What's new in Guardium DAM V10: A technical overview

David Rozenblat
Director, Guardium Development
IBM Security

Kathy Zeidenstein
Guardium Evangelist and Community Advocate
IBM Security

September 17, 2015
Logistics

- This tech talk is being recorded. If you object, please hang up and leave the webcast now.
- We’ll post a copy of slides and link to recording on the Guardium community tech talk wiki page: http://ibm.co/Wh9x0o
- You can listen to the tech talk using audiocast and ask questions in the chat to the Q and A group.
- We’ll try to answer questions in the chat or address them at speaker’s discretion.
  - If we cannot answer your question, please do include your email so we can get back to you.
- When speaker pauses for questions:
  - We’ll go through existing questions in the chat
Guardium community on developerWorks

bit.ly/guardwiki

Important Bookmarks

- 4-Part series on Data Flow and Policy rules
- Deployment Guide for InfoSphere Guardium
- Tech Talk schedule and recordings

Members

View All (73 people)

Upcoming Events

- Tech Talk: Managing SOX Co...
  Aug 7 8:30 AM
- Tech Talk: Technical deep ...
  Aug 27 8:30 AM
- Atlanta-area user group
  Aug 28 9:00 AM

View All Events
Reminder: Next Guardium Tech Talk

Next tech talk: A Technical Overview of IBM Security Activity Monitor for Files

Speakers: Daniel Stanca, Product Manager
Sagi Shechter, Guardium Development Manager

Date and time: Thursday, October 15th
11:30 AM US Eastern (60 minutes)

Register here: https://ibm.biz/BdX5cZ

- Link to more information about this and upcoming tech talks can be found on the Guardium developerWorks community: http://ibm.co/Wh9x0o
- Please submit a comment on this page for ideas for tech talk topics.
Agenda

- Business overview
- Enhancement that support analysis
- Enhancements that support adaptability
- Enhancements that support protection
- Platform changes and upgrade roadmap - Important survey question
Data is challenging to secure

**DYNAMIC**
Data multiplies continuously and moves quickly

**DISTRIBUTED**
Data is everywhere, across applications and infrastructure

**IN DEMAND**
Users need to constantly access and share data to do their jobs
Guardium uses intelligence and automation to safeguard data

**ANALYZE**
Automatically discover critical data and uncover risk

**PROTECT**
Complete protection for sensitive data, including compliance automation

**ADAPT**
Seamlessly handle changes within your IT environment
ANALYZE. PROTECT. ADAPT.

Discovery, classification, vulnerability assessment, entitlement reporting

Encryption, masking, and redaction

Data and file activity monitoring

Dynamic blocking and masking, alerts, and quarantine

Compliance automation and auditing

IBM Security Guardium

Cloud Environments

Applications

Big Data Platforms

Databases and Data Warehouses

File Systems

ANALYTICS
Analyze
Analyze

- New navigation and user experience
- Quick Search for Enterprise and Investigation Dashboard
- Classifier enhancements (backup)
UI simplification and modernization

- Assignable tasks with SOD
- At a glance operational dashboards
- Guided Processes
- Enterprise wide Quick Search
- Customizable Reports
- Drill-down analytics
Demo
Banner

**To-do list**

**Notifications**

**Use to navigate through the UI or to search data or files (Quick Search)**

![Image of the banner with the To-do list, Notifications, and Quick Search features highlighted.](image-url)

*Take a tour and see what's new.*
Customizable navigation

Common navigation

Tools and reports related to the task
Report dashboard example

Important charts

- See tabular report
- Mark as favorite

- Customize display
- Configure runtime parameters

Same chart, customized
Report dashboard creation

- Type-ahead filter to quickly find reports / charts

- Additional filters
  - Favorites
  - Charts
  - User defined (not pre-defined) reports

- Select report / chart to add it to dashboard
Dashboard layout

- Customize layout into 1, 2, or 3 columns
- Drag and drop to move reports / charts
### Services Status: before and after

**Setup → Tools and Views → Services Status**

#### Centralized view of services

<table>
<thead>
<tr>
<th>Services Status</th>
<th>Filter By:</th>
<th>Running/Scheduled</th>
<th>Paused</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application User Translation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom ID Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Uploads</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flat Log Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guardian for 2/0S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Generation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inspection Engines</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP-to-Hostname Aliasing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Inference</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit Utilization Levels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload Key File</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Information Gathering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Information Results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Taps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guardian Definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Classes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module Installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Direct access to enable or disable the service

- **V9**
- **V10**
Accelerators now included in the base

Add roles to a user

Accelerators navigation menu
Managing permissions has never been easier!
Customizing navigation is a snap

Customize Navigation Menu for Role "Myfavoriteauditor"

Create a custom navigation menu by selecting available tools and reports from the left and copying them into a menu group on the right. Use drag and drop or the icon controls to add, delete, and rearrange items within the

Specify what will show up in navigation
Customized navigation

**Default navigation**

- IBM Guardium
  - Welcome
  - Setup
  - Manage
  - Discover
  - Harden
  - Investigate
  - Protect
  - Comply
  - Reports
  - My Dashboards

**Customized navigation**

- Reports
  - Welcome
  - Investigate
  - Comply
  - Reports

-Simplified, targeted layout for specific roles.
Lifecycle workflow: Discover, review, schedule, protect

- Creates a classification process and policy
- Creates a security policy
- Creates an audit process with receivers and a schedule.
Investigation Dashboard

- Color depth represents Intensity of usage
- Hover over cells for details
- Click a cell or title for interactive filtering

Click to view details in Quick Search without losing context.
Animation chart

Adds a time dimension to the investigation dashboard.

Size of bubble reflects amount of data

Hover over circle to see details.

Activity over the last 48 hours is replayed.
Adapt

- Enterprise load balancing
- GIM improvements for deployment and security
- Enhanced instance discovery
- S-TAP enhancements for performance and capability
- Auto-run dependent jobs for scheduled processes (backup)
- Database platform enhancements (backup)
- MongoDB as an audit repository (backup)
- Softlayer backup (backup)
- Troubleshooting enhancements (backup)
Enterprise load balancing

- Removes the headache of manually managing collector allocation for new S-TAPs
  - Configure S-TAP to connect to a Load Balancer on CM and let load balancer find an appropriate Managed Unit
- **Dynamically rebalances** workloads based on relatively current load data (such as sniffer queues)
- Complete redesign of 9.5 deliverable
Enterprise load balancer keeps track of how busy the collectors are

Two types of collection:
- Full load collection
- Single MU load collection

Full load collection happens dynamically (recommended) or statically

Single MU collection when load characteristics change (such as number of S-TAPs)

Rebalancing occurs only after full load collection
Using groups to create load balancing zones

Central Manager

Load Balancer

Load Map

MU 1=loaded

MU n= vacant

MU _Group1

MU _Group2

S-TAP Group 1

S-TAP Group 2

STAP 1

STAP 2

STAP 3

STAP n

STAP A

STAP B

STAP F

STAP n

Zone 1

Zone 2
Guardium installation manager (GIM) enhancements

- **Easier deployment of GIM clients**
  - From GIM server, remotely activate GIM clients that were installed in “listener” mode
  - Use GIM listener ‘auto discovery’ to find any servers that have GIM clients and activate (next slide)
  - Guardium admins don’t need access to the database server

- **Improved security using remote certification authority**
  - Install the GIM client with the relevant certificate information or update it using the GIM GUI or API.

- **Installer enhancements to specify failover GIM server when installing GIM Client for first time**
  - `--failover_sqlguardip <ip or hostname>`
GIM Auto-discovery process results in support of listener

The original scanned IP range/port

Specific IP where GIM listener is running

Host name where listener is running

"Check" to activate

Make the association

Auto-populated collector (default: localhost)
Enhanced instance discovery using S-TAP

- Removed dependency on Java and external libraries
- Enable on S-TAP installation:
  - Noninteractive install flag --use-discovery
  - GIM install – set STAP_USE_DISCOVERY to 1
- When S-TAP is installed, inspection engines will be configured for discovered instances
- After install, invoke process from S-TAP control
- Can also invoke inspection engine creation via API from Discovered Instances report
S-TAP enhancements

- S-TAP multithreading for intensive workloads such as warehouse
  - Preserves ‘threadedness’ from point of interception through to the collector
  - Configure using participate_in_load_balancing = 4 and specify sql_guard sections up to 5 - this determines number of main threads
  - No failover support in this release.

- 64-bit UNIX/Linux binaries, which increases amount of data that can be buffered (approx. 2GB per collector IP)

- Recommended performance parameters turned on by default
  - ktap_fast_tcp_verdict: Port information loaded into K-TAP on startup
  - ktap_fast_shmem_verdict: Used for DB2 shared memory improvements

- New platforms
  - RHEL 7 x86_64
  - SUSE 12 x86_64
  - Ubuntu 14 x86_64
  - Debian (supported via Ubuntu installer)
  - Dropped support for AIX 5.3, SLES 9, Solaris 9
Guardium supports complex IT environments …

Examples of supported databases, Big Data environments, file shares, etc
Protect
Protect (Advanced)

- Fine grained access control
- Blocking and redaction for Hadoop queries from Hive and Impala (Backup)
Fine-grained access control

Protect sensitive data without impacting your business

Use cases:
- Outsource production DB access
- Protect PII from privileged users
- Testing on production data
- Honey pot

Supported databases: DB2 (LUW), Oracle, SQL Server
Fine-grained access control architecture

1. User issues SQL
2. STAP holds SQL and checks policy rules for conditions.
3. If conditions are met, Guardium rewrites query and sends to S-TAP
4. S-TAP releases rewritten query to database server.
5. Results are sent back to user.

FGAC and firewall cannot be used on same session.

Rule actions: query rewrite attach, query rewrite apply definition, query rewrite detach
Workflow through runtime

1. Create query rewrite definition...

Rewritten query: `select * from customer WHERE CUST_TYPE <> 'GOVERNMENT'

2. Create security policy...

When database type = Oracle and User = Joe and Object = Customer… then

3. Joe queries the Customer table...

Do not return rows of Government customers
**Use case: Production database for testing**

Exposing a database to a production environment for testing purposes without exposing private data.

<table>
<thead>
<tr>
<th>Before – Displaying all values in the database</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL&gt; select ssn from customer_demo1;</td>
</tr>
<tr>
<td>SSN</td>
</tr>
<tr>
<td>112-34-5678</td>
</tr>
<tr>
<td>123-45-6780</td>
</tr>
<tr>
<td>123-45-6781</td>
</tr>
<tr>
<td>123-45-6782</td>
</tr>
<tr>
<td>123-45-6783</td>
</tr>
<tr>
<td>123-45-6784</td>
</tr>
<tr>
<td>123-45-6785</td>
</tr>
<tr>
<td>123-45-6786</td>
</tr>
<tr>
<td>123-45-6787</td>
</tr>
<tr>
<td>123-45-6788</td>
</tr>
<tr>
<td>123-45-6789</td>
</tr>
<tr>
<td>11 rows selected.</td>
</tr>
</tbody>
</table>

| SQL> select email from customer_demo1;        |
| EMAIL                                         |
| Joe.Antany@abcd.gov                          |
| Joe.Thomas@abcd.gov                          |
| Joe.Antany@abcd.gov                          |
| Joe.Jones@bank.com                           |
| Joe.Murphy@bank.com                          |
| Joe.Smith@abcd.gov                           |
| Joe.King@telco.net                           |
| Joe.Lynch@telco.net                          |
| Joe.Lee@nonprofit.org                        |
| Joe.Davis@health.com                         |
| Joe.Wilson@health.com                        |
| 11 rows selected.                            |

<table>
<thead>
<tr>
<th>After – Guardium uses fine grained access control to change columns / mask data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query rewrite report shows actual runtime queries.</td>
</tr>
</tbody>
</table>

| SQL> select email from customer_demo1;        |
| EMAIL                                         |
| Joe.Antany@abcd.gov                          |
| Joe.Thoma...                          |
| Joe.Smith...                          |
| Joe.Jon...                          |
| Joe.Mur...                          |
| Joe.Sha...                          |
| Joe.Kin...                          |
| Joe.Lyn...                          |
| Joe.Lee...                          |
| Joe.Day...                          |
| Joe.Wil...                          |
| 11 rows selected.                            |
Use case: Multi tenancy Scenario

Enhance access controls in which multiple users and applications share a single database.

- Display data based on runtime parameters (eg USER)
- Enhance existing access controls

Rows and columns returned for non-government customers

User TSHIRAI cannot see name or birth date

User ADMIN cannot see name
Benefits of fine-grained access control

- Dynamic data masking at database layer
- May reduce dependence on test data systems
- Support multi-tenancy environments
- Does not require the involvement of the DBA
- Centralized policy for supported database types (MS SQL, Oracle, and DB2)
Upgrade/migration roadmap
Appliance technical specs

- Underlying appliance OS upgraded to RHEL v6.5 64-bit version (v9.5 RHEL 5.11)
- MySQL DB version upgraded to v5.6.24
- RAM - Minimum 24GB
- CPU/vCPU – Minimum 4 cores
- HD – Minimum 300 GB
  - Upgraded system hard drive range (300 < 2 TB)
  - Newly built system (300 GB to >2TB (MUCH GREATER)
Upgrade limitations

*Upgrade procedure limitations*
- V10 upgrade patch available only for 64-bit version appliances at GPU level v9.0p200 or higher
- Upgrade procedure is not available for customers with customized partitions
- Upgrade procedure does not support resizing or realignments of the partitions.

*Restore from system backup stored in previous version*
- V10 supports restoring system backup file from any v9.x version.
Upgrade roadmap

See the V10 Knowledge Center upgrade topic for more details.

For a limited time: Customers on 64-bit 9.5 environments may be eligible for a controlled upgrade program for a limited number of appliances. Send a note to Carrie Rogers (carriero@us.ibm.com) to see if you are eligible.

<table>
<thead>
<tr>
<th>Source appliance</th>
<th>Transition path to V10 appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rebuild/Restore backup</td>
</tr>
<tr>
<td>64-bit v9.0p200 or later</td>
<td>yes</td>
</tr>
<tr>
<td>32-bit v9.0200 or later</td>
<td>yes</td>
</tr>
<tr>
<td>v9.0 - v9.0p100</td>
<td>yes</td>
</tr>
<tr>
<td>v8.2 or earlier</td>
<td>no</td>
</tr>
</tbody>
</table>
Important survey question

- If you are currently running 32-bit Guardium, would you be interested in having IBM services contact you about a migration to Version 10?
  1. Yes
  2. No
  3. N/A (We have 64-bit Guardium)
  4. N/A (I am an IBMer or BP)
Guardium supports the whole data protection journey

- **Comprehensive data protection**: Dynamic blocking, alerting, quarantine, encryption and integration with security intelligence.
- **Sensitive data discovery**: Perform vulnerability assessment, discovery and classification.
- **Address data privacy**: Find and address PII, determine who is reading data, leverage masking.
- **Expand platform coverage**: Big data platforms, file systems or other platforms also require monitoring, blocking, reporting.
- **Acute compliance need**: Database monitoring focused on changed data, automated reporting.

Sensitive data discovery also requires monitoring, blocking, reporting.

Database monitoring focused on changed data, automated reporting.

Sensitive data discovery also requires monitoring, blocking, reporting.
Resources

- **V10 Overview webcast** (includes activity monitoring for files)
- **Overview Solution Brief**
- **DAM solution brief**
- **Announcement letter**
- **Detailed Release notes**
- **System requirements**
- **DeveloperWorks article – coming soon!**
- **UI demo on YouTube** (more coming)
- **High level Upgrade Roadmap**

Activity Monitoring for Files resources:

- **Activity Monitoring for Files Demo on YouTube**
- **Supported files for FAM**
Information, training, and community cheat sheet

- **Guardium Tech Talks** – at least one per month. Suggestions welcome!
- **Guardium YouTube Channel** – includes overviews, technical demos, tech talk replays
- **developerWorks forum** (very active)
- **Guardium DAM User Group on Linked In** (very active)
- **Community on developerWorks** (includes discussion forum, content and links to a myriad of sources, developerWorks articles, tech talk materials and schedules)
- **Guardium on IBM Knowledge Center** (was Info Center)
- **Deployment Guide for InfoSphere Guardium Red Book**
- **Technical training courses** (classroom and self-paced)

IBM Security Guardium Virtual User Group. Open, technical discussions with other users. Not recorded!

Send a note to krzeide@us.ibm.com if interested.
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security
Classifier enhancements

- Classifier has seen an upsurge of interest from the user community
- Improvements in user experience, performance, and management of false positives

One match per column
Classifier will record the first hit for any given column and ignore it thereafter for subsequent rules.

Easy to set up exclusion groups
## Database platform support highlights

NOT a complete list.

<table>
<thead>
<tr>
<th>Database</th>
<th>Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 LUW</td>
<td>UID chain captured through DB2_Exit</td>
</tr>
<tr>
<td>DB2 for i</td>
<td>TLS encryption to collector and S-tAP-based load balancing</td>
</tr>
<tr>
<td>z/OS platforms</td>
<td>Multi-stream load balancing. Quarantine for DB2 users. (many more to be covered in a separate talk).</td>
</tr>
<tr>
<td>Hadoop</td>
<td>Improved collection/parsing (targeted inspection engines). Blocking and redaction for Hive and Impala. (will be covered in detail in a separate talk)</td>
</tr>
<tr>
<td>Informix</td>
<td>New exit (ifxguard) for Informix shared memory processing (replaces A-TAP). Supports firewall (blocking) and UID chaining. Informix 12.10xC5W1 and later.</td>
</tr>
<tr>
<td>Oracle</td>
<td>Added SSL for 12c. Added ASO for Windows 12c</td>
</tr>
<tr>
<td>Sybase</td>
<td>Added support for 16</td>
</tr>
<tr>
<td>Sybase IQ</td>
<td>Added shared memory support via A-TAP</td>
</tr>
<tr>
<td>Teradata</td>
<td>Added support for 15.10 including A-TAP for encrypted user names and traffic</td>
</tr>
</tbody>
</table>

NOT a complete list.
MongoDB as audit repository

- For use cases such as:
  - Post processing audit data
  - For longer online retention requirements
- Audit data is written simultaneously to Guardium repo and JSON files on collector
- Use grdapi to send JSON data to a MongoDB database
Job scheduling dependency management

- Helps ensure accurate data before running a job (eg groups populated from classifier)
- Applies to all ‘schedulable’ jobs (audit processes, policy installations, group population from query…)
- Scheduler will automatically find all the subordinate jobs and run them in order
  - For example, group population for groups in the policy should run first
- There is a retry sequence in case of a failure (default is 3 tries)
- APIs to list job dependency tree, scheduled jobs, job dependencies….

![Create New Audit Process](image-url)
Softlayer as a backup store
Supportability enhancements

- Banner notifications
  - Low system memory (RAM)
  - Quick Search memory + CPU cores minimum requirement
  - Certificate expiration (mysql, GUI, GIM, etc.)
  - Central Management failure
  - SSLv3 enabled
  - No License
- Improved user-friendly license acceptance process through UI
- Centralized supportability and troubleshooting tools in Manage>Maintenance
- See tech talk “Best kept secrets of Guardium supportability” for other items you may not be aware of. Contact Kathy Zeidenstein for replay links and slides.
Hadoop blocking (Hive/Impala) (S-GATE TERMINATE)

1. Policy: Block privileged user access to customer data through Hive

2. Privileged user attempts to read customer data and is blocked

3. Access attempt is reported as a policy violation

Important: Because of the way Hive and Impala traffic is processed in Hadoop, you must do the following in the blocking policy rules:

- Specify the DBTYPE in the blocking (S-GATE ATTACH and S-GATE TERMINATE) policy rules; that is, either Impala or Hive.
- Ensure that ATTACH happens on a combination of user and object/command.
Hadoop Redaction (Hive / Impala)

Important: Specify Hive or Impala in DBTYPE for Redact rules

Masked Hive data in Hue/Beeswax

Masked Hive data command line
Query rewrite workflow

Create query definitions based on what you want to control
- Restrict columns
- Restrict rows
- Limit what users can do
- Restrict what user can access
- Completely replace part or all of a query

Test the query rewrite definitions with real test queries.
(Note, you will likely need to use policies to fine tune the behavior)

Determine the conditions in which to rewrite the query
- specific users, client IPs, objects, commands?

Validate runtime effect in a QA environment

Query Rewrite Builder

Policy Builder

Query rewrite report
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 in connection with 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 PARTICULAR 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.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml