ORACLE

Oracle Database
Attack Surface Reduction

An Oracle Consulting Services - Security Workshop

Daniel Morgan
Technical Director Database Security
Oracle Consulting Services

November 14, 2023

for
NYOUG

Agenda

Introduction

Ransomware

Dual Use

Secure Configuration

Attack Surface Reduction Assessments

daniel.d.morgan@oracle.com

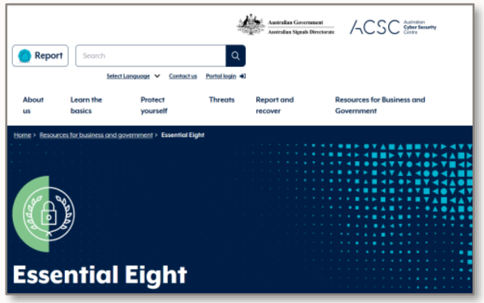
- Oracle Professional Services, Technical Director, Database and Cloud Security
- Member, Oracle Security Tiger Team
- Oracle ACE Director Alumnus
- Educator
  - Adjunct Professor, University of Washington, Oracle Program, 1998-2009
  - Oracle Consultant: Harvard University
  - Guest lecturer at universities and colleges in Canada, Chile, Costa Rica, New Zealand, Norway, Panama, US
  - Frequent conference speaker … OpenWorld + 151 country visits in 47 countries, since 2008
  - @NYOUG 2014, 2015, 2016, 2017
- IT Professional
  - Member Oracle Database Security Partner Advisory Council 2019-2021
  - The Morgan behind www.morganslibrary.org and www.dbsecworx.com
  - Founding Chair Washington Software Association's Database Special Interest Group
  - Oracle Database and Database Beta Tester since 1988-9

No Matter Where Our Customers Are Located

United Nations

UNCCT › Programmes and projects › Cybersecurity and New Technologies

Cybersecurity and New Technologies


Australian Government Australian Signals Directorate ACSC Australian Cyber Security Centre

Report | Search | Select Language | Contact us | Portal login

About us | Learn the basics | Protect yourself | Threats | Report and recover | Resources for Business and Government

Home > Resources for business and government > Essential Eight

Essential Eight

NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

本文へ 文字サイズ English

ホーム | 内閣サイバーセキュリティセンター(NISC)について | お知らせ | 政策 | 会議 | 関連法令等 | 普及啓発活動

自由、公正かつ安全な
サイバー空間を確保するために。

サイバーセキュリティ 関係法令Q＆A ハンドブック

新着情報

2023年08月

2023年08月15日 重要インフラグループ 関係規程集を更新しました （PDF形式:9.6MB）

2023年08月08日 NISCを騙った不審な電話やメール等にご注意ください

2023年08月04日 内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について

2023年07月

2023年07月04日 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書を公開しました （PDF形式:1307KB）

NISC関係の重要文書

一般の方向け情報

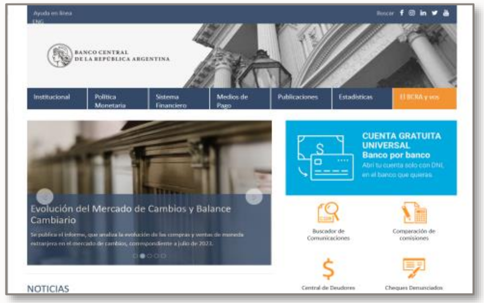
Government of Canada Gouvernement du Canada

Français | Search | MENU | Canada.ca

Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (the Cyber Centre) is part of the Communications Security Establishment. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.

Report a cyber incident


Banco Central de la República Argentina

Institucional | Política Monetaria | Sistema Financiero | Medios de Pago | Publicaciones | Estadísticas | El BCRA y vos

Evolución del Mercado de Cambios y Balance Cambiario

Se publica el informe, que analiza la evolución de las compras y ventas de moneda extranjera en el mercado de cambios, correspondiente a julio de 2023.

CUENTA GRATUITA UNIVERSAL Banco por banco

Abrí tu cuenta solo con DNI, en el banco que quieras.

Buscador de Comunicaciones | Comparación de comisiones | Central de Deudores | Cheques Denunciados

NOTICIAS

تعزيز مكانة دبي كمدينة عالمية رائدة في الابتكار
والسلامة والأمن

gov.br Government Agencies | Access to Information | Legislation | Accessibility | EN | Entrar com o gov.br

Serviços e Informações do Brasil | What are you looking for?

Government of Brazil › Latest News › 2022 › Cybersecurity

Cybersecurity

Published in Jan 14, 2022 05:25 PM | Updated in Feb 09, 2022 04:50 PM | Share

English | हिंदी

cert-in साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre

मुख्य पृष्ठ | हमारे बारे में | सर्ट-इन | सुरक्षा उपकरण | चेतावनी | सुरक्षा सर्वोत्तम अभ्यास | घोषणाएँ | सभी | सामान्य प्रश्न | संपर्क करें

सबका साथ सबका विकास सबका विश्वास सबका प्रयास

साइबर स्वच्छता केन्द्र में आपका स्वागत है।

Australian Government Australian Signals Directorate ASD AUSTRALIAN SIGNALS DIRECTORATE

HOME | ABOUT | CAREERS | CYBER SECURITY | PUBLICATIONS | 75TH ANNIVERSARY | CONTACT | Search

Home / Cyber Security

Cyber Security

The Australian Cyber Security Centre (ACSC) within ASD leads the Australian Government's efforts on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.

ASD cyber security advice is published at our Australian Cyber Security Centre (ACSC) website, cyber.gov.au. You can also report cyber incidents and sign up for cyber security

TRAFICOM Liikenne- ja viestintävirasto Kyberturvallisuuskeskus

Hae sivustolta | Suomi

AJANKOHTAISTA | PALVELUMME | TOIMINTAMME | OTA YHTEYTTÄ

Ilmoita tietoturvaloukkauksesta

Ajankohtaista > Haavoittuvuudet

Haavoittuvuudet

Ajankohtaista tietoa ohjelmistohaavoittuvuuksista

National Cyber Security Centre

ABOUT NCSC | CISP | REPORT AN INCIDENT | CONTACT US

Home | Information for... | Advice & guidance | Education & skills | Products & services | News, blogs, events...

The National Cyber Security Centre

Helping to make the UK the safest place to live and work online.

Featured

BLOG POST 'Online safety' vs 'cyber security'

KISA 한국인터넷진흥원 고객서비스 | 지식플랫폼 | 사업소개 | 주요성과 | 알림마당 | 환경·사회·투명 경영 | KISA 소개

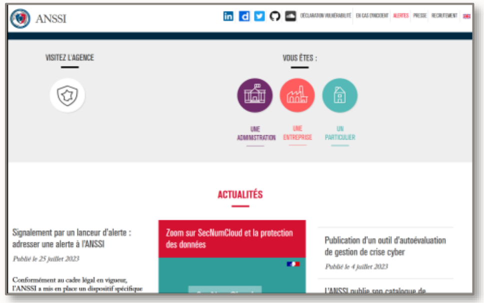
Korea Internet & Security Agency

[KISA]와
함께 가꾸는 미래 인터넷
함께 꿈꾸는 안전한 세상

02 / 03

KISA BUG BOUNTY

GDPR


ANSSI

DÉCLARATION VULNÉRABILITÉ | EN CAS D'INCIDENT | ALERTES | PRESSE | RECRUTEMENT

VISITEZ L'AGENCE

VOUS ÊTES :

UNE ADMINISTRATION | UNE ENTREPRISE | UN PARTICULIER

ACTUALITÉS

Signalement par un lanceur d'alerte : adresser une alerte à l'ANSSI

Publié le 25 juillet 2023

Conformément au cadre légal en vigueur, l'ANSSI a mis en place un dispositif spécifique

Zoom sur SecNumCloud et la protection des données

Publication d'un outil d'autoévaluation de gestion de crise cyber

Publié le 4 juillet 2023

L'ANSSI publie son catalogue de

No Matter Our Customer's Infrastructure Sector

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Chemical Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector
Emergency Services Sector

CHEMICAL SECTOR

Identifying Critical Infrastructure During COVID-19

The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely. Securing these chemicals against growing and evolving threats requires vigilance from both the private and public sector.

The Department of Homeland Security—identified as the Chemical Sector Risk Management Agency (SRMA) in Presidential Policy Directive (PPD) 21—leads the Chemical Sector's public-private partnership and works with

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Critical Manufacturing Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector

CRITICAL MANUFACTURING SECTOR

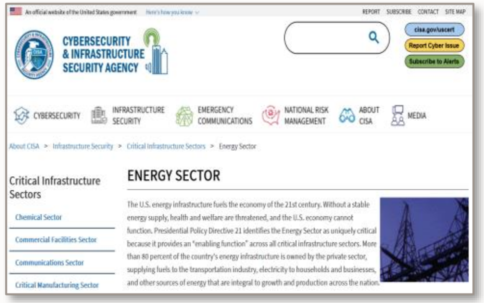
The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors.

Expand All Sections

Sector Overview +

Sector-Specific Plan +

Critical Manufacturing Resources +


An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Energy Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector

ENERGY SECTOR

The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation.

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Government Facilities Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector

GOVERNMENT FACILITIES SECTOR

The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions. In addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Critical Manufacturing Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector

CRITICAL MANUFACTURING SECTOR

The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors.

Expand All Sections

Sector Overview +

Sector-Specific Plan +

Critical Manufacturing Resources +

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Defense Industrial Base Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector
Emergency Services Sector

DEFENSE INDUSTRIAL BASE SECTOR

The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The Defense Industrial Base partnership consists of Department of Defense components, more than 100,000 Defense Industrial Base companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities. Defense Industrial Base companies include domestic and foreign entities, with production assets located in many countries. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements. These commercial infrastructure assets are addressed by other Sector Risk Management Agencies.

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Financial Services Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector

FINANCIAL SERVICES SECTOR

The Financial Services Sector represents a vital component of our nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyberattacks demonstrate the wide range of potential risks facing the sector.

Expand All Sections

Sector Overview

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Healthcare and Public Health Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector
Emergency Services Sector
Energy Sector

HEALTHCARE AND PUBLIC HEALTH SECTOR

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure. Operating in all U.S. states, territories, and tribal areas, the sector plays a significant role in response and recovery across all other sectors in the event of a natural or manmade disaster. While

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Communications Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector

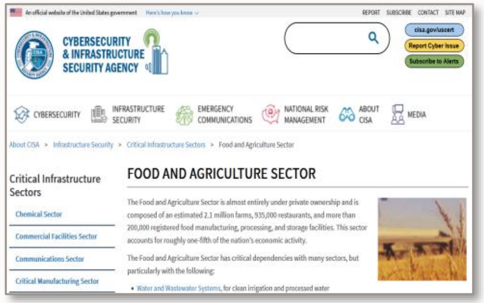
COMMUNICATIONS SECTOR

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability.

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Emergency Services Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector

EMERGENCY SERVICES SECTOR

The Emergency Services Sector (ESS) is a community of millions of highly-skilled, trained personnel, along with the physical and cyber resources, that provide a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response. The ESS includes geographically distributed facilities and equipment in both paid and volunteer capacities organized primarily at the federal, state, local, tribal, and territorial levels of government, such as city police departments and fire stations, county sheriff's offices, Department of Defense police and fire departments, and town public works departments. The ESS also includes private sector resources, such as industrial fire departments, private security organizations, and private emergency medical services providers.

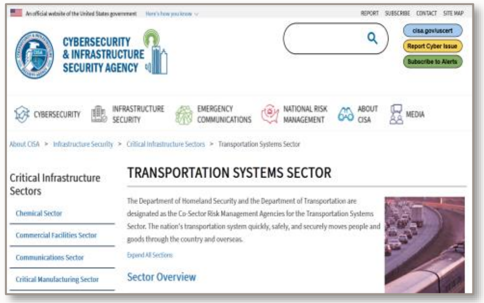

An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Food and Agriculture Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector

FOOD AND AGRICULTURE SECTOR

The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity.

The Food and Agriculture Sector has critical dependencies with many sectors, but particularly with the following:

- Water and Wastewater Systems, for clean irrigation and processed water


An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
About CISA > Infrastructure Security > Critical Infrastructure Sectors > Transportation Systems Sector
Critical Infrastructure Sectors
Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector

TRANSPORTATION SYSTEMS SECTOR

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas.

Expand All Sections

Sector Overview

We Must Be Able To Support Our Customer's Security Initiatives

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Special Publication
NIST SP 800-66r2 ipd

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule:
A Cybersecurity Resource Guide

Initial Public Draft

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST National Institute of Standards and Technology U.S. Department of Commerce

NISTIR 8374

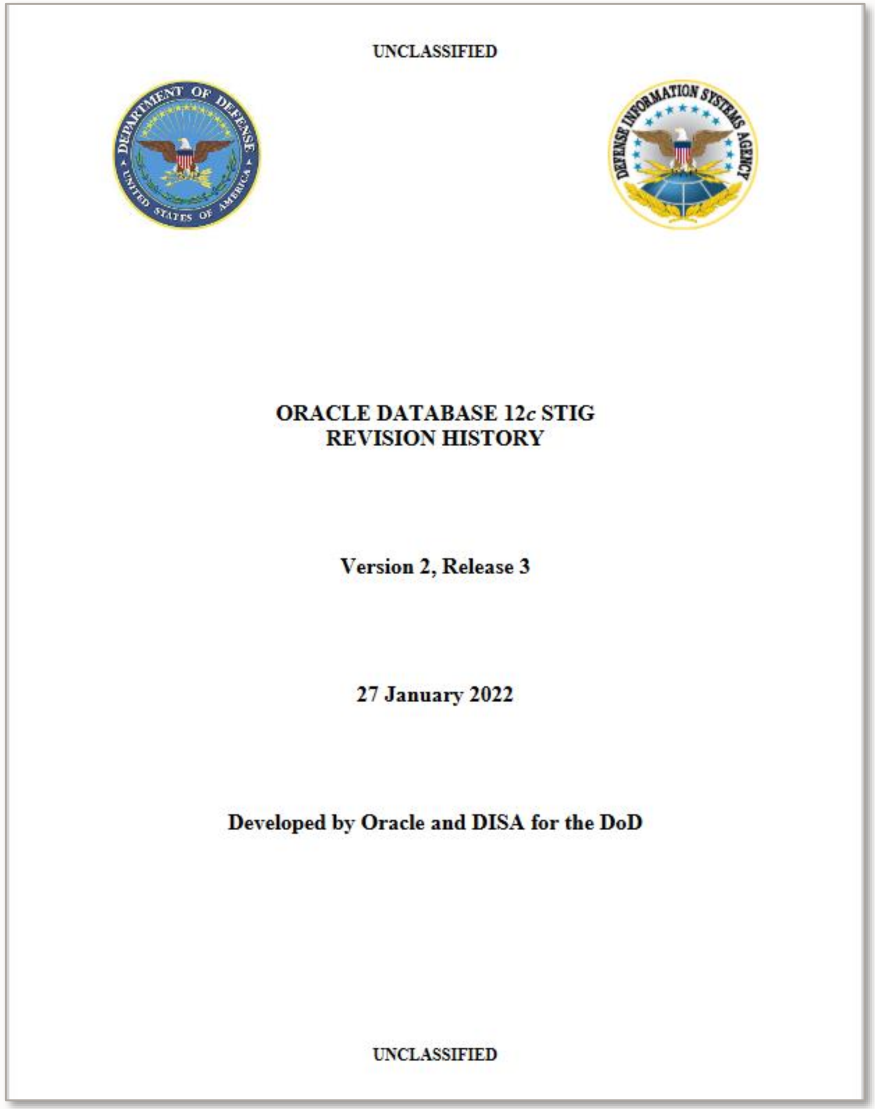
Ransomware Risk Management:
A Cybersecurity Framework Profile

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

NIST National Institute of Standards and Technology U.S. Department of Commerce

Not Just For PII and PHI but for DFARS, EAR, ITAR, and ….



UNCLASSIFIED

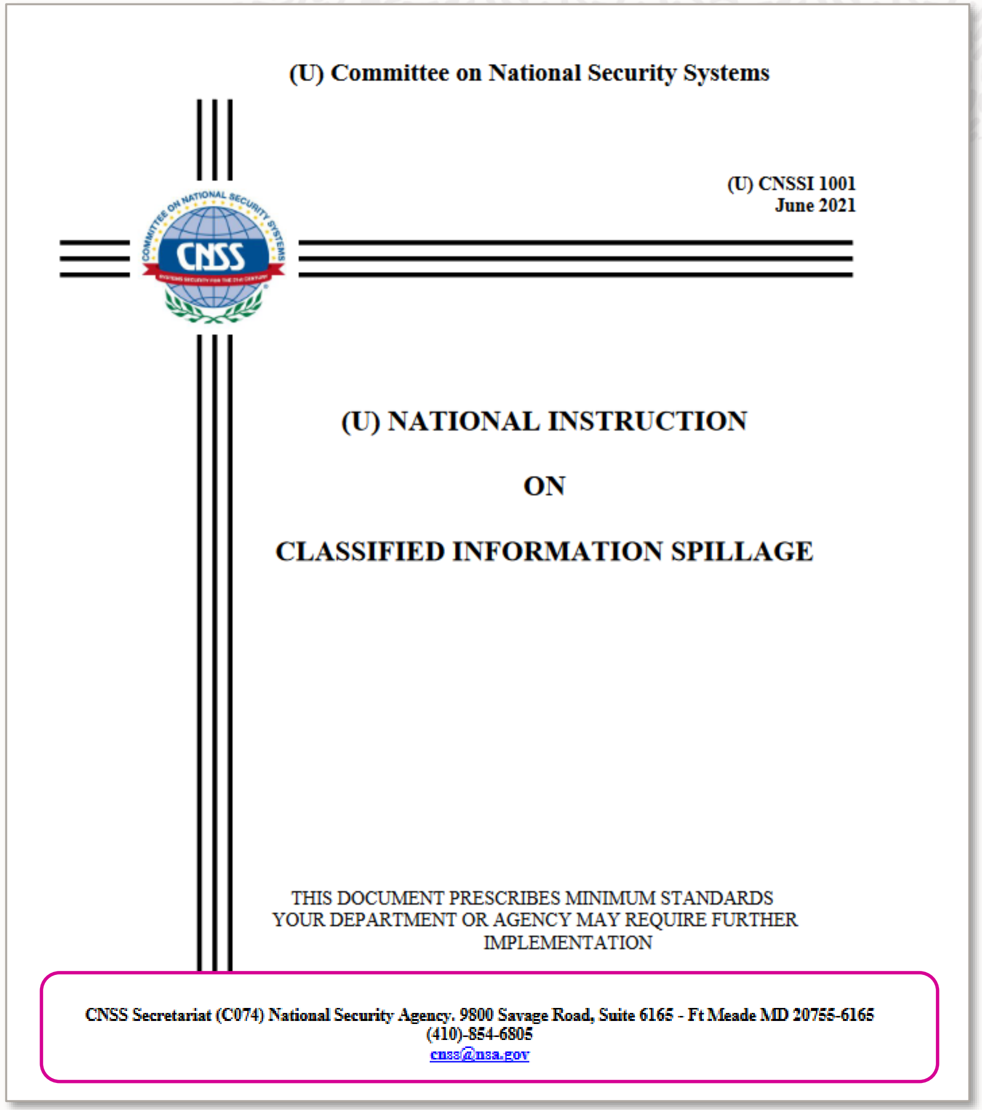
ORACLE DATABASE 12*c* STIG
REVISION HISTORY

Version 2, Release 3

27 January 2022

Developed by Oracle and DISA for the DoD

UNCLASSIFIED



(U) Committee on National Security Systems

(U) CNSSI 1001
June 2021

(U) NATIONAL INSTRUCTION

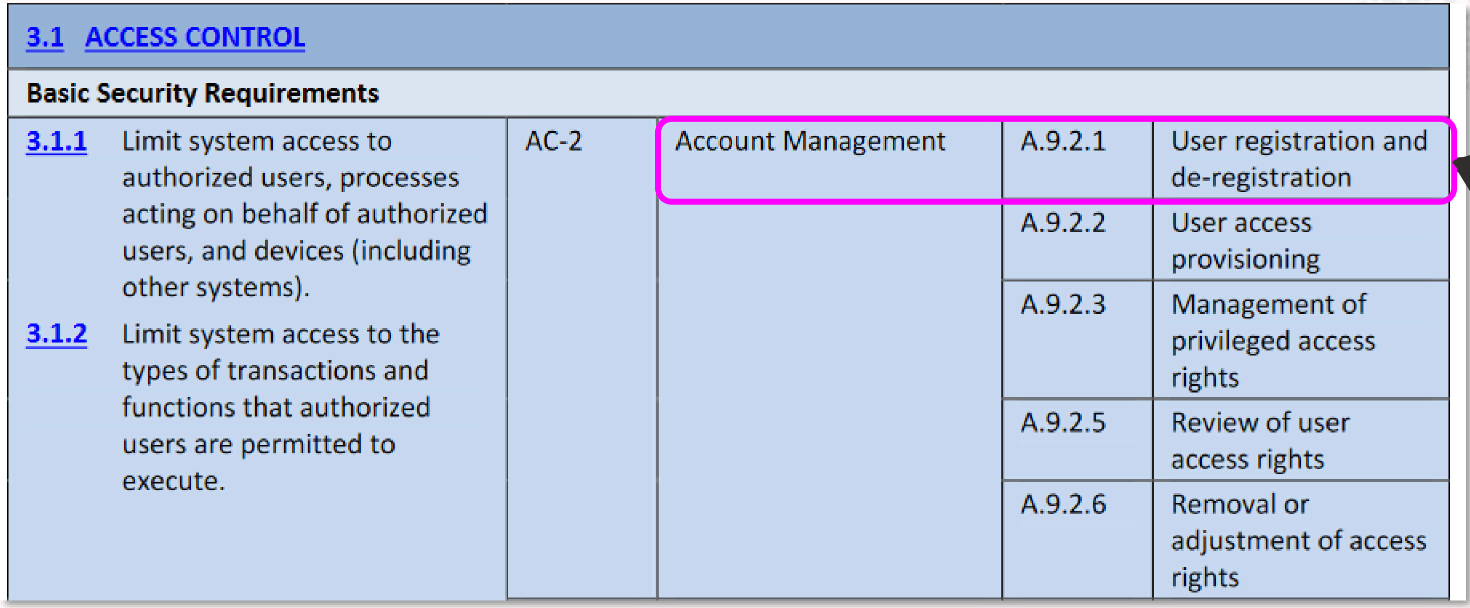
ON

CLASSIFIED INFORMATION SPILLAGE

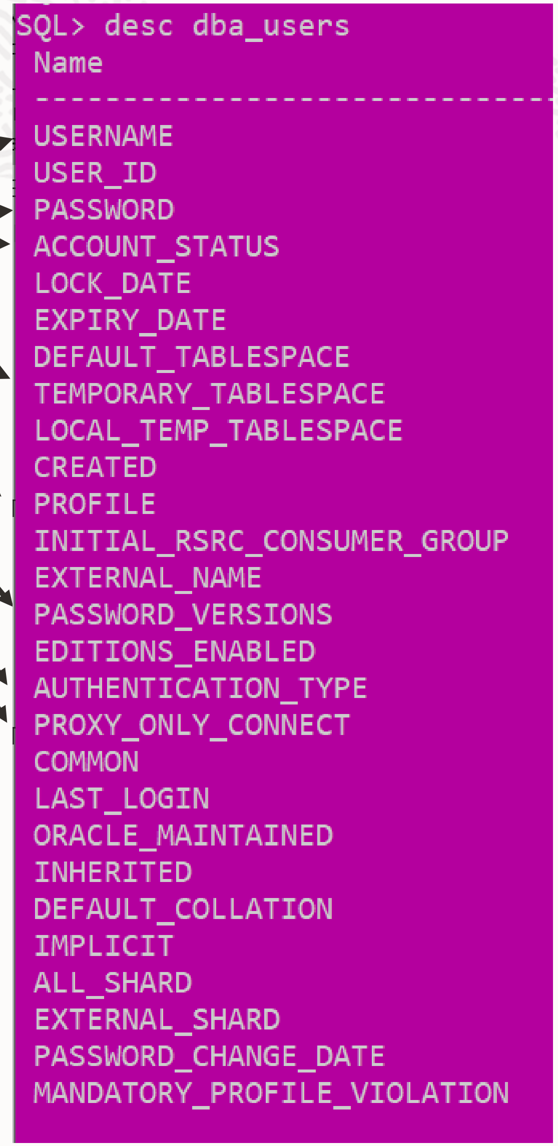
THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

CNSS Secretariat (C074) National Security Agency. 9800 Savage Road, Suite 6165 - Ft Meade MD 20755-6165
(410)-854-6805
cnss@nsa.gov

Access Controls: Account Management



3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights



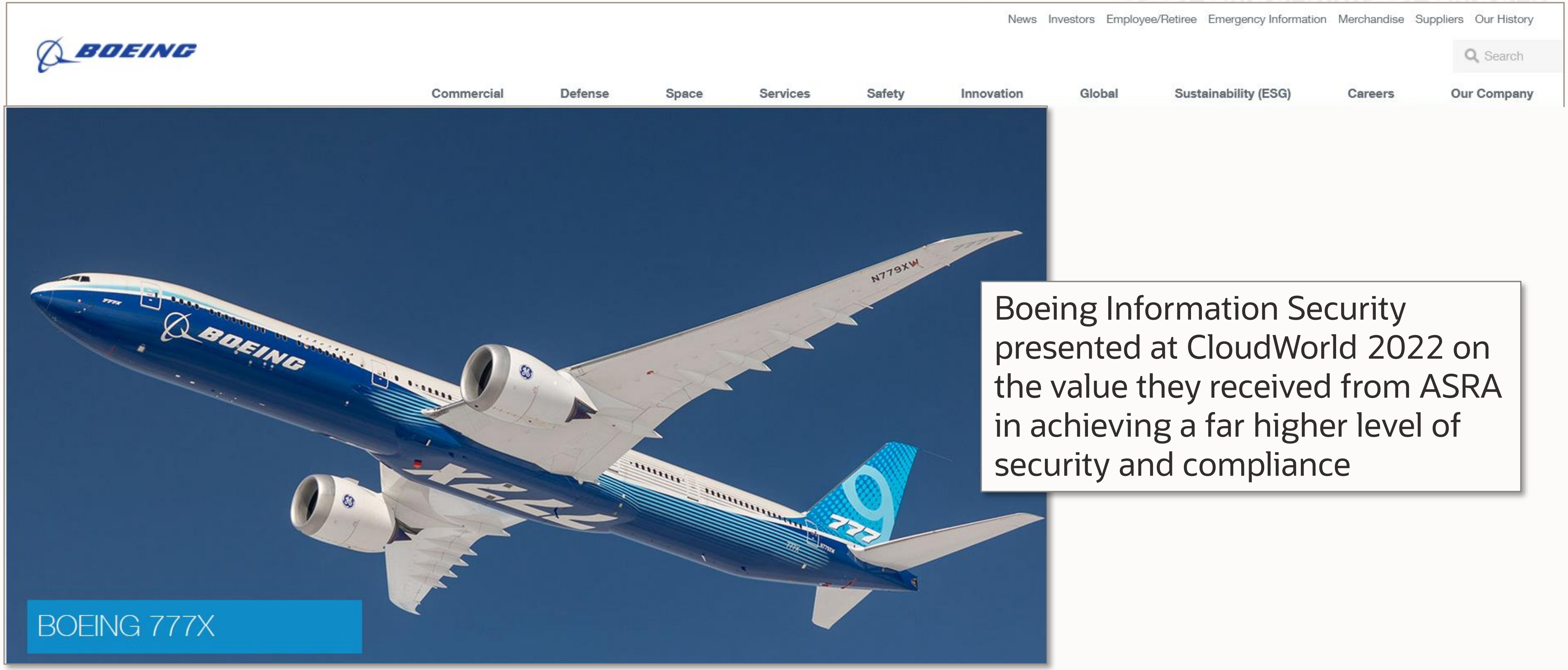
```
SQL> desc dba_users
 Name
 -----------------------------
 USERNAME
 USER_ID
 PASSWORD
 ACCOUNT_STATUS
 LOCK_DATE
 EXPIRY_DATE
 DEFAULT_TABLESPACE
 TEMPORARY_TABLESPACE
 LOCAL_TEMP_TABLESPACE
 CREATED
 PROFILE
 INITIAL_RSRC_CONSUMER_GROUP
 EXTERNAL_NAME
 PASSWORD_VERSIONS
 EDITIONS_ENABLED
 AUTHENTICATION_TYPE
 PROXY_ONLY_CONNECT
 COMMON
 LAST_LOGIN
 ORACLE_MAINTAINED
 INHERITED
 DEFAULT_COLLATION
 IMPLICIT
 ALL_SHARD
 EXTERNAL_SHARD
 PASSWORD_CHANGE_DATE
 MANDATORY_PROFILE_VIOLATION
```

Principle of Least Privilege is more than system and object privileges

Principle of Least Privilege is also Database Profiles and Consumer Groups

Our Beta Partner and Reference

A "small" aerospace company with security issues very similar to yours



Boeing Information Security presented at CloudWorld 2022 on the value they received from ASRA in achieving a far higher level of security and compliance

Ransomware

Oracle Database Ransomware Risk

Ransomware is a plague impacting a wide variety of IT environments with many accepting that there is little they can do outside of standard protocols related to perimeter defense and phishing pre

For the Orac minimize the risk by fc

The risk pro example, ca how different components can be installed and configured to reduce the attack surface

If you do not have immutable copies of ORACLE_BASE and ORACLE_HOME you could suffer a substantial loss of service.

If you do not have your data files, control files, redo logs, and wallet on ASM you could have a catastrophic failure.

		Safe *
	m	
	m	
Data Files		ASM & ZFS
Control Files		ASM & ZFS
Redo Log Files		ASM & ZFS
Archived Redo Log Files		ASM & ZFS
Standby Redo Logs		ASM & ZFS
Server Parameter File (SPFILE)		ASM & ZFS
Password File		ASM & ZFS
RMAN Backup Files		ASM & ZFS
Wallet and Key Vault (OKV)		ASM & ZFS

* Oracle cannot guarantee that future attacks will not include ASM but, to date, there is no known successful attack on raw disk managed with Oracle ASM

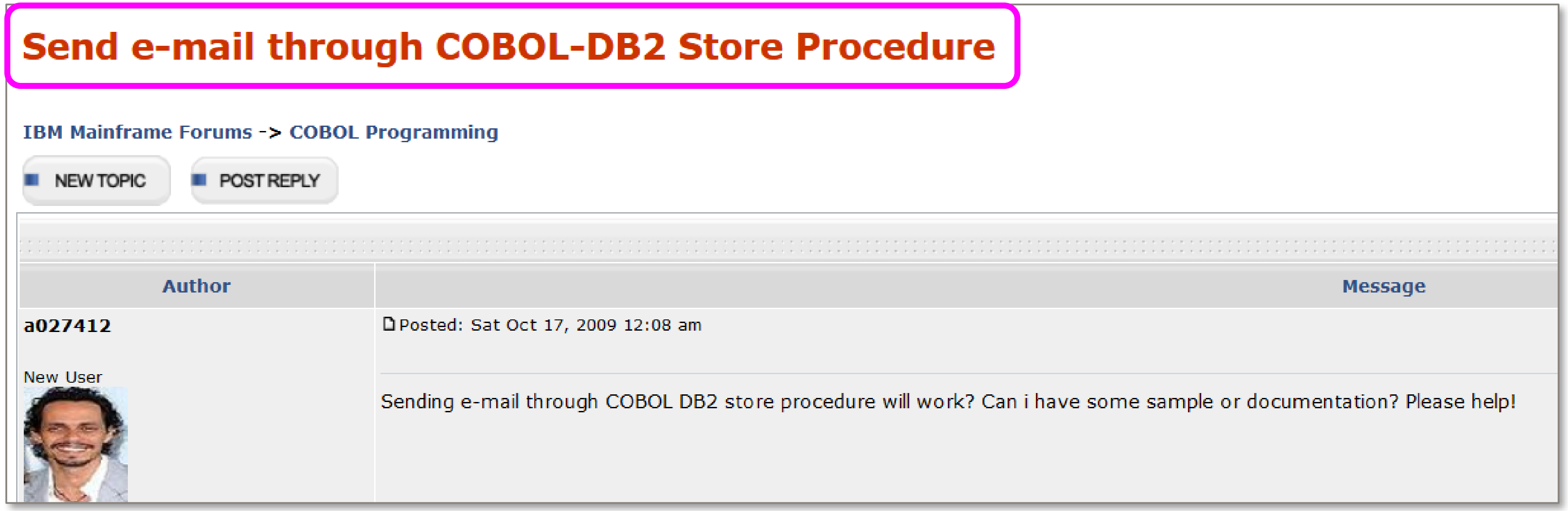
Dual-Use

Evaluating Risk

Should Oracle Database 24c include a new feature that would allow PUBLIC to:

- run a query
- attach the results to an email
- send the email to a foreign intelligence agency?

Would You Change Your Mind If It Was On IBM Mainframes?

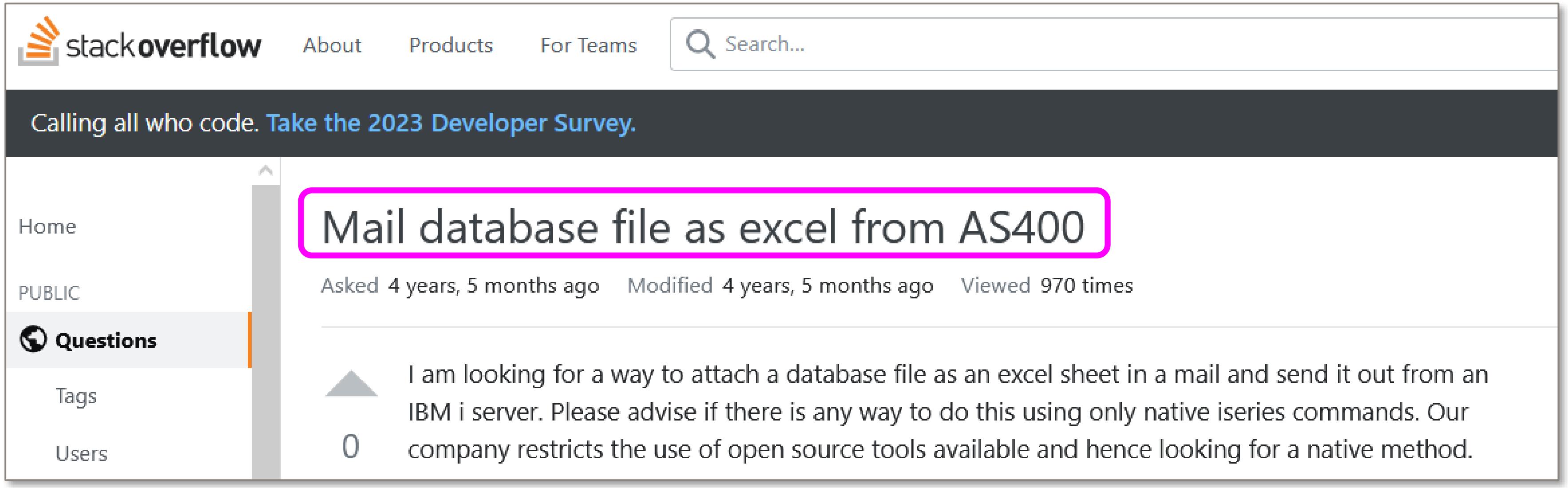


Send e-mail through COBOL-DB2 Store Procedure

IBM Mainframe Forums -> COBOL Programming

Author	Message
a027412 New User	Posted: Sat Oct 17, 2009 12:08 am Sending e-mail through COBOL DB2 store procedure will work? Can i have some sample or documentation? Please help!

On IBM AS400s?



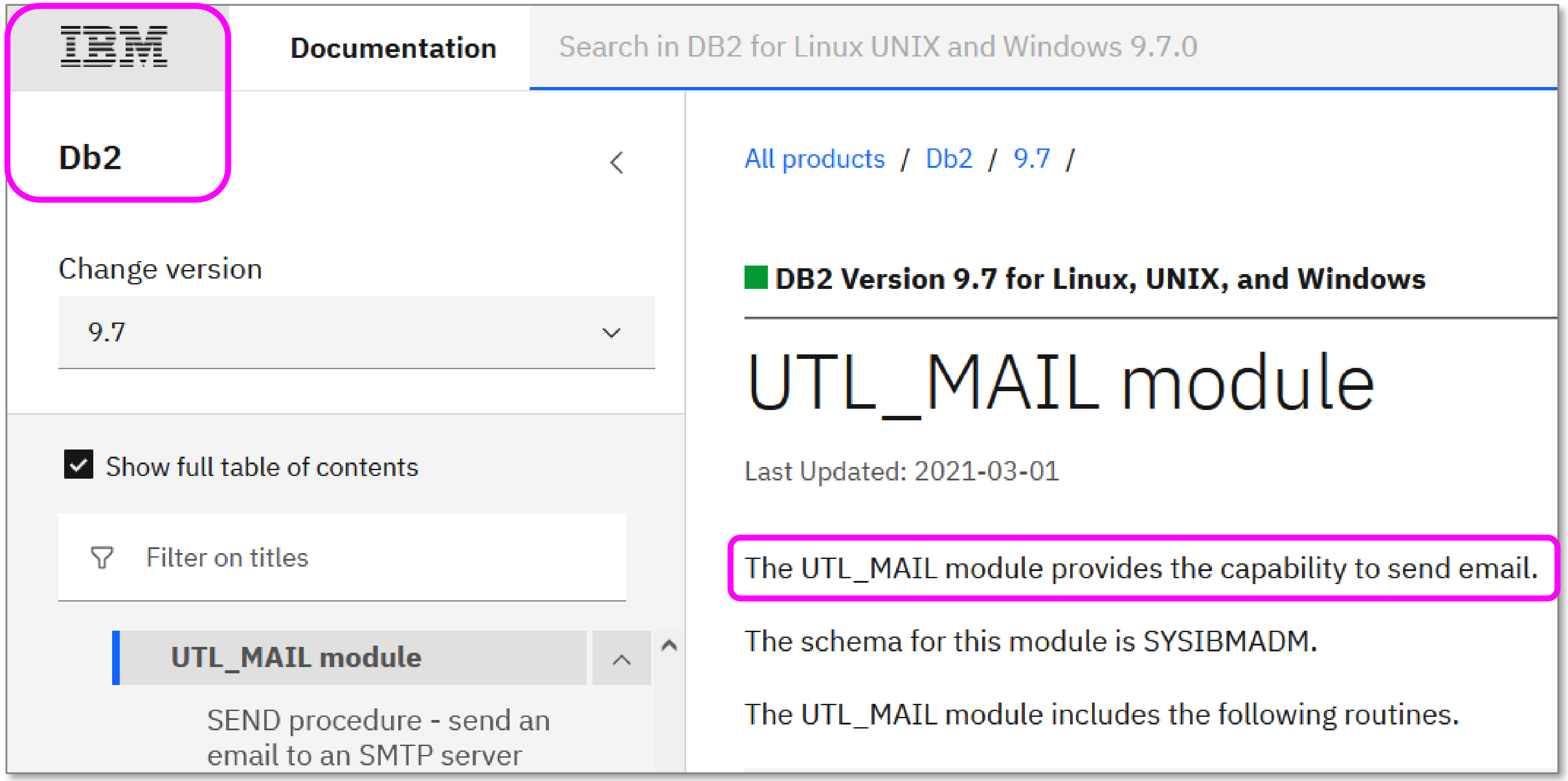
Calling all who code. Take the 2023 Developer Survey.

Mail database file as excel from AS400

Asked 4 years, 5 months ago Modified 4 years, 5 months ago Viewed 970 times

I am looking for a way to attach a database file as an excel sheet in a mail and send it out from an IBM i server. Please advise if there is any way to do this using only native iseries commands. Our company restricts the use of open source tools available and hence looking for a native method.

In IBM DB2 on Linux, Unix and Windows?



IBM
Documentation
Search in DB2 for Linux UNIX and Windows 9.7.0
Db2
Change version
9.7
☑ Show full table of contents
Filter on titles
UTL_MAIL module
SEND procedure - send an email to an SMTP server

All products / Db2 / 9.7 /

🟩 **DB2 Version 9.7 for Linux, UNIX, and Windows**

UTL_MAIL module

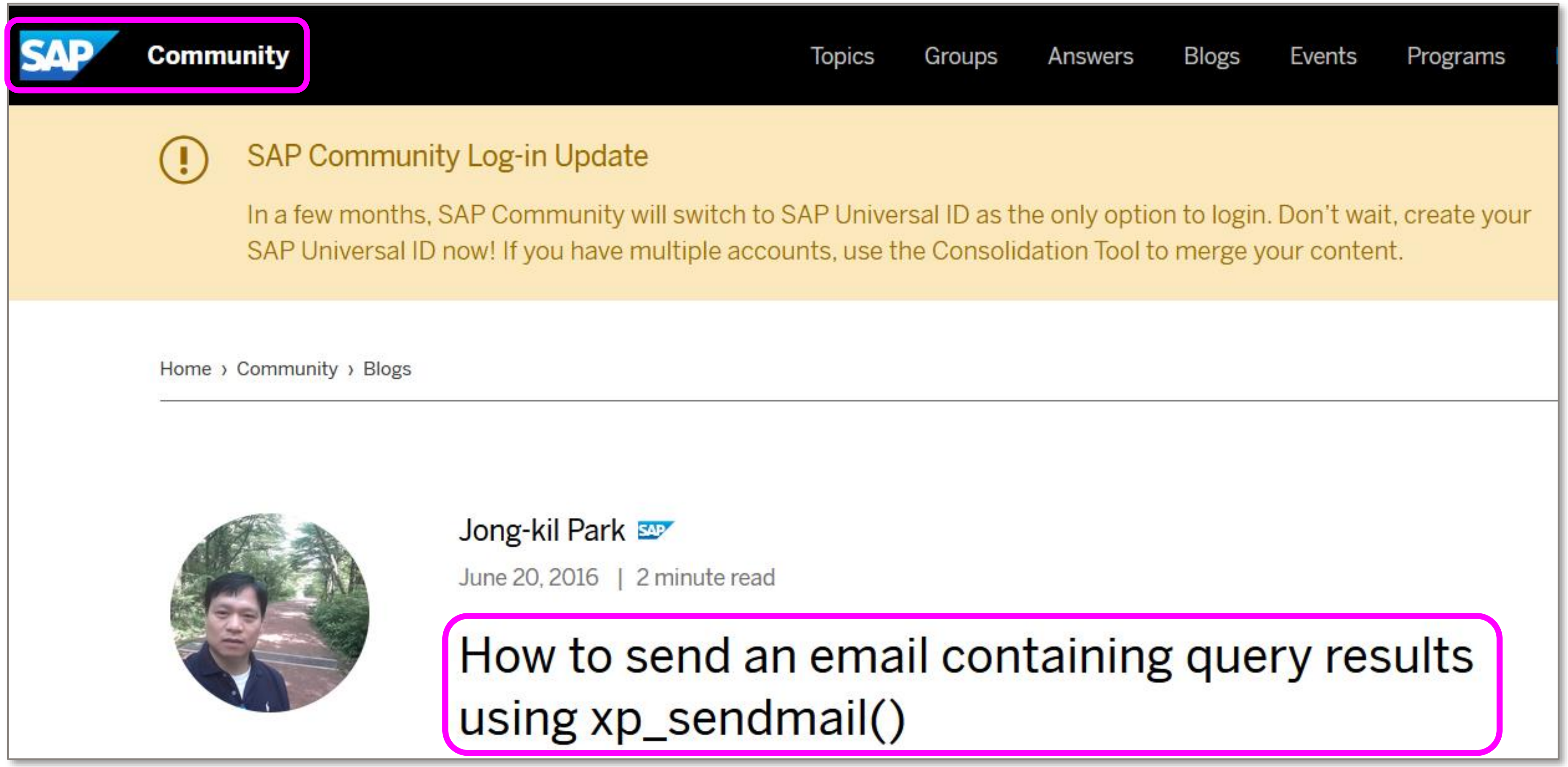
Last Updated: 2021-03-01

The UTL_MAIL module provides the capability to send email.

The schema for this module is SYSIBMADM.

The UTL_MAIL module includes the following routines.

In SAP Sybase?



SAP Community Log-in Update

In a few months, SAP Community will switch to SAP Universal ID as the only option to login. Don't wait, create your SAP Universal ID now! If you have multiple accounts, use the Consolidation Tool to merge your content.

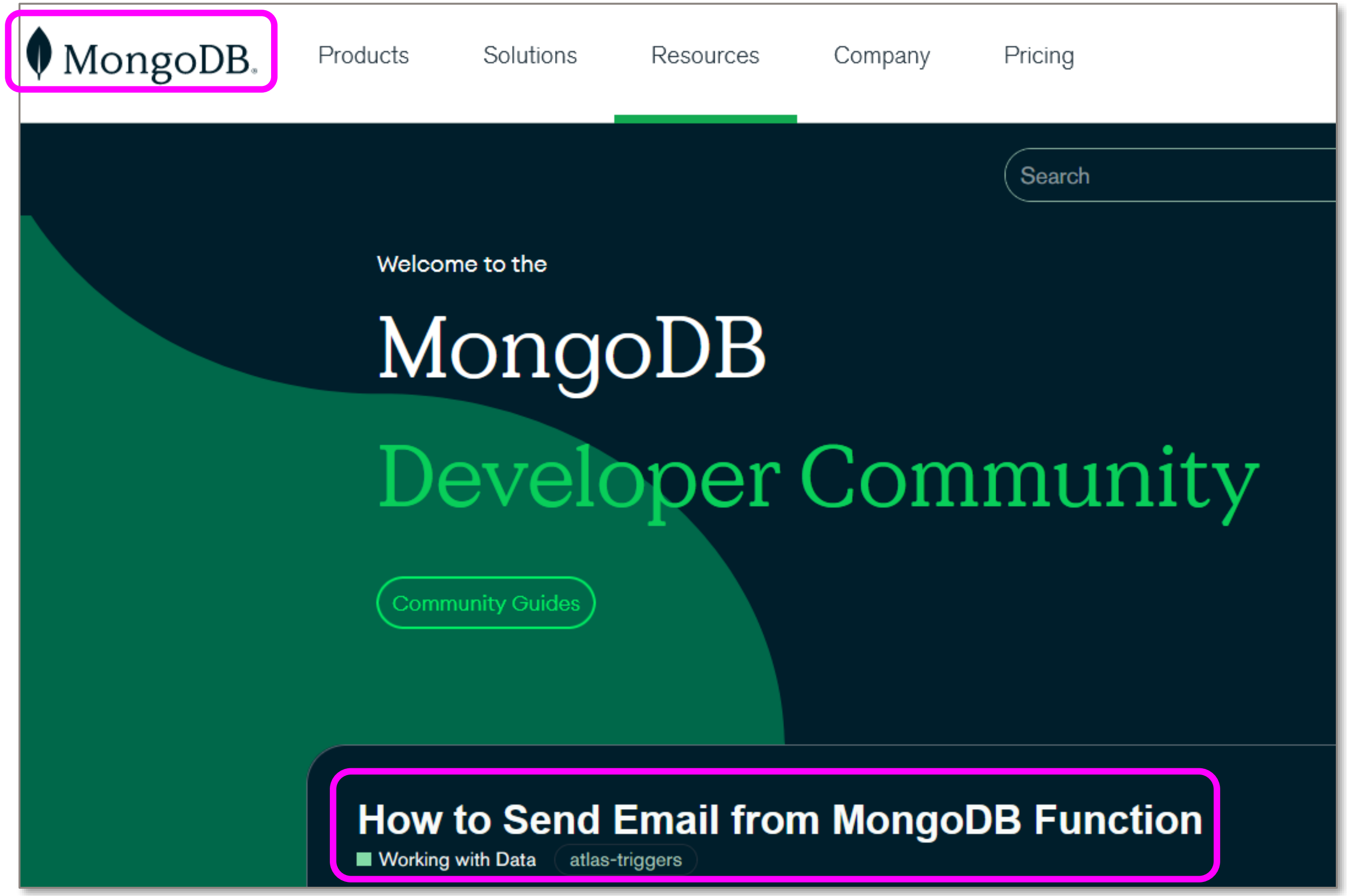
Home › Community › Blogs

Jong-kil Park

June 20, 2016 | 2 minute read

How to send an email containing query results using xp_sendmail()

In MongoDB?



Welcome to the

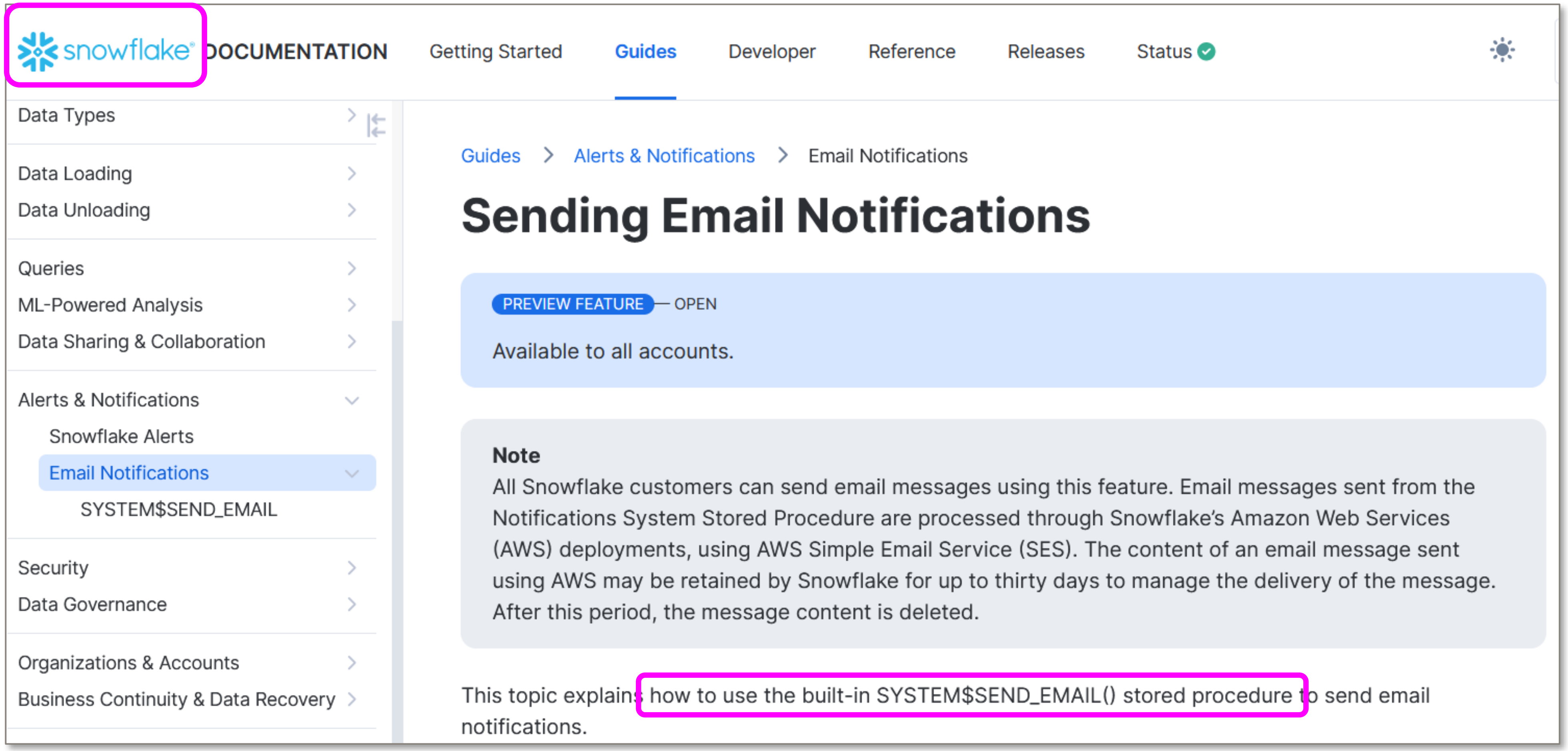
MongoDB

Developer Community

How to Send Email from MongoDB Function

🟩 Working with Data atlas-triggers

In Snowflake?



Sending Email Notifications

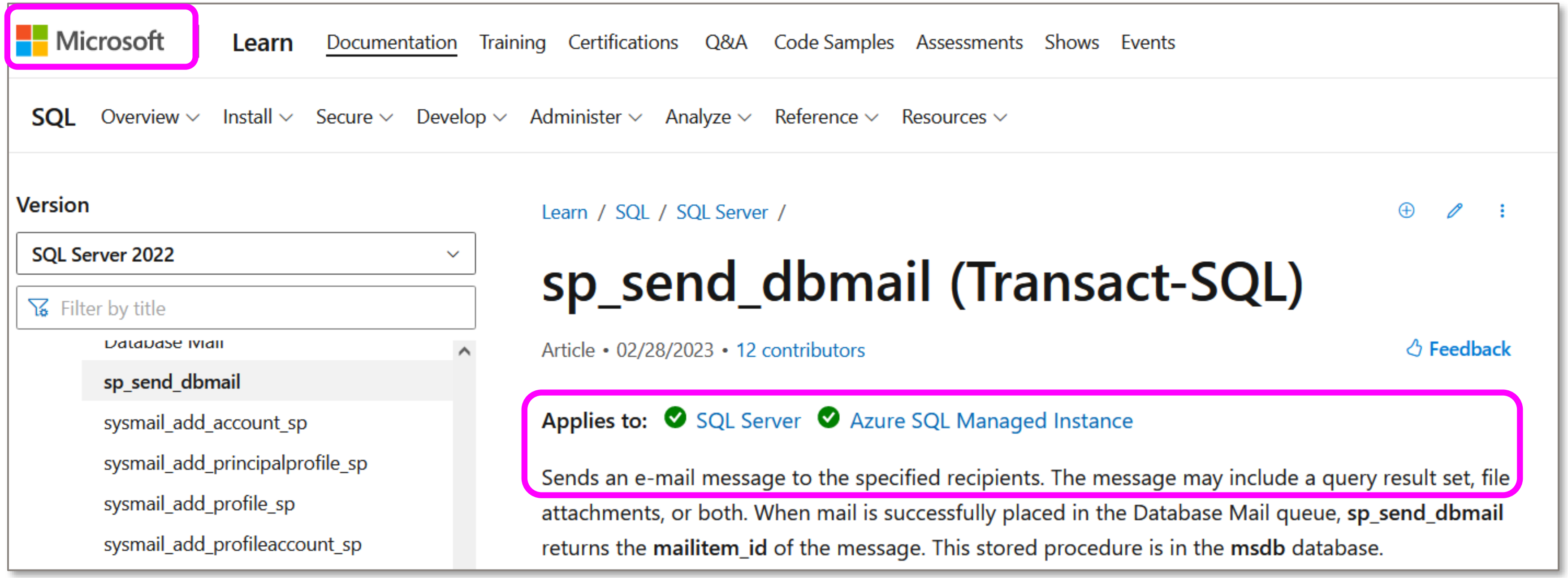
PREVIEW FEATURE — OPEN

Available to all accounts.

Note
All Snowflake customers can send email messages using this feature. Email messages sent from the Notifications System Stored Procedure are processed through Snowflake's Amazon Web Services (AWS) deployments, using AWS Simple Email Service (SES). The content of an email message sent using AWS may be retained by Snowflake for up to thirty days to manage the delivery of the message. After this period, the message content is deleted.

This topic explains how to use the built-in SYSTEM$SEND_EMAIL() stored procedure to send email notifications.

In Microsoft SQL Server and the Azure Cloud?



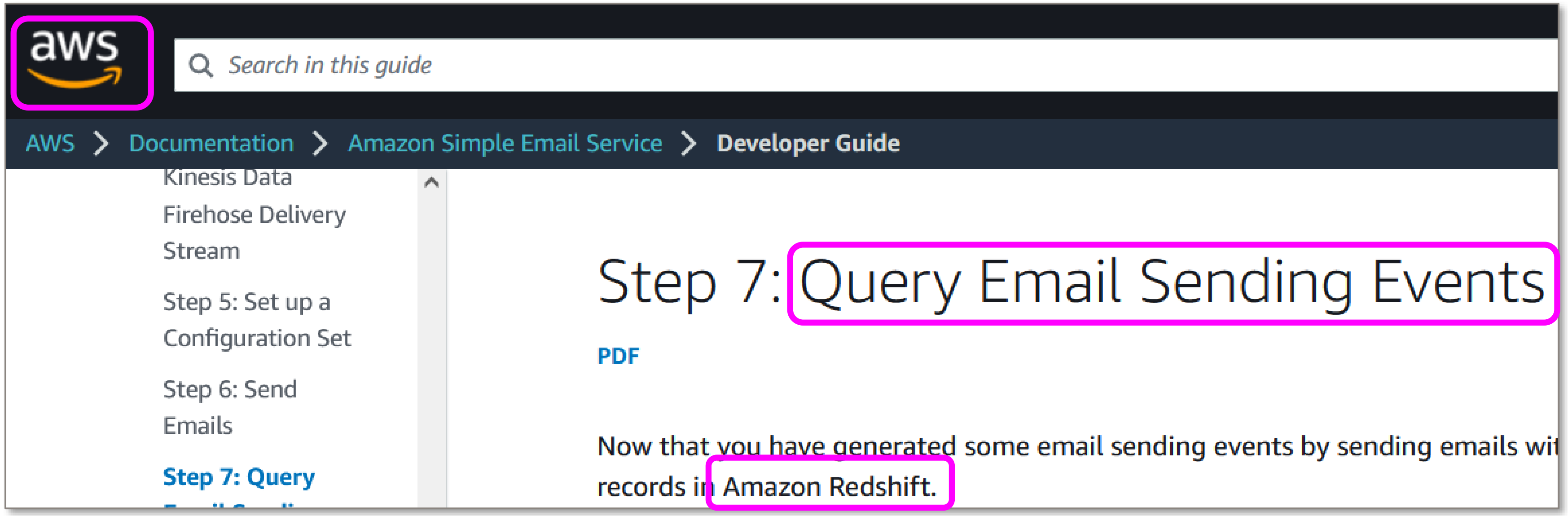
sp_send_dbmail (Transact-SQL)

Article • 02/28/2023 • 12 contributors

Applies to: ✓ SQL Server ✓ Azure SQL Managed Instance

Sends an e-mail message to the specified recipients. The message may include a query result set, file attachments, or both. When mail is successfully placed in the Database Mail queue, **sp_send_dbmail** returns the **mailitem_id** of the message. This stored procedure is in the **msdb** database.

In Amazon Redshift and the AWS Cloud?

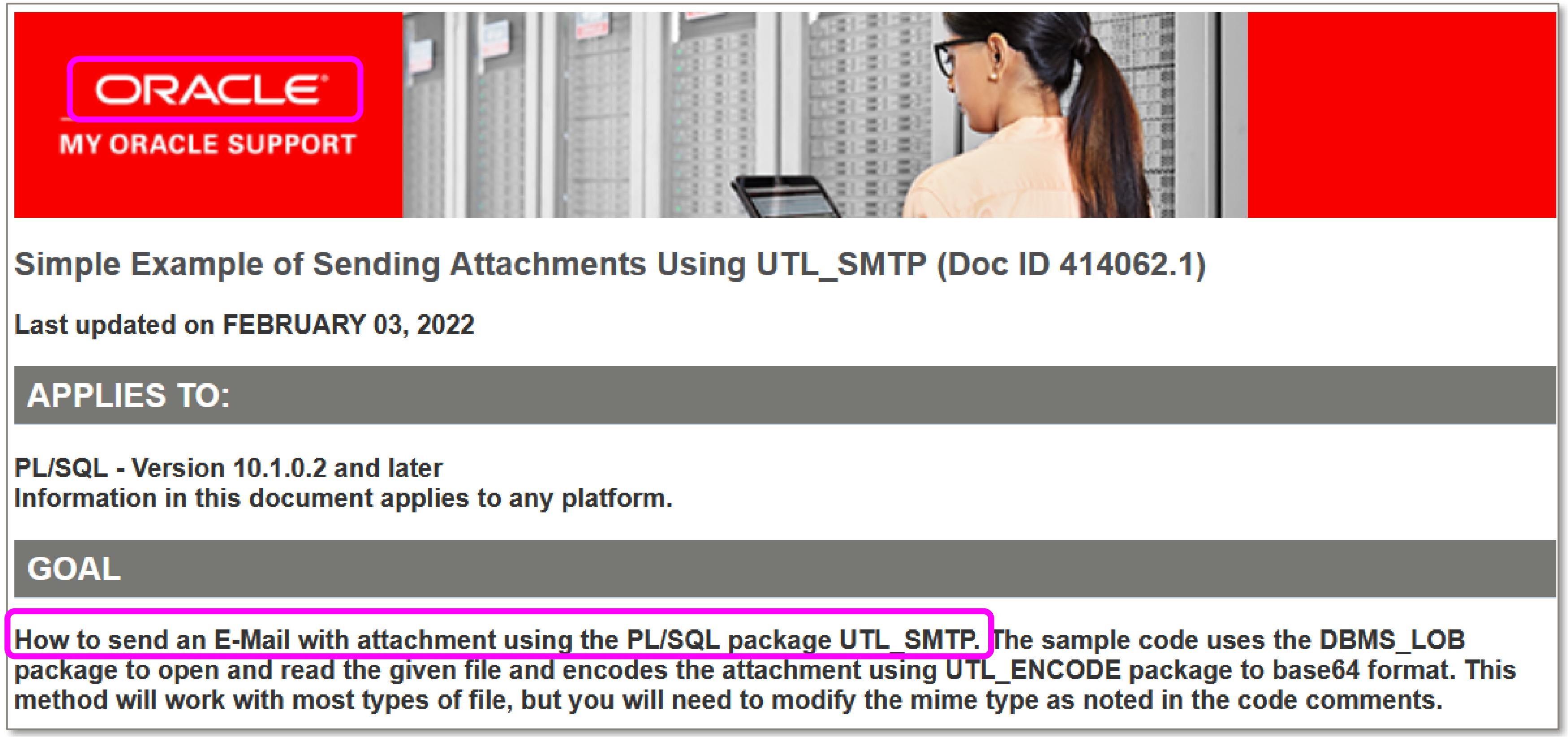


aws
Search in this guide
AWS > Documentation > Amazon Simple Email Service > Developer Guide
Kinesis Data Firehose Delivery Stream
Step 5: Set up a Configuration Set
Step 6: Send Emails
Step 7: Query
PDF

Step 7: Query Email Sending Events

Now that you have generated some email sending events by sending emails wit
records in Amazon Redshift.

Dual-Use Technology has been in our Database for 30+ years



Simple Example of Sending Attachments Using UTL_SMTP (Doc ID 414062.1)

Last updated on FEBRUARY 03, 2022

APPLIES TO:

PL/SQL - Version 10.1.0.2 and later
Information in this document applies to any platform.

GOAL

How to send an E-Mail with attachment using the PL/SQL package UTL_SMTP. The sample code uses the DBMS_LOB package to open and read the given file and encodes the attachment using UTL_ENCODE package to base64 format. This method will work with most types of file, but you will need to modify the mime type as noted in the code comments.

Dual-Use Technology Examples

Category	Example
Exfiltration: File System	CREATE EXTERNAL TABLE DBMS_ADVISOR.CREATE_FILE DBMS_DATAPUMP.OPEN DBMS_LOB.CLOB2FILE DBMS_XMLDOM.WRITETOFILE DBMS_XSLPROCESSOR.CLOB2FILE JVMFCB.PUT UTL_FILE.PUT_LINE
Exfiltration: TCP/IP Network	DBMS_AQELM DBMS_DATAPUMP DBMS_DEBUG_JDWP.CONNECT_TCP UTL_SMTP.OPEN_CONNECTION UTL_TCP.OPEN_CONNECTION
Reconnaissance	OEM RMAN UTL_INADDR.GET_HOST_NAME
SQL Rewrite	DBMS_ADANCED_REWRITE DBMS_SQLDIAG DBMS_SQL_TRANSLATION

Demos Live in SQL*Plus

One of these exploits was demonstrated at Blackhat 2005.

The other has been published in at least 2 books: One by Oracle Press.

These are not bugs any more than macros in Microsoft Excel are bugs …
these are examples of dual-use functionality
that can be easily blocked and monitored.

Imaged by Heritage Auctions, HA.com

Secure Configuration

A Few Important Points Before We Get Started

Everything you are about to see in this section relates to an emergent threat or a "recommended practice" that will assist you in reducing the attack surface of your Oracle Databases

We are sharing this information with you so that you can better protect your data, your databases, and your organization

In doing so, it is not our goal to make computing more dangerous, so please treat this information appropriately and do not share it outside of your IT and Security groups

Every capability and remediation I will show is available in Enterprise Edition and does not require use of any additional options or products

Who Is Responsible for Secure Configuration (1:3)

The Oracle Database on installation can be configured to be the most secure enterprise ready commercial database but, by default, the majority of the database's security features are configured for maximum backward compatibility

Let's go back more than 30 years to look at two examples that demonstrate that it is DBAs that must configure database security

<u>Database Profile</u>

Think of the Logical Reads and other DB Profile resources as privileges that should be granted based on the Principle of Least Privilege: **`UNLIMITED`** is not the smallest

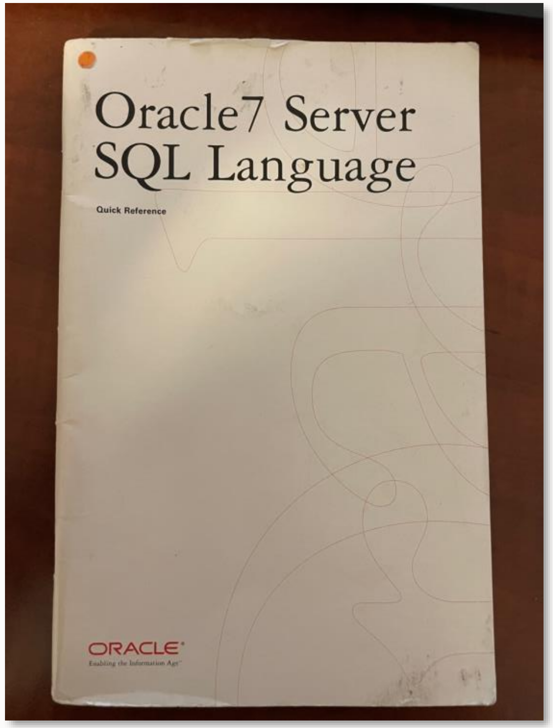
```
create profile "DEFAULT" limit
  composite_limit                 unlimited
  sessions_per_user               unlimited
  cpu_per_session                 unlimited
  cpu_per_call                    unlimited
  logical_reads_per_session       unlimited
  logical_reads_per_call          unlimited
  idle_time                       unlimited
  connect_time                    unlimited
  private_sga                     unlimited
  failed_login_attempts           10
  password_life_time              unlimited
  password_reuse_time             unlimited
  password_reuse_max              unlimited
  password_verify_function        null
  password_lock_time              unlimited
  password_grace_time             unlimited
  inactive_account_time           365
  password_rollover_time          0
  container=current;
```

`ALTER PROFILE` was created to provide customers the ability to modify kernel resource limits based on the needs of the applications and, as Oracle doesn't know that requirement, set them at the time of installation at the highest level

Who Is Responsible for Secure Configuration (2:3)

Privilege Grants

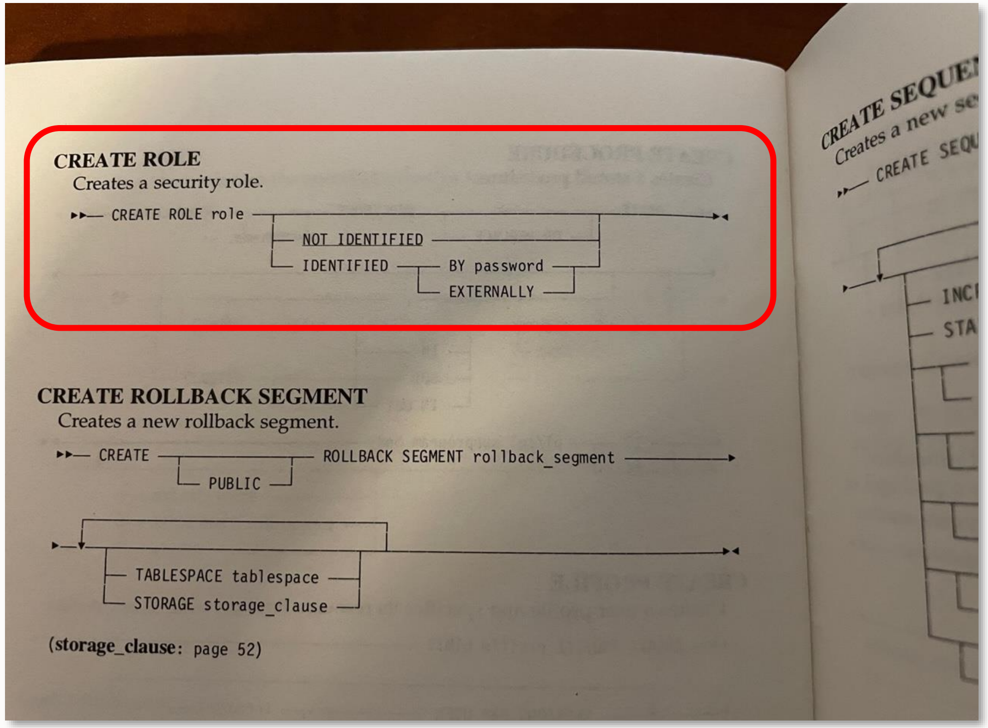
For more than 30 years the Oracle Database has enabled MFA to password protect escalated privileges from abuse: Oracle cannot know what roles, requiring what privileges, for every application purchased or built by every one of its customers



Oracle7 Server SQL Language

Quick Reference

ORACLE



CREATE ROLE

Creates a security role.

```
▸▸— CREATE ROLE role ──┬──────────────────────────────────┬──▸◂
                       ├─ NOT IDENTIFIED ─────────────────┤
                       └─ IDENTIFIED ──┬─ BY password ──┬─┘
                                       └─ EXTERNALLY ───┘
```

CREATE ROLLBACK SEGMENT

Creates a new rollback segment.

```
▸▸— CREATE ─┬──────────┬─ ROLLBACK SEGMENT rollback_segment ──────▸
            └─ PUBLIC ─┘

▸─┬─┬─────────────────────────┬─┬────────────────────────────────▸◂
  │ ├─ TABLESPACE tablespace ─┤ │
  │ └─ STORAGE storage_clause ┘ │
  └─────────────────────────────┘
```

(**storage_clause:** page 52)

CREATE SEQUE

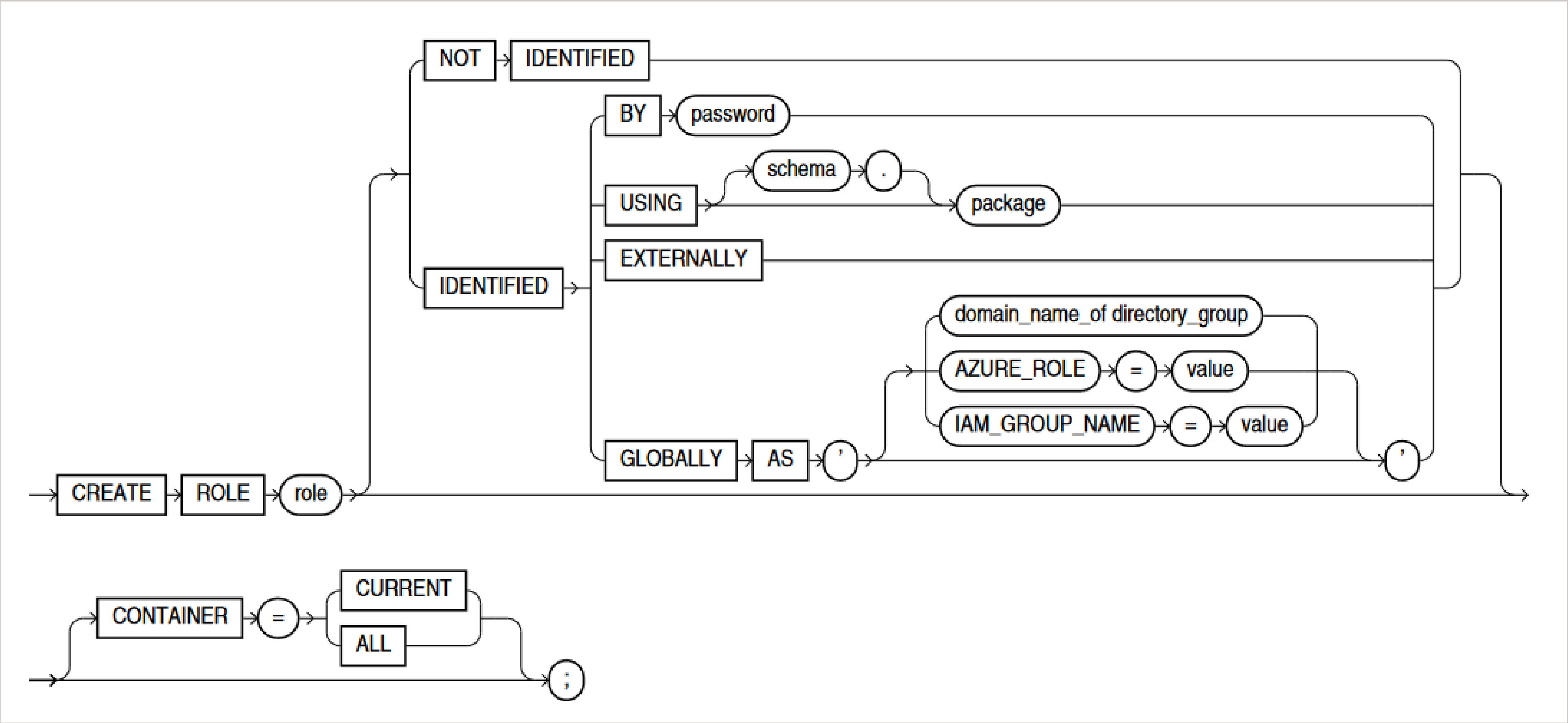
Creates a new se

```
▸▸— CREATE SEQU

▸─┬─ INC
  └─ STA
```

Again, the syntax supports our customers customizing configuration to meet their needs

Who Is Responsible for Secure Configuration (3:3)



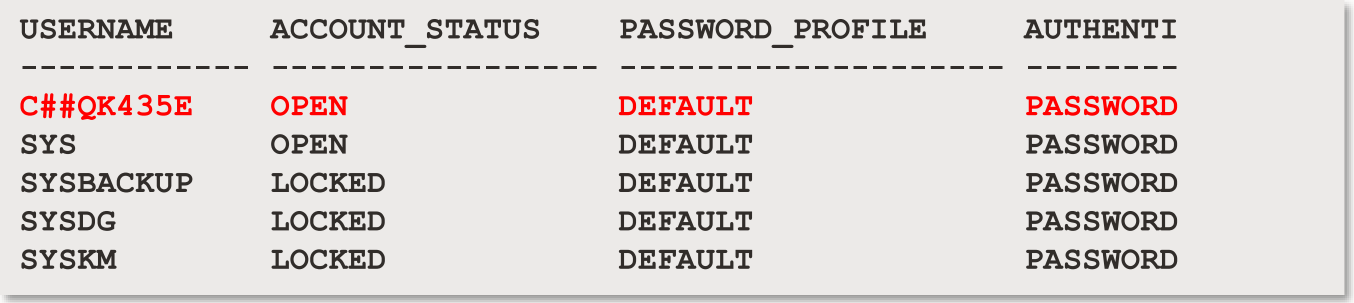
IAM: Oracle Identity and Access Management

Authentication

It is not unusual to find Oracle 19c databases that have been upgraded version-after-version for decades with legacy users and configurations impacting current security.

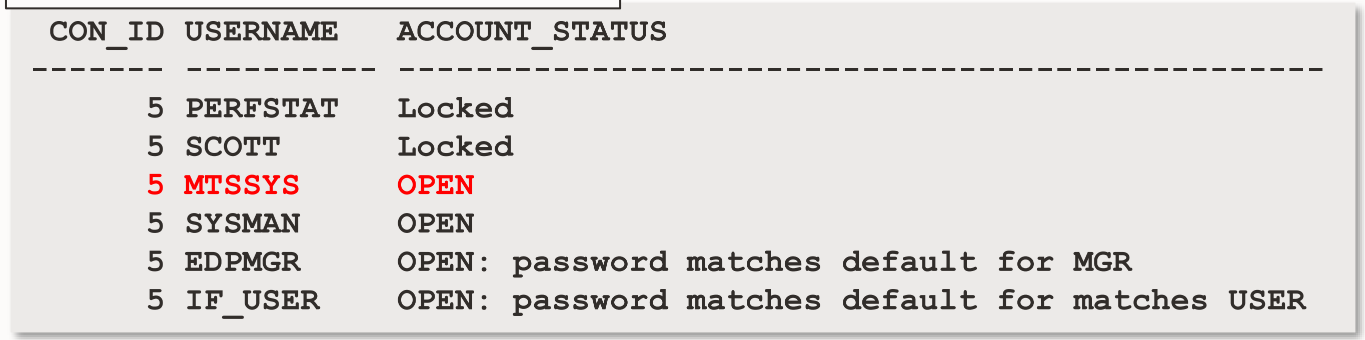
The user accounts highlighted bypass central user management (LDAP) and violate Zero Trust and compliance frameworks like CIS

Found in a Password File



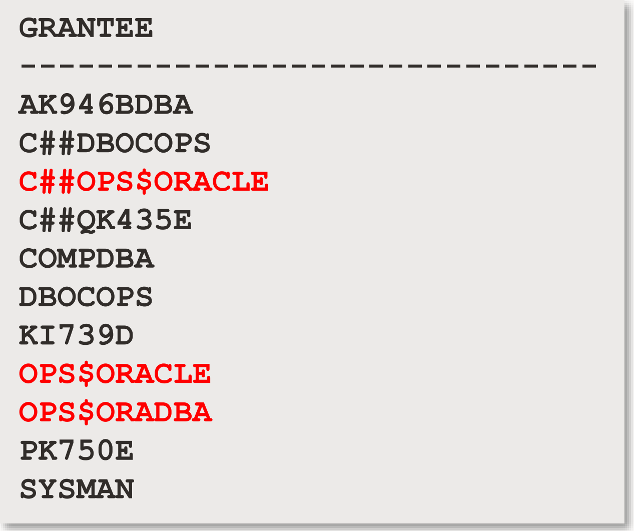
```
USERNAME     ACCOUNT_STATUS     PASSWORD_PROFILE      AUTHENTI
------------ ------------------ --------------------- --------
C##QK435E    OPEN               DEFAULT               PASSWORD
SYS          OPEN               DEFAULT               PASSWORD
SYSBACKUP    LOCKED             DEFAULT               PASSWORD
SYSDG        LOCKED             DEFAULT               PASSWORD
SYSKM        LOCKED             DEFAULT               PASSWORD
```

Default Users with Default Passwords



```
 CON_ID USERNAME   ACCOUNT_STATUS
------- ---------- ----------------------------------------------------
      5 PERFSTAT   Locked
      5 SCOTT      Locked
      5 MTSSYS     OPEN
      5 SYSMAN     OPEN
      5 EDPMGR     OPEN: password matches default for MGR
      5 IF_USER    OPEN: password matches default for matches USER
```

Externally Authenticated Users



```
GRANTEE
------------------------------
AK946BDBA
C##DBOCOPS
C##OPS$ORACLE
C##QK435E
COMPDBA
DBOCOPS
KI739D
OPS$ORACLE
OPS$ORADBA
PK750E
SYSMAN
```

Central User Management

Most medium to large enterprises deploy LDAP and similar solutions to simplify user management. These systems may employ Oracle products or third-party solutions such as CyberArk and Microsoft Active Directory

What they all have in common is a database configuration vulnerability that can be exploited by a sophisticated attack and which Oracle Consulting can address through a ***Consulting Configuration Extension***

What all CMU solutions have in common is that the database must be configured to validate a connection outside of the database and the local operating system

```
CREATE USER safeadmin IDENTIFIED GLOBALLY AS 'cn=safeadmin,cn=Users,dc=dbsecworx,dc=com';
```

and it is this requirement that provides an opportunity to prevent exploitation

If you are interested in learning more about this Extension, please ask and we would be happy to set up a separate workshop to explain how it works

DBA

Authentication Attack Surface Reduction Report

Regularly monitor the Oracle Database password file for inappropriate entries

Regularly monitor C

Regularly monitor C s and SYSTEM authenticated by pa

Regularly monitor C words

Performing a manua ve conditions from time-to-time to veri system, triggers an alert captured by your security team, and that the DBA team is alerted to the violation and has a standard protocol for addressing the issue

If you do not strictly observe recommended authentication security practices, internal users and users with phished credentials can bypass your Centrally Managed User controls and log in with escalated privileges even if they have been removed from the system.

Exfiltration

DBA

A majority of database break-ins require exfiltration, a way to successfully get stolen data off of the victim's premises, and one of the most common is writing it to a file system in a way that won't be observed or detected: This will require that they gain access to TCP/IP network or a file system

As an Oracle professional you are likely to immediately think of the UTL_FILE built-in package and it is for that reason, that you'd think about it, that it is likely a serious professional would decide not to use it but instead use other built-in tools

Exfiltration Options that should be on your radar

- CREATE EXTERNAL TABLE
- DBMS_ADVISOR
- DBMS_LOB
- DBMS_XMLDOM
- DBMS_XSLPROCESSOR
- JVMFCB
- UTL_FILE

Time to exfiltrate 200,000 lines of source code from SYS.SOURCE$

Package	Procedure	File Size (MB)	Run Time (sec.)
UTL_FILE	PUT_LINE	13.4	07.33
DBMS_ADVISOR	CREATE_FILE	16.1	01.04
DBMS_XSLPROCESSOR	CLOB2FILE	15.8	00.93

Exfiltration Attack Surface Reduction Report

DBA

What all of these attacks, except one, have in common:

- Require privileges to use a DIRECTORY object
- CREATE TABLE privilege is almost universally ignored as a security risk
- Built-in packages have EXECUTE granted to PUBLIC
- Our customers do not require security authorizations for their use
- Creation and use are rarely audited and, if in the audit trail, do not raise an alarm

A database user with access to DBMS_XSLPROCESSOR can write your data and your source code to disk at more than 200,000 lines per second.

Audit the grants and actions related to these exploits, both successful and unsuccessful

Educate your internal auditors about the associated risks and develop an action plan for how to respond if misuse is detected

DBA

Rewrite Vulnerabilities

Many of our customers use end-point monitoring and firewalls to detect database accesses that fit a defined risk profile. Attackers know this and look for ways to use existing SQL to bypass detection: One way they do it is through rewrite which transforms SQL inside the database's memory

The following rewrite options should be on your radar

Package	Procedure	Risk
DBMS_ADVANCED_REWRITE	DECLARE_REWRITE_EQUIVALENCE	Can refactor a SQL statement inside the optimizer
DBMS_SQLDIAG	CREATE_SQL_PATCH	Can add hints to existing SQL creating a Denial-of-Service attack
DBMS_SQL_TRANSLATION	REGISTER_SQL_TRANSLATION	Can refactor a SQL statement inside the optimizer

DBA

Rewrite Vulnerability Examples

DBMS_ADVANCED_REWRITE (version 10.1) stealing data

```
BEGIN
  dbms_advanced_rewrite.declare_rewrite_equivalence(
   'GFRW',
   'SELECT cc_final4 FROM gf.credit_card',
   'SELECT ccno FROM gf.credit_card',
    FALSE,
   'RECURSIVE');
END;
/

PL/SQL procedure successfully completed.
```

```
SQL> SELECT cc_final4 FROM gf.credit_card;

CC_FINAL4
-------------------
4370-1234-5678-0042
3704-4321-8765-1950
```

DBMS_SQL_TRANSLATOR (version 12.1) generating data corruption

```
exec dbms_sql_translator.register_sql_translation(
  profile_name    => 'GF_TSQLTRANS',
  sql_text        => 'SELECT srvr_id INTO gf.tsql_target FROM gf.servers',
  translated_text => 'INSERT INTO gf.tsql_target SELECT srvr_id FROM gf.servers');
```

DBMS_SQLDIAG (version 12.2) creating a DDOS attack

```
SELECT /*+ FULL(mr) NO_INDEX(mr.pk_med_records) NO_PARALLEL */ patient_name
FROM med_records mr
WHERE mr.transaction# = 999999991;
```

REWRITE Attack Surface Reduction Report

DBA

Oracle has used a variety of techniques to protect our customers from these attacks, but you must be aware of the risks and how to detect and prevent them

Audit all grant cutions of DBMS_ADVAN TION

Monitor the u or changes such as **`SYS.SUM$`**

Rewrite attacks are, by definition, not detectable by end-point, tripwire, or firewall technologies.

They can only be prevented or detected by DBAs managing securely configured environments.

Monitor system privilege grants such as **`EXECUTE`**, **`EXECUTE ANY`**, **`ALTER ANY SQL TRANSLATION PROFILE`**, **`CREATE ANY SQL TRANSLATION PROFILE`**, **`TRANSLATE ANY SQL`** and **`USE ANY SQL TRANSLATION PROFILE`**

Educate your internal auditors about the associated risks and develop an action plan for how to respond if misuse is detected

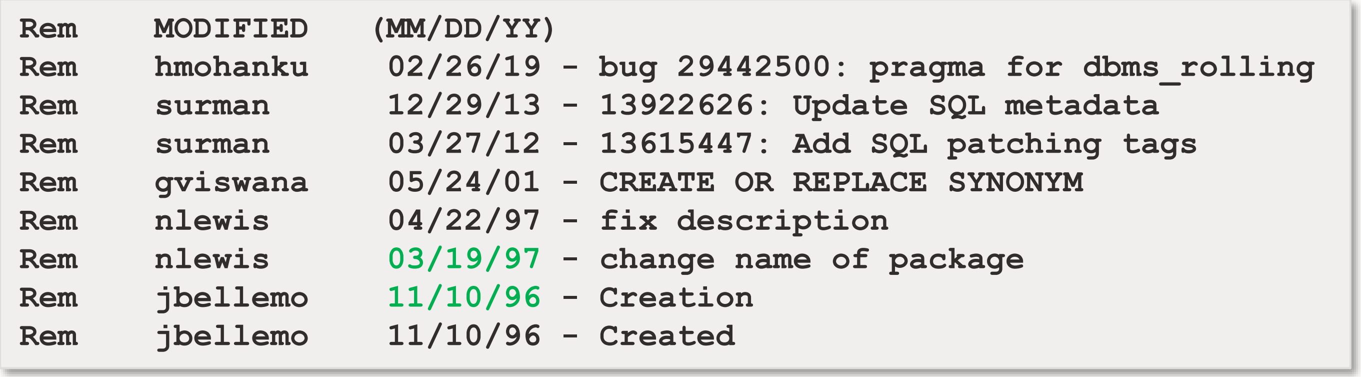
DBA

DBMS_DISTRIBUTED_TRUST_ADMIN (1:2)

By default, a user with the **CREATE [ANY] DATABASE LINK** privilege can create a link to any database they wish because, by default, trust administration is set to **ALLOW ALL**

With our focus these days on Zero Trust it may be a bit disheartening to know that every database in your enterprise has Distributed Trust configured to **ALLOW ALL**, but this default was established more than 30 years ago when security was not the issue it is today

Oracle realized this was a security risk and, with backward compatibility in mind, released the fully documented DBMS_DISTRIBUTED_TRUST_ADMIN package in 9.0.1 to allow customers to change the default to `DENY_ALL` and then grant permissions for database links on a host-by-host basis



```
Rem    MODIFIED   (MM/DD/YY)
Rem    hmohanku    02/26/19 - bug 29442500: pragma for dbms_rolling
Rem    surman      12/29/13 - 13922626: Update SQL metadata
Rem    surman      03/27/12 - 13615447: Add SQL patching tags
Rem    gviswana    05/24/01 - CREATE OR REPLACE SYNONYM
Rem    nlewis      04/22/97 - fix description
Rem    nlewis      03/19/97 - change name of package
Rem    jbellemo    11/10/96 - Creation
Rem    jbellemo    11/10/96 - Created
```

DBA

DBMS_DISTRIBUTED_TRUST_ADMIN (2:2)

Look at how Distributed Trust is currently configured: Likely to ALLOW ALL (+*)

```
SELECT * FROM trusted_list$;

DBNAME                          USERNAME
------------------------------- --------------
+*                              *
```

Reduce the attack surface by updating Trust Administration to DENY_ALL (-*)

```
exec dbms_distributed_trust_admin.deny_all;

SELECT * FROM trusted_list$;

DBNAME                          USERNAME
------------------------------- --------------
-*                              *
```

Then create an ALLOW statement for specific servers as required

```
exec dbms_distributed_trust_admin.allow_server('ENCLAVE.ORCL.COM');

SELECT * FROM trusted_list$;

DBNAME                          USERNAME
------------------------------- --------------
-*                              *
enclave.orcl.com                *
```

DBA

TRUST ADMIN Attack Surface Reduction Report

The DBMS_DISTRIBUTED_TRUST_ADMIN package is owned by SYS with EXECUTE granted to the EXECUTE_CATALOG_ROLE role

The EXECUT SE and
IMP_FULL_ istration

White-listing servers and hosts will reduce the likelihood that an attacker with access to a low priority database will use that foothold to tunnel into a higher priority system.

Revoke the grant of EXECUTE from EXECUTE_CATALOG_ROLE and grant it explicitly to schemas that require it

Audit all grants of EXECUTE for DBMS_DISTRIBUTED_TRUST_ADMIN
Audit all executions of DBMS_DISTRIBUTED_TRUST_ADMIN, both successful and unsuccessful
Audit all database links is required and drop all database links that are no long in use

Update Distributed Trust to DENY_ALL and execute ALLOW_SERVER statements for servers to which database links are required

Data-in-Motion Encryption (1:2)

DBA

The overwhelming majority of SQLNET.ORA files we see look like one of the following

```
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
```

```
NAMES.DEFAULT_DOMAIN              = zzyzx.com
NAMES.DIRECTORY_PATH              = (LDAP, TNSNAMES, EZCONNECT)
NAMES.REQUEST_RETRIES             = 2
SQLNET.EXPIRE_TIME                = 0
SQLNET.INBOUND_CONNECT_TIMEOUT = 250

SQLNET.ALLOWED_LOGON_VERSION_CLIENT=8
SQLNET.ALLOWED_LOGON_VERSION_SERVER=8

WALLET_LOCATION =
  (SOURCE = (METHOD = File)
    (METHOD_DATA =
      (DIRECTORY = /oradba/app/oracle/admin/cde01p65/wallet)))
```

Note the complete lack of encryption

DBA

Data-in-Motion Encryption (2:2)

What we would like to see as it is included in every customer's existing license agreement

```
NAMES.DIRECTORY_PATH=(TNSNAMES, EZCONNECT)
SQLNET.EXPIRE_TIME=10
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT=(SHA256,SHA384,SHA512,SHA1)
SQLNET.ENCRYPTION_SERVER=REQUESTED
SQLNET.CRYPTO_CHECKSUM_SERVER=ACCEPTED
SQLNET.ENCRYPTION_TYPES_SERVER=(AES256,AES192,AES128)
SQLNET.IGNORE_ANO_ENCRYPTION_FOR_TCPS=TRUE
SQLNET.ENCRYPTION_CLIENT=REQUESTED
SQLNET.ENCRYPTION_TYPES_CLIENT=(AES256,AES192,AES128)
SQLNET.CRYPTO_CHECKSUM_CLIENT=ACCEPTED
HTTPS_SSL_VERSION=1.2
SSL_VERSION=1.2
SSL_CIPHER_SUITES=(SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA38
4,SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256,SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
                        (METHOD_DATA=(DIRECTORY=/var/opt/oracle/dbaas_acfs/grid/tcps_wallets)))
SQLNET.WALLET_OVERRIDE=FALSE
SSL_CLIENT_AUTHENTICATION=FALSE
```

This is part of the reason the OCI Cloud has a higher level of security than most customer environments (this is the default configuration for Oracle Exadata Cloud@Customer)

Valid Node Checking

When we think about the concept of Principle of Least Privilege, we often accept the narrowest possible definition of the term

Without Valid Node Checking your databases can be compromised by anyone with valid credentials or an attack on your Identity Management system.

Valid Node Checking adds an additional factor that requires knowledge that cannot be phished.

Allowing conn rough
255.255.255

Valid Node Ch d allows listener conne

- Improves d node
- Nodes can also be excluded with a list of excluded nodes
- Eliminates complex COST* setups to ensure malicious servers do not register with a listener

```
VALID_NODE_CHECKING_REGISTRATION_LISTENER=ON
TCP.INVITED_NODES=(appserver.us.oracle.com, 144.185.5.*, 10.3.0.4)
```

A newer version, Valid Node Checking for Registration (VNCR), requires that RAC nodes originate only from a list of known, white-listed, IP addresses

* Class Of Secure Transport

Valid Node Checking Attack Surface Reduction Report

DBA

Multi-Factor Authentication should mean "multiple factors" and should not be limited to the generic and predictable such as userid, password, and a token

The Oracle Database supports additional factors the majority of which do not require changes in application coding or an additional burden on human users

Valid Node Checking can transparently restrict logins to only application servers, monitoring applications (for example OEM), RAC cluster nodes, and specific individuals with escalated privileges allowing using a limited number of approved desktops or jump servers

Password Rollover

DBA

A new password resource has been added to Database Profiles that makes it possible to eliminate all downtime associated with changing application database passwords

It is not unusual for an application password change to require an extended outage while application servers are reconfigured with the new password

PASSWORD_ROLLOVER_TIME, makes it possible to access a database schema simultaneously, with two different passwords (both old and new), while password changes are taking place

At the end of the rollover time the old password is automatically invalidated

Released in 21c, Backported to 19.12

```
SELECT profile, limit
FROM dba_profiles
WHERE resource_name = 'PASSWORD_ROLLOVER_TIME';

PROFILE                        LIMIT
------------------------------ ------------------
DEFAULT                        0
ORA_CIS_PROFILE                0
ORA_STIG_PROFILE               DEFAULT

ALTER PROFILE ora_cis_profile LIMIT password_rollover_time 3;

Profile altered.

SELECT profile, limit
FROM dba_profiles
WHERE resource_name = 'PASSWORD_ROLLOVER_TIME';

PROFILE                        LIMIT
------------------------------ ------------------
DEFAULT                        0
ORA_CIS_PROFILE                3
ORA_STIG_PROFILE               DEFAULT
```

DBA

Password Rollover Attack Surface Reduction Report

Setting and using Password Rollover Time makes it possible to alter application passwords, enterprise-wide, without a loss of service

Password management rules for applications and service accounts can be brought in line with rules and regulations governing all passwords with respect to change frequency and reuse

Failure to regularly change passwords …
Failure to change passwords after key personnel changes …
Are known causes for a substantial percentage of breaches.

Using the new Password Rollover feature means that password changes for complex system no longer require a loss of service.

Blockchain Tables

Dev

Blockchain relational tables provide an extremely tamper resistant means of storing relational data in a form wherein it can be accessed using SQL and where there is a dependency (chain) between rows

Hashing with SHA2 512 guarantees chain integrity
ALTER TABLE statements can increase, but never decrease, the protections

```
CREATE BLOCKCHAIN TABLE <schema_name>.<table_name>(
<column_name> <column_data_type>)
NO DROP [UNTIL <integer> DAYS IDLE]
NO DELETE [UNTIL <integer DAYS AFTER INSERT]
HASHING USING "<hashing_algorithm>" VERSION "<version_number>"
 [sharing_clause]
 [memoptimize_clause]
 [relational_properties];
```

```
CREATE BLOCKCHAIN TABLE ledger0(
tx_id    INTEGER,
tx_date  DATE,
tx_value NUMBER(10,2))
NO DROP UNTIL 17 DAYS IDLE
NO DELETE UNTIL 17 DAYS AFTER INSERT
HASHING USING "SHA2_512" VERSION "v1"
TABLESPACE nist;
```

Immutable Tables

Immutable relational tables provide an extremely tamper resistant means of storing relational data in a form wherein it can be accessed using SQL

Immutable tables are for use when rows, once committed, must be tamper proof, such as in an audit trail and where inter-row dependencies are not important, such as in an audit trail

As demonstrated in the example below, integrity is guaranteed by constraints on dropping and deleting

```
CREATE IMMUTABLE TABLE <schema_name>.<table_name>(
<column_name> <column_data_type>)
NO DROP [UNTIL <integer> DAYS IDLE]
NO DELETE [UNTIL <integer> DAYS AFTER INSERT
[sharing_clause]
[memoptimize_clause]
[relational_properties];
```

```
CREATE IMMUTABLE TABLE audit0(
tx_id    INTEGER,
tx_date  DATE,
tx_value NUMBER(10,2))
NO DROP UNTIL 365 DAYS IDLE
NO DELETE UNTIL 95 DAYS AFTER INSERT
TABLESPACE nist;
```

Blockchain & Immutable Table Integrity Testing (1:5)

Dev

```
UPDATE ledger0 SET tx_value = 200;
UPDATE ledger0 SET tx_value = 200
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain table

DELETE FROM ledger0;
DELETE FROM ledger0
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain table

TRUNCATE TABLE ledger0;
TRUNCATE TABLE ledger0
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain table

DROP TABLE ledger0 PURGE;
DROP TABLE ledger0 PURGE
           *
ERROR at line 1:
ORA-05723: dropping LEDGER0, which is a non-empty blockchain or immutable table, is not allowed
```

Dev

Blockchain & Immutable Table Integrity Testing (2:5)

```
ALTER TABLE ledger0 ADD new_col VARCHAR2(20);
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain or immutable table

ALTER TABLE ledger0 RENAME COLUMN testcol TO diffcol;
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain or immutable table

ALTER TABLE ledger MODIFY (tx_value NUMBER(12,2));
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain or immutable table

ALTER TABLE ledger DROP COLUMN tx_value;
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain or immutable table
```

Blockchain & Immutable Table Integrity Testing (3:5)

Dev

```
SQL> ALTER TABLE ledger0 NO DROP UNTIL 16 DAYS IDLE;
ALTER TABLE ledger0 NO DROP UNTIL 16 DAYS IDLE
*
ERROR at line 1:
ORA-05732: retention value cannot be lowered

SQL> ALTER TABLE ledger0 NO DELETE UNTIL 16 DAYS AFTER INSERT;
ALTER TABLE ledger0 NO DELETE UNTIL 16 DAYS AFTER INSERT
*
ERROR at line 1:
ORA-05732: retention value cannot be lowered
```

Blockchain & Immutable Table Integrity Testing (4:5)

Renaming is also not allowed

```
SQL> RENAME ledger1 TO ledger2;
RENAME ledger1 TO ledger2
*
ERROR at line 1:
ORA-05715: operation not allowed on the blockchain or immutable table
```

Dropping a tablespace with a Blockchain or Immutable table will be equally unsuccessful

```
SQL> DROP TABLESPACE uwdata INCLUDING CONTENTS AND DATAFILES;
DROP TABLESPACE uwdata INCLUDING CONTENTS AND DATAFILES
*
ERROR at line 1:
ORA-00604: error occurred at recursive SQL level 1
ORA-05723: drop blockchain or immutable table LEDGER1 not allowed
```

I will not be able to drop this table until next year because I forgot to change the NO DROP parameter to the minimum, 16 days, when I built it

Immutable Table Attack Surface Reduction Report

Dev

Deploy blockchain tables where you must guarantee data integrity and there is a dependency (chaining) of rows such as in a ledger

Deploy immuta /
dependencies

Blockchain and espectively but
have been bac

Tables holding e storage

Zero Trust is not a checkbox.

To achieve Zero Trust, you need to start working today to create a trusted environment.

Blockchain and Immutable tables add a layer of trust that cannot be achieved with any other technology.

DBMS_LOG

DBMS_LOG is an undocumented, unsupported package with four subprograms that, prior to 12.1, were in DBMS_SYSTEM: Attackers don't care if something is undocumented

These subprograms can be used to write messages to the ALERT LOG from which they may trigger alerts, and lead to destructive mistakes, as demonstrated here

```
SQL> conn / as sysdba

BEGIN
  dbms_log.ksdfls;      -- flush any pending messages to the alert log
  dbms_log.ksdddt;      -- print the current date-time to make this look official
  dbms_log.ksdwrt(2, 'ORA-00600: look out, too late, something bad just happened');
  dbms_log.ksdwrt(2, 'ORA-00911: open a Sev 4 service request at MyOracleSupport');
  dbms_log.ksdwrt(2, 'ORA-07445: start drinking beer while waiting for MOS to respond');
  dbms_log.ksdwrt(2, 'ORA-07446: after the 7th beer run the following SQL statement');
  dbms_log.ksdwrt(2, 'ORA-07447: DROP PACKAGE sys.standard;');
END;
/
```

The message above was written to illustrate the point, but the intended target for a malicious message might be an automated service account utilized by a monitoring application

DBMS_LOG Attack Surface Reduction Report

DBA

DBMS_LOG is owned by SYS with no privileges granted

Audit all grants of EXECUTE for DBMS_LOG: There shouldn't be any

Audit all executions of DBMS_LOG, both successful and unsuccessful, not executed by SYS

Educate your internal auditors that use of this package, unless explicitly authorized, should trigger an alarm

Review any configuration or auditing changes made prior to 12.1, targeted at DBMS_SYSTEM, that may no longer be appropriate

The governments and organized crime families attacking our customers do not play by the rules.

They focus on ways to evade auditing through the use of undocumented tools and utilities.

ATTENTION LOG (1:2)

DBMS_LOG focused us on the ALERT LOG and the possibility of its misuse, so this is a good time to talk about the ATTENTION LOG, new in 21c, which is a structured JSON file containing information about critical and highly visible database events

- There is one attention log for each database instance
- A log contains pre-determined, translatable series of messages, with one message per event

```
[oracle@test21 log]$ pwd
/u01/app/oracle/diag/rdbms/test21db_iad25g/test21db/trace/

[oracle@test21 log]$ ls
attention attention.log ddl debug debug.log hcs hcs_test21db.log imdb test

[oracle@test21 log]$ more attention.log
```

The following slide has some ATTENTION LOG examples

ATTENTION LOG (2:2)

```
{
"NOTIFICATION" : "Starting ORACLE instance (normal) (OS id: 65129)",
"URGENCY" : "INFO",
"INFO" : "Additional Information Not Available",
"CAUSE" : "A command to startup the instance was executed",
"ACTION" : "Check alert log for progress and completion of command",
"CLASS" : "CDB Instance / CDB ADMINISTRATOR / AL-1000",
"TIME" : "2020-12-11T18:04:18.224+00:00"
}

{
"ERROR" : "GEN0 (ospid: 24229): terminating the instance due to ORA error 495",
"URGENCY" : "IMMEDIATE",
"INFO" : "Additional Information Not Available",
"CAUSE" : "The instance termination routine was called",
"ACTION" : "Check alert log for more information relating to instance termination rectify the
error and restart the instance",
"CLASS" : "CDB Instance / CDB ADMINISTRATOR / AL-1003",
"TIME" : "2021-01-17T02:19:27.281+00:00"
}
```

ATTENTION LOG Attack Surface Reduction

DBA

Access to the ALERT_LOG and TRACE FILES in the DIAG directory is not necessary to monitor routine operations such as opening and closing databases except in rare cases where an error is encountered in which case the ATTENTION LOG will provide guidance as to where to look

DIAG directory access should be justified on the basis of the Principle of Least Privilege

In 21c, and above, use the attention log to reduce your workload of database management and to shield the alert log from unnecessary access.

ACCESSIBLE BY Clause (1:3)

Dev

Much of our effort in database security is focused on DBAs but developers have an equally, if not more important, role to play

Enabling and properly configuring every feature and licensing every option cannot make up for an application with baked-in vulnerabilities created by the lack of permissions granularity

Prior to version 12.1 a schema owner, or a DBA with SYSDBA permissions could not be prevented from calling application PL/SQL functions, packages, and procedures: That is no longer the case

The PL/SQL Accessible By clause makes it possible to provide control permissions at the object and subprogram levels

Dev

ACCESSIBLE BY Clause (2:3)

The PL/SQL package ocs_utils has two subprogram functions

getSeed is protected by an ACCESSIBLE BY clause and can only be called from a stand-alone stored procedure named driver

getName is not protected by an ACCESSIBLE BY clause and can be called by any user or code with execute on the ocs_utils package

```
CREATE OR REPLACE PACKAGE ocs_utils AUTHID DEFINER IS
  FUNCTION getSeed RETURN VARCHAR2 ACCESSIBLE BY (PROCEDURE driver);
  FUNCTION getName RETURN VARCHAR2;
END ocs_utils;
/

CREATE OR REPLACE PACKAGE BODY ocs_utils IS
  FUNCTION getSeed RETURN VARCHAR2 ACCESSIBLE BY (PROCEDURE driver) IS
   x dbms_id;
  BEGIN
    SELECT standard_hash('Morgan') into x FROM dual;
    RETURN x;
  END getSeed;

  FUNCTION getName RETURN VARCHAR2 IS
  BEGIN
    RETURN dbms_crypto.randombytes(30);
  END getName;
END ocs_utils;
/

CREATE OR REPLACE PROCEDURE driver AUTHID DEFINER IS
 seedVal dbms_id;
BEGIN
  seedVal := ocs_utils.getSeed;
  dbms_output.put_line(seedVal);
END driver;
/
```

Dev

ACCESSIBLE BY Clause (3:3)

getName, a function in the SYS schema, returns the requested string when called by SYS

```
SQL> SELECT ocs_utils.getName FROM dual;

GETNAME
-------------------------------------------------------------
518BBCBF41EF7314FD9407C71F23BAEF0CB1D8D8082766482DDCE4E941E8
```

getSeed, also a function in the SYS schema, returns an exception with an identical call

```
SQL> SELECT ocs_utils.getSeed FROM dual;
SELECT ocs_utils.getSeed FROM dual
       *
ERROR at line 1:
ORA-06553: PLS-904: insufficient privilege to access object GETSEED
```

getSeed can only be run if called by the driver procedure

```
SQL> exec driver;
8E4408B475D63385A73AED2FE911DD9818E82FB5

PL/SQL procedure successfully completed.
```

Dev

ACCESSIBLE BY Attack Surface Reduction Report

All PL/SQL objects in Oracle databases that are not Oracle Maintained should be reviewed to determine whether they need to be accessible to every user and every other object with privileged schema access

or

whether they are a subprogram in a PL/SQL package that would reduce the attack surface if access to them was restricted to a greater extent than other subprograms in the same package

Where attack surface reductions are possible header information should be modified to include the ACCESSIBLE BY clause and the object tested in an Integrated Unit Test (IUT) environment, and certified, before release into a production environment

PL/SQL code, written without use of the ACCESSIBLE BY clause, cannot be protected against misuse by users with phished credentials.

Code Based Access Control (CBAC)

Prior to version 12.1 the privileges required by an object or a user to access an object had to be granted to the schema that owned the object or to every user that accessed the object

Following the Principle of Least Privilege CBAC eliminates the need to grant privileges to users that could potentially misuse those privileges for other purposes and focuses the grant selectively on the object that requires them which also reduces complexity

The following example shows the creation of a role, granting the READ privilege on a data dictionary table to the role, and granting the role to the package that requires table access

The package can read the table … but the user(s) cannot

```
CREATE ROLE c##cbac;

GRANT read ON sys.user_history$ TO c##cbac;

GRANT c##cbac TO PACKAGE accby;
```

Access Control Attack Surface Reduction Report

Dev

All Pl/SQL objects in Oracle databases that require or are accessed through privileges granted to users and/or schemas should be evaluated to determine opportunities to reduce the attack surface by granting the privileges directly to the object

Where opportunities are identified, in an Integrated Unit Test (IUT) environment the existing grants should be replaced with CBAC grants and the change validated and approved before release to production

Granting privileges to objects, rather than users, greatly reduces the risk of the credentials being misused during an internal attack or used in an attack by an agent with phished credentials.

Unified Auditing (1:2)

Unified Auditing Policies were introduced in 12c and are a substantial enhancement of Oracle's Legacy auditing simplifying maintenance costs minimizing coverage gaps, and reducing risk

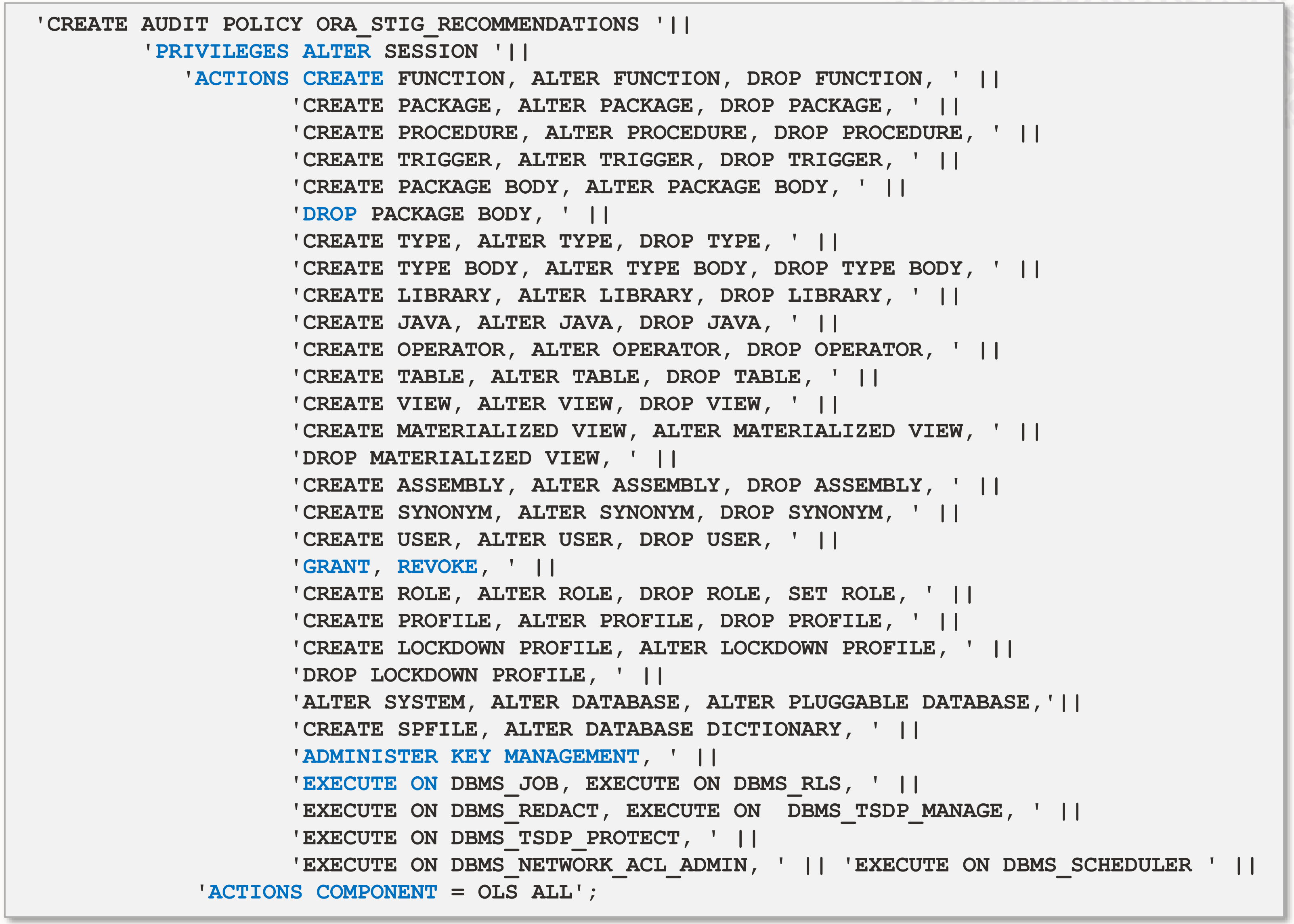
The enhancement that makes the new policy-based auditing ideal for DBAs is the ability to build a single policy that addresses the organization's needs

```
CREATE AUDIT POLICY <policy_name>
[PRIVILEGES <comma_delimited_system_privileges_list>]
[<standard_actions | component_actions>]
[ROLES <comma_delimited_roles_list>]
[WHEN '<audit_condition>' EVALUATE PER <STATEMENT | SESSION | INSTANCE>]
[ONLY TOPLEVEL]
[CONTAINER = <ALL | CURRENT>];
```

Oracle provides audit policies that can be enabled with every database installation in the file **`$ORACLE_HOME/rdbms/admin/secconf.sql`** which includes policy recommendations for CIS and STIG compliance

Unified Auditing (2:2)

DBA



```
'CREATE AUDIT POLICY ORA_STIG_RECOMMENDATIONS '||
        'PRIVILEGES ALTER SESSION '||
           'ACTIONS CREATE FUNCTION, ALTER FUNCTION, DROP FUNCTION, ' ||
                   'CREATE PACKAGE, ALTER PACKAGE, DROP PACKAGE, ' ||
                   'CREATE PROCEDURE, ALTER PROCEDURE, DROP PROCEDURE, ' ||
                   'CREATE TRIGGER, ALTER TRIGGER, DROP TRIGGER, ' ||
                   'CREATE PACKAGE BODY, ALTER PACKAGE BODY, ' ||
                   'DROP PACKAGE BODY, ' ||
                   'CREATE TYPE, ALTER TYPE, DROP TYPE, ' ||
                   'CREATE TYPE BODY, ALTER TYPE BODY, DROP TYPE BODY, ' ||
                   'CREATE LIBRARY, ALTER LIBRARY, DROP LIBRARY, ' ||
                   'CREATE JAVA, ALTER JAVA, DROP JAVA, ' ||
                   'CREATE OPERATOR, ALTER OPERATOR, DROP OPERATOR, ' ||
                   'CREATE TABLE, ALTER TABLE, DROP TABLE, ' ||
                   'CREATE VIEW, ALTER VIEW, DROP VIEW, ' ||
                   'CREATE MATERIALIZED VIEW, ALTER MATERIALIZED VIEW, ' ||
                   'DROP MATERIALIZED VIEW, ' ||
                   'CREATE ASSEMBLY, ALTER ASSEMBLY, DROP ASSEMBLY, ' ||
                   'CREATE SYNONYM, ALTER SYNONYM, DROP SYNONYM, ' ||
                   'CREATE USER, ALTER USER, DROP USER, ' ||
                   'GRANT, REVOKE, ' ||
                   'CREATE ROLE, ALTER ROLE, DROP ROLE, SET ROLE, ' ||
                   'CREATE PROFILE, ALTER PROFILE, DROP PROFILE, ' ||
                   'CREATE LOCKDOWN PROFILE, ALTER LOCKDOWN PROFILE, ' ||
                   'DROP LOCKDOWN PROFILE, ' ||
                   'ALTER SYSTEM, ALTER DATABASE, ALTER PLUGGABLE DATABASE,'||
                   'CREATE SPFILE, ALTER DATABASE DICTIONARY, ' ||
                   'ADMINISTER KEY MANAGEMENT, ' ||
                   'EXECUTE ON DBMS_JOB, EXECUTE ON DBMS_RLS, ' ||
                   'EXECUTE ON DBMS_REDACT, EXECUTE ON  DBMS_TSDP_MANAGE, ' ||
                   'EXECUTE ON DBMS_TSDP_PROTECT, ' ||
                   'EXECUTE ON DBMS_NETWORK_ACL_ADMIN, ' || 'EXECUTE ON DBMS_SCHEDULER ' ||
            'ACTIONS COMPONENT = OLS ALL';
```

DBA

Unified Auditing Attack Surface Reduction Report

Auditing cannot reduce the attack surface but eliminating errors and omissions in auditing is critical not just to meet compliance objects but so as to no leave gaps that might allow an attacker unmonitored access

Unified Audit Policies make possible

- Writing a single policy, or small group of policies and implementing them enterprise-wide
- Testing audit policies at the enterprise-level
- A substantially reduction in management costs

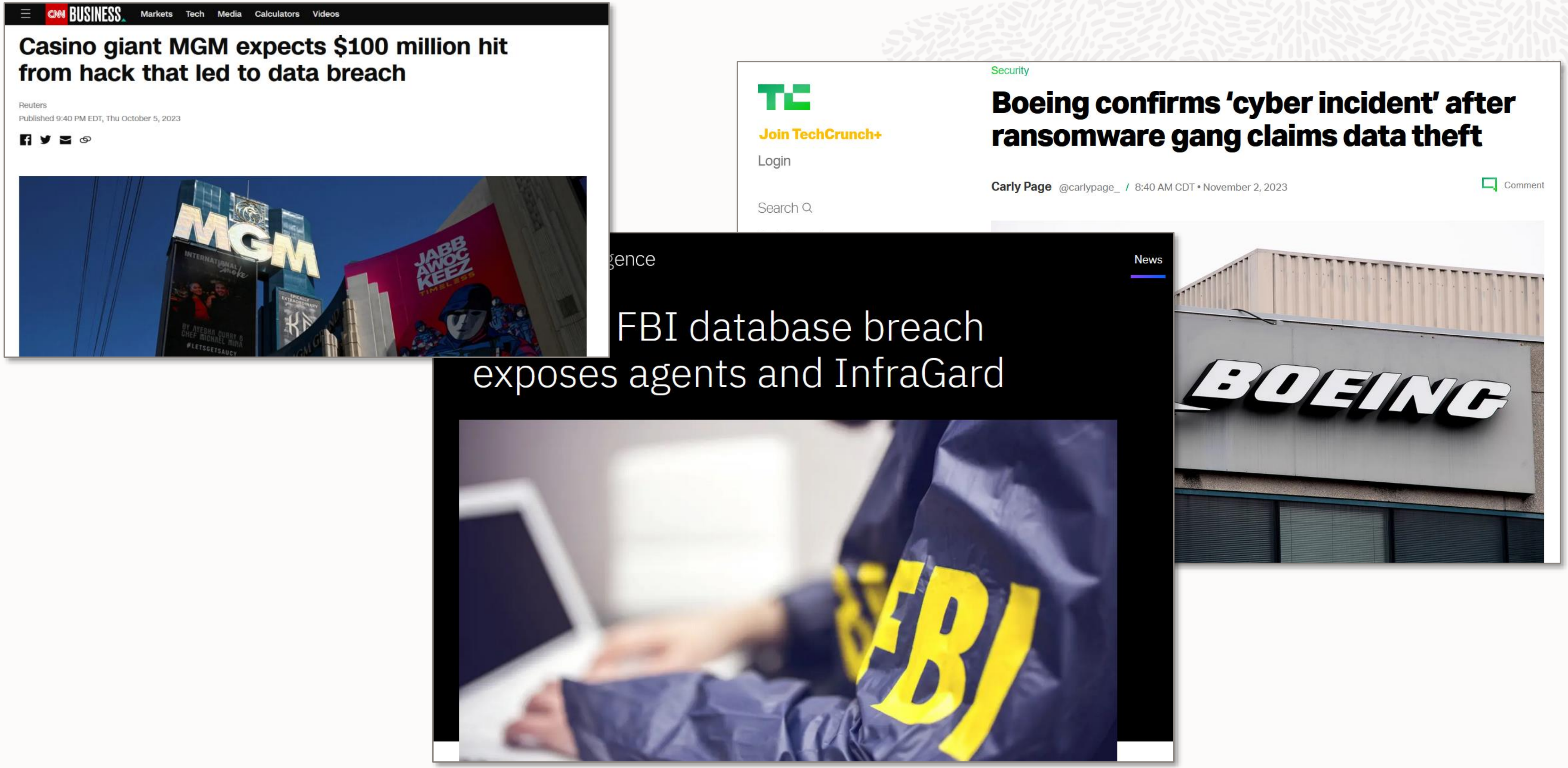
Policy based Unified Auditing increases your security through ease of deployment, ease of management, and gap elimination.

Oracle Database legacy ("basic") auditing is approaching end of life.

To be ready for your next upgrade complete your move to Unified Auditing in 19c.

Wrap Up

If You Don't Want To Be On One Of My Slides …



Casino giant MGM expects $100 million hit from hack that led to data breach

Reuters
Published 9:40 PM EDT, Thu October 5, 2023

Boeing confirms 'cyber incident' after ransomware gang claims data theft

Carly Page @carlypage_ / 8:40 AM CDT • November 2, 2023

FBI database breach exposes agents and InfraGard

Attack Surface Reduction Assessments

This Workshop addresses only 15 of more than 800 configuration-related vulnerabilities and
practices that directly impact your ability to thwart an attempt to compromise your databases
and corrupt or exfil llectual property

Assessments are targeted by Oracle Version

- 12c, 19c, 21c

by architecture

- Stand-alone, RAC, Container, Hadoop, Graph

by Application

- EBS, SAP, PeopleSoft, Siebel

by Compliance Requirements

- SOX, GDPR, GLB, DFARS, ITAR, EARS, CIS, STIG

Attack Surface Red his year meets the
requirements of the **nize applications**
as our nation's adv ustomers
providing a service ent service
provided to boat ow

You know that you
weak foundation and that the best door is not secure
if it isn't locked

Our goal, through assessments, is to enable our customers to move from Zero Trust to a foundation built on a security-optimized configuration

Assessment Value

Attack Surface Reduction assessments provide a unique value our customers require. An assessment encapsulates Oracle Consulting's unique knowledge of the Oracle Database integrated with the knowledge of members of Oracle's Security Tiger Team, Product Management, Developers and Support

Assessment Reports, unlike compliance frameworks such as CIS and STIG, are flexible and dynamic and address zero-day and emergent threats as we become aware of them

ASR assessments allow adding, altering, and dropping what is collected, how it is analyzed, and the conclusions that are reported based on current knowledge of editions, versions, patch levels, what is happening in the wild, and active research in our environments and labs

Unlike tools and assessments made available for public download, ASR data collection and recommendation mapping is proprietary so that information about potential vulnerabilities is not made available to attackers

Metadata Collection

What

- Identifying information: The minimum required to identify the assessment target
- Database configuration files and metadata (never application data)

How

- Manual input from written and oral questions
- Customer runs a single script provided by Oracle and can review and mask output

Use

- Collected files and metadata analyzed by an Expert System and OCS subject matter experts
- Our algorithms, and your files and metadata, are not shared inside of Oracle

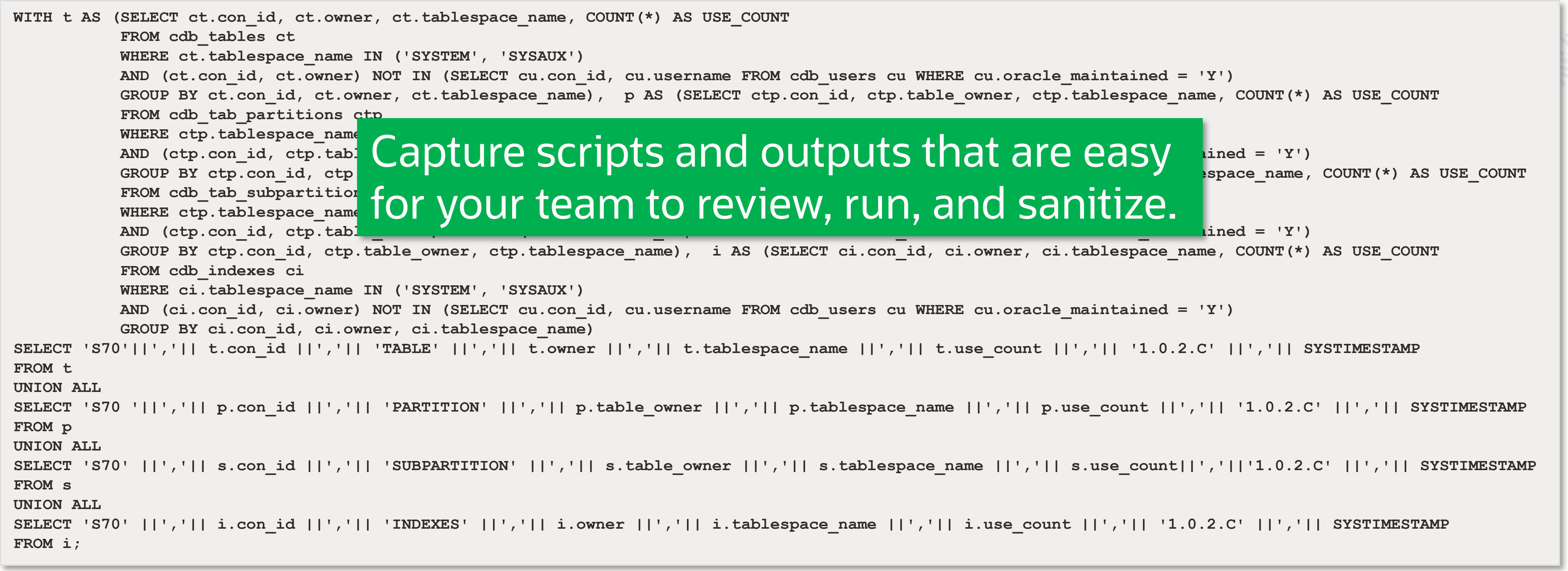
Deliverables

- Executive Summary Report with actionable recommendations
- Technical Detail Report with specific findings and recommended remediation

Destruction

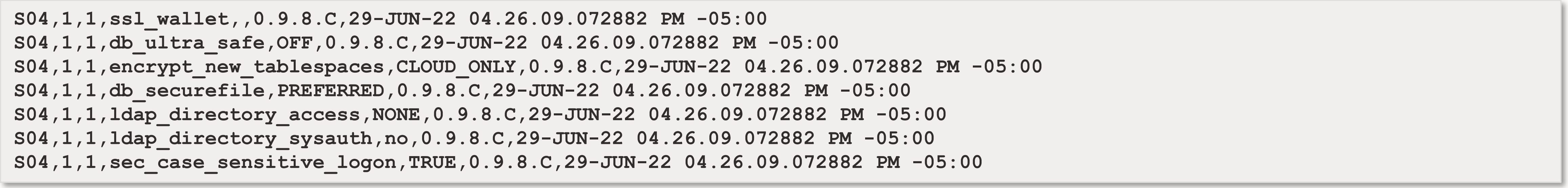
- All files and metadata collected from clients is destroyed at the conclusion of an assessment engagement unless a customer specifically requests that they be retained

Metadata Collection Examples (1:2)



```
WITH t AS (SELECT ct.con_id, ct.owner, ct.tablespace_name, COUNT(*) AS USE_COUNT
           FROM cdb_tables ct
           WHERE ct.tablespace_name IN ('SYSTEM', 'SYSAUX')
           AND (ct.con_id, ct.owner) NOT IN (SELECT cu.con_id, cu.username FROM cdb_users cu WHERE cu.oracle_maintained = 'Y')
           GROUP BY ct.con_id, ct.owner, ct.tablespace_name),  p AS (SELECT ctp.con_id, ctp.table_owner, ctp.tablespace_name, COUNT(*) AS USE_COUNT
           FROM cdb_tab_partitions ctp
           WHERE ctp.tablespace_name
           AND (ctp.con_id, ctp.tabl                                                                    ined = 'Y')
           GROUP BY ctp.con_id, ctp                                                                     espace_name, COUNT(*) AS USE_COUNT
           FROM cdb_tab_subpartition
           WHERE ctp.tablespace_name
           AND (ctp.con_id, ctp.tabl                                                                    ined = 'Y')
           GROUP BY ctp.con_id, ctp.table_owner, ctp.tablespace_name),  i AS (SELECT ci.con_id, ci.owner, ci.tablespace_name, COUNT(*) AS USE_COUNT
           FROM cdb_indexes ci
           WHERE ci.tablespace_name IN ('SYSTEM', 'SYSAUX')
           AND (ci.con_id, ci.owner) NOT IN (SELECT cu.con_id, cu.username FROM cdb_users cu WHERE cu.oracle_maintained = 'Y')
           GROUP BY ci.con_id, ci.owner, ci.tablespace_name)
SELECT 'S70'||','|| t.con_id ||','|| 'TABLE' ||','|| t.owner ||','|| t.tablespace_name ||','|| t.use_count ||','|| '1.0.2.C' ||','|| SYSTIMESTAMP
FROM t
UNION ALL
SELECT 'S70 '||','|| p.con_id ||','|| 'PARTITION' ||','|| p.table_owner ||','|| p.tablespace_name ||','|| p.use_count ||','|| '1.0.2.C' ||','|| SYSTIMESTAMP
FROM p
UNION ALL
SELECT 'S70' ||','|| s.con_id ||','|| 'SUBPARTITION' ||','|| s.table_owner ||','|| s.tablespace_name ||','|| s.use_count||','||'1.0.2.C' ||','|| SYSTIMESTAMP
FROM s
UNION ALL
SELECT 'S70' ||','|| i.con_id ||','|| 'INDEXES' ||','|| i.owner ||','|| i.tablespace_name ||','|| i.use_count ||','|| '1.0.2.C' ||','|| SYSTIMESTAMP
FROM i;
```

Capture scripts and outputs that are easy for your team to review, run, and sanitize.



```
S04,1,1,ssl_wallet,,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,db_ultra_safe,OFF,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,encrypt_new_tablespaces,CLOUD_ONLY,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,db_securefile,PREFERRED,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,ldap_directory_access,NONE,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,ldap_directory_sysauth,no,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
S04,1,1,sec_case_sensitive_logon,TRUE,0.9.8.C,29-JUN-22 04.26.09.072882 PM -05:00
```

Deliverables

Executive Summary Report

Overview & actionable recommendations
Audience: CTO, CISO, CFO

Technical Details Report

Findings & recommended remediation
Audience: DBA, System & App Admins

Detail Report Grading

Findings are graded as belonging to one of three categories in a format similar to the following to assist in making findings actionable

CONFIGURATION COMPONENT	OPTION 1	OPTION 2	OPTION 3
Item 1	🟥	🟨	🟩
Item 2	🟨	🟨	🟩
Item 3	🟨	🟨	🟩
Item 4	🟥	🟥	🟩
Item 5	🟥	🟥	🟩
Item 6	🟨	🟥	🟩
Item 7	🟨	🟥	🟥
Item 8	🟨	🟥	🟥
Item 9	🟩	🟩	🟩

Parameter	Finding
Insecure Configuration	10
Options Available	8
Secure Configuration	9

Report Example: STARTUP PARAMETERS

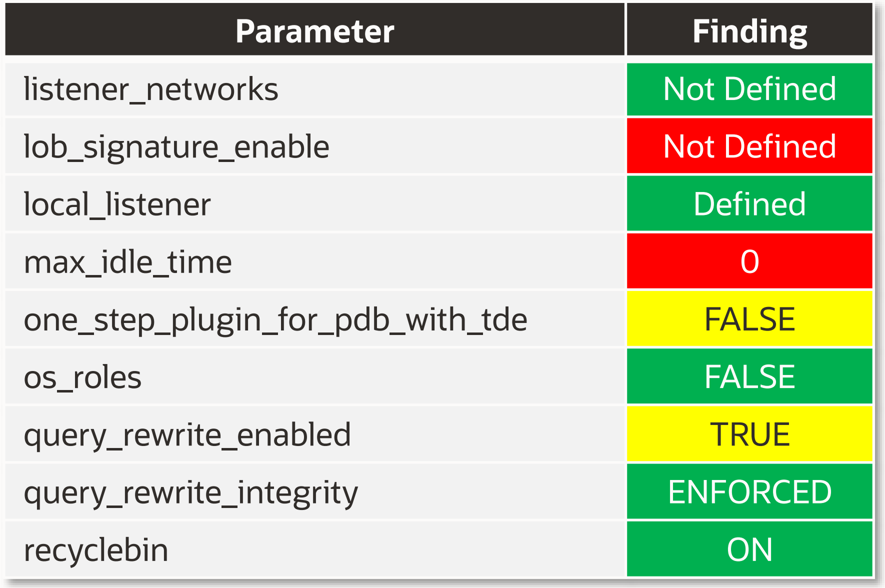
LOB_SIGNATURE_ENABLED: is a new feature in 19c and adds an additional layer of security to BLOB and CLOB columns: Set to TRUE to decrease the attack surface

MAX_IDLE_TIME: number of idle minutes before a session is automatically terminated.
0 = unlimited. Setting a value such as 60 provides a slight decrease in the attack surface

ONE_STEP_PLUGIN_FOR_PDB_WITH_TDE: set to TRUE eliminate the need to manually provide a keystore password when importing TDE keys after a move

QUERY_REWRITE_ENABLED: enables/disables query rewrite globally for the database. Disabling provides a slight decrease in the attack surface

RECYCLEBIN: provides a safety margin against corruption by enabling many flashback technologies but dropped tables and indexes can be recovered and mined for data. We recommend the ON configuration but that active measures be taken to ensure sensitive data is not left in the recyclebin or be secured with Database Vault



Parameter	Finding
listener_networks	🟩 Not Defined
lob_signature_enable	🟥 Not Defined
local_listener	🟩 Defined
max_idle_time	🟥 0
one_step_plugin_for_pdb_with_tde	🟨 FALSE
os_roles	🟩 FALSE
query_rewrite_enabled	🟨 TRUE
query_rewrite_integrity	🟩 ENFORCED
recyclebin	🟩 ON

For live delivery of this complimentary presentation to your organization email me asra_us@oracle.com

Oracle Consulting Services - Security Practice

Daniel Morgan, Technical Director Database Security
daniel.d.morgan@oracle.com

Questions

Oracle Consulting Services - Security Practice

Daniel Morgan, Technical Director Database Security
daniel.d.morgan@oracle.com

Thank you

Oracle Consulting Services - Security Practice

Daniel Morgan, Technical Director Database Security
daniel.d.morgan@oracle.com

ORACLE