From (near) Zero to Advanced Database Security

JANUS
PROFESSIONAL SERVICES

mediaMENTE
consulting

- Oracle Database & Near Zero Security → FALSE!
- DB supports several authentication services (password, external, kerberos…), no one can login anonymously and take any action
- DB implements RBAC: users can do only what they are explicitely allowed (system/object/role privileges)
- Several powerful roles exist by default
- SYSDBA can do everything on database.
- <u>Weak security depends on a uncorrect usage of privileges, it's a human fault and not database fault</u>

- How to improve security
  - Assess privileges assigned to users (least privilege)
  - Pay attention to powerful system privileges
  - Use database roles for an effective management
  - Enable database auditing
  - Protect audit trails (e.g. SYSLOG)
- Tools:
  - Database Security Assessment Tool (DBSAT)
  - Database Vault Privilege Analysis (12c+)
- Evaluate/implement Advanced Security features

Five W’s and H

- *Who* was involved?
- *What* happened?
- *Where* did it take place?
- *When* did it take place?
- *Why* did that happen?
- *How* did it happen?

We have to make sure we’ll be able to answer, but most important we have to make sure we have full control on what’s happening on our systems

Prevent / Analyze

- How a DBA, or security officer, can answer «Five w's and H» questions?
- How a DBA, or security officer, can be sure that
  - every answer is correct?
  - every action has been taken to guarantee full control of what's happening to our data?

- How to answer: Need to trace every action over our data.
  - What are the impacts on databases?
  - What are the impacts on db operations?
  - What are the impacts on applications?

- How to prevent malicious activities: Need to design for security.
  - Which data within the database?
  - How it’s to be accessed, and by whom?
  - What are the impacts on our database system?

Who was involved?

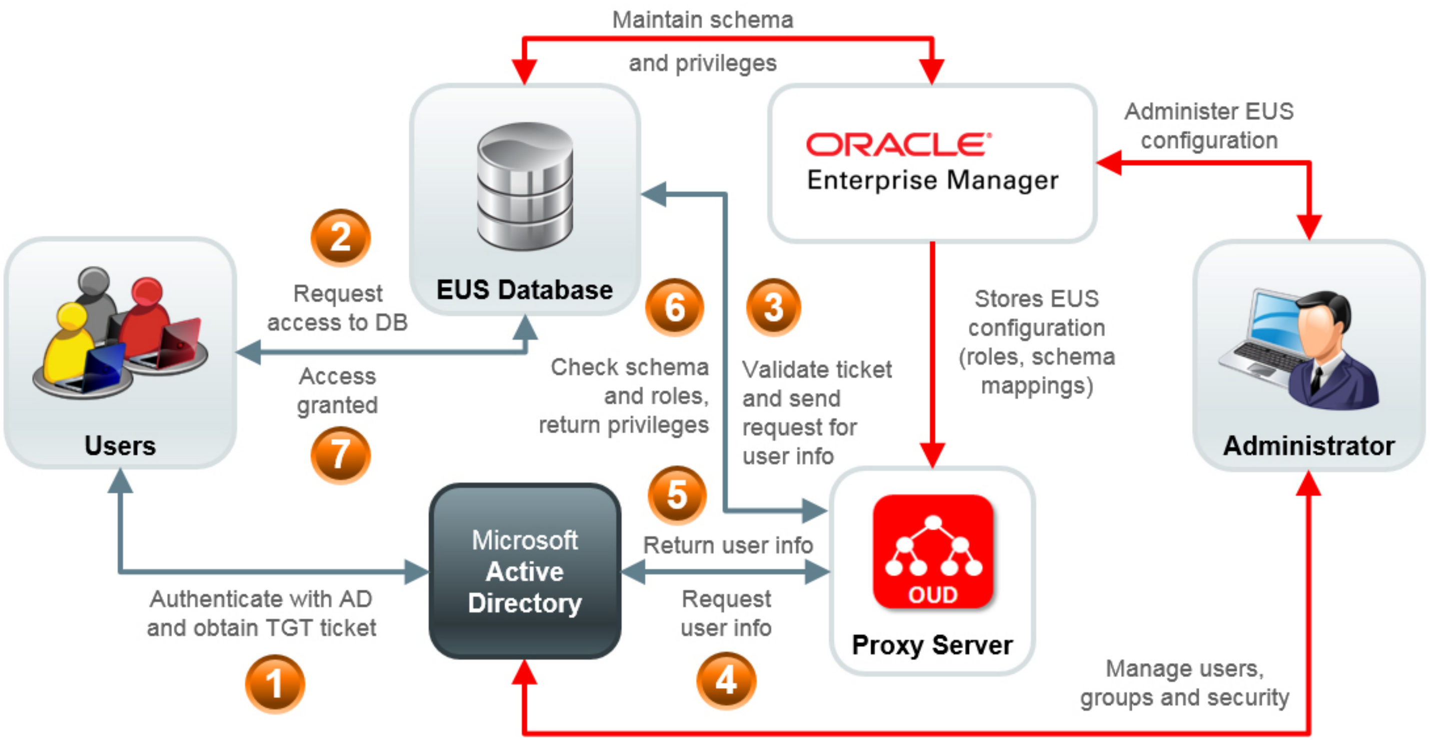
- Need to know who has access to database and data within.
- Take care of authentication methods
- Properly configure your users with well defined profiles
- Evaluate all authentication methods:
  - Database
  - External (OS and/or Kerberos)
  - Global (Enterprise User Security)

JANUS PROFESSIONAL SERVICES

mediaMENTE consulting

- Oracle Database demands authentication of users to an external authority (LDAP Server)
- Enables centralization of database access management (both authentication and authorization)
- Requires Oracle Unified Directory
- Users' identities can be stored in the standard corporate LDAP server (typically Microsoft Active Directory)
- Users' Privilege Management can be completely managed on Active Directory

EUS – Authentication and Authorization flow



Enterprise User Security - Impacts

- Another system to be managed (OUD)
- DBAs do not directly control privileges assigment
- Need to keep privileges (Global Roles, Proxy Users) on db synchronized with EUS typical entities (Enterprise Roles, Proxy Permissions) on OUD
- Need to update DB Access Management processes accordingly with new infrastructure

JANUS PROFESSIONAL SERVICES

mediaMENTE consulting

What happens?

- It depends on what your users are allowed to do
- Apply the «Least Privilege Principle»
- Apply the Segregation of Duties (read-only profiles, read-write profiles, and so on)
- Enforce Segregation of duties and fine grained data access control (*) by using Oracle Database Vault

(*) Table level

- Segregation of duties between DBA and Security administrators
- Enhanced security against insider threats:
  - Security administrators can «limit» DBA privileges so that business data cannot be accessed by them
  - Application owners can be (and should be) responsible of privileges on business data (DBA cannot grant no privileges on business data)
  - Powerful commands can be disabled through well defined command rules

- *Who* was involved?
  - Use DB Vault Realms to protect business data, together with Rule Sets and Rules to strictly control who can access them (these authorizations enforce RBAC)
- *What* happened?
  - Use Command Rules to eventually disable commands
- *Where* did it take place?
  - Use Factors to enable access to data from a well defined set of IP addresses

JANUS PROFESSIONAL SERVICES

mediaMENTE consulting

- *When* did it take place?
    - Use Factors to enable a well defined subset of commands in a well defined timeframe only
- *Why* did that happen?
    - Configure logging on Realms, either on rules’ violation or on successful evaluation of them
- *How* did it happen?
    - Analyze Database Vault’s audit trail

- Existing processes (deploy, management, data movement) should be rewritten in order to comply with new restrictions
- SYSDBA is not as powerful as usual (cannot CREATE/DROP/ALTER users and profiles)
- DB Management now involves both DBA and Security office

Auditing

- Privilege Management, Access Control, Database Vault are useful/required to prevent unauthorized access to data.
- Security and recent regulations (IT privacy law, GDPR) require that actions performed on data must be audited as well, especially if performed with ad-hoc tools (SQL*Plus, SQLDeveloper, …)
- Database Auditing is the answer.

Oracle Database Auditing

- Available on every edition of RDBMS
- Proper setup is required to avoid overhead in terms of performance and availability
- Fine tune Auditing:
  - Personal users
  - Administrative access (DBA)
  - Consider Fine Grained Auditing (e.g. audit all queries with a specific WHERE condition)

JANUS PROFESSIONAL SERVICES
mediaMENTE consulting

- Ensure you audit trail is protected
  - Use SYSLOG
  - Protect database audit trail with Database Vault
  - Use Unified Auditing (rel. 12c+, suggested starting from 12.2)
- Develop reports and alerts on Audit trails
  - Analyze audit data
  - Catch/Analyze unauthorized access
- Oracle Audit Vault & Database Firewall

- Oracle Database Access Management: consolidate management of database privileges at enterprise level, leveraging the existing Active Directory privilege management:
    - Enable EUS on databases
    - Integrate OUD with MS AD
    - Configure EUS entities on OUD and Databases
    - Users' db privileges are inherited from MS AD group membership. Enterprise's Access Management team is responsible of database access

- Oracle Database Access Management and Segregation of Duties:
    - Integration of EUS with Database Vault

JANUS PROFESSIONAL SERVICES

Via Roma n. 235, 09123 Cagliari (CA)
info@janusps.com

MEDIAMENTE CONSULTING

via Piovola 138, 50053 Empoli (FI)
T + 0571 9988 | **F** + 0571 993366