ORACLE

Oracle Database Security Assessment Tool 3.0

Oracle DBSATによって自社のデータベースがどれほどセキュアになるかを把握する

Pedro Lopes
Product Manager
Oracle Database Security2023年11月

知らないことで損害を被ることも

データベースはオラクルのベスト・プラクティスに従って構成されているか?

セキュリティ制御はすでに設定されているか?

ほかにどのようなセキュリティ制御を使用できるか?

データベースにはどのようなユーザーがいるか?

ユーザーはどのようなアクセス権を持っているか?

このデータベースにはどのような機密データがあるか?

トップ10の評価結果

データベース・セキュリティ評価から

- データベース・セキュリティ・ポリシー/戦略が設定されていない
- パッチ適用/パッチ管理ポリシーが設定されていない
- アカウントが個人向けに設定されていない、職務分離がされていない、アカウントが必要以上の権限を持っている
- 機密データ/規制対象データが暗号化されていない
- 監視/監査が実施されていない
- パスワード・ポリシーが存在しない、パスワード管理が貧弱である
- 非本番システム（開発/テスト/トレーニング）に本番データが使用されている
- テスト/サンプル・アカウントがクリーンアップされていない
- 第三者に送信されるデータが匿名化されていない
- OSハードニングが実施されていない

Oracle DBSATとは

ハッカーが攻撃する前にデータベース・セキュリティを評価

構成の評価

パッチ

データ暗号化

監査ポリシー

OSファイル権限

データベース構成

リスナー構成

ファイングレイン・アクセス制御

高リスク・ユーザーの特定

データベース・アカウント

ユーザー権限

ユーザー・ロール

機密データの検出

種類、場所、量

ギリシャ語、ドイツ語、オランダ語、フランス語、スペイン語、イタリア語、ポルトガル語に対応したデータ・モデル用のサンプル・パターン・ファイル

評価レポート

サマリーと詳細情報

優先順位付けされた、すぐに実行可能な、ターゲット固有の推奨事項

EU GDPR、STIG、CISベンチマークとの紐付け

Oracle Database 11g～23cで実行

Oracle DBSAT 3.0の新機能（2023年11月）

Oracle Database向けのSTIG V2R8に更新

- 30のSTIGの評価結果を追加
- STIG関連のあらゆる評価結果を更新してSTIGグループIDを使用

評価結果の追加/向上

- 追加:Oracle Database 23c SQL Firewall
- 追加:5つの新しい監査評価結果
- 更新：すべての監査評価結果を更新
- 機密データおよびTSDPに関する新しい評価結果を1点追加
- 更新：INFO.PATCH、ENCRYPT.TDE、NET.ENCRYPT、USER. AUTHVERSION
- その他

Discoverer

- インドPANおよびAadhaar番号の機密タイプを追加

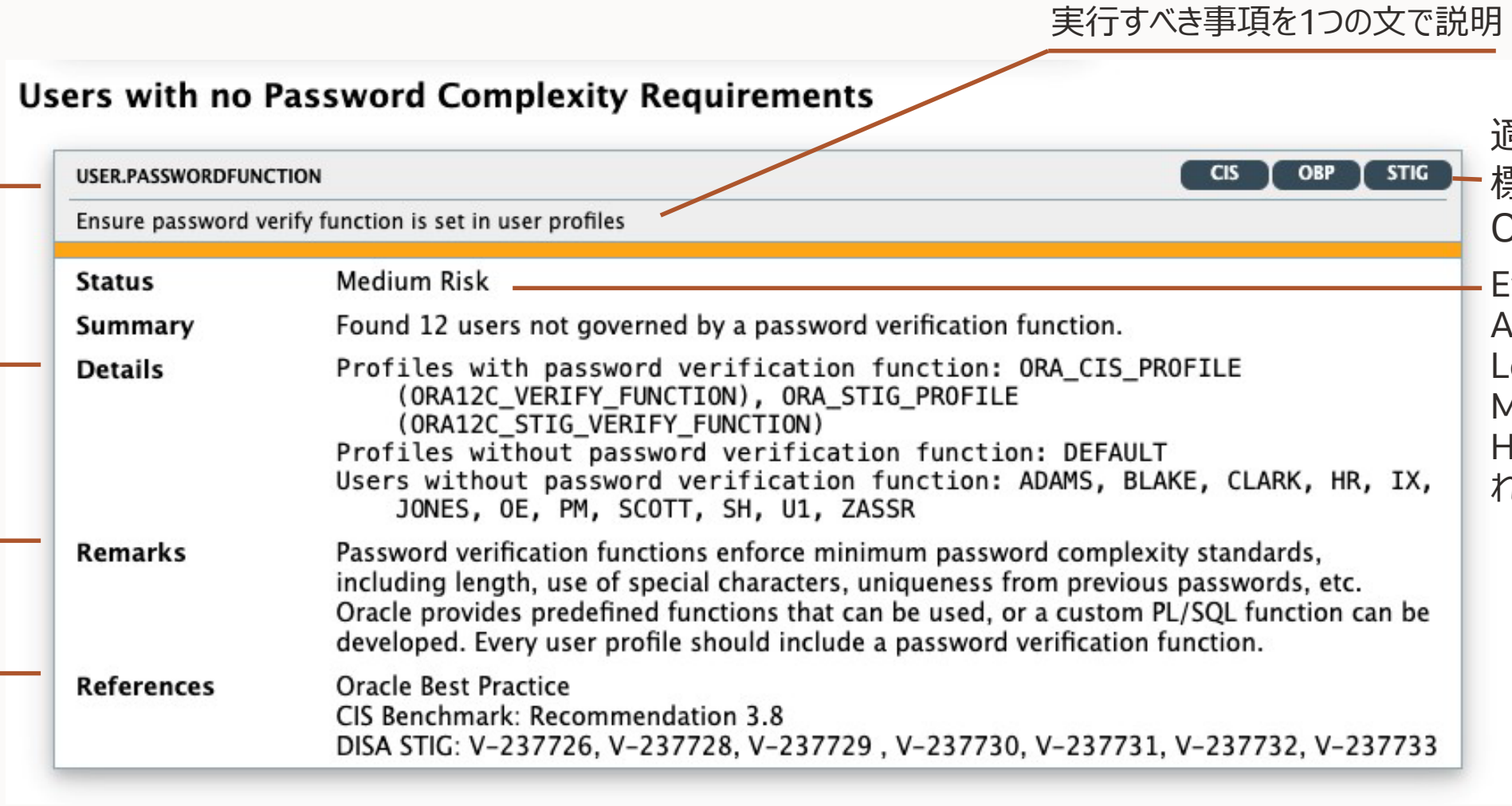
透明性と品質が向上

- すべての注釈と推奨事項を確認して更新
- 新しい1行サマリーにより、各チェックの目的とコンテキストを表示
- “Oracle Best Practice”による評価結果を明確にタグ付け
- Oracle Database 23cでサポートされない機能を注釈で説明
- ルールIDの更新および拡張により透明性が向上

コア

- ユーザーを除外するための新しいコマンドライン・オプション（レポートでの-u）
- Oracle DBSATの実行にPythonはもはや不要
- 最適化されたパフォーマンスによりデータ収集が高速化
- Linux 64ビットARMおよび23cのサポートを追加

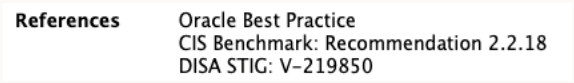
評価結果のサンプル



Oracle Best Practice（OBP）

New

Oracle Best Practiceであるチェックを明確に特定 ➡ OBP



あるチェックがOBPになり得るものの、CISまたはSTIGの一部にはならないのは以下の理由による。

- **特殊化：オラクルの深い知識**
  Oracle Databaseとその機能について広範で深い見識を持つオラクル
- **リリース・サイクル：Oracle Databaseのリリース・サイクルと標準/フレームワークの更新**
  リリースはさまざまな時期に発生
- **テクノロジーの更新：Oracle Databaseのイノベーション**
  新機能はすべてのリリースにおいてパッチで導入され、バックポートが可能
- **標準/フレームワークでは、機能が特定されなかったか、またはリスクを認識しない**

Oracle Database 23cのサポート廃止通知

New

サポート廃止通知では、廃止予定または廃止済みのデータベース機能およびパラメータが表示されるため、
事前に対策をとって段階的に使用をやめることが可能

Label Security

ACCESS.LABELSECURITY	GDPR
Classify sensitive data and authorize access using labels	
Status	Advisory
Summary	Label Security is not enabled.
Remarks	Oracle Label Security (OLS) provides a framework for implementing and enforcing multi-level security (MLS) policies within a database. MLS is a security model that allows you to classify data into different security levels and assign users different levels of clearance for accessing that data. With OLS, you can define classification labels, associate them with table rows, and then control access to the rows based on the security labels and the user's clearance level. This helps to ensure that sensitive information is protected and only available to authorized users. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by the Label Security policies. Each policy has a corresponding administrative role; users who have this role can administer the policy. Starting Oracle Database 23c, Oracle Label Security cannot be used with Oracle Internet Directory (OID) since Directory Integration Platform is being deprecated. Oracle recommends moving from OLS-OID configuration to stand-alone OLS configuration before upgrade to Oracle Database 23c.
References	EU GDPR: Article 18, 29, 32; Recital 67

Audit System Privileges

AUDIT.SYSTEMPRIVS	CIS	OBP
Ensure use of system privileges is audited		
Status	Medium Risk	
Summary	Auditing enabled for 44 privileges.	
Details	Traditional Audit (1): CREATE ANY TABLE Unified Audit (43): ADMINISTER FINE GRAINED AUDIT POLICY, ADMINISTER KEY MANAGEMENT, ADMINISTER REDACTION POLICY, ADMINISTER ROW LEVEL SECURITY POLICY, ADMINISTER SQL FIREWALL, ALTER ANY DOMAIN, ALTER ANY MLE, ALTER ANY PROCEDURE, ALTER ANY SQL TRANSLATION PROFILE, ALTER ANY TABLE, ALTER DATABASE, ALTER SESSION, ALTER SYSTEM, AUDIT SYSTEM, BECOME USER, CREATE ANY DOMAIN, CREATE ANY JOB, CREATE ANY LIBRARY, CREATE ANY MLE, CREATE ANY PROCEDURE, CREATE ANY SQL TRANSLATION PROFILE, CREATE ANY TABLE, CREATE EXTERNAL JOB, CREATE PUBLIC SYNONYM, CREATE SQL TRANSLATION PROFILE, CREATE USER, DROP ANY DOMAIN, DROP ANY MLE, DROP ANY PROCEDURE, DROP ANY SQL TRANSLATION PROFILE, DROP ANY TABLE, DROP PUBLIC SYNONYM, DROP USER, EXEMPT ACCESS POLICY, EXEMPT REDACTION POLICY, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, GRANT ANY ROLE, GRANT ANY SCHEMA PRIVILEGE, LOGMINING, PURGE DBA_RECYCLEBIN, SELECT ANY DICTIONARY, TRANSLATE ANY SQL Unified Audit Policies (3): ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, ORA_STIG_RECOMMENDATIONS	
Remarks	System privileges are powerful as they allow access to objects across multiple schemas or make changes that could impact the entire database. This finding shows the system privileges that are audited by enabled audit policies. It is recommended that system privileges such as ALTER SYSTEM, ALTER DATABASE, SELECT ANY TABLE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, and DROP ANY PROCEDURE are audited. Traditional audit is desupported in Oracle Database 23c. Post upgrade to Oracle Database 23c, creation of new traditional audit configurations will fail. Oracle recommends migrating to unified audit.	
References	Oracle Best Practice CIS Benchmark: Recommendation 5.1.14, 5.1.15, 5.1.16, 5.1.17, 5.2.18	

STIGの新しい評価結果（1/6）

評価結果のサンプル

Application Owner Account

USER.APPOWNER	OBP STIG
Evaluate authorizations to object owner account	
Status	Evaluate
Summary	Found 1 Potential Application owner. Found 1 Potential application owner that can log in to database. Found 1 object owned by application owner(s) that can be accessed by non-application owner(s).
Details	Application owner(s): HCM1 Application 1 owner that can log in to database: HCM1 Objects owned by application owner(s) that can be accessed by non-application owner(s): HCM1.TICKETINFO_PKG -> (PUBLIC)
Remarks	Restricting access to application service/owner accounts is crucial, especially since these accounts typically hold sensitive data or highly privileged procedures and functions that can access and modify sensitive data. As a best practice, these accounts should be locked or converted into schema-only accounts. This prevents unauthorized users from accessing these accounts. You should audit these accounts' activity if, for any reason, they require interactive use. This finding lists the non-Oracle-maintained schema with the most number of objects.
References	Oracle Best Practice DISA STIG: V-219851

- オブジェクトを所有する、オラクルが維持しないアカウントのトップ・ユーザー

詳細情報

Shared Accounts

USER.SHARED	OBP STIG
User accounts should not be shared	
Status	Evaluate
Summary	Found 6 users who share accounts with Administrative Privileges. Found 3 default Administrative Users being enabled. Found 1 user who can connect through proxy users.
Details	Shared users who can exercise one or more Administrative Privileges: SCOTT, SYSBACKUP, SYSDG, SYSKM, SYSTEM, ZEUS Default Administrative Users enabled: SYSBACKUP, SYSDG, SYSKM Following proxy and client combination found: USERX-SCHEMAAPP, USERY-SCHEMAAPP
Remarks	Having shared accounts to interact with the database may prevent the application from recording an individual user's identity used to read, insert, update and delete records. Use accounts assigned to individual users where feasible. You should audit shared or proxy users' activity. Configure user accounts, the database and/or the application to provide personal accountability. To accurately identify individual application users in connection pools, utilize the SET_IDENTIFIER procedure of DBMS_SESSION in SQL or the appropriate method/attribute in your programming language. Enterprise-packaged applications may have methods for achieving this, so check with the vendor and My Oracle Support for more information. It is also vital to monitor proxy users, who can connect to the database as their client users. Also, you should not have accounts with multiple administrative privileges (sysdba, sysoper, sysbackup, sysdg, syskm). You should assign one administrative privilege per user account for better separation of duties. Users requiring to execute multiple administrative functions can have specific accounts for each activity type.
References	Oracle Best Practice DISA STIG: V-220310, V-220311, V-220313, V-237724

- プロキシ・ユーザーを含む共有アカウントが可能

New

Users with Administrative SYS* Privileges

PRIV.SYSADMIN	OBP STIG
Segregate administrative privileges among different user accounts	
Status	Advisory
Summary	Found 6 users granted administrative SYS* privileges. Found 2 administrative SYS* privileges not granted to any user.
Details	SYSDBA (0): (none) SYSOPER (0): (none) SYSBACKUP (1): SYSBACKUP SYSDG (3): SCOTT, SYSDG, ZEUS SYSKM (3): SYSKM, SYSTEM, ZEUS
Remarks	Administrative SYS* privileges allow a user to perform maintenance operations, including some that may occur while the database is not open. The SYSDBA privilege allows the user to run as SYS and perform virtually all privileged operations. Starting with Oracle Database 12.1, Oracle introduced less powerful administrative privileges to allow users to perform specific administrative tasks with less than full SYSDBA privileges. To benefit from this separation of duty, you should grant each of these administrative privileges to at least one named user account.
References	Oracle Best Practice DISA STIG: V-237709

- 複数の管理権限を持つユーザー – SoDが侵害される可能性

STIGの新しい評価結果（2/6）
評価結果のサンプル

New

Users with Sensitive Data

USER.SENSITIVEDATA — OBP STIG

Check access granted on data marked sensitive by TSDP

Status	Evaluate
Summary	Found 5 user schemas that contain sensitive data. Found 1 user that has access to the sensitive data.
Details	`Schemas containing sensitive data: P46890UAD, HR, REDACT_USR, TKZGTSDPVPD, HCM1` `Users who have access to sensitive data: OE`
Remarks	In the current context, sensitive data refers to any data flagged as sensitive by Transparent Sensitive Data Protection (TSDP). To ensure secure access to sensitive information, it is best to grant access through roles rather than directly to individual accounts. Prompt revocation of access granted to individual accounts is recommended.
References	Oracle Best Practice DISA STIG: V-237704

透過的機密データ保護（TSDP）への洞察の向上

Data Masking

AUTHZ.DATAMASKING — GDPR OBP STIG

Anonymize sensitive data in non-production environments

Status	Evaluate
Summary	Found 8 tables classified by transparent sensitive data protection (TSDP) as containing sensitive data.
Details	`Tables that may expose sensitive information: HCM1.LOCATIONS, P46890UAD.ACCOUNT, HCM1.EMP_EXTENDED, HCM1.EMPLOYEES, TKZGTSDPVPD.EMP, REDACT_USR.ACCOUNT, HR.LOCATIONS, HR.EMPLOYEES`
Remarks	Clones of live production data are typically shared with development, testing, and data analytics teams so that they have access to realistic data to support their activities. Attackers have learned that valuable and sensitive data often ends up in non-production environments, which are generally less protected than production. Masking sensitive data before handing it over to development and analytics teams eliminates the risk of data breaches in non-production environments by irreversibly replacing the original sensitive data with realistic but fictitious data. Procedures that ensure copies of production data are kept away from non-secured locations must also be in place. Oracle Data Safe or Oracle Data Masking and Subsetting Pack can help you anonymize sensitive data transferred to non-production systems.
References	Oracle Best Practice EU GDPR: Article 5; Recital 26 DISA STIG: V-219844, V-220299

STIGの新しい評価結果（3/6）

評価結果のサンプル

New

Objects Accessible by PUBLIC

PRIV.OBJPUB　OBP　STIG

Disallow unnecessary object privileges granted to PUBLIC

Status	Evaluate
Summary	Found 1 object that can be accessed by PUBLIC
Details	`Objects accessible by PUBLIC: HCM1.TICKETINFO_PKG`
Remarks	Object grants to PUBLIC must be avoided and should be removed using the REVOKE command. If this database supports a package application, work with the application provider and Oracle support to understand to what extent you can revoke role grants made to PUBLIC.
References	Oracle Best Practice DISA STIG: V-219837

STIGの新しい評価結果（4/6）

評価結果のサンプル

New

Source Code Analysis

CONF.SOURCEANALYSIS OBP STIG

Check sensitive data exposed through error messages in stored programs

Status	Evaluate
Summary	Found 2 application schemas that contain Program Units.
Details	`Schemas containing program units: HR, OE`
Remarks	Messages generated by stored program units can inadvertently provide sensitive business, personal or system information that a malicious user can misuse. You should analyze the application code to verify that error messages do not contain information beyond what is needed for troubleshooting the issue. Program units should not access and print restricted user data.
References	Oracle Best Practice DISA STIG: V-220301, V-220302

Read-only ORACLE_HOME

CONF.READONLYHOME OBP STIG

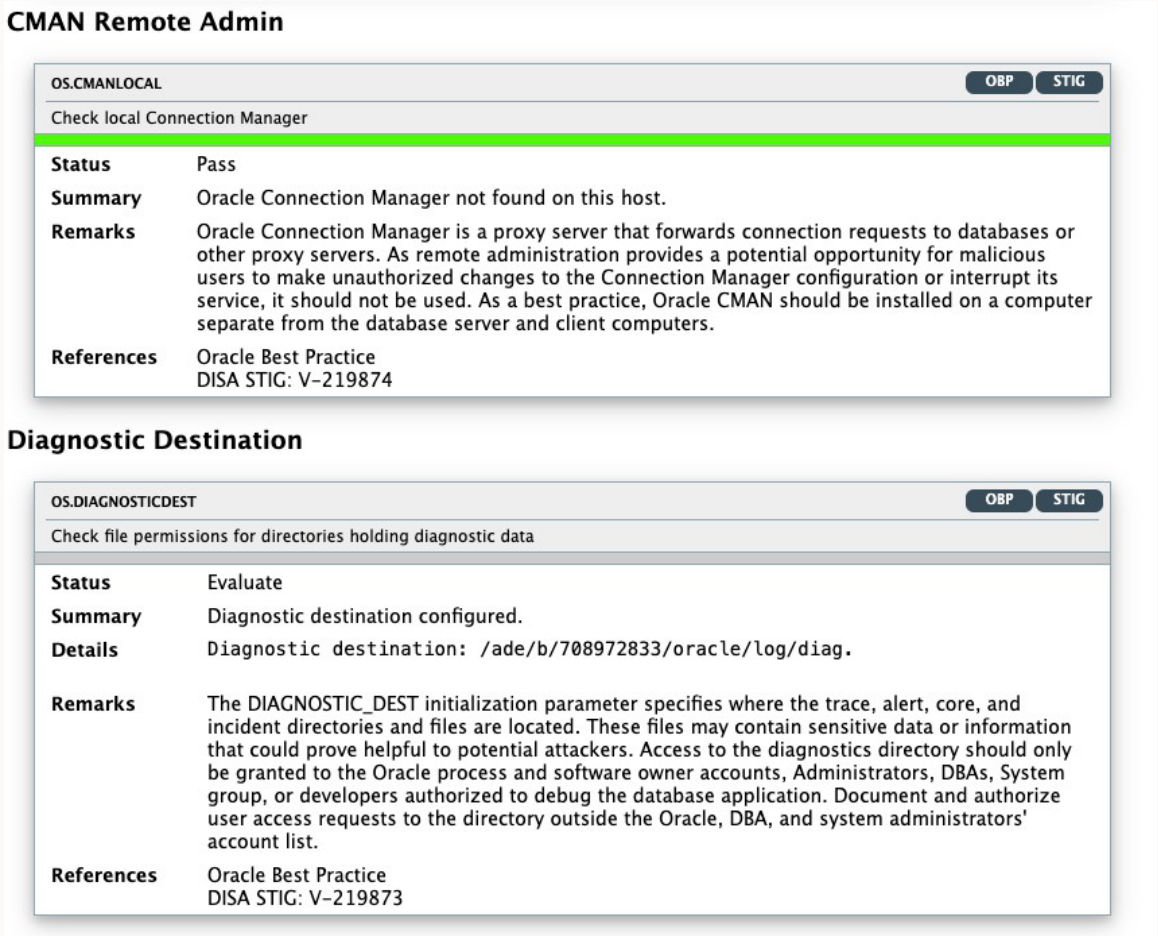
Check if ORACLE_HOME needs to be read-only

Status	Evaluate
Summary	Database has read/write ORACLE_HOME.
Details	`ORACLE_HOME: /u01/app/oracle/product/19.0.0/dbhome_1`
Remarks	An Oracle home is a directory into which all Oracle software is installed. In a read-only Oracle home, all the configuration data and log files reside outside the read-only Oracle home directory. This feature allows you to use the read-only Oracle home as a software image that you can distribute across multiple servers. A read-only Oracle home also helps with seamless patching and updating of Oracle databases.
References	Oracle Best Practice DISA STIG: V-220306

STIGの新しい評価結果（5/6）

評価結果のサンプル

New



CMAN Remote Admin

OS.CMANLOCAL — OBP STIG

Check local Connection Manager

Status	Pass
Summary	Oracle Connection Manager not found on this host.
Remarks	Oracle Connection Manager is a proxy server that forwards connection requests to databases or other proxy servers. As remote administration provides a potential opportunity for malicious users to make unauthorized changes to the Connection Manager configuration or interrupt its service, it should not be used. As a best practice, Oracle CMAN should be installed on a computer separate from the database server and client computers.
References	Oracle Best Practice DISA STIG: V-219874

Diagnostic Destination

OS.DIAGNOSTICDEST — OBP STIG

Check file permissions for directories holding diagnostic data

Status	Evaluate
Summary	Diagnostic destination configured.
Details	`Diagnostic destination: /ade/b/708972833/oracle/log/diag.`
Remarks	The DIAGNOSTIC_DEST initialization parameter specifies where the trace, alert, core, and incident directories and files are located. These files may contain sensitive data or information that could prove helpful to potential attackers. Access to the diagnostics directory should only be granted to the Oracle process and software owner accounts, Administrators, DBAs, System group, or developers authorized to debug the database application. Document and authorize user access requests to the directory outside the Oracle, DBA, and system administrators' account list.
References	Oracle Best Practice DISA STIG: V-219873

STIGの新しい評価結果（6/6）

監査評価結果のサンプル

New

Audit Management Configuration Parameters

Parameter Name	Audit Trail	Configured Value
DB AUDIT CLEAN BATCH SIZE	FGA AUDIT TRAIL	10000
DB AUDIT TABLESPACE	FGA AUDIT TRAIL	SYSAUX
AUDIT FILE MAX AGE	OS AUDIT TRAIL	5
AUDIT FILE MAX SIZE	OS AUDIT TRAIL	10000
OS FILE CLEAN BATCH SIZE	OS AUDIT TRAIL	1000
DB AUDIT CLEAN BATCH SIZE	STANDARD AUDIT TRAIL	10000
DB AUDIT TABLESPACE	STANDARD AUDIT TRAIL	SYSAUX
AUDIT FILE MAX AGE	UNIFIED AUDIT TRAIL	5
AUDIT FILE MAX SIZE	UNIFIED AUDIT TRAIL	10000
AUDIT WRITE MODE	UNIFIED AUDIT TRAIL	QUEUED WRITE MODE
DB AUDIT TABLESPACE	UNIFIED AUDIT TRAIL	SYSAUX
AUDIT FILE MAX AGE	XML AUDIT TRAIL	5
AUDIT FILE MAX SIZE	XML AUDIT TRAIL	10000
OS FILE CLEAN BATCH SIZE	XML AUDIT TRAIL	1000

新規付与が必要：
grant read on sys.dba_audit_mgmt_config_params to dbsat_user;

Audit Storage

AUDIT.TABLESPACE　OBP　STIG

Audit trail should be stored on a tablespace of its own

Status	Advisory
Summary	One or more audit trail is in SYSAUX tablespace. Examined 3 audit trails. Audit tablespace with acceptable free space.
Details	STANDARD AUDIT TRAIL is in SYSAUX UNIFIED AUDIT TRAIL is in SYSAUX FGA AUDIT TRAIL is in SYSAUX 2628 Records found in Unified Audit Trail from Oct 26 2023 to Oct 27 2023
Remarks	Auditing is the most effective way to record what happens in the database. Auditing tracks the use of privileges, activities of highly privileged users, access to sensitive data, actions performed on database objects, and modifications made to database settings. Auditing can be helpful for forensic investigations in the event of a data breach and to demonstrate regulatory compliance. Database audit trails use the SYSAUX tablespace by default and can fill it up. That can affect other database operations that rely on that tablespace. If the tablespace exhausts, audit record writes will spill over to OS audit files, and a message is written to the ALERT LOG. If the OS file system space also becomes full, audited operations will start to fail. It is recommended to relocate the audit trail to another tablespace using DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION procedure. Relocating to a dedicated tablespace will improve system performance and eliminate the probability of some other component taking up the free space. You can encrypt the new tablespace. Also, make sure you allocate adequate space. Oracle recommends that you configure a different tablespace for the audit trail. You can encrypt the new tablespace. Also, make sure you allocate adequate space.
References	Oracle Best Practice DISA STIG: V-220305, V-237717, V-237718

その他：

- AUDIT.CONDITION
- AUDIT.SHAREDPROXY
- AUDIT.TABLESPACE
- AUDIT.CLEANUPJOBS
- AUDIT.DATAPUMP
- AUDIT.STIGPOLICY
- AUDIT.DATABASEVAULT
- AUDIT.LABELSECURITY

Oracle Database 23c SQL Firewallの新しい評価結果

New

SQL Firewall

CONF.SQLFIREWALL — OBP

Check SQL Firewall configuration

Status	Evaluate
Summary	SQL Firewall is enabled.
Details	Found 1 database user with SQL Firewall policies: U1 U1 (blocking mode): Context allow-list (not enforced), SQL allow-list (not enforced)
Remarks	Built into Oracle Database kernel, SQL Firewall inspects all the incoming SQL statements and database connections and can detect and/or block unauthorized SQL and connections. SQL Firewall provides real-time protection against common database attacks such as SQL Injection. Once activated, SQL Firewall will learn SQL and connection activities and build user based allow-lists from collected data; the allow-lists can be modified and enforced in a desired mode.
References	Oracle Best Practice

Oracle DBSATの役割

ハッカーが攻撃する前にデータベース・セキュリティを評価

始めるには

シンプルで簡単

3ステップの流れ

1 次のファイルを
実行します。
./dbsat collect

2 次のファイルを
実行します。
./dbsat report

3 次のファイルを
実行します。
./dbsat discover

ORACLE

Collector & Reporter

設定済みのユーザー、ロール、権限、セキュリティ構成、ポリシーに関するメタデータ情報を収集。セキュリティ評価レポートを生成。

- **優先度別の評価結果を含むサマリー出力を生成**

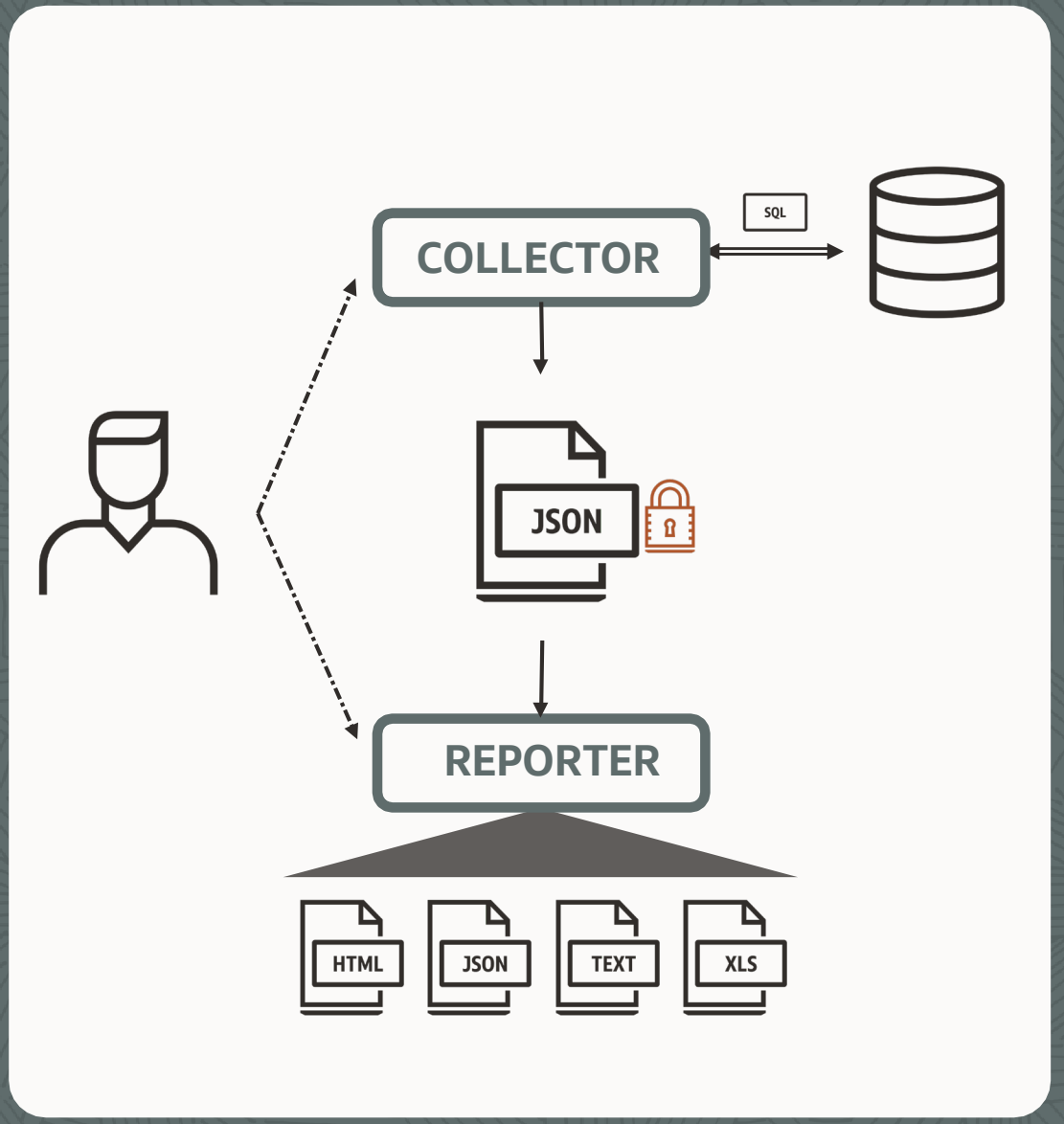
  優先度別の評価結果を含むサマリー出力を生成特定されたリスクをドメイン別にまとめたサマリー表：基本情報、ユーザー・アカウント、権限とロール、認可制御、きめ細かなアクセス制御、監査、暗号化、構成など。

- **120以上の詳細な評価結果と注意事項**

  各評価結果には、予測される内容の1行の説明、リスク・レベル、詳細、およびベスト・プラクティスに関する注釈が含まれます。

- **Oracle Best Practice、CISベンチマーク、STIGルール、GDPR条項/備考への参照**

  Oracle Databaseセキュリティ開発組織のベスト・プラクティスに加えて、CIS、STIGルール、EU GDPR条項/備考へ紐付け。



Discoverer

列名およびコメントのメタデータをスキャンして機密データを検出。
機密データ評価レポートを生成。

- **機密データを検出**

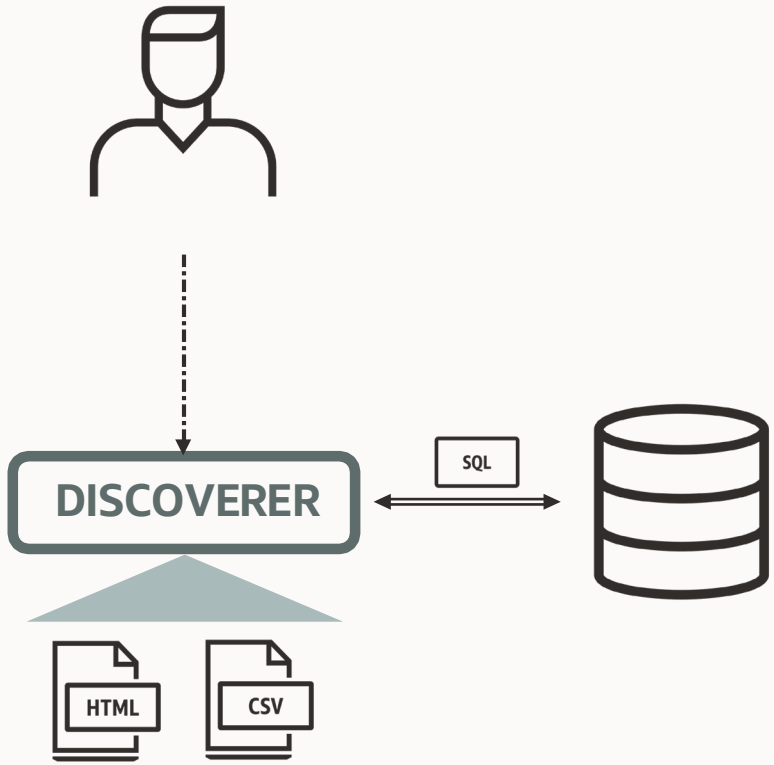
  機密データのカテゴリとタイプ（125以上）、表、列、行、リスク・レベルに関するサマリーと詳細を取得。

- **セキュリティ制御に関する推奨事項を提供**

  機密データを保護するために設定すべきセキュリティ制御に関する推奨事項を取得。

- **カスタマイズ可能**

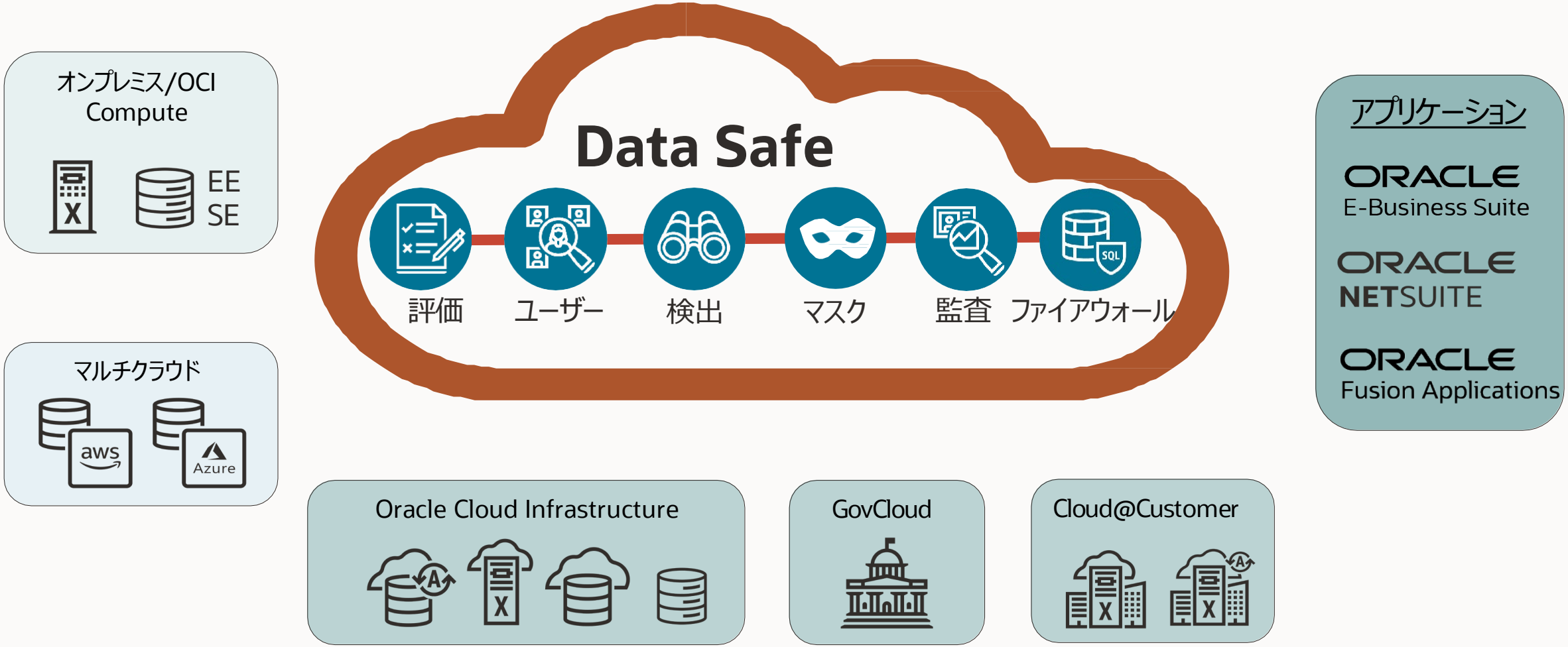
  既存のサンプル・ファイルを利用して拡張または固有のニーズに適応。



その他の機能

スケジュール設定した定期的な評価、ベースライン設定、評価履歴、ずれに関するレポート、ユーザー・リスク評価

Oracle Data SafeはOracleデータベース・ターゲットをあらゆる場所で保護



データベース・セキュリティ評価

不要なリスクが生じる可能性のある構成に関する瞬時フィードバック

包括的な評価

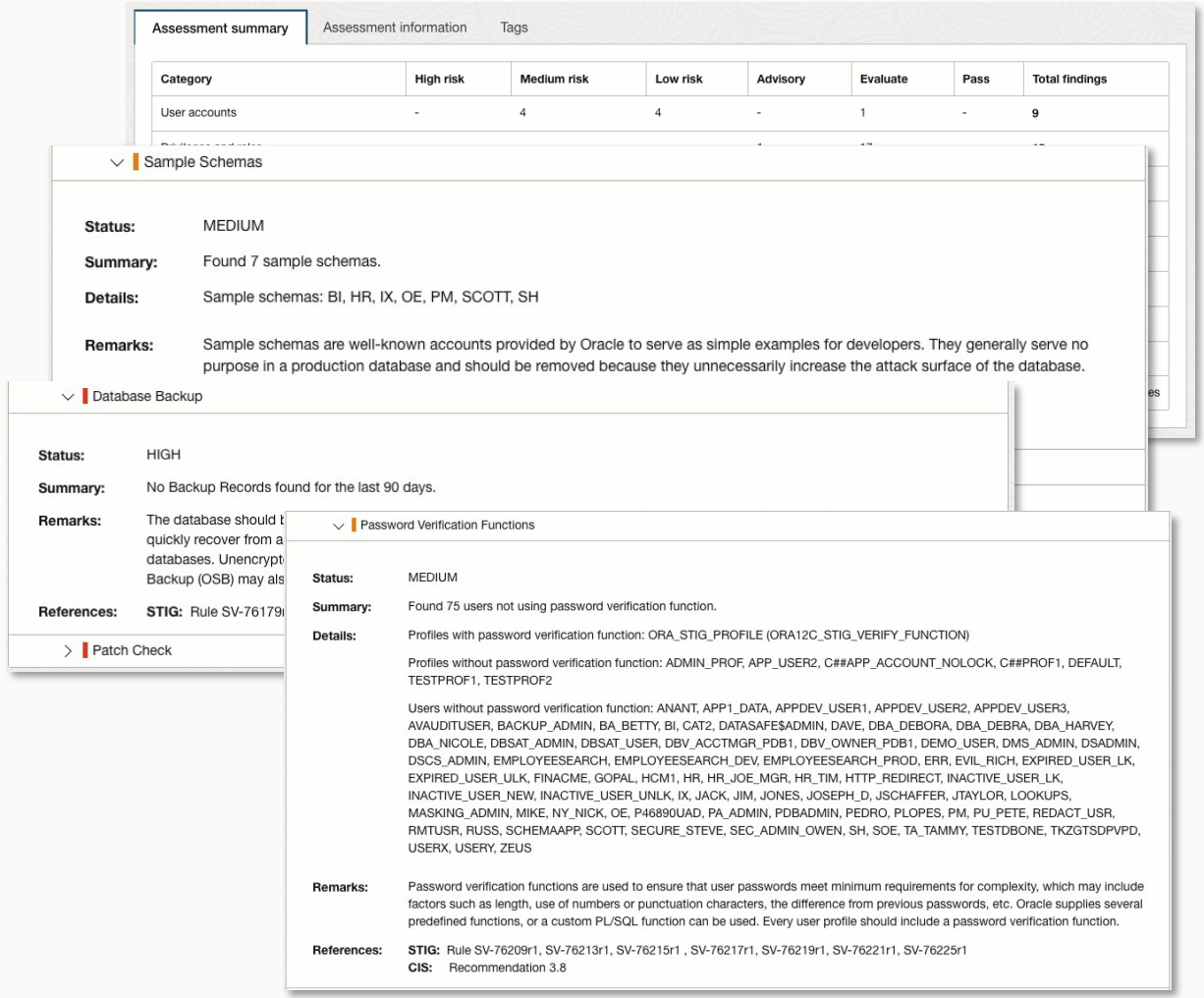
- セキュリティ・パラメータ
- 使用中のセキュリティ制御
- ユーザーのロールと権限

ベスト・プラクティスからのずれを特定

- ベースラインの設定
- 比較レポート
- イベントと通知
- 評価履歴

対策レポート

- 優先順位付けされた推奨事項
- 遵守すべき規制との紐付けとフィルタリング（GDPR、STIG、CIS）



ユーザー・リスク評価

ロール/権限およびポリシーの管理によってユーザー・リスクを低減

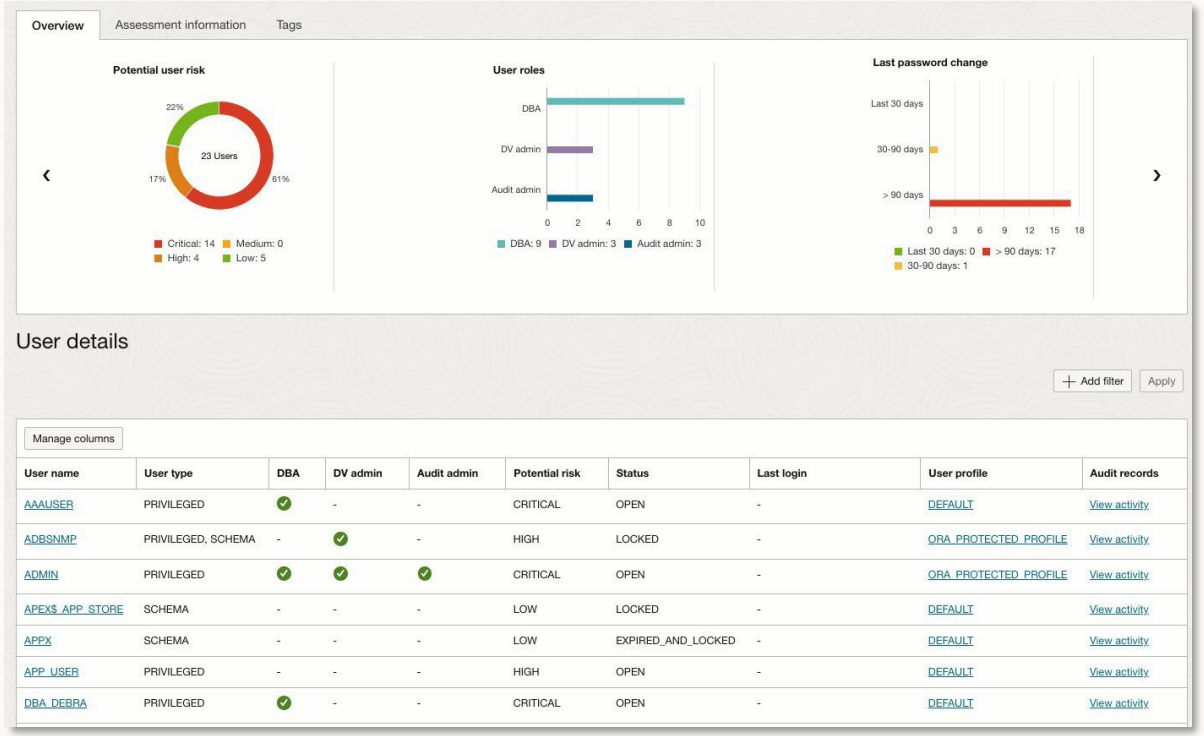
過度な権限を持つ高リスク・ユーザーを特定

ユーザー・アカウント、それらの権限とロールの付与、およびそれらの潜在的なリスクを特定

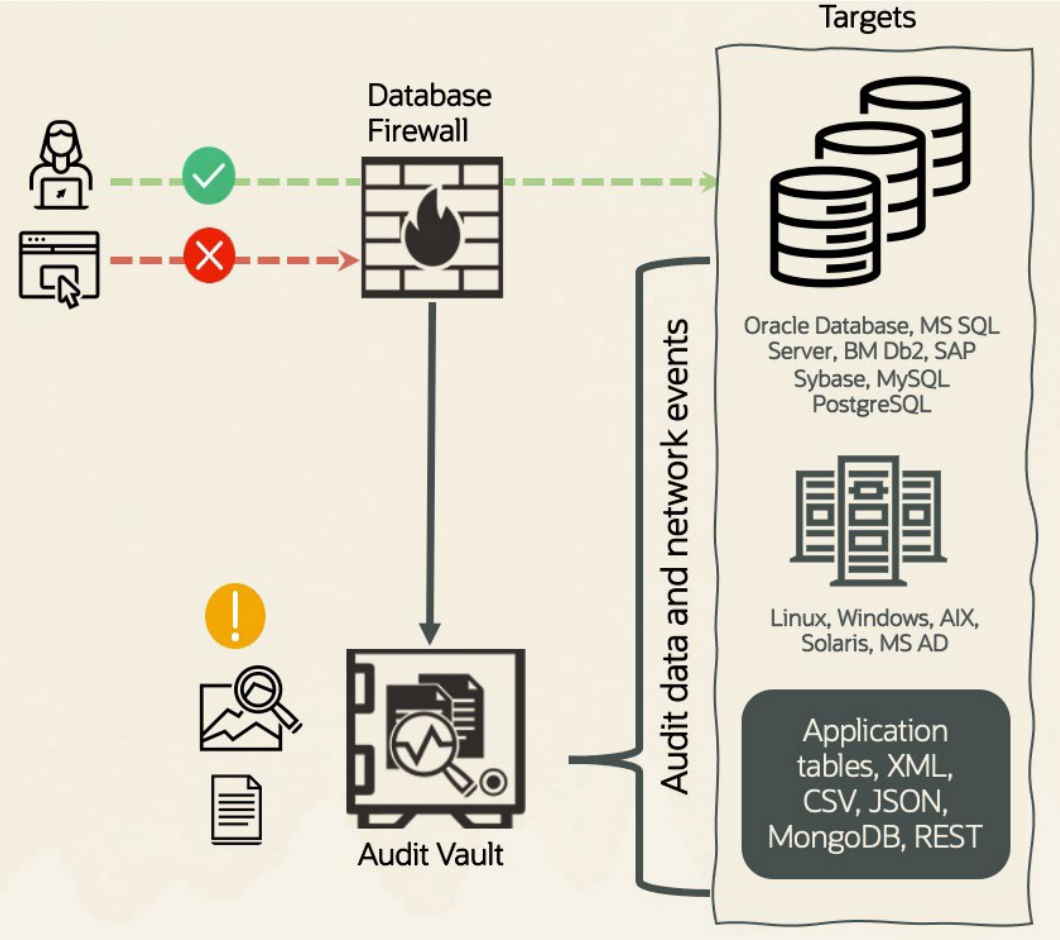
個々のターゲットとフリート表示

ユーザー・プロファイル・インサイト

- パスワードの複雑性の検証関数を含むパスワード・パラメータを確認
- パスワード・ガバナンス・ポリシーがないユーザーおよびプロファイルを特定
- どのプロファイルがどのユーザーに割り当てられているかを特定
- 複数のターゲット間でのユーザー・プロファイルのパスワード属性の不一致を特定



Oracle Audit Vault and Database Firewall



Oracle Audit Vault and Database Firewall（Oracle AVDF）は、本来の監査データとネットワークベースのSQLトラフィック・キャプチャを組み合わせる完全なデータベース・アクティビティ・モニタリング（DAM）ソリューション

特権ユーザー・アクティビティの監視
インシデント後、何が起きたかを認識
不正アクセスをブロック
疑わしいアクティビティへの警告
規制遵守の簡素化

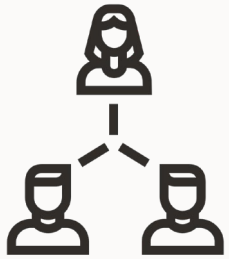
Oracle AVDFによるデータベース・セキュリティ状況の管理

セキュリティ評価

セキュリティ構成を把握し、承認済みのセキュリティ・ベースラインとのずれを特定

機密データの検出

機密オブジェクトがどのようなものでそれらがどこに保存されているかを把握



権限のあるユーザーの検出

権限のあるユーザーが誰でどのような権限を持っているのかを把握

監査インサイト

機密データがデータベース・ユーザーにどのように使用されたかを把握

Oracle DBSAT、Data Safe、Oracle AVDFの機能

機能	Data Safe	Oracle AVDF	Oracle DBSAT
全体的なセキュリティ構成ステータス	対応	あり	対応
構成のずれの検出とレポート	Yes	Yes	-
ユーザー・リスク評価/ユーザー・エンタイトルメント・レポート	Yes	Yes+	-
機密データの検出	対応	対応*	対応*
複数のターゲットに関する評価の一元管理	Yes	Yes	-
履歴のレポートと管理	Yes	Yes	-
クラウド、オンプレミス、Cloud@Customerターゲットのサポート	対応	あり	Yes
使用可能	OCI Cloud Service	OCI Marketplace イメージまたはオンプレミス・インストール	コマンドライン

+ リスク・スコアリングなし。*Oracle AVDF*エンタイトルメント・レポートには、ユーザー・ロールおよび権限の付与、システム権限の付与、オブジェクト権限の付与が含まれます（ずれを含む）。
* 列名とコメントのみのチェック（データのチェックなし）

サマリー

インストールと実行が容易

Oracle DBSAT 3.0を今すぐダウンロード：
https://www.oracle.com/jp/security/database-security/assessment-tool/

ターゲットで‘dbsat collect’を実行してセキュリティ構成データを収集する ‘dbsat report’を実行してセキュリティ評価レポートを生成する

‘dbsat discover’を実行して機密データ・レポートを生成する

サポート契約が有効なすべてのOracleデータベースのお客様がダウンロード可能

アクション・プラン

月曜朝

Oracle DBSATを実行して現在のデータベース・セキュリティの状態を評価する。

計測結果を得る。

次の30日間

明らかなミスや高リスクの評価結果に対応する。

データ侵害はビジネスに影響する。

次の90日間

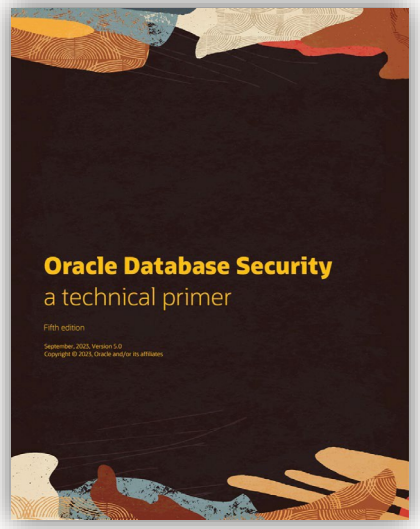
データ・セキュリティ戦略にデータベース・セキュリティのベスト・プラクティスを追加する。

計画を。信頼を得るのは困難だが、失うのは簡単。

詳細情報

O.com ： www.oracle.com/jp/security/database-security/
ブログ： https://blogs.oracle.com/cloudsecurity/category/ocs-database-security

新登場：eBook第5版：www.oracle.com/securingthedatabase



Oracle LiveLabs - お試しください：

- Oracle DBSAT: https://bit.ly/dbsat-livelab
- Data Safe: https://bit.ly/datasafe-livelabs
- Oracle AVDF: https://bit.ly/avdf-livelab
- その他のデータベース・セキュリティ：https://bit.ly/golivelabsdbsec

AskTOM Office Hoursは、Oracle Database PM/エキスパートによる、オープンなQ&Aセッションを無料で提供します。毎月の第2水曜日（15:00 UTC）にライブ・セッションを開催しています（https://bit.ly/asktomdbsec）。

Q&A


ORACLE

当社のミッションは、人々が新たな方法で
データを参照し、インサイトを発見し、
無限の可能性を解き放つことができるよう
支援することです。