Oracle ACE Director

Strategic Security Planning for EBS: Key risks and recommendations for business users and the technical team

Name: Susan Behn
Company: Rite Software
Title: ERP Strategy & Transformation, Oracle Ace Director
LinkedIn Handle: susan-behn-a9597b3

Oracle ACE Director

Agenda

- Introduction
- Assessing Cybersecurity Insurance: Ensuring comprehensive coverage for releases in sustaining support.
- Beyond the Firewall: Mitigating Inside Threats.
- Unraveling the Patching Dilemma: Understanding security patch availability for databases below 19c.
- Proactive Contingency Planning: Safeguarding against the next log4j threat.
- Access Management and Compliance: Developing processes for seamless access during key user absences, aligning with SOX and other regulatory standards.
- E-Business Suite Security Readiness Analyzer
- HTTPS/TLS and JAR Signing Certificates -- Explained

Panel Members

- Susan Behn, Rite Software, susan.behn@rite.digital
- Michael Barone, OATC, michael.barone@oatcinc.com
- David Channell, OATC, david.channell@oatcinc.com

Cybersecurity Insurance
Are you protected?

Cybersecurity Insurance & Liability

- **Coverage** may be limited based on risk profile – Keep your risk low by staying current on patching
  - Risk profile could be higher for customers with database or applications on sustaining support
- **Compliance** – Some insurance policies may require supported software versions
  - Make sure whoever buys insurance is aware of support dates and potential impact
  - Schedule a quarterly review meeting to review status/risks to maintain awareness
- **Cost** – Premiums and deductibles are higher for higher risk profiles
- **Exclusions** – policies may exclude certain types of risks related to a breach originating on unsupported systems
- **Claims** – In the event of a cybersecurity incident, claims may be subject to scrutiny to determine whether the insured organization took reasonable steps to mitigate risk.
  - Insurance adjusters are becoming more educated to ask pertinent questions
- **Business partner compliance** – (customers, suppliers, other) may require cybersecurity insurance coverage to do business or may require all systems are eligible for support including security patches
  - Are you compliant with customer requirements?
- **Liability** - Are you liable to your employees/customers if there is a cyberattack?
  - Are you negligent if your systems are at risk/out of date?
  - How many free credit monitoring letters did you get this year and did you read the fine print?

Mitigating Threats

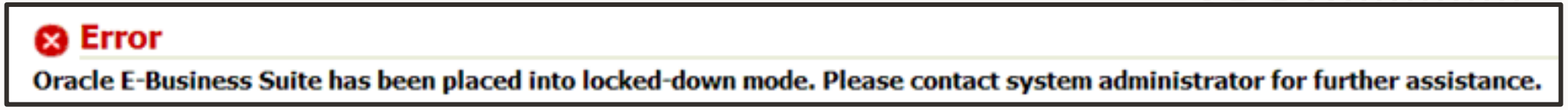
Beyond the Firewall: Mitigating Inside Threats

- What are the options to mitigate the breaches originating inside the organization?
  - Employee training – Do you have an annual program and are you tracking completion?
  - Define and follow employee exit procedures
  - Antivirus software and automated patching - use automated patching tools where possible
    - ✓ EBS Technology Patch Automation Tool for Application Tier (ETPAT-AT)
      - MOS ID: 2749774.1 EBS Technology Patch Automation Tool for Application Tier (ETPAT-AT)
      - Blog post: https://blogs.oracle.com/ebstech/post/new-ebs-technology-patch-automation-tool-for-application-tier-etpat-at
  - Implement unified auditing in 12.2 or traditional auditing prior to 12.2
    - ✓ Oracle recommends auditing privileged user activity, security events, and sensitive data access
    - ✓ MOS ID: 2777404.1 (Enabling Unified Auditing in Oracle E-Business Suite Release 12.2 with Oracle Database 19c or 12c)
    - ✓ The biggest value add for unified auditing is the policies for sensitive data
    - ✓ MOS ID: 1334930.1 (Sensitive Objects and Administrative Pages in Oracle E-Business Suite)

Secure Configuration Console

Secure Configuration Console

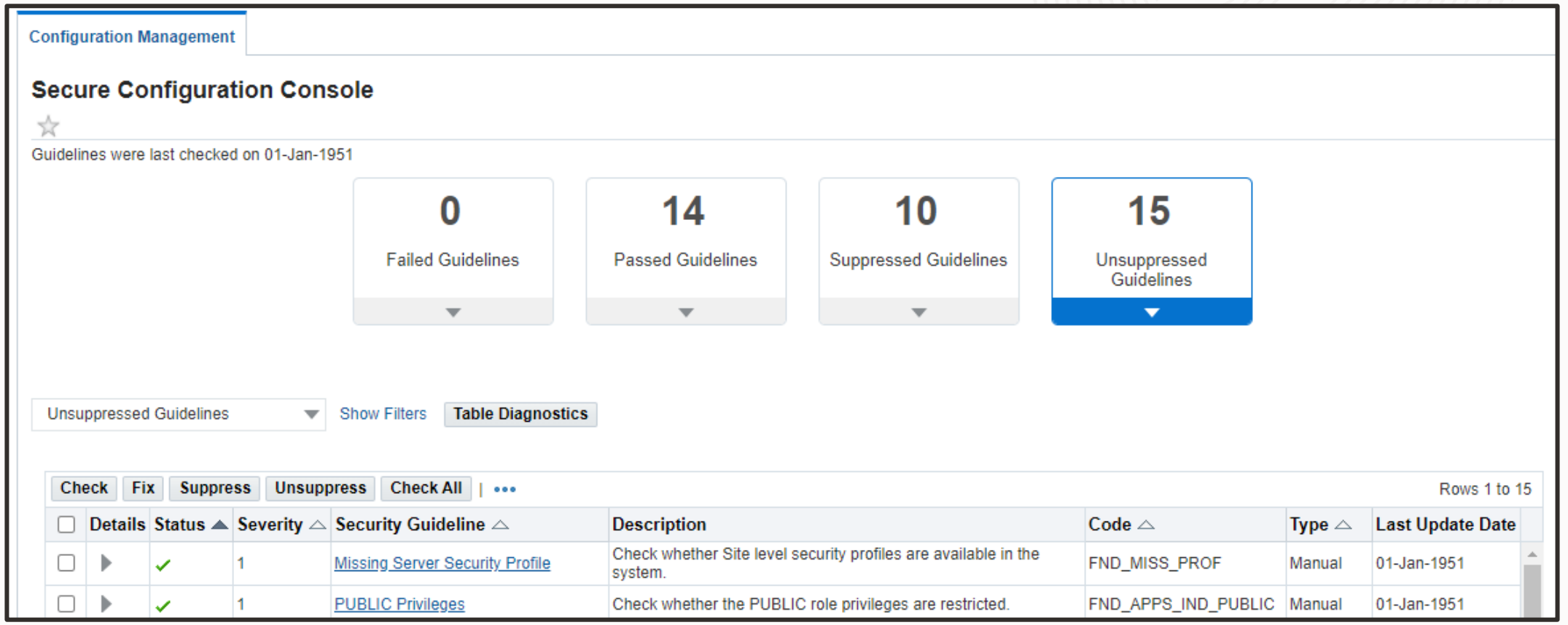
- 12.2.6 – The Secure Configuration Console UI which provides central UI to configure security features is introduced
- 12.2.9 – Verification of security configurations is required
  - EBS is locked down until the system administrator configures or acknowledges the recommended security configurations in the Secure Configuration Console



  - Log into EBS using the local login page (http(s)://[host]:[port]/OA_HTML/AppsLocalLogin.jsp)
    - ✓ Navigate to the console and unlock the system
    - ✓ If a user with local system administrator privileges is not available, you can access the Secure Configuration Console through a command line utility AdminSecurityCfg
  - Do NOT just suppress the failed guidelines without verifying they are not applicable to your system
  - For more information, see "Secure Configuration Console" in the Oracle E-Business Suite Security Guide, Part No. E22952

Secure Configuration Console

- 12.2.10+ – The Secure Configuration Console UI includes four new info tiles with predefined filters
  - Consider saved search notifications for these searches



Secure Configuration Console Checks

- Access to the Secure Configuration Console
  - System Administrator → Oracle Applications Manager → Dashboard → Security → Secure Configuration Console
  - Functional Administrator → Configuration Manager
- Additional security checks added in 12.2.7+
  - Clickjacking Protection
  - Diagnostic Web Pages Protected
  - PUBLIC Privileges
  - Workflow Email Link Login
  - Allowed Resources Configuration
  - Allowed Resources Whitelist Configuration
  - Database Parameters (init*.ora)
  - Database Password Profiles
  - iRecruitment File Upload Profile
  - Workflow Admin Access

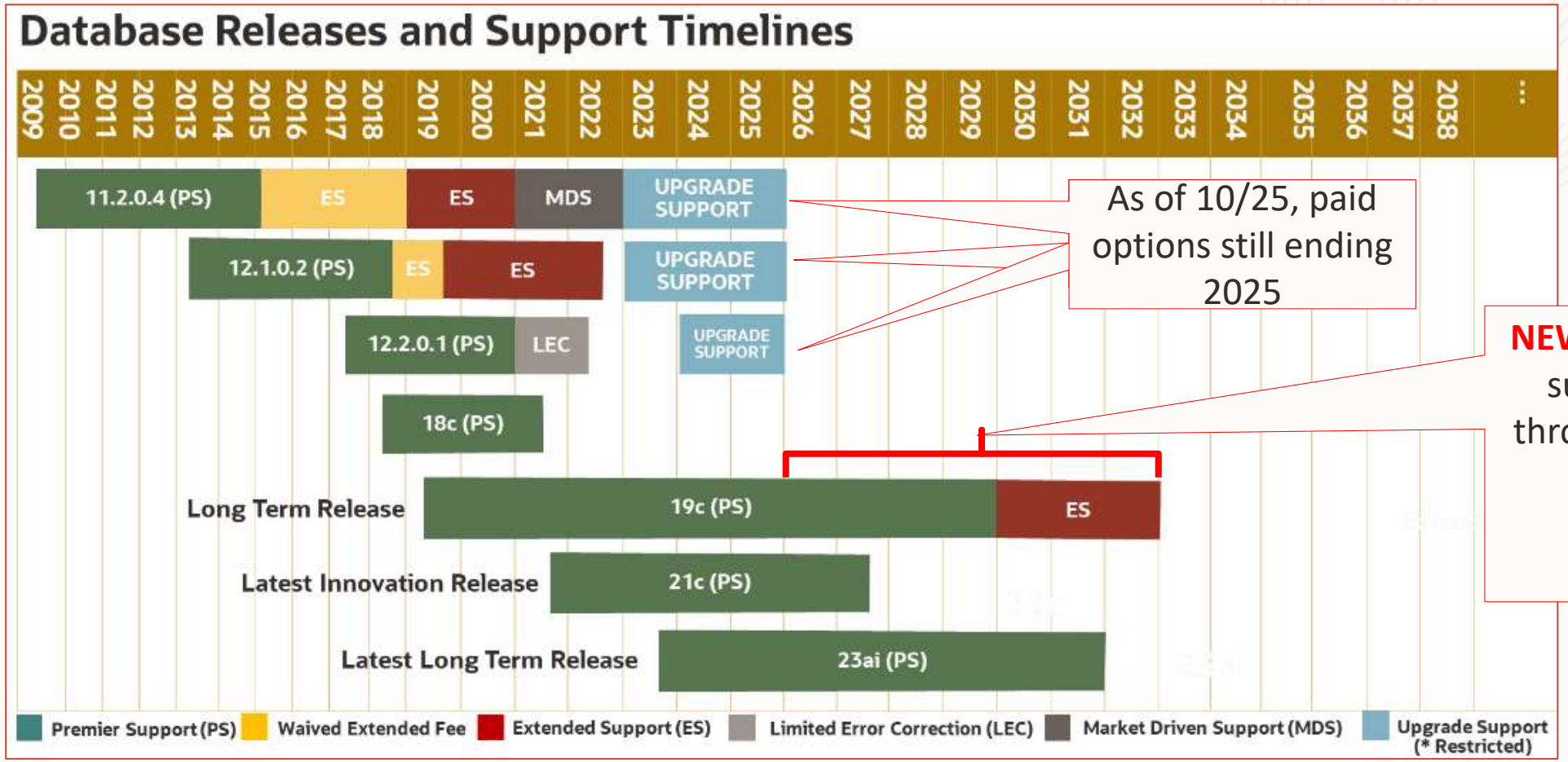
Secure Configuration Console Checks

- Additional security checks added to the secure console in 12.2.10
  - Database Network Access Control List
- Additional security checks added to the secure console in 12.2.11
  - CPU Level
  - FND Global File Manager Authorization
  - Unused Resources
  - Increased Severity to Sev 1 for Allowed Resources Configuration Check
- Additional security checks added or updated to the secure console in 12.2.15
  - Unified Auditing is enabled
  - Allowed Resources that are unused are denied (Updated to disable check if allowed resources is not enabled)
  - Critical security profile values are set correctly (Updated to confirm developer console is disabled)
  - Database users default passwords have been changed to non-default values (Updated to no longer check databases prior to 11.2.0.4)
  - Oracle E-Business Suite CPU patch level is the expected level or later (Updated to default to verifying the last CPU has been applied)

Patching/Supported Releases

Patch Availability – limited options prior to 19c

- Keep up to date with patching and stay on releases that provide security patches
- Database security patches are available for 19c and higher - MOS ID: 742060.1



As of 10/25, paid options still ending 2025

NEW as of 3/25 Premier support for 19c now through December 2029 Extended support through 2032

Oracle ACE Director

Patch Availability – Support Policy

- Software | Lifetime Support Policy (oracle.com)

	Premier Support	Extended Support	Sustaining Support
Major product and technology releases	✓	✓	✓
24/7 assistance with service requests	✓	✓	✓
Access to My Oracle Support including Knowledge Base	✓	✓	✓
Software updates	✓	✓	Pre-existing
Security alerts and updates	✓	✓	Pre-existing
Critical patch updates	✓	✓	Pre-existing
Tax, legal, and regulatory updates	✓	✓	Pre-existing
Upgrade tools and scripts	✓	✓	Pre-existing
Access to Platinum Services	✓	✓	✗
Certification with most existing Oracle products/versions	✓	✓	Pre-existing
Certification with most existing third-party products	✓	✓	Pre-existing
Certification with most new third-party products	✓	✗	✗

23ai Upgrade for EBS customers-Considerations

- The next text stack upgrade will require 23ai
- 19c to 23ai is more similar to the 11 to 12 upgrade
  - The 19c upgrade was more difficult and required a significant learning curve due to the change to the multi-tenant architecture
  - There is not a significant learning curve going to 23ai

Contingency Planning and Additional Recommendations

Contingency Planning / Recommendations

- Proactive Contingency Planning: Safeguarding against the next log4j threat – Read the Security FAQ MOS note and subscribe to notifications when updated
  - Security FAQ Sections 1 – 4 are most critical
    - ✓ Section 1: Oracle E-Business Suite Secure Configuration and Architecture
      - ➢ Includes general guidelines, database patching and security and HTTP security
    - ✓ Section 2: Oracle E-Business Suite and Auditing and Logging
    - ✓ Section 3: Oracle E-Business Suite Access and Authentication
      - ➢ Includes authorizations/segregation of duties and authentication/single sign on
    - ✓ Section 4: Oracle E-Business Suite Data Encryption and Data Protection
      - ➢ Includes credit card security, personal data removal, masking, redaction and more
    - ✓ Section 5: Oracle E-Business Suite Connection Encryption
  - Update and maintain your incident response plan
    - ✓ Consider Data Loss Prevention Solutions. Examples include:
      - ➢ Sophos – Threat detection, incident response services
      - ➢ CrowdStrike – Threat detection, incident response services, security assessments
      - ➢ Fortinet – Threat detection, incident response services, advisory services

Access Management / Compliance

- Identity management and Governance
  - Follow recommendations documented in EBS Security Guide and Security FAQ
  - Set policies for Users/Roles
    - ✓ Managed in System Administration and User Management
    - ✓ Access – (Authentication) and password management
    - ✓ Role management – (Authorization) - permissions to access data and functions
  - Set policies for database configurations for access management/single sign on
  - Security Console – checks P1s and P2s - Required for EBS starting in 12.2.8
- Managing user absences - Do you have a process for seamless access during key user absences?
  - EBS Proxy User functionality
    - ✓ Grant authority to another user for limited time to cover out of office events
      - ➢ Can limit responsibilities and workflow notifications
      - ➢ Can limit which users can delegate and limit who they can delegate to (i.e. force delegation up the chain)
      - ➢ UMX Part II Data Security Wizards and Proxy Users
  - What are the other options?
- How is your organization aligning with SOX and other regulatory standards?
  - GRC – moved from EBS to cloud
  - Fastpath – alternative to GRC

Contingency Planning / Recommendations

- Proactive Contingency Planning: Safeguarding against the next log4j threat
  - Two years after the historic disclosure of the log4j threat allowing hackers to take over remote servers, many systems are still not patched
    - ✓ A patch was available for Oracle systems months before this vulnerability came to widespread attention in Dec 2021
- Prioritize a plan to bring systems to supported release levels
  - October, 2024 – Use the Oracle E-Business Suite Java Critical Patch Update Checker (EJCPUC) to identify java patches for EBS
  - Apply the CPU to EBS and all tech stack components (Do this at a minimum!)
    - ✓ Minimal to no impact to customizations and extensions but follow standard migration processes starting with a patch instance
    - ✓ Use the EBS Critical Patch Update Checker (ECPUC) MOS ID: 2484000.1
  - Use the ETCC utility to identify missing database patches/bug fixes needed by E-Business Suite 12.2
- Michael and David will discuss more details on the next few slides…

E-Business Suite Critical Patch Update Checker (ECPUC)

- EBS Critical Patch Update Check (ECPUC)
  - Identifies current CPU level, critical CPU patches and security fixes for your environment
  - See EBS Blogs
  - ECPUC - https://blogs.oracle.com/ebstech/post/oct-2023-updates-to-ebs-critical-patch-update-checker-ecpuc
  - EJCPUC - https://blogs.oracle.com/ebstech/post/identifying-ebs-122-java-cpu-patches-and-fixes-using-ejcpuc

- Example
  - <Download> Latest E-Business Suite Critical Patch Update
    - ✓ https://blogs.oracle.com/ebstech
    - ✓ Locate the ECPUC SQL-Script in the Critical Patch Update (download)

    [unix/linux] cd E-BusinessSuite-CPU-Download-Directory
    sqlplus APPS @ECPUC.sql

E-Business Suite Critical Patch Update (CPU) Checker Example Output

```
================================================================================
SECTION-1 ECPUC Version
================================================================================
 EBS CPU Checker Version
------------------------
              2024.01
================================================================================
SECTION-2 Oracle E-Business Suite (EBS): Instance Information
================================================================================
EBS Release EBS CPU Level
----------- -------------
12.2.12     2024.01
Instance Name    Database         Database Version
---------------- ---------------- ------------------
oacdb            OATCTST1         19.21.0.0.0

ATG Product  Product Name                          Code Level
------------ ----------------------------------- ----------
ad           Applications DBA                      C.15
txk          Oracle Applications Technology Stack  C.15
atg_pf       Oracle Applications Technology Family C.11
fwk          Oracle Applications Framework         C.11
================================================================================
SECTION-3 Required EBS CPU and Security Fixes
================================================================================
The following output is a list of required patches and security fixes
that are missing in your environment.
<None>
```

Oracle E-Business Suite Java Critical Patch Update Checker (EJCPUC)

- NEW October, 2024 – Oracle E-Business Suite Java Critical Patch Update Checker (EJCPUC)
  - Section 2.2 of the ECPUC now includes a strong recommendation to run the EJCPUC utility to identify the Java CPU level and critical patches
  - Available with Patch 37171025

  - For more information:
    - ✓ See the following blog showing sample output and other updates: https://www.bluestonesolutionsgroup.com/?p=101
    - ✓ https://blogs.oracle.com/ebstech/post/april-2025-updates-to-ebs-java-critical-patch-update-checker-ejcpuc

EBS 12.2 TECHNOLOGY CODELEVEL CHECKER (ETCC)

- Use the ETCC utility to identify missing database patches/bug fixes needed by E-Business Suite 12.2
  - Oracle strongly recommends using this utility
  - Includes two scripts – one for the database and one for the application tier
  - Download Patch 17537119

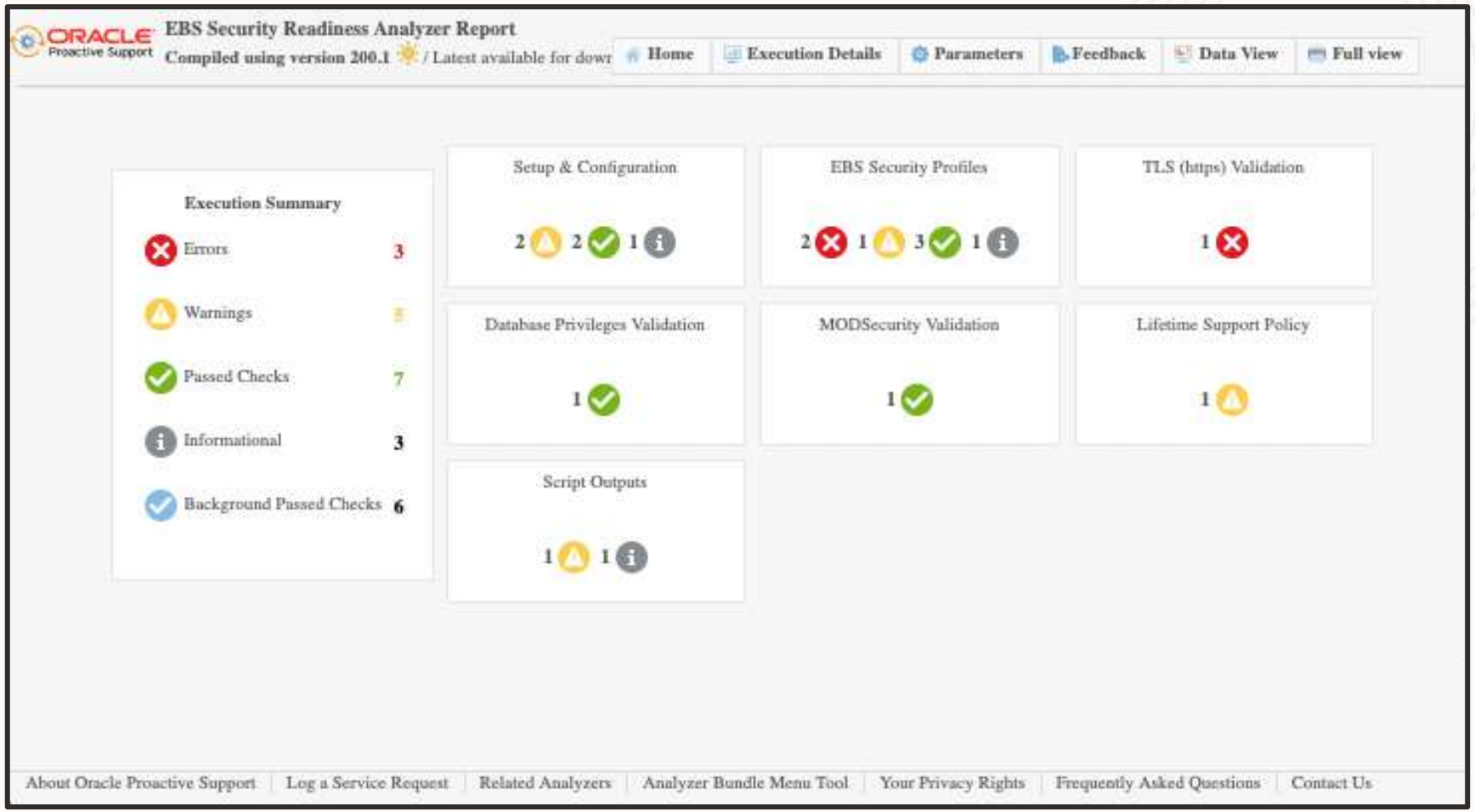
- For more information:
  - https://blogs.oracle.com/ebstech/post/identifying-missing-app-tier-and-database-tier-patches-for-ebs-122
  - Oracle Support Document 1633974.2

E-Business Suite Security Readiness Analyzer

- E-Business Suite Security Readiness Analyzer – MOS ID: 2603839.1
  - Sample Output
  - <Download> Latest E-Business Suite Security Functional Analyzer

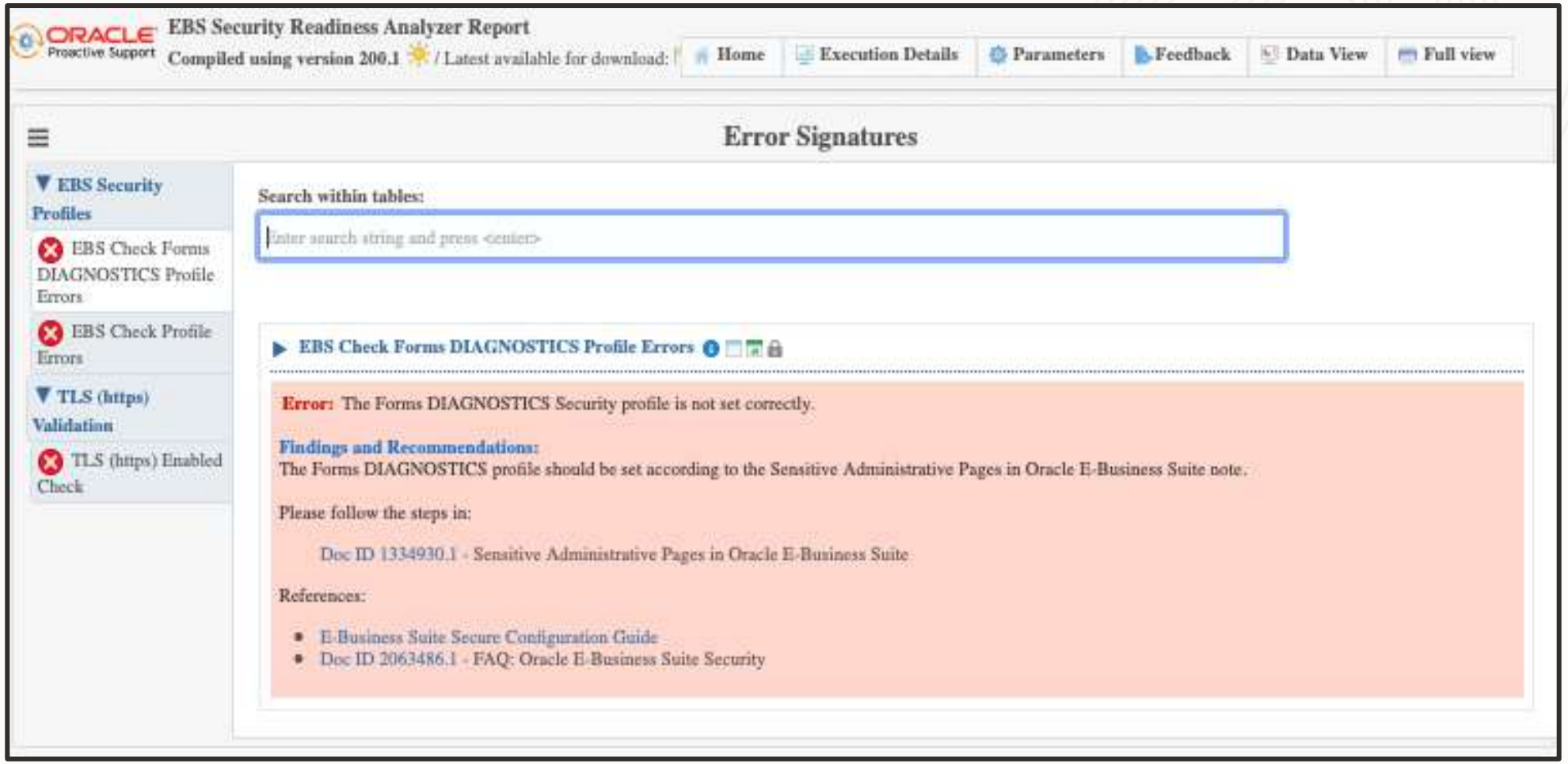
[unix/linux] cd E-BusinessSuite-FunctionalAnalyzer-Directory/MENU
perl Menu.pl

E-Business Suite Security Readiness Functional Analyzer Example



Oracle ACE Director

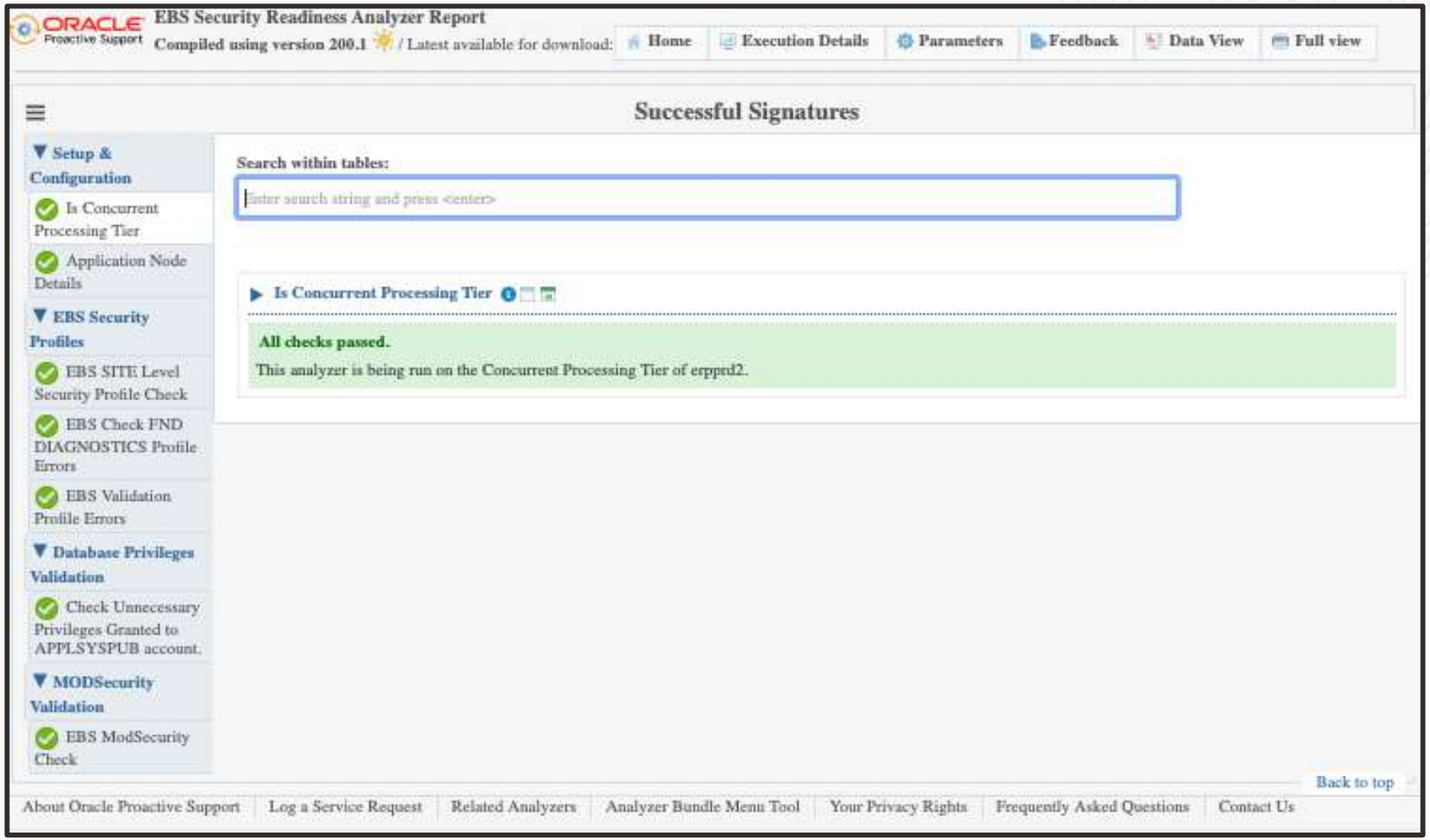
E-Business Suite Security Readiness Functional Analyzer Example



Oracle ACE Director

E-Business Suite Security Readiness Functional Analyzer Example

E-Business Suite Security Readiness Functional Analyzer Example



Oracle ACE Director

Certificates/TLS

- Summer of 2023 Changes
  - Commercial Code Signing Certificates (CSC) for signing jar files required for EBS starting June 1, 2023
    - ✓ Self signing still possible but must push out exception to every desktop
- August, 2024 – Oracle announced enhancements for signing Jar files
  - Two Options:
    - ✓ Use private CA issued code signing certificate and keep existing AD tools
    - ✓ Use commercial CA issued certificate and implement custom signing process
  - See the following references
    - ✓ Oracle Support Document 1591073.1 (Enhanced Jar Signing for Oracle E-Business Suite) can be found at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=1591073.1
    - ✓ EBS technical blog: https://blogs.oracle.com/ebstech/post/update-new-configurable-options-for-signing-ebs-122-jar-files-now-available
- Enabling TLS browser security which uses SSL certificates is highly recommended
- For more information, see CERTIFICATES IN E-BUSINESS SUITE PANEL in the OATUG Knowledge Base

Thank You

Susan Behn

Oracle ACE Director