The Case of the Missing DB Users:

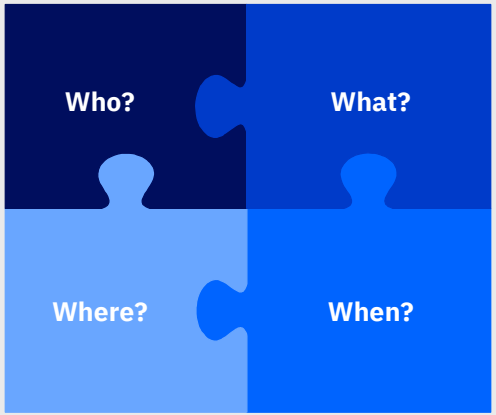
Troubleshooting DB USER issues in IBM Security Guardium Data Protection

Monitoring Access

The DB User is a critical piece in answering the most basic audit questions.

- What was done?
- Who accessed the data?
- When did it happen?
- Which data were affected?

Program
DB User
OS User



Commands

Objects
Fields
Services

Access Period
Session Start

Root Cause: the login packet.

Packets were dropped.

- Analyzer Queue
- Logger Queue
- STAP buffer
- KTAP buffer
- Network Issue

Login packet can't be read.

- ATAP or other decryption issue
- Protocol limitation
- Parsing bug

Session started when STAP wasn't running.

- Login only sent once, at the start of the session
- Session may be open for months
- Common for pooled connections

New resources to help with an old, common problem.

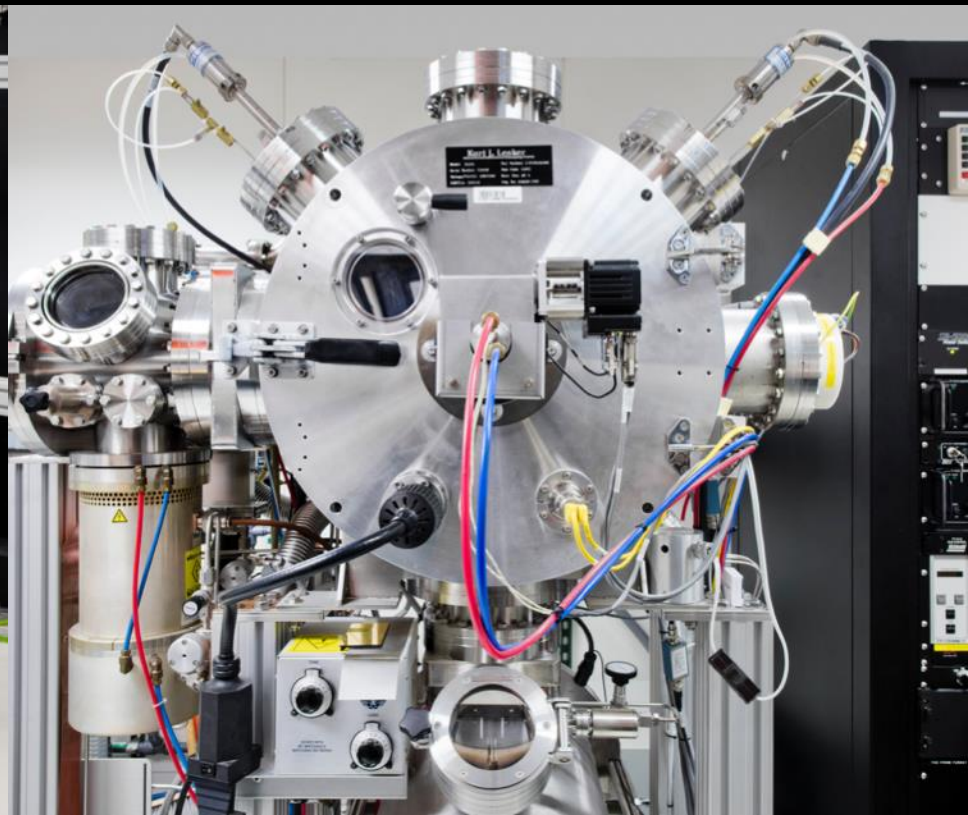
In August 2018 the Guardium team published …

“How to troubleshoot Guardium missing DB User problems”

- Technote #0719941
- Youtube video demonstration
- Downloadable dashboard for Guardium GUI
- Link:

www.ibm.com/support/docview.wss?uid=ibm10719941

Analysis you can do on your own



Getting Started

Understand the issue by answering questions like …

- What percentage of sessions are missing the DB USER? All? Most? Just a few?
- Are those sessions also missing SOURCE PROGRAM?
- Is the issue coming from many STAPs or just one?
- Is a specific protocol or DBMS type affected?
- Is the issue random or consistent?
- Does it happen at specific times each day?

Read the technote.

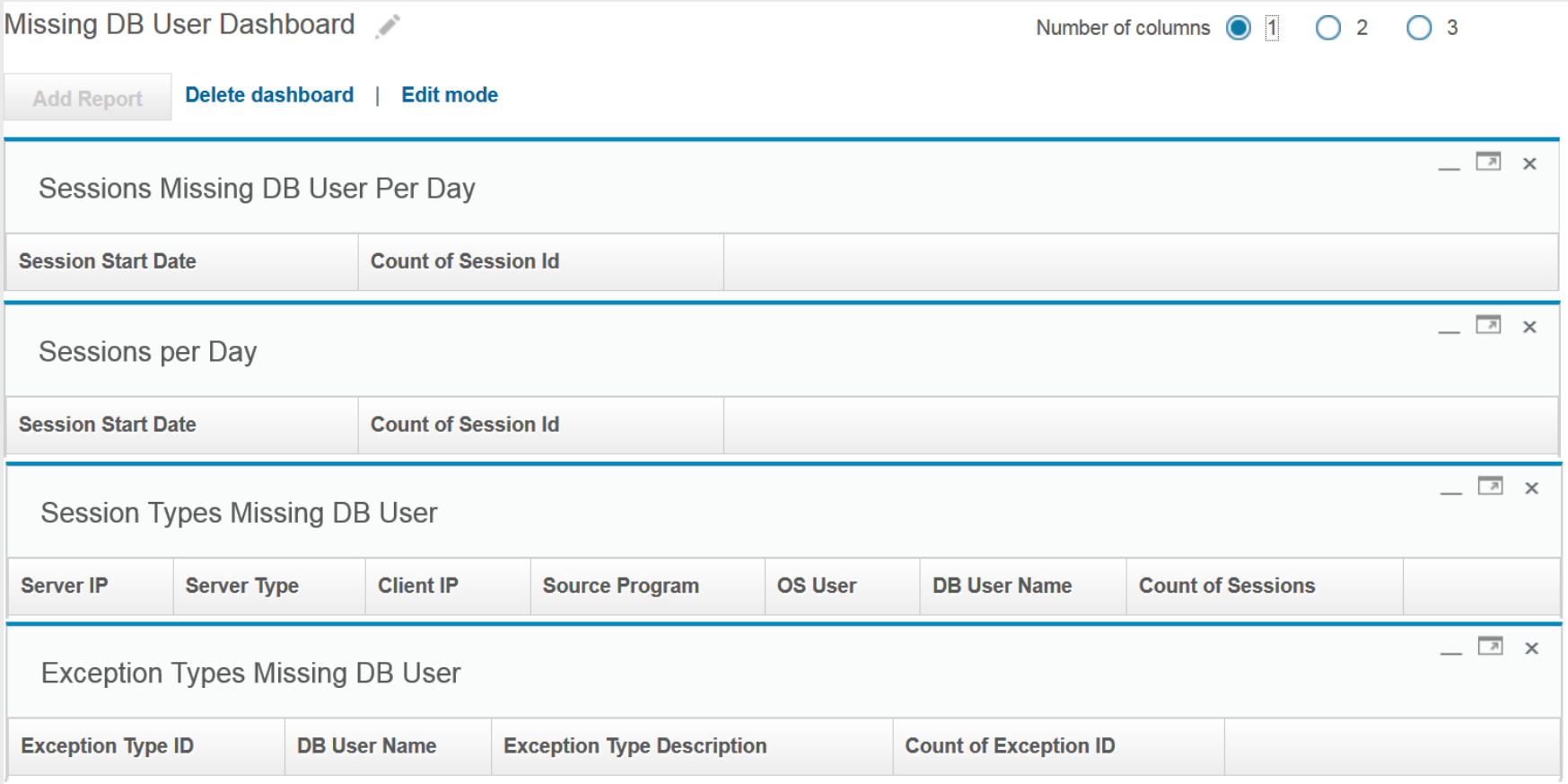
Watch the video.

(25 minutes)

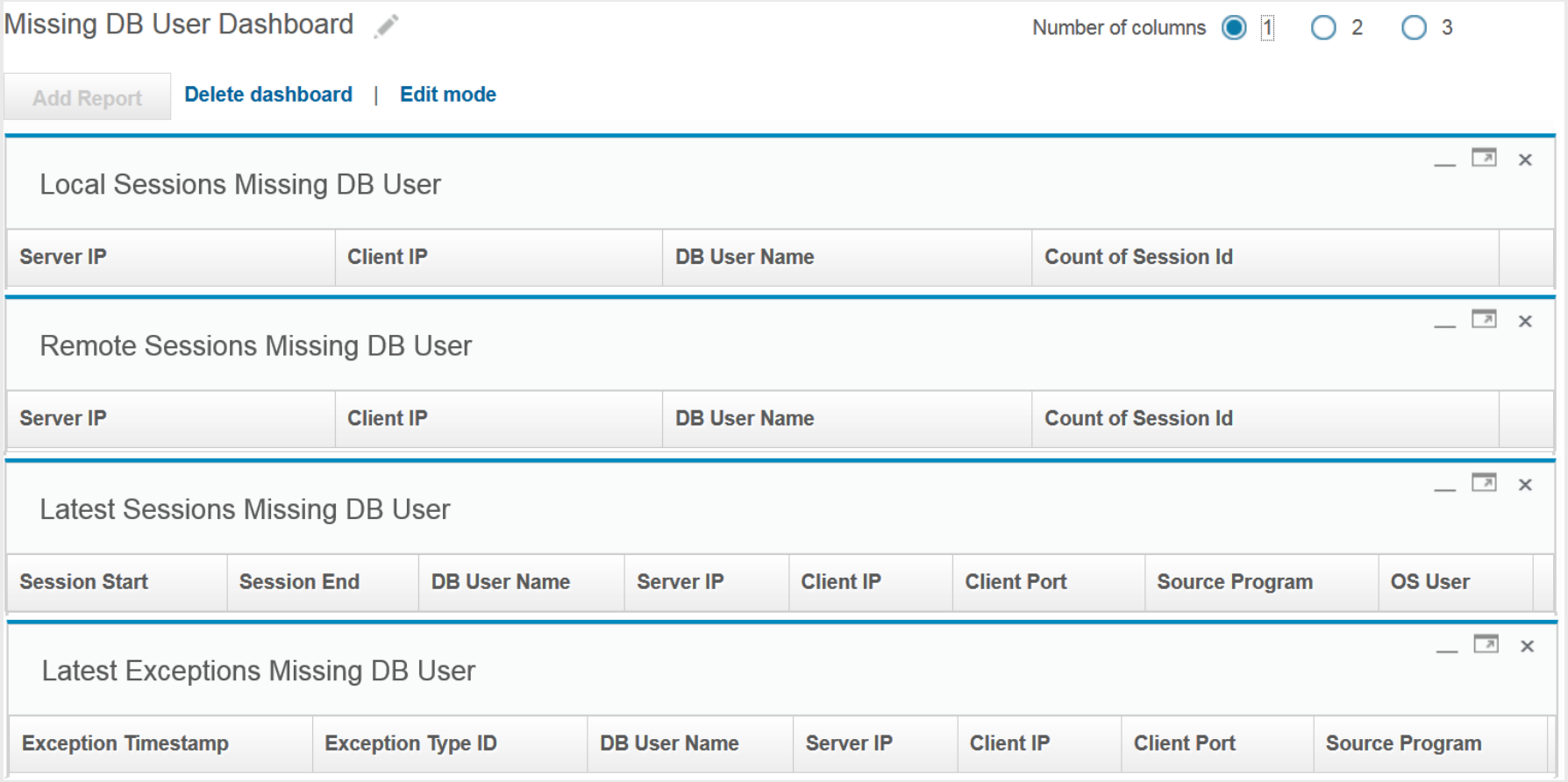
Download the dashboard.

Import it on your Central Manager.

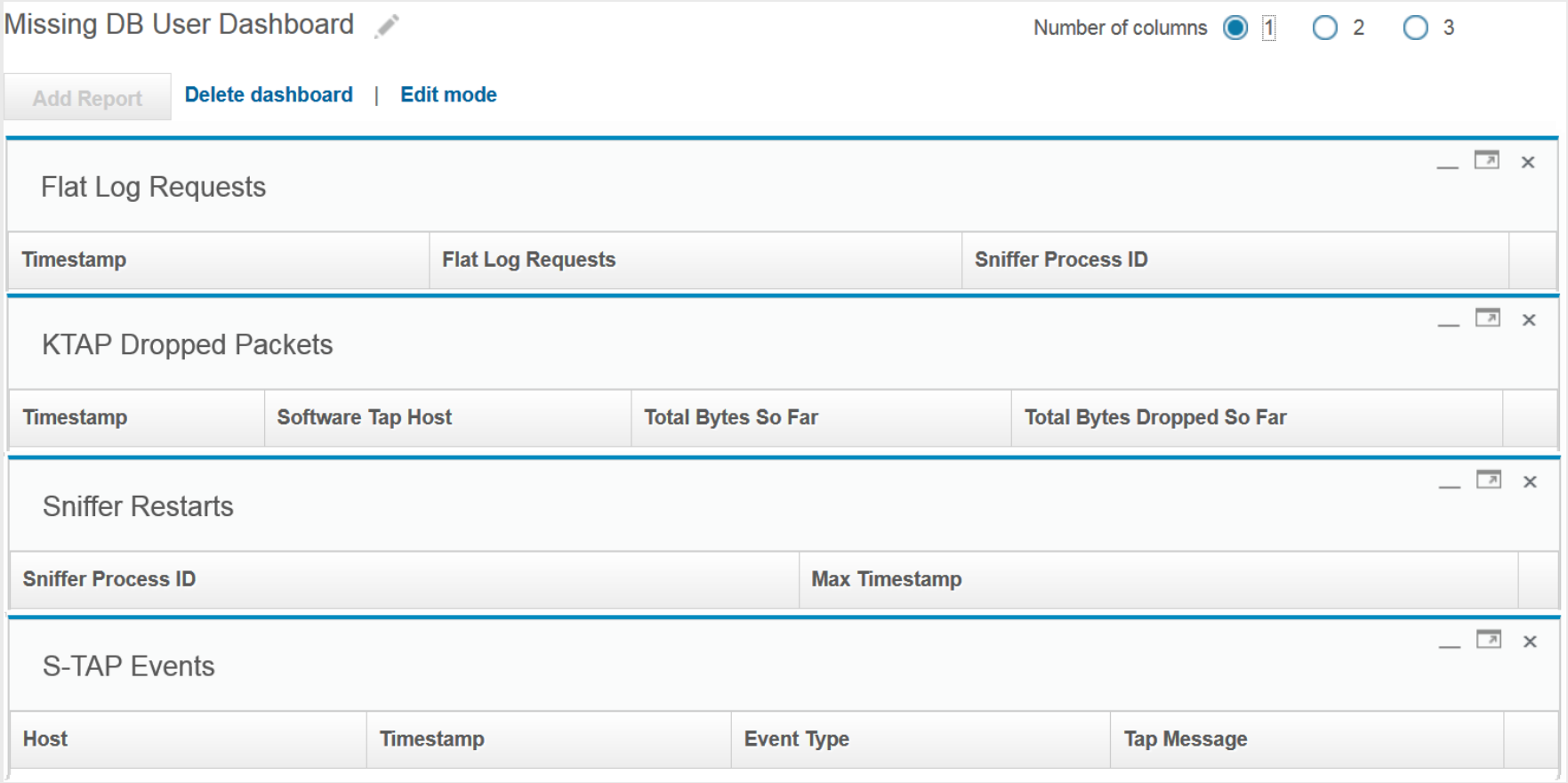
Dashboard


Missing DB User Dashboard
Number of columns 1 2 3
Add Report
Delete dashboard | Edit mode
Sessions Missing DB User Per Day
Session Start Date
Count of Session Id
Sessions per Day
Session Start Date
Count of Session Id
Session Types Missing DB User
Server IP
Server Type
Client IP
Source Program
OS User
DB User Name
Count of Sessions
Exception Types Missing DB User
Exception Type ID
DB User Name
Exception Type Description
Count of Exception ID

Dashboard


Missing DB User Dashboard
Number of columns 1 2 3
Add Report
Delete dashboard | Edit mode
Local Sessions Missing DB User
Server IP
Client IP
DB User Name
Count of Session Id
Remote Sessions Missing DB User
Server IP
Client IP
DB User Name
Count of Session Id
Latest Sessions Missing DB User
Session Start
Session End
DB User Name
Server IP
Client IP
Client Port
Source Program
OS User
Latest Exceptions Missing DB User
Exception Timestamp
Exception Type ID
DB User Name
Server IP
Client IP
Client Port
Source Program

Dashboard


Missing DB User Dashboard
Number of columns 1 2 3
Add Report
Delete dashboard | Edit mode
Flat Log Requests
Timestamp
Flat Log Requests
Sniffer Process ID
KTAP Dropped Packets
Timestamp
Software Tap Host
Total Bytes So Far
Total Bytes Dropped So Far
Sniffer Restarts
Sniffer Process ID
Max Timestamp
S-TAP Events
Host
Timestamp
Event Type
Tap Message

Case Studies

Using the dashboard reports to solve real customer issues.

Case study: STAP Overflow

A single Windows host showed missing DB USER for a few sessions, all starting between 20:00 and 20:10 every day.

Most sessions starting at that time had a DB USER.

Root Cause

At 20:00 daily a busy application was restarted. The STAP buffer overflowed in the sudden burst of traffic and lost a few login packets.

After a few minutes, the STAP caught up and the issue went away.

Solution

Use v10.5 STAP which can prioritize login packets during high-traffic periods.

Performance issues are random or occur at specific times. Both DB User and Source Program will be blank.

Case study: Sniffer Overflow

Many sessions from many hosts on one collector were missing DB USER.

Session start times were random but occurred in clusters.

Sniffer restarts were found near the time these sessions started.

Root Cause

The collector was overloaded. When the Logger Queue hit its memory limit it dumped tens of thousands of packets.

Solution

Enable flat log processing.

Load balance the collector.

Use policy to SKIP LOGGING when appropriate.

See technote #1994083

Sniffer load issues affect random sessions from several hosts.

Case study: Sniffer Crash

Many sessions from many hosts on one collector were missing DB USER.

Sniffer restarts were found near the time these sessions started.

The issue started shortly after a sniffer patch was applied.

Root Cause

The sniffer was crashing. The snif.log and syslog showed SEGFAULTs at the time the sniffer restarted.

must_gather sniffer_issues

Solution

This was a bug which required a new sniffer patch.

Snif crashes often happen when traffic load is low.

Check the Buff Usage Monitor!

Check the Session Start times for affected sessions.

Check times when the TID changed.

- Analyzer Queue
- Logger Queue

Check Flat Log Requests value.

Is it growing?

If TID changed and traffic was low, check logs for SEGFAULTs.

- Syslog (messages)
- Snif.log

Case study: Timing Issue

DB USER was missing for all user sessions from an application, but sessions by the DBA on that host had a DB USER.

All were local connections with a session start shortly after the STAP for this host was installed.

Root Cause

These sessions were pooled connections which existed prior to STAP starting. We never saw the login because it happened months before STAP was installed.

In this case, session start time had to be inferred.

Solution

Restart the pooled connections while STAP is running.

Timing issues can be traced to specific applications.

Case study: Encryption

All traffic from a specific Oracle instance was missing DB USER.

Sessions from other Oracle hosts on the same collector consistently had DB USER.

Root Cause

The Oracle instance used encryption, so the collector could not read the DB USER.

Solution

Enable ATAP.

Encryption issues affect all traffic from a specific database.

Case study: Protocol Issue

DB USER was ‘?’ for some sessions from an Oracle host, but many sessions from that same host had the DB USER.

The number and timing of the affected sessions was random.

No SQLs were run in these sessions.

Root Cause

Exception reports showed Oracle exceptions ORA-12505 or ORA-12514 for these sessions.

See technote #2008887.

Solution

This is working as designed.

These are failed connections to the database and Oracle does not provide a DB USER Guardium can use.

Protocol issues are random but always affect the same DBMS type.

Case study: Protocol Issue

DB USER was missing for some Oracle sessions, but many sessions had a DB USER.

The timing was random, but all were local connections.

Source Program was captured.

SQLs were run from these sessions.

Root Cause

These sessions used Oracle OS user authentication.

See technote #2008755

Solution

This is a protocol limitation.

Oracle does not provide a DB USER Guardium can use in these cases.

Protocol issues might only affect specific Source Programs or Client IPs.

Questions and Discussion