What’s New in Guardium 11.1

Shay Harel
Director of Engineering / Data Security
Notices and disclaimers

• © 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

• U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

• Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

• IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

• Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

• Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

• References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

• Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

• It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.
Notices and disclaimers (continued)

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.
Today’s topics

• Mapping Applications to Databases and Support for Specific Industries
• Active Analytics and Risk spotter enhancements
• ServiceNow Integration
• Automatic Creation of Inspection Engine
• IPV6
• DBaaS Monitoring without S-TAP – AWS and Azure additions
• New VA Capabilities
• New S-TAP Changes (Oracle Unified Audit and External S-TAP)
• Mainframe
• And a new cool feature for DB access investigation
• Mapping Applications to Databases and Support for Specific Industries

What is it?
Mapping between database and applications in order to show coverage of critical application databases

What’s New
• Wizard flow for setting up compliance for an application group
• Dashboard showing key metrics per application group
• Out-of-the-box examples of application groups by industry

Benefits
• Easily manage Guardium coverage in a business centric way (ie. Are all my CRM databases covered?)
<table>
<thead>
<tr>
<th>Application name</th>
<th>Instance name</th>
<th>Database name</th>
<th>Type</th>
<th>Host</th>
<th>Unconfigured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Management (Retail)</td>
<td></td>
<td>sample</td>
<td>DB2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ON9CRH7V</td>
<td></td>
<td>ORACLE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: 3 Selected: 0
Active Threat Analytics 11.0

- Outliers
  - Data leak
  - Denial of service
  - Account take-over
  - Schema tempering
  - Data tempering
  - Anomaly

Threat Diagnostics (AKA Eagle Eye)

- SQL injection
- Malicious stored procedure

Active Threat Analytics
Active Threat Analytics 11.1

Outliers
- Data leak
- Denial of service
- Account take-over
- Schema tempering
- Data tempering
- Anomaly
- Massive grants

Threat Diagnostics (AKA Eagle Eye)
- SQL injection
- Malicious stored procedure
- Suspicious use of new grants

Threat Finder
- Cross-Site Scripting (XSS)
- OS Command Injection
- SQL Injection - Denial Of Service
- SQL Injection - Side channel
- SQL Injection – Tautology
Active Threat Analytics in 11.1
Risk Spotter changes in 11.1

Continuously assesses all risk indicators to identify potential risks across your entire system. Risk indicators include Threat analytics, violations, vulnerabilities, volume of activities, access to sensitive data and more.

Risk Spotter Dynamic Auditing policy audits top risky users, watchlist users, and samples random and non-audited users.

**New capabilities**
- Integrated new Threat analytics as a risk indicator
- Simplified and flexible Dynamic auditing policy
- View most risky users across a period of time
- Add users to Watchlist
- Open Audit process or ServiceNow ticket to initiate investigation

**Benefits**
- Investigate most risky users first
- Consolidated risk assessment (10 risk indicators)
- Dynamic auditing policy selects which users to audit, according to available resources, including a sample of random users
Risky users over a period of Time

Changed chart to Users per max risk range (v11 had Users’ risk level)

149 [distinct] risky users in 7 days.

• 135 of them had a max risk between 6-10/10 during this period
## Risky users > Actions

View the aggregated top daily 50 risky users. Users appear once in the table, with full details of the current risk, and maximum risk, over the selected time period.

You can take actions on either selected, or all users.

<table>
<thead>
<tr>
<th>DB User</th>
<th>Server</th>
<th>No. risky days</th>
<th>Max risk</th>
<th>Ticket/audit ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2_PZEV</td>
<td>SIGRID</td>
<td>1</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
<tr>
<td></td>
<td>DB2_Q0KM</td>
<td>1</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
<tr>
<td></td>
<td>PHILLIE</td>
<td>1</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
<tr>
<td></td>
<td>CHRSTE</td>
<td>2</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
<tr>
<td></td>
<td>ABBI</td>
<td>1</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
<tr>
<td></td>
<td>DARCY</td>
<td>1</td>
<td>●</td>
<td>Not Assigned</td>
</tr>
</tbody>
</table>
### Risky users > Actions

Create ticket in ServiceNow

<table>
<thead>
<tr>
<th>Date</th>
<th>User</th>
<th>Score</th>
<th>Risk</th>
<th>DB User</th>
<th>Service</th>
<th>Assigned to</th>
<th>Ticket/Audit status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/19</td>
<td>VIDA</td>
<td>9.32</td>
<td>42</td>
<td>9.32</td>
<td>SIGRID</td>
<td></td>
<td>Not Viewed</td>
</tr>
<tr>
<td>9/19</td>
<td>DANIEL</td>
<td>9.32</td>
<td>42</td>
<td>9.32</td>
<td></td>
<td></td>
<td>Not Viewed</td>
</tr>
<tr>
<td>9/19</td>
<td>TILLIE</td>
<td>9</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td>Not Viewed</td>
</tr>
<tr>
<td>9/19</td>
<td>ELANA</td>
<td>9</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td>Not Viewed</td>
</tr>
</tbody>
</table>

**Create an incident report in ServiceNow...1 of 1**

**ServiceNow field**

<table>
<thead>
<tr>
<th>Short description</th>
<th>Computed value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>IBM Guardium risky behavior detected from user: BILL, Server IP:</td>
</tr>
</tbody>
</table>

**Options**

- Comments
- Assignment group
- Description
- Assigned to

**Button Options**

- Save
- Close
Dynamic Auditing policy

<table>
<thead>
<tr>
<th>Status</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Risk Spotter is running</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
</tr>
<tr>
<td>✔</td>
<td>Dynamic auditing (recommended)</td>
</tr>
<tr>
<td>✔</td>
<td>Enterprise search (required)</td>
</tr>
<tr>
<td>✔</td>
<td>Unit utilization data processing (required)</td>
</tr>
<tr>
<td>✔</td>
<td>S-TAP information (required)</td>
</tr>
<tr>
<td>✔</td>
<td>Database Protection Subscription service (recommended)</td>
</tr>
<tr>
<td>✔</td>
<td>Active Threat Analytics (recommended)</td>
</tr>
</tbody>
</table>

Related modules:
- Dynamic auditing
- Show policy template
- Upload file
- Disable
- Logs and status
IBM Guardium now provides integration with ServiceNow to provide a ticketing service to track tasks related to Guardium.

Users will now be able to create a ticket for:
• Any security assessment test failure
• Any alert
• Any active threat
• Any risk assessment

What’s New
• Ability to create a ticket as opposed to sending e-mail

Benefits
• Tickets can be assigned to groups
• E-mail service can be slow
• E-mail can get lost
• Ticket progress can be tracked
Setting up the connection to Seevice-Now

Edit account

- Type: ServiceNow
- URL: https://<username>/
- User name: guardium
- Password: *****

Test connection

Save
Close
Creating a Ticket

Create a ticket in ServiceNow

IBM Guardium database assessment failure: Default Accounts Pa:

Assessment name: VA-Oracle-10
datasource_id: 20007
datasource_name: gat-rh68db10-oracle
datasource_type: ORACLE
datasource_ip: [blank]
datasource_port: 1521
test_id: 2312
test_category: Authentication

Assignment group: Database

Additional field

Save  Close
# Automatic creation of Inspection Engine

New process for automatically synchronizing S-TAP inspection engines with discovered instances

<table>
<thead>
<tr>
<th>What’s New</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Discovered Instances Rules</td>
<td>Facilitate creating inspection engines for new database instances in large environments</td>
</tr>
<tr>
<td>Grdapi’s</td>
<td>Automated editing of S-TAP inspection engines</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Create, keep, update, delete inspection engines</td>
</tr>
</tbody>
</table>
Database Discovered Instances Rules

- Two global rule specifications
  - Separate rules for Linux-Unix S-TAP and Windows S-TAP
    - Pre-defined default
    - User-defined custom
Database Discovered Instances Rules

- Four types of custom rules in order of precedence
  - Exclude (delete)
  - Ignore (keep)
  - Replace (update)
  - Add (create)
IPV6 Support

Customers can choose to run their Guardium system in a traditional IPv4 only environment, IPv6 only environment or “dual” mode where the Guardium system can be configured for both IPv4 and IPv6.

What’s New

• The system can be configured to run in IPv6 network.
• The system can be configured to run in both an IPv6 and IPv4 environment, simultaneously.

Benefits

• The Guardium appliance features can now utilize data collected using the IPv6 protocol.
• The Guardium Appliance can utilize IPv6 with features such as backup/restore, ldap, datamart, data sources, Gim etc…
IPv6 vs IPV4

- IPv4, uses a 32-bit addressing scheme to support 4.3 billion devices
- IPv6, which instead uses 128-bit addressing to support approximately 340 trillion trillion devices
- IPv4 address method of four sets of one- to three-digit numbers, IPv6 uses eight groups of four hexadecimal digits, separated by colons
  - Example 2001:cdba:9abc:5678::/64
Use Cases for IPV6 Setting

IPv4 only: Guardium appliance can only run on an IPv4 network.

IPv6 only: Guardium appliance can only run on an IPv6 network.

Dual: Both the IPv4 and IPv6 are enabled allowing a user to configure network settings for each network type and the Guardium appliance can run on both networks simultaneously. Customer must have both IPv4 and IPv6 address configured.

The default ipmode is IPv4 only for both ISO install and GPU upgrade.
Infrastructure – Best Practices

• IPv6 Features require all devices to have an IPv6 address
• DNS Setup should resolve only 1:1 to make hostname lookups deterministic
• Hosts need DNS entries to allow features such as Hostname Aliasing
• Services may need to be bound to IPv6 protocols, such as FTP
Amazon AWS DBaaS – New Authentication types

[Image of a web interface for creating a cloud definition with options for Cloud DB Service Account, AWS Configuration, and an option to select IAM Role or IAM Instance Profile.

Please follow link to read more about AWS roles.

Architecture: Azure support

- DB
- VM Clients
- Event-hub
- Storage
- Guardium
Azure Supported Databases

- Azure SQL (database / server)
- Cosmos: SQL, Table, Gremlin, Cassandra, MongoDB
Guardium VA Supporting DataStax Cassandra

IBM Guardium VA Customers will now be able to scan multiple DataStax versions to detect and remediate vulnerabilities, such as:

- Excessive User & Group Privilege
- Mis-configurations and Default settings
- Privilege Escalation
- Un-patched Databases
- Old Versions, not supported by product
- OS file permission, ownership and group
- CVEs

What’s New

- Supporting DSE v5.1, v6.0 & v6.7
- Supporting JDBC connection
- Supporting native and LDAP authentication with SSL
- Providing CVE, latest version and patches from quarterly DPS
- Our VA solution for DSE Clusters can be run on all nodes.
- There are currently 83 new VA tests
Other VA enhancements in 11.1

- Run an Audit Process upon completion of a Security Assessment execution.
- Setup an Audit Process for Security Assessment from grdapi commands.
- Security Assessment deletion.
Unix STAP in 11.1

- Added Support for new platforms
  - RHEL 8 – ppc64le, s390x, & x86_64
  - Ubuntu 18.04 on s390x
  - Informix 14

- Support for **Oracle Unified Audit** (no need for an ATAP)
  - Pull data from Oracle with no need for a Kernel module and no need to restart the DB
  - STAP uses the OCI (**Oracle Call Interface**) libraries to communicate with the Oracle instance and pull data from the Unified Audit tables
  - OCI libraries support encrypted and unencrypted connections over TCP, as well as TCPS, BEQ, and IPC connections
External S-TAP Changes

• New Databases
  • MongoDB Atlas
  • RedShift
  • AWS Aurora PostgreSQL
  • AWS Aurora MySQL
  • Sybase ASE
  • Sybase IQ
  • Redis
  • DB2 Warehouse
• New Cloud vendor support
  • IBM

• Kubernetes namespace
  • GUI can deploy to non-default namespace

• Advanced Features Added
  • Firewall (S-GATE)
    • STAP config parameters for firewall only available after deployment
  • Redaction
  • S-TAP Terminate
    • Firewall, Redact, and S-TAP Terminate policies available in Policy Builder just like for classic S-TAP

Watch the installation video: https://youtu.be/etD_I8ngT_Y
Updated Supported Databases List

- Cloudera 6.2
- Greenplum 5.19 and 6
- Vertica 9.2
- CouchDB 2.3.1
- Informix 14.0 (Not supported in Windows S-TAP)
- Redis 5.04
- DB2 11.5
Mainframe Changes in 11.1

• IPV6 Support

• New out of the box Z reports and policies for:
  • DB2 on Z
  • IMS
  • Datasets

• Support for filtering on CONNECTION_NAME
Sankey Diagram for advanced investigation

Date

2017-01-08
2017-01-09
2017-01-10

OS User

Leroy
Abby
Wilmer
Lonl

Client Hostname

PROD_W/S03
HD_PROD4
PROD_W/S09
HD_PROD2
PROD_W/S06
TERMINAL

Source Program

JDBC1
JDBC2
Sankey Diagram for advanced investigation

Date | OS User | Client Hostname | Source Program
---|---|---|---
2017-01-09 | Leroy | PROD_WS03 | JDBC1
| | HD_PROD4 | |
| | Abby | PROD_WS09 | |
| | Wilmer | HD_PROD2 | |
| | Loni | PROD_WS06 | |
| | | TERMINAL | |
2017-01-10 | | | |
Sankey Diagram for advanced investigation
The real fun is just starting.
Go to the backup slides for all the details
Useful Links

• What's new in 11.1:

• New site for checking database and platform support (V11 and above only):

• Sankey video:
  • https://cdnapisec.kaltura.com/index.php/externalwidget/preview/partner_id/1773841/uiconf_id/39954662/entry_id/1_s5h1ldec/embed/dynamic