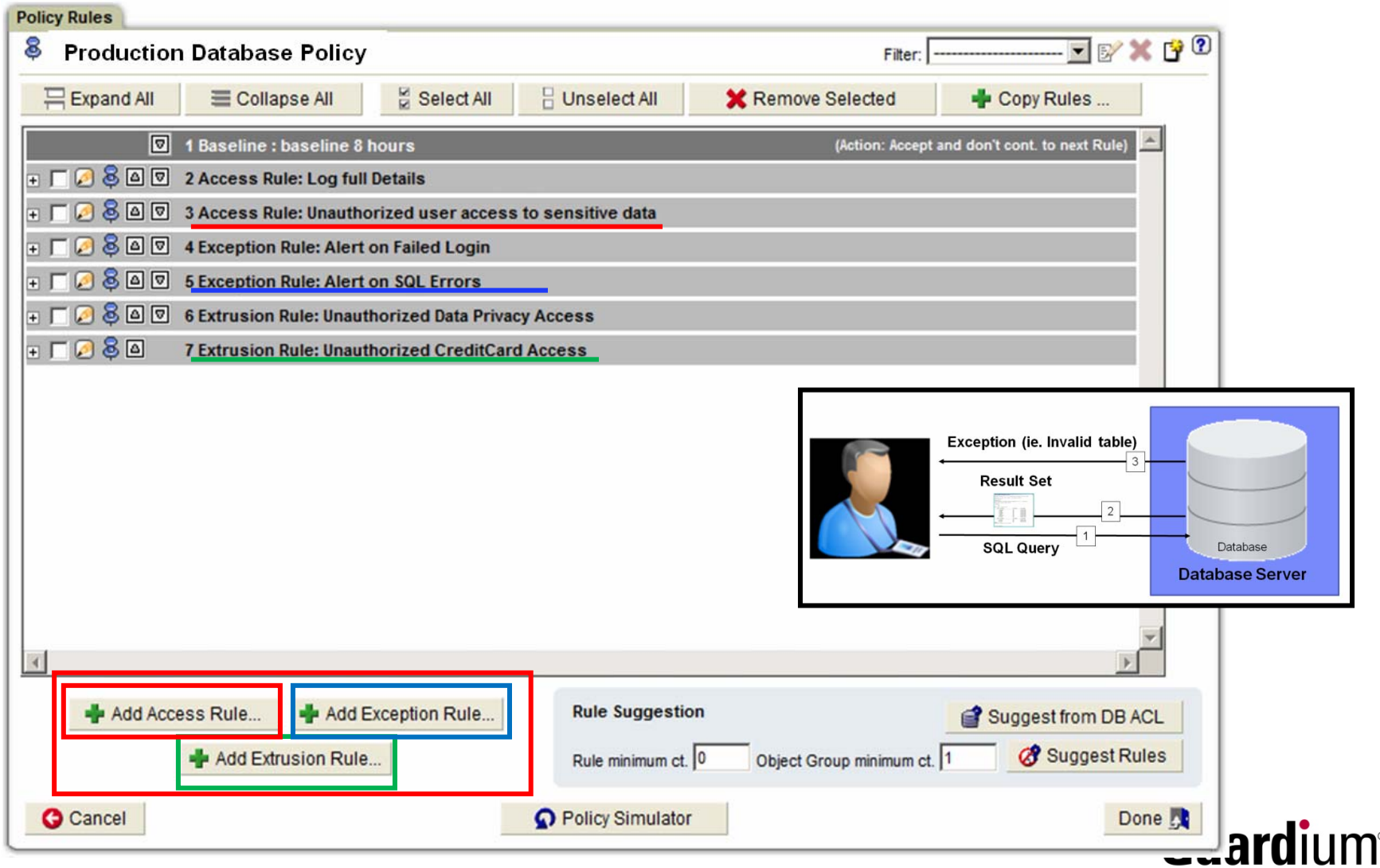
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Addressing the Full Lifecycle

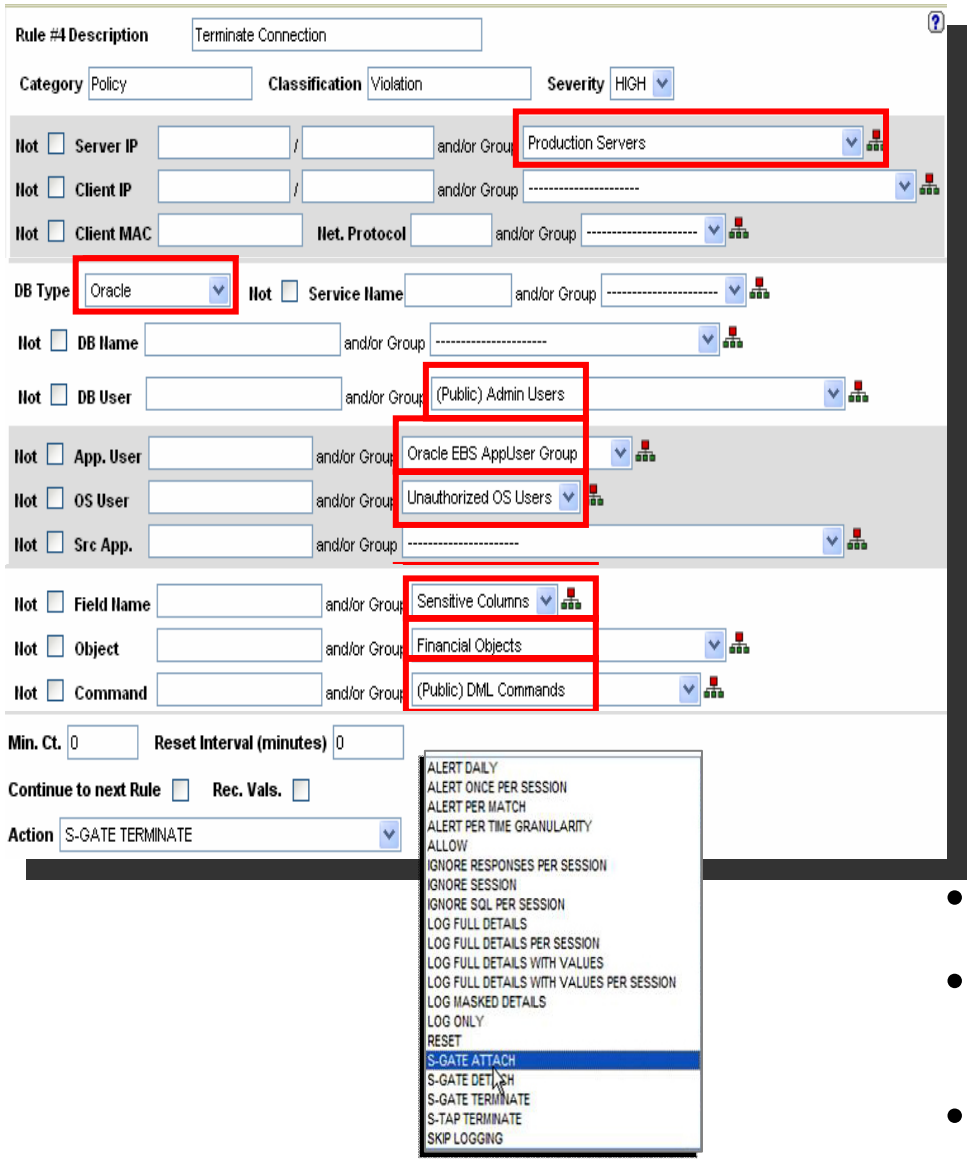



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

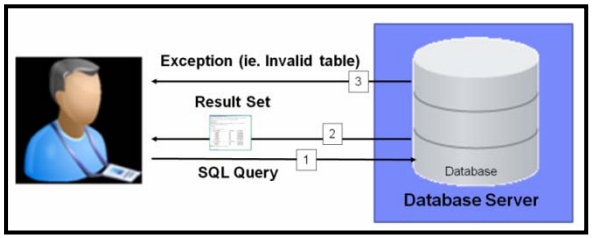
# Policies



# 1. Access Policy – Very Granular to Meet Customer Requirements




**Which Servers**




**Which Databases**

**Which Users**

**Which Fields**

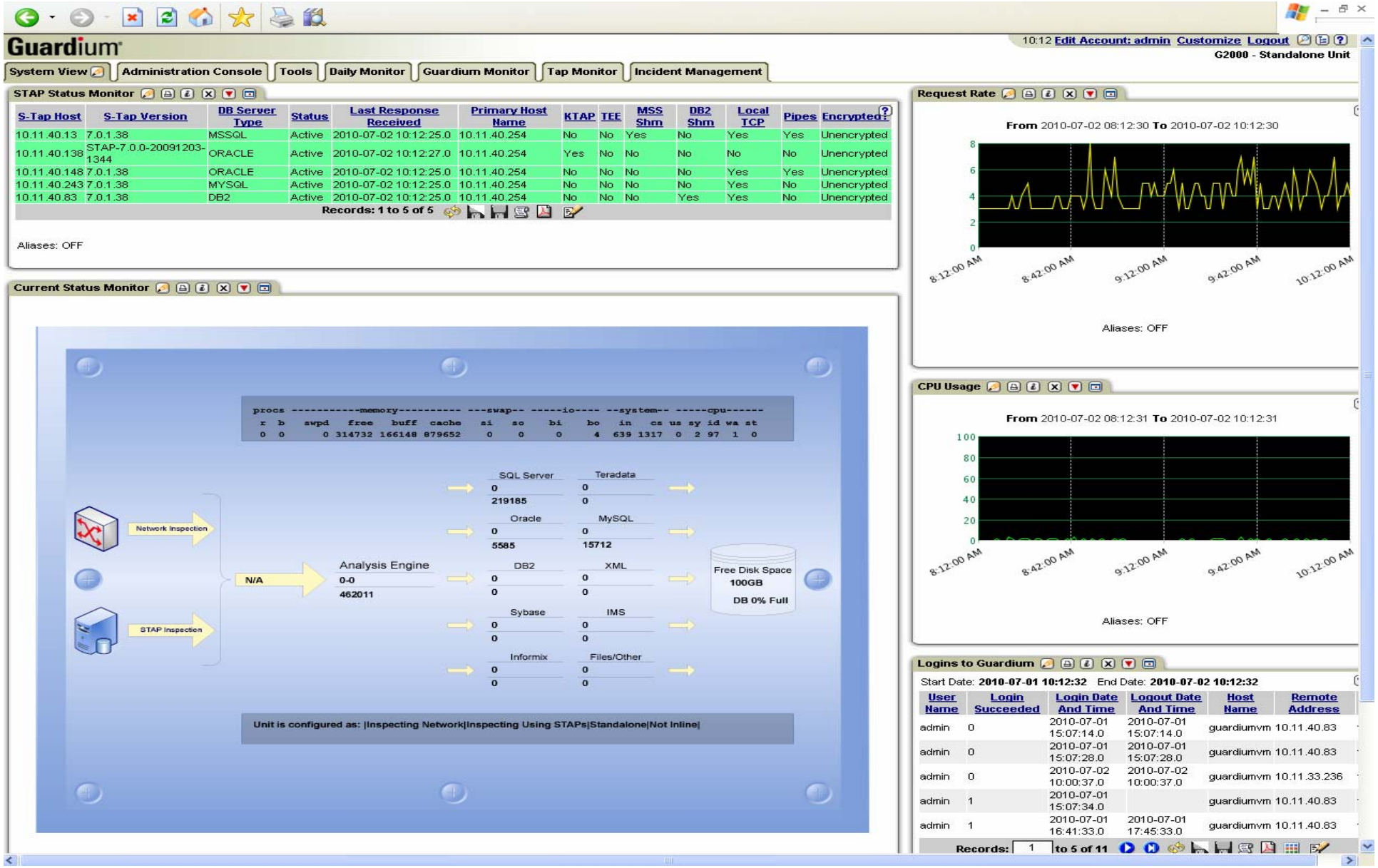
**Which Tables**

**Which SQL Commands**

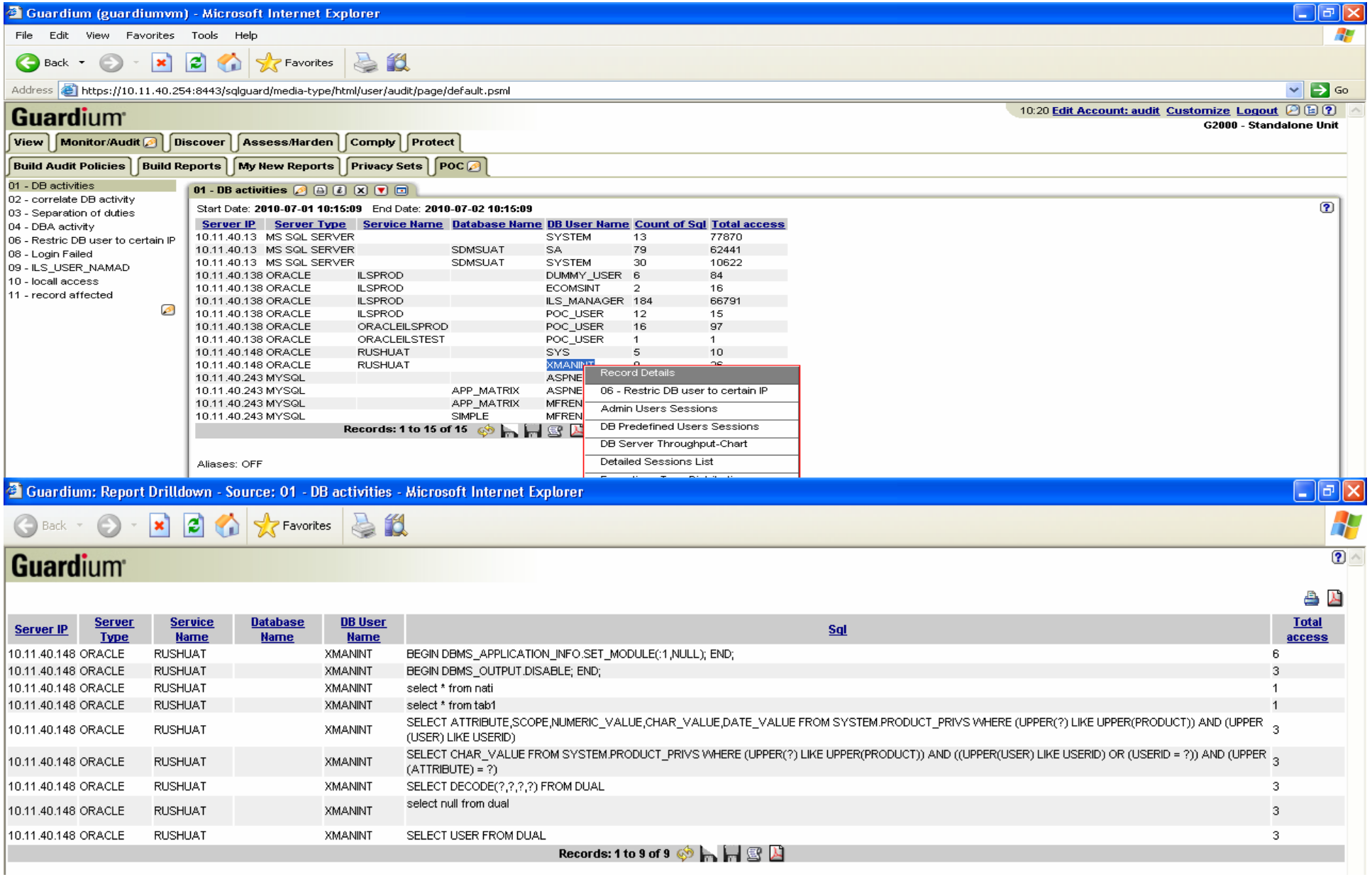
- **What Action?**
- **Allow, Log, Log Full Details, Log full Details with Values**
- **Alert, Ignore, Terminate**

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

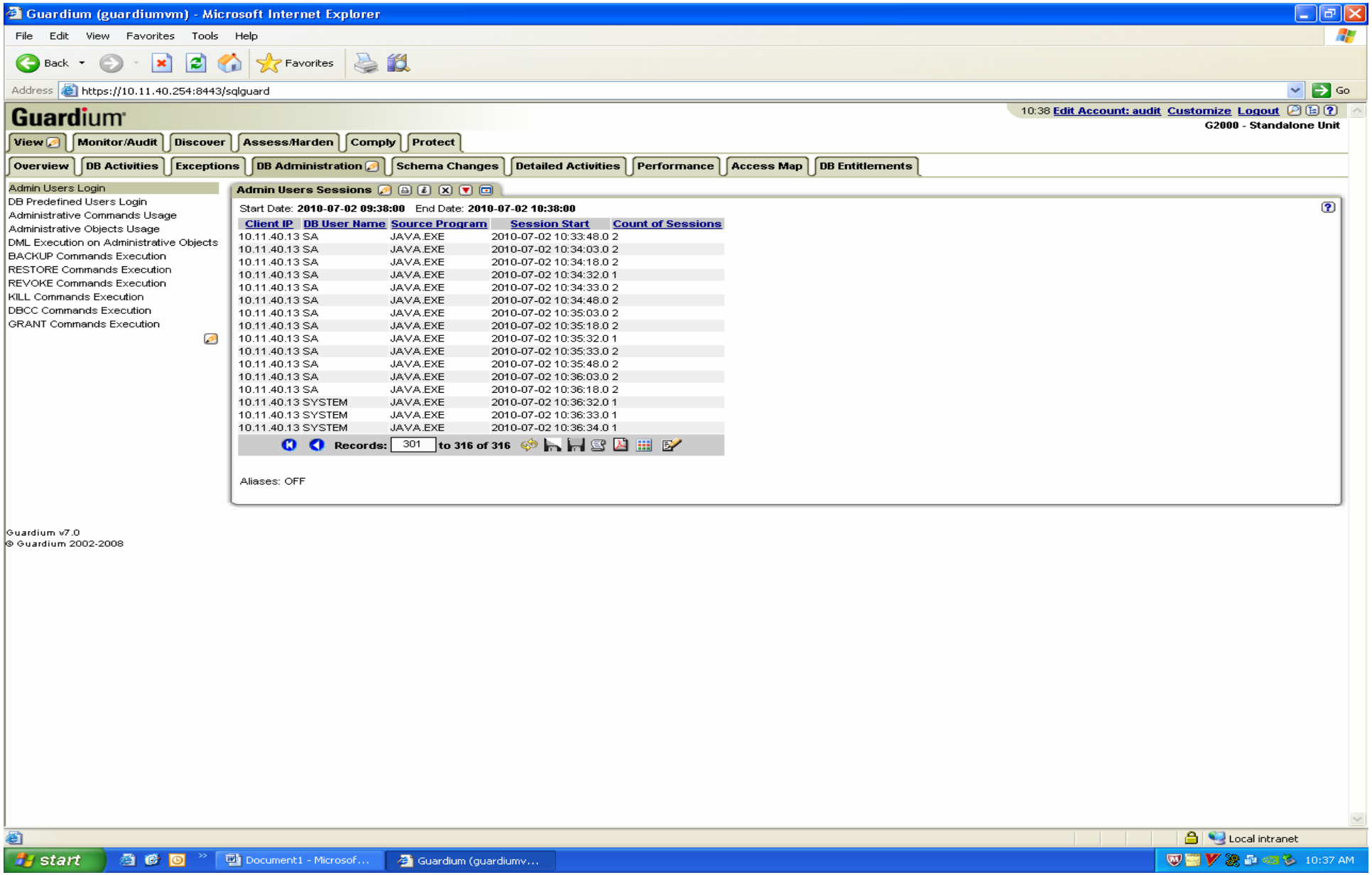
# Dashboard


Guardium
10:12 Edit Account: admin Customize Logout
G2000 - Standalone Unit
System View
Administration Console
Tools
Daily Monitor
Guardium Monitor
Tap Monitor
Incident Management
STAP Status Monitor
S-Tap Host | S-Tap Version | DB Server Type | Status | Last Response Received | Primary Host Name | KTAP | TEE | MSS Shm | DB2 Shm | Local TCP | Pipes | Encrypted
10.11.40.13 | 7.0.1.38 | MSSQL | Active | 2010-07-02 10:12:25.0 | 10.11.40.254 | No | No | Yes | No | Yes | Yes | Unencrypted
10.11.40.138 | STAP-7.0.0-20091203-1344 | ORACLE | Active | 2010-07-02 10:12:27.0 | 10.11.40.254 | Yes | No | No | No | No | No | Unencrypted
10.11.40.148 | 7.0.1.38 | ORACLE | Active | 2010-07-02 10:12:25.0 | 10.11.40.254 | No | No | No | No | Yes | Yes | Unencrypted
10.11.40.243 | 7.0.1.38 | MYSQL | Active | 2010-07-02 10:12:25.0 | 10.11.40.254 | No | No | No | No | Yes | No | Unencrypted
10.11.40.83 | 7.0.1.38 | DB2 | Active | 2010-07-02 10:12:25.0 | 10.11.40.254 | No | No | No | Yes | Yes | No | Unencrypted
Records: 1 to 5 of 5
Aliases: OFF
Request Rate
From 2010-07-02 08:12:30 To 2010-07-02 10:12:30
8:12:00 AM
8:42:00 AM
9:12:00 AM
9:42:00 AM
10:12:00 AM
Aliases: OFF
Current Status Monitor
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu------
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 314732 166148 879652 0 0 0 4 639 1317 0 2 97 1 0
Network Inspection
STAP Inspection
N/A
Analysis Engine
0-0
462011
SQL Server
0
219185
Teradata
0
0
Oracle
0
5585
MySQL
0
15712
DB2
0
0
XML
0
0
Sybase
0
0
IMS
0
0
Informix
0
0
Files/Other
0
0
Free Disk Space
100GB
DB 0% Full
Unit is configured as: |Inspecting Network|Inspecting Using STAPs|Standalone|Not Inline|
CPU Usage
From 2010-07-02 08:12:31 To 2010-07-02 10:12:31
Aliases: OFF
Logins to Guardium
Start Date: 2010-07-01 10:12:32 End Date: 2010-07-02 10:12:32
User Name | Login Succeeded | Login Date And Time | Logout Date And Time | Host Name | Remote Address
admin | 0 | 2010-07-01 15:07:14.0 | 2010-07-01 15:07:14.0 | guardiumvm | 10.11.40.83
admin | 0 | 2010-07-01 15:07:28.0 | 2010-07-01 15:07:28.0 | guardiumvm | 10.11.40.83
admin | 0 | 2010-07-02 10:00:37.0 | 2010-07-02 10:00:37.0 | guardiumvm | 10.11.33.236
admin | 1 | 2010-07-01 15:07:34.0 | | guardiumvm | 10.11.40.83
admin | 1 | 2010-07-01 16:41:33.0 | 2010-07-01 17:45:33.0 | guardiumvm | 10.11.40.83
Records: 1 to 5 of 11

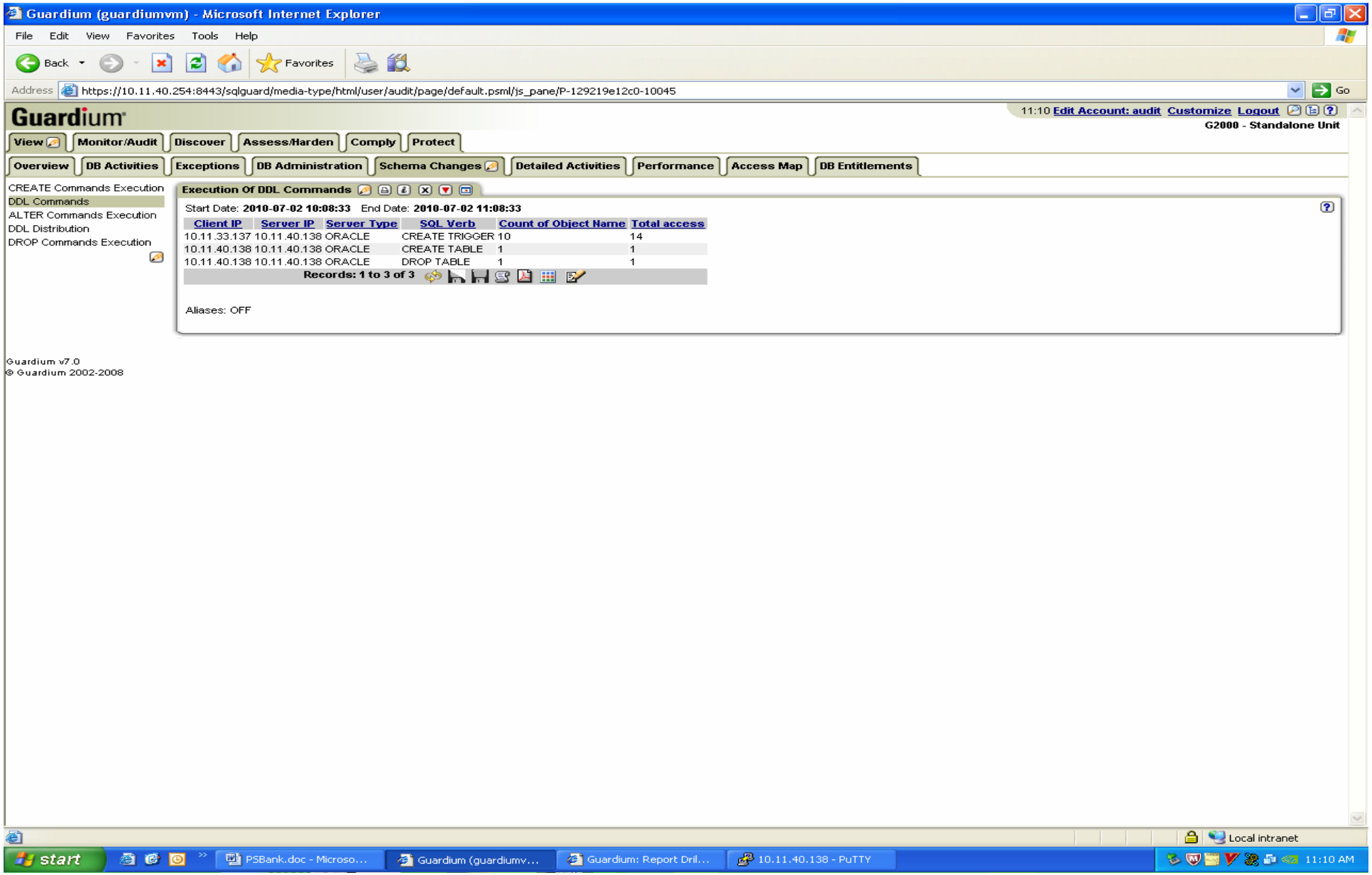
# DB Activities



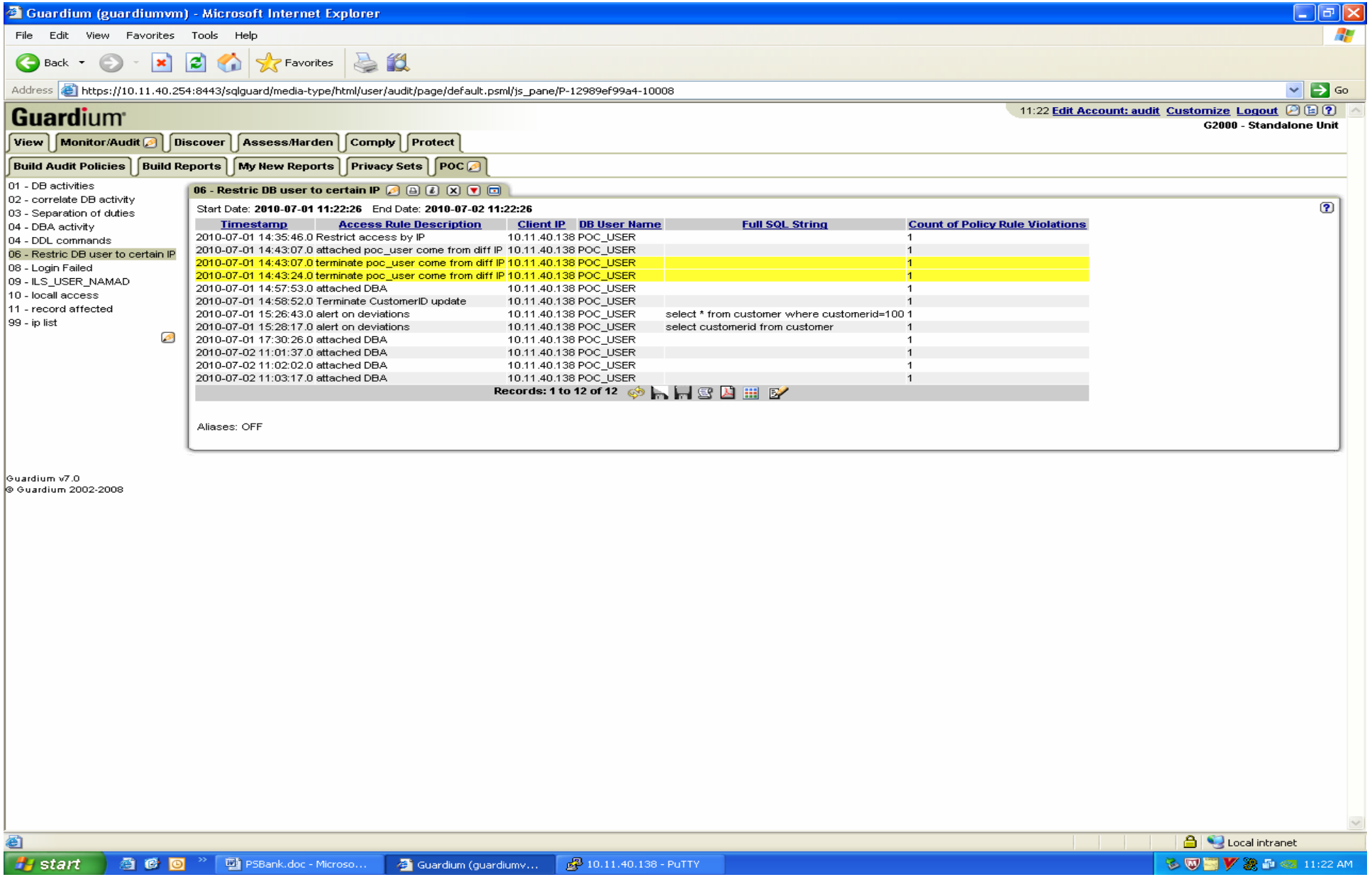
# Admin User Sessions



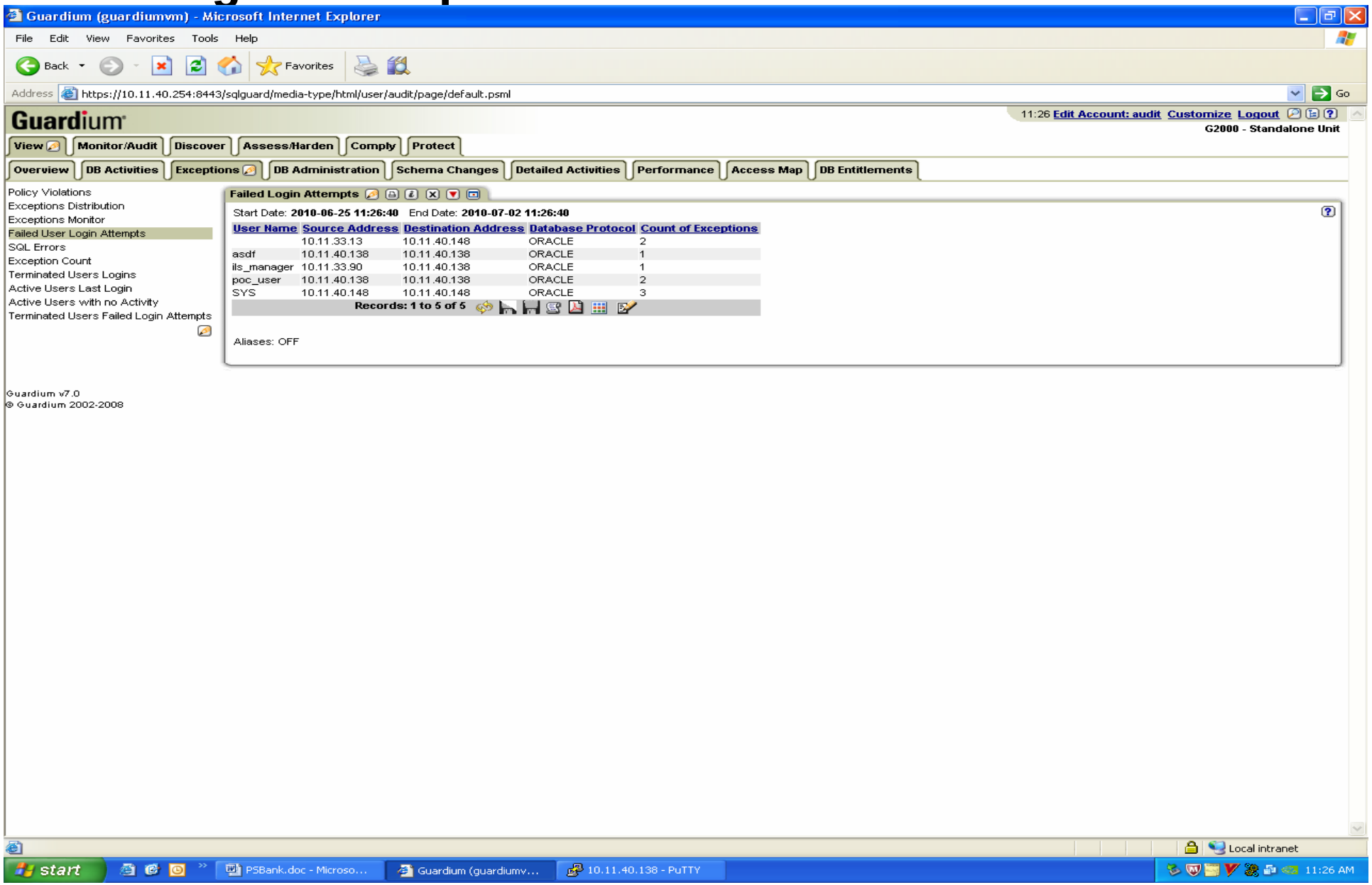
# Execution of DDL Commands



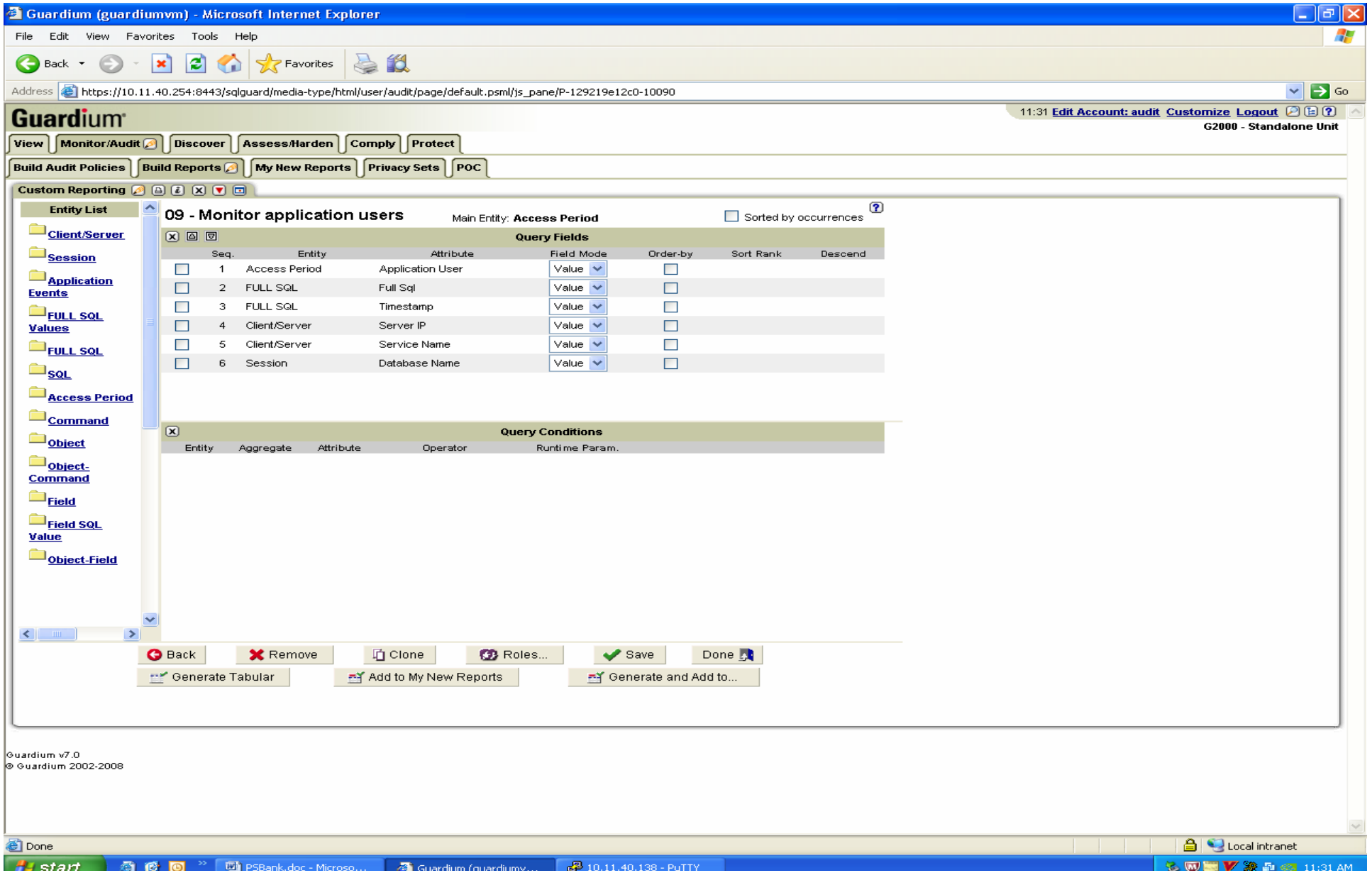
# Restrict DB Users to Certain IP Address



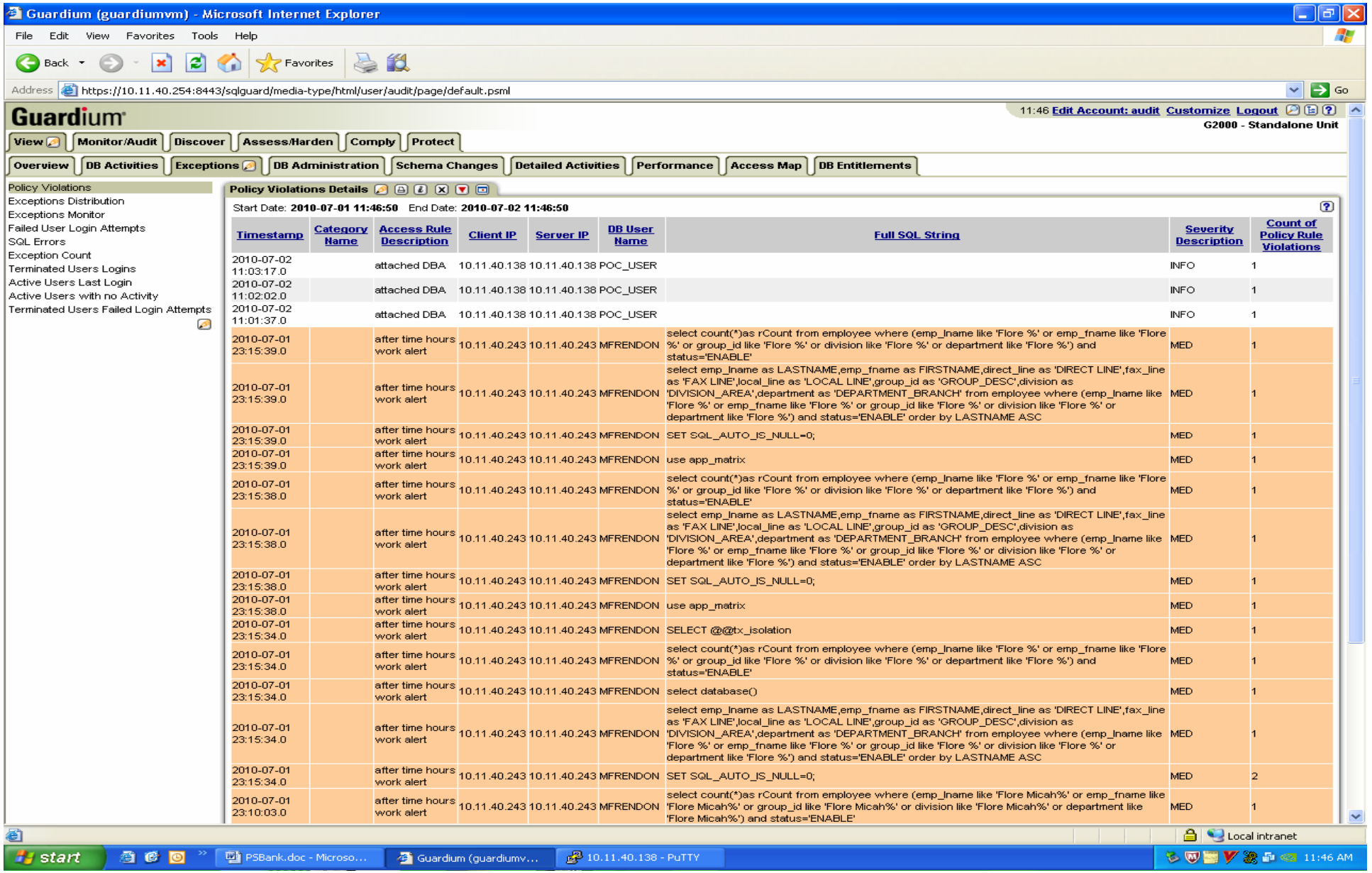
# User Login Attempts



# Monitor Application Users

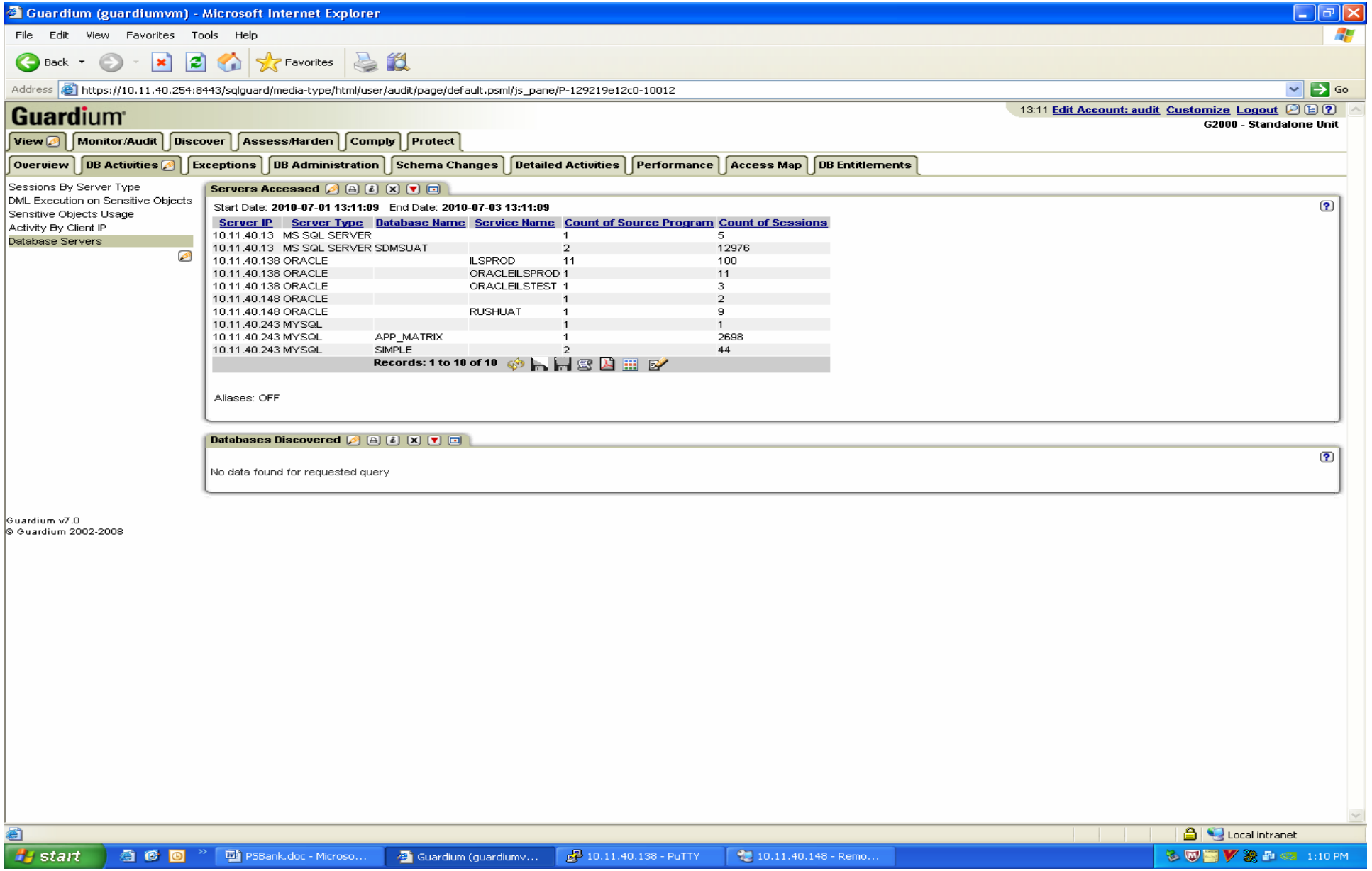


# Policy Violation Details

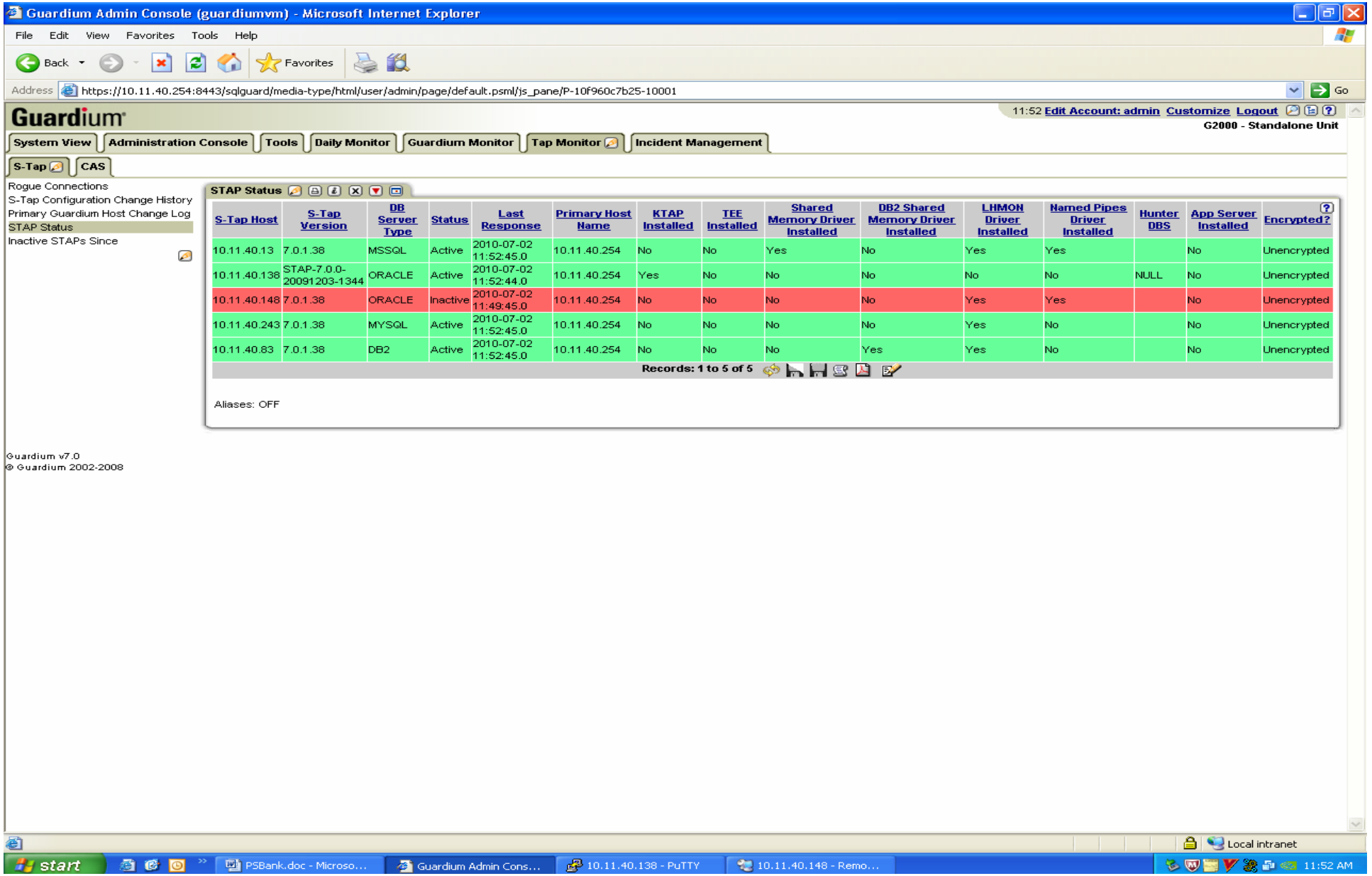



| Timestamp | Category Name | Access Rule Description | Client IP | Server IP | DB User Name | Full SQL String | Severity Description | Count of Policy Rule Violations |
|---|---|---|---|---|---|---|---|---|
| 2010-07-02 11:03:17.0 | | attached DBA | 10.11.40.138 | 10.11.40.138 | POC_USER | | INFO | 1 |
| 2010-07-02 11:02:02.0 | | attached DBA | 10.11.40.138 | 10.11.40.138 | POC_USER | | INFO | 1 |
| 2010-07-02 11:01:37.0 | | attached DBA | 10.11.40.138 | 10.11.40.138 | POC_USER | | INFO | 1 |
| 2010-07-01 23:15:39.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select count(*)as rCount from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' | MED | 1 |
| 2010-07-01 23:15:39.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select emp_lname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC | MED | 1 |
| 2010-07-01 23:15:39.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | SET SQL_AUTO_IS_NULL=0; | MED | 1 |
| 2010-07-01 23:15:39.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | use app_matrix | MED | 1 |
| 2010-07-01 23:15:38.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select count(*)as rCount from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' | MED | 1 |
| 2010-07-01 23:15:38.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select emp_lname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC | MED | 1 |
| 2010-07-01 23:15:38.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | SET SQL_AUTO_IS_NULL=0; | MED | 1 |
| 2010-07-01 23:15:38.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | use app_matrix | MED | 1 |
| 2010-07-01 23:15:34.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | SELECT @@tx_isolation | MED | 1 |
| 2010-07-01 23:15:34.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select count(*)as rCount from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' | MED | 1 |
| 2010-07-01 23:15:34.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select database() | MED | 1 |
| 2010-07-01 23:15:34.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select emp_lname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_lname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC | MED | 1 |
| 2010-07-01 23:15:34.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | SET SQL_AUTO_IS_NULL=0; | MED | 2 |
| 2010-07-01 23:10:03.0 | | after time hours work alert | 10.11.40.243 | 10.11.40.243 | MFRENDON | select count(*)as rCount from employee where (emp_lname like 'Flore Micah%' or emp_fname like 'Flore Micah%' or group_id like 'Flore Micah%' or division like 'Flore Micah%' or department like 'Flore Micah%') and status='ENABLE' | MED | 1 |

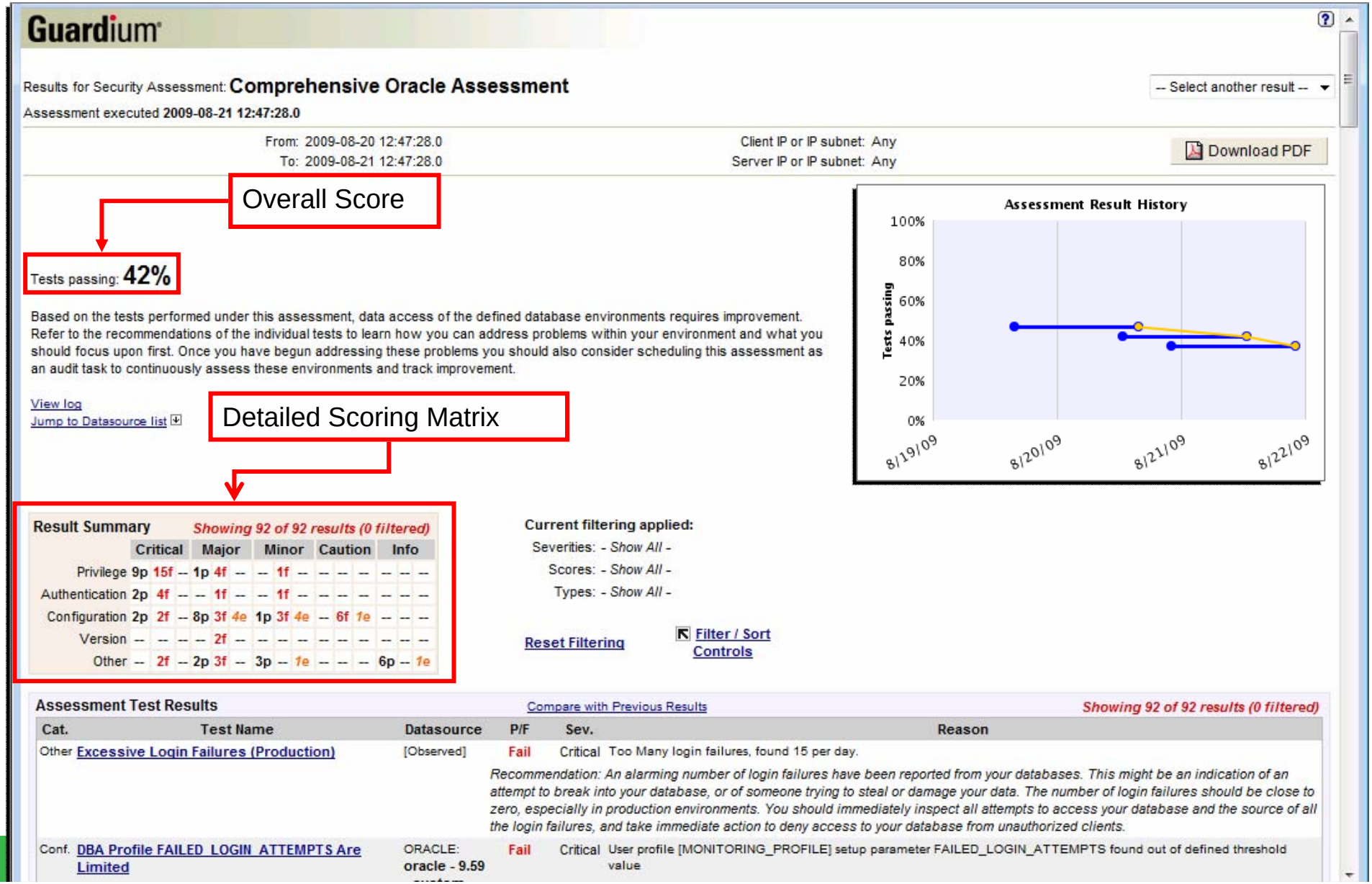
# Database Servers Monitored



# S-TAP Status


Guardium Admin Console (guardiumvm) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Favorites
Address https://10.11.40.254:8443/sqlguard/media-type/html/user/admin/page/default.psml/js_pane/P-10f960c7b25-10001
Go
Guardium
11:52 Edit Account: admin Customize Logout
G2000 - Standalone Unit
System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management
S-Tap CAS
Rogue Connections
S-Tap Configuration Change History
Primary Guardium Host Change Log
STAP Status
Inactive STAPs Since
STAP Status
S-Tap Host | S-Tap Version | DB Server Type | Status | Last Response | Primary Host Name | KTAP Installed | TEE Installed | Shared Memory Driver Installed | DB2 Shared Memory Driver Installed | LHMON Driver Installed | Named Pipes Driver Installed | Hunter DBS | App Server Installed | Encrypted?
10.11.40.13 | 7.0.1.38 | MSSQL | Active | 2010-07-02 11:52:45.0 | 10.11.40.254 | No | No | Yes | No | Yes | Yes | | No | Unencrypted
10.11.40.138 | STAP-7.0.0-20091203-1344 | ORACLE | Active | 2010-07-02 11:52:44.0 | 10.11.40.254 | Yes | No | No | No | No | No | NULL | No | Unencrypted
10.11.40.148 | 7.0.1.38 | ORACLE | Inactive | 2010-07-02 11:49:45.0 | 10.11.40.254 | No | No | No | No | Yes | Yes | | No | Unencrypted
10.11.40.243 | 7.0.1.38 | MYSQL | Active | 2010-07-02 11:52:45.0 | 10.11.40.254 | No | No | No | No | Yes | No | | No | Unencrypted
10.11.40.83 | 7.0.1.38 | DB2 | Active | 2010-07-02 11:52:45.0 | 10.11.40.254 | No | No | No | Yes | Yes | No | | No | Unencrypted
Records: 1 to 5 of 5
Aliases: OFF
Guardium v7.0
© Guardium 2002-2008
Local intranet
start
PSBank.doc - Microso...
Guardium Admin Cons...
10.11.40.138 - PuTTY
10.11.40.148 - Remo...
11:52 AM

# Vulnerability Assessment Example



# Chosen by Leading Organizations Worldwide

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world's favorite beverage brands
- The most recognized name in PCs
- 15 of the world's leading telcos
- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

# The *Continuing* Choice of Telco/Utility Market Leaders


Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# The *Continuing* Choice of Financial Market Leaders


Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# The *Continuing* Choice of Oil and Gas Leaders

# The *Continuing* Choice of Government Leaders


Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Validated by Industry Experts

FORRESTER®

*"Dominance in this space"*
#1 Scores for Current Offering, Architecture & Product Strategy

ChannelWeb

**"Most Powerful Compliance Regulations**

SC MAGAZINE

*"5-Star Ratings*: Easy installation, sophisticated reporting, strong policy-based security."

the 451 group

InformationWeek

*"Top of DBEP Class"*
"Practically every feature you'll need to lock down sensitive data."

**"Guardium is ahead of the pack and gaining speed."**

**"Guardium is ahead of the pack and gaining speed."**

RED HERRING N. AMERICA WINNER 100

SQL SERVER MAGAZINE

*2007 Editor's Choice Award in "Auditing and Compliance"*

SECURITY MAGAZINE

"Enterprise-class data security product that should be on every organization's radar."

INFORMATION SECURITY Hotpick

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Guardium Value Proposition

- Ensure privacy & integrity of enterprise data
  - Enforce change controls & access controls for critical systems
  - Across entire application & database infrastructure
  - Oracle, SQL Server, IBM DB2 & Informix, Sybase, MySQL, Teradata
  - SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects, …
- Increase operational efficiency
  - Automate & centralize internal controls
  - Across heterogeneous & distributed environments
  - Rapidly troubleshoot performance issues & application errors
  - Highly-scalable platform proven in most demanding data center environments worldwide
- No degradation of infrastructure or business processes
  - Non-invasive architecture
  - No changes required to applications or databases

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Summary & Conclusions

- Databases contain your most critical data
- Traditional technologies can't give you the visibility to identify & prevent unauthorized access
- Guardium is the most widely-deployed solution
  - Broad heterogeneous support
  - Granular visibility & real-time policies
  - Deep automation
  - Scalable architecture

# General Discussion

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY


Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Customer Case Studies

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Financial Services Firm with 1M+ Sessions/Day


- **Who:** Global NYSE-traded company with 75M customers
- **Need:** Enhance SOX compliance & data governance
  - *Phase 1*: Monitor all privileged user activities, especially DB changes.
  - *Phase 2:* Focus on data privacy.
- **Environment:** 4 data centers managed by IBM Global Services
  - 122 database instances on 100+ servers
  - Oracle, IBM DB2, Sybase, SQL Server on AIX, HP-UX, Solaris, Windows
  - PeopleSoft plus 75 in-house applications
- **Alternatives considered:** Native auditing
  - Not practical because of performance overhead; DB servers at 99% capacity
- **Results:** Now auditing 1M+ sessions per day (GRANTs, DDL, etc.)
  - Caught DBAs accessing databases with Excel & shared credentials
  - Producing daily automated reports for SOX with sign-off by oversight teams
  - Automated change control reconciliation using ticket IDs
  - Passed 2 external audits

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Major Retailer with PCI & SOX Controls

- **Who:** National retailer with $50B+ in sales & 6,400 stores
- **Need:** Initially PCI, then extended to SOX, SAS70, data privacy
- **Environment:** 5 major data centers (via M&A)
  - Oracle, SQL Server, DB2, UDB on AIX, Solaris, Windows
  - Dell, IBM midrange, Sun, IBM Z10 on RACF
  - PeopleSoft, SAP plus proprietary claims engines
- **Alternatives considered:**
  - Native auditing; DB encryption; DB appliance from major security vendor
- **Results:**
  - Implemented in ~ 4 weeks
  - PCI certified in stipulated time, saving millions in potential penalties
  - Requirement 3.4: Compensating control for DB encryption
  - Requirement 6: Maintain secure systems (enforce change controls)
  - Requirement 10: Track & monitor all access to cardholder data [automated]
  - Failed DB calls identified for performance optimization
  - Load distribution quantified between servers

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Major European Telco

- **Who:** Global telco with 70M mobile customers; €30B revenue.
- **Need:** Ensure privacy of call records for compliance with data privacy laws.
  - Phase 1: Safeguard OSS systems
  - Phase 2: Safeguard BSS systems
- **Environment:** 15 heterogeneous, geographically-distributed data centers
  - Oracle, SQL Server, Informix, Sybase
  - HP-UX, HP Tru64, Solaris, Windows, UNIX
  - SAP, Remedy plus in-house applications (billing, Web portal, etc.)
- **Alternatives considered:** Native auditing; Oracle Audit Vault.
  - Not practical because of performance overhead; lack of granularity; non-support for older versions; need for multi-DBMS support.
- **Results:**
  - Deployed to 12 initial data centers in only 2 weeks!
  - Now auditing all traffic in high-traffic environment; centrally managed.
  - Passed several external audits
  - Future plans: Implement application user monitoring; 2-factor authentication; expand scope to other applications.

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Simplifying Enterprise Security for Dell


CASE STUDY:
SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Vanugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Securely maintaining sensitive financial and customer information in enterprise data cen- desk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed

*Published case study in Dell Power Solutions*

- **Need:**
  - Improve database security for SOX, PCI & SAS70
  - Simplify & automate compliance controls
- **Guardium Deployment:**
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deployed to additional 725 database servers
- **Environment :**
  - Oracle & SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion plus in-house applications
- **Previous Solution:** Native logging (MS) or auditing (Oracle) with in-house scripts
  - Supportability issues; DBA time required; massive data volumes; SOD issues.
- **Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration
  - Guardium “successfully met Dell’s requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases.”

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Washington Metropolitan Area Transit Authority (Metro) Safeguards Customer Information

- **Who:** The Metro operates the 2nd largest U.S. rail transit system and transports more than a third of the federal government to work
- **Need:** Metro needed to safeguard sensitive customer data and simplify compliance with PCI-DSS -- without impacting performance or changing database configurations
  - Protecting customer data
  - Passing audits more quickly and easily
  - Monitoring for potential fraud in PeopleSoft system
  - Leveraging scalable architecture; automated oversight workflows (electronic sign-offs, escalations); library of best practices PCI policies and reports; application-layer monitoring
- **Environment:**
  - More than 9 million transactions per year (Level 1 merchant)
  - Complex, multi-tier heterogeneous environment
- **Alternatives considered:** Native logging and auditing impractical
- **Customer Impact**: "Our customers trust us to transport them safely and safeguard their personal information."
  - "We looked at native DBMS logging and auditing, but it's impractical because of its high overhead, especially when you're capturing every SELECT in a high-volume environment like ours. In addition, native auditing doesn't enforce separation of duties or prevent unauthorized access by privileged insiders."

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Why Enterprises Choose Guardium

- Most widely-deployed in production environments
  - *Continuously enhanced since 2002, based on real-world enterprise feedback*
- Most scalable & automated solution (enterprise-ready)
  - *Federated multi-tier system with centralized, cross-DBMS security policies and audit repository, groups, auto-discovery, compliance workflow automation, incident management, role-based management, …*
- Most flexible
  - *Multiple deployment options, configurable policies, drag-and-drop reporting, API, …*
- Broadest support for heterogeneous environments
  - *Database & OS platforms, enterprise applications, authentication, data import, integration with SIEM & ticketing systems,*
- Richest suite of security & compliance applications
  - *Security & forensics, compliance reporting & oversight, change control, data mining, log data management, …*

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# Supported Platforms

| Supported Platforms | Supported Versions |
|---|---|
| Oracle | 8i, 9i, 10g (r1, r2), 11g, 11i |
| Microsoft SQL Server | 2000, 2005, 2008 |
| IBM DB2 UBD (Windows, Unix, z/Linux) | 8.0, 8.2, 9.1, 9.5 |
| IBM DB2 for z/OS | 7, 8, 9, 9.5 |
| IBM DB2 UBD for iSeries (AS/400) | V5R2, V5R3, V5R4, V6R1 |
| IBM Informix | 7, 8, 9, 10,11 |
| MySQL | 4.1, 5.0, 5.1 |
| Sybase ASE | 12, 15 |
| Sybase IQ | 12.6 |
| Teradata | 6.01, 6.02 |