ORACLE

Oracle Database Security Assessment Tool

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

2023年11月、バージョン1.0.1

公開

ORACLE

データ侵害が発生し、データ保護やプライバシー規制が進化し続ける時代では、組織が自社のデータベースはセキュアであると確信することが以前に増して重要になっています。ただし、データベースが正しく構成されているかどうか、誰がデータベースにアクセスできるのか、そして機密データがどこに保存されているかを把握するのは困難な場合があります。オラクルの多層防御機能の一部であるOracle Database Security Assessment Tool（Oracle DBSAT）は、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定します。そして、それらのリスクを緩和するために必要な変更内容と制御方法を提案します。

進化する規制の順守

セキュリティ構成の調査は、EU一般データ保護規則（EU GDPR）、クレジット・カード業界のデータ・セキュリティ基準（PCI DSS）、州法および現地法、業界標準をはじめとする多くの規制において、重要な要素となっています。さらに、Center for Internet Security（CIS：米国インターネット・セキュリティ・センター）、米国国防総省など、さまざまな組織が、セキュリティ構成のベスト・プラクティスに関する推奨事項を設けています。多くの組織のもっとも価値ある資産、すなわちデータを保護するべく、新たな規制が発表され、既存の規制が進化している中で、セキュリティ制御の重要性を軽視することはできません。

新たな制御を実装する前に組織が直面する最大の課題の1つは、自社のデータベースのセキュリティ状況を把握することです。組織は、データベースがどのようにセキュアに構成されているか、機密データがどこに保存されているか、機密データをどの程度保持しているか、どのユーザーが機密データにアクセスできるか、それらのユーザーはどのような権限を有しているか、そしてどのようなセキュリティ制御が実装されているかを迅速に特定する必要があります。

データベースがオンプレミスで実行されていようと、クラウドで実行されていようと、Oracle Database Security Assessment Tool（Oracle DBSAT）は、潜在的な機密データを発見し、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定します。Oracle DBSATは、さまざまな種類のデータをデータベースから収集し、分析することで、セキュリティ・リスクを特定します。さらに、それらのリスクを緩和するために必要なターゲット固有の変更内容と制御方法を提案します。

ハッカーのように考える

攻撃者は通常、標的を理解するために相当な時間を費やします。データベース、バージョン、オープン・ポート、既知の脆弱性、および特権ユーザー・アカウントの発見を自動化するツールを複数使用する可能性があります。その後で、パスワード窃盗、総当たりパスワード・クラッキング、権限昇格攻撃、SQLインジェクション攻撃など、さまざまな攻撃を仕掛けます。厳密な調査が終了すると、もっとも脆弱なリンクを特定し、次のステップを決定します。攻撃者は、基本的にまず現在のセキュリティ状態を評価し、捕まることなく機密データにアクセスできるもっとも容易な方法を見つけます。

たとえば、データが暗号化されている場合は、おそらく権限を持つユーザーとしてデータベースにアクセスする必要があります。デフォルトのパスワードを使用しているユーザーはいますか?認証が済むと、権限をエスカレーションできますか?監査が実施されていますか?どのユーザーが管理権限を持っていますか?このデータベース・バージョンにはどのような既知の脆弱性がありますか?その脆弱性にはパッチが当てられていますか?どのようなパッケージ・アプリケーションが実行されていますか?それらのアプリケーションは強力なシステム権限を使用して実行されていますか?どのような種類の機密データを処理しますか?これらはハッカーの頭の中にある問いのほんの一部で、その解答が、データベースに侵入し、データを盗むための計画を思いつくのに役立ちます。

組織は、所有者、管理者、データ処理者として、ハッカーと同じように考える必要がありますが、その目的は、ハッカーが自社のデータベースを標的にする前に、セキュリティ状況を改善することです。

現在のセキュリティ状況を評価し、不意を突かれないようにするために何が必要であるかを把握しているにもかかわらず、多くの組織は、データベース・セキュリティの専門知識がない、時間が不足している、適切な優先順位付けができない、リスクを誤解しているなどの理由から、自社のデータベース・セキュリティを評価することに苦心しています。データベースの保護に関する知識が、データベース管理者（DBA）と、ネットワークやエンドポイントの保護をもっとも重視しているITセキュリティ・チームとに、組織的に分散されている場合もあります。

Oracle DBSATは、適切な構成情報をデータベースから収集し、現在のセキュリティ状態を評価することで、評価プロセスを迅速化させるとともに、特定されたリスクの緩和について提案します。Oracle DBSATは、データベースがどの程度セキュアに構成されているか、どのようなユーザーがデータベースにアクセスでき、それらのユーザーはどのような権限を有しているか、どのようなセキュリティ・ポリシーが導入されているか、どのようなセキュリティ制御が実装されているか、機密データはどこに保存されているかに関するインサイトを素早く提供します。以下の図は、サンプル・データベースのセキュリティ状態をまとめたものであり、評価結果をリスク・レベルで分類しています。

図1：Oracle Databaseの現在のセキュリティ状態のサマリー

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	5	0	0	4	2	1	12
Privileges and Roles	5	16	0	0	0	0	21
Authorization Control	0	1	1	0	0	0	2
Fine-Grained Access Control	0	1	4	0	0	0	5
Auditing	0	4	2	0	6	0	12
Encryption	0	1	1	0	0	0	2
Database Configuration	5	3	0	3	2	1	14
Network Configuration	1	1	0	0	3	0	5
Operating System	1	0	0	2	1	1	5
Total	**17**	**27**	**8**	**9**	**14**	**4**	**79**

Oracle DBSATは、一連の評価結果という形で、分析の結果を報告します。それぞれの評価結果では、ステータスの概要、リスク・レベル、サマリー、詳細、および参考資料を必要に応じて提供します。また、結果がOracle Best Practice、Oracle DatabaseのSTIGルール、Center for Internet Security（CIS）ベンチマークの推奨事項、またはGDPRの条項/備考に関連しているかを指摘します。以下の2つの評価結果は、どのユーザーが強力なDBAロールを有しているか、そのロールはどのように取得されたか（直接付与、他のロールを介した付与）、およびどのユーザーがデフォルトのパスワードを使用しているかを示しています。チェック項目、詳細、注意事項はデータベース・ターゲットに固有で、デプロイ先がオンプレミスかクラウド内か（Autonomous Database Serverless、Autonomous Database Dedicated、またはBase Database）によって変わります。

図2：DBAロールを付与されたユーザーとその付与パス

Users with DBA Role

PRIV.DBA　CIS　OBP　STIG

Ensure DBA and PDB_DBA roles are granted only to necessary users

Status Evaluate

Summary 6 out of 54 users have been directly or indirectly granted highly sensitive DBA/PDB_DBA role via 6 grants. 1 user is granted highly sensitive DBA/PDB_DBA role with admin option via 1 grant. No Objects owned by DBA(s) can be accessed by non-DBA(s).

Details

```
Users with DBA/PDB_DBA role:

DBA_DEBRA: DBA

DBA_HARVEY: DBA

DBA_NICOLE: DBA

EVIL_RICH: DBA

PDB_ADMIN: PDB_DBA(*)

SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3: DBA

(*) = granted with admin option.
```

Remarks The DBA and PDB_DBA roles are powerful and can bypass many security controls. You should only grant them to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with the minimum set of privileges that users require to execute their tasks (least privilege principle) and not grant the DBA or PDB_DBA roles. Privilege Analysis can assist in identifying used/unused privileges and roles. Different roles with minimum required privileges based on the types of operations database administrators execute also help achieve Separation of Duties.

Furthermore, each trusted user should have an individual account for accountability reasons. You should audit users with the DBA or PDB_DBA roles to detect unauthorized privileged activity. Avoid granting the DBA, PDB_DBA, or custom DBA-like powerful roles with WITH ADMIN option unless necessary. Please note that Oracle may add or remove roles and privileges from the DBA or PDB_DBA role.

References Oracle Best Practice
CIS Benchmark: Recommendation 4.4.4
DISA STIG: V-237710

Oracle Databaseでは、DBAロールは強力で、多数のセキュリティ制御の迂回に使用できます。上記の例では、ユーザーSCOTTは他のロールが付与されたことによって（APPROLE3、APPROLE2、APPROLE1の順で）間接的にDBAロールが付与されており、DBA_DEBRAユーザーはDBAロールが直接付与されていることがOracle DBSATのレポートに示されています。

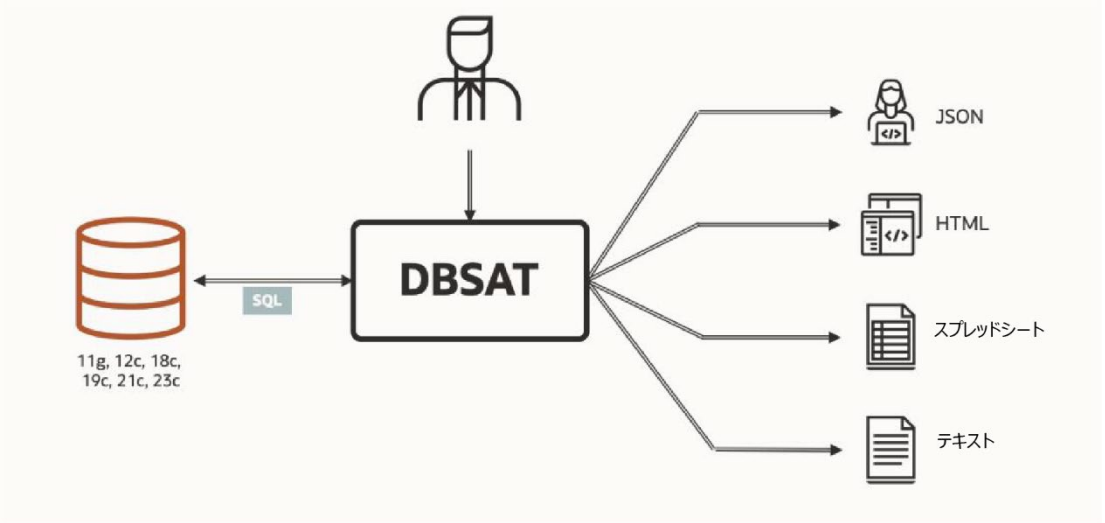
図3：デフォルトのパスワードを使用しているユーザー

Users with Default Passwords

USER.DEFPASSWORD	CIS OBP STIG
User accounts should not have default passwords	
Status	High Risk
Summary	Found 10 unlocked user accounts with default password.
Details	Users with default password: ADAMS, BLAKE, CLARK, HR, IX, JONES, OE, PM, SCOTT, SH
Remarks	Default passwords for predefined Oracle accounts are well known and provide a trivial means of entry for attackers. Database or account administrators should also change well-known passwords for locked accounts. Having default passwords can lead to unauthorized data manipulation and theft of confidential information. Note that if a script creates the database and the SYS or SYSTEM user password remains unchanged, these users are considered to possess a default password. Your database may be at risk due to the password presence within the script. Change the password to improve security.
References	Oracle Best Practice CIS Benchmark: Recommendation 1.2 DISA STIG: V-237698

Oracle DBSATの評価結果は、HTML、Microsoft Excel、JSON、テキスト・ファイルなど、複数の形式で提供されるため、組織はこのデータを構成やリスク管理ツールに統合することができます。

図4：Oracle DBSATがサポートするターゲット・バージョンとレポートの出力形式



機密データを検出する

EU GDPRなどの規制により、組織は個人情報（PII）データを保護することが義務付けられていますが、まずどのような個人データがどこに保存されているかを把握する必要があります。

Oracle DBSATは、カスタマイズ可能な正規表現パターンを使用して機密データのデータベース・メタデータをスキャンし、発見された機密データの量と種類を報告します。機密データは、英語のデータ・ディクショナリ（列名およびコメント）を使用して検索できるほか、欧州の主要言語（オランダ語、フランス語、イタリア語、ドイツ語、ギリシャ語、ポルトガル語、スペイン語など）でも検索できます。これにより、保有している機密データの量とその存在場所についてより詳しく把握できるため、組織はアクセス制御、監査、マスキング、暗号化を適切に実施してデータベースを保護できます。以下の図は、データベース・メタデータのスキャンを基に作成されたサマリー・レポートです。

図5：機密データ状況のサマリー

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO – ADDRESS	7	18	244
FINANCIAL INFO – CARD DATA	2	2	256
HEALTH INFO – PROVIDER DATA	1	1	149
IDENTIFICATION INFO – PERSONAL IDS	3	3	356
IDENTIFICATION INFO – PUBLIC IDS	3	12	321
IT INFO – USER DATA	1	1	149
JOB INFO – COMPENSATION DATA	7	10	527
JOB INFO – EMPLOYEE DATA	12	25	569
JOB INFO – ORG DATA	7	8	412
TOTAL	21*	80	989**

Oracle Data Safeの使用による評価

Oracle Data Safeクラウド・サービスを使用して、クラウド上およびオンプレミスで実行しているデータベースのセキュリティを評価することもできます。Oracle Data Safeは、ユーザーとセキュリティの評価を含む、包括的なセキュリティ機能一式を提供するデータベース・セキュリティのクラウド・サービスです。Oracle Data Safeの緊密に統合された評価機能では複数のデータベース評価の同時実行、評価のスケジュール設定、セキュリティ・ベースラインの確立、そのベースラインと現在のデータベース・セキュリティ評価のずれを表した比較レポートの取得が可能です。Oracle Data Safeでは、データベース・セキュリティ評価を自動化してCI/CDパイプラインに統合するために使用できるAPIが提供されます。

Oracle Data Safeについて詳しくは、https://www.oracle.com/jp/security/database-security/data-safe/をご覧ください。

Oracle Audit Vault and Database Firewallの使用による評価

Oracle Audit Vault and Database Firewall（Oracle AVDF）20.9では、データベース・セキュリティ状況管理が導入されました。Oracle AVDFは、Oracle Database向けの一般的なDatabase Security Assessment Toolを統合することによって、エンタープライズ向けの一元化されたセキュリティ評価ソリューションを提供するようになりました。コンプライアンス・マッピングや推奨事項を備えたフル機能の評価により、組織はすべてのOracle Databaseのセキュリティ状況を一元的に把握できます。

Oracle Audit Vault and Database Firewallについて詳しくは、
https://www.oracle.com/jp/security/database-security/audit-vault-database-firewall/を参照してください。

サマリー

機密データがどこにあり、データベースがどのように構成されているかを把握することは、多層防御戦略を実装する上での基礎となります。100 %セキュアなシステムはありませんが、基礎に目をつぶることは、攻撃者の侵入を容易にします。

Oracle Database Security Assessment Tool（Oracle DBSAT）は、機密データを素早く発見し、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定します。

Oracle DBSATは、有効なサポート契約を結んでいるオラクルのお客様には追加費用なしで提供されます。詳細およびOracle DBSATのダウンロードについては、www.oracle.com/database/technologies/security/dbsat.htmlを参照してください。

おもな機能

- リスクの発生を増加させる可能性のある構成の設定を特定
- 慎重に扱うべきユーザー・アカウントとその権限、およびセキュリティ・ポリシーを特定
- 英語のデータ・ディクショナリと欧州の主要言語による機密データの発見
- 適切なセキュリティ制御および評価結果を推奨および優先順位付け

関連製品

- Oracle Data Safe
- Oracle Audit Vault and Database Firewall
- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting pack
- Oracle Label Security

ORACLE

Connect with us

+1.800.ORACLE1までご連絡いただくか、**oracle.com**をご覧ください。北米以外の地域では、**oracle.com/contact**で最寄りの営業所をご確認いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle