ORACLE

Best Practices for Identity and Access Management (IAM) in Oracle Cloud Infrastructure

2023年5月、2.1版

免責事項

このドキュメントには、ソフトウェアまたは印刷物などの形式を問わず、オラクルが独占的な権利を有する財産的情報が含まれています。この機密資料へのアクセスと使用は、オラクルとの間で締結され遵守に同意したオラクル・ソフトウェア・ライセンスおよびサービス契約の条件に従うものとします。このドキュメントとその内容の開示、コピー、複製および配布には、オラクルによる事前の承諾を必要とします。このドキュメントはライセンス契約の一部となるものではなく、オラクルおよびその子会社や関連会社との契約を構成するものではありません。

このドキュメントは情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。このドキュメントはマテリアルやコード、機能の提供をコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。このドキュメントに記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。製品アーキテクチャの性質により、コードの大幅な不安定化を招くリスクを冒さずに本書に記載されているすべての機能を安全に組み込むことは不可能な場合もあります。

改訂履歴

このドキュメントには、初版の発行以降、次の改訂が加えられています。

日付	改訂内容
2023年5月	Break Glass (緊急用)アカウントに関するガイダンスを修正
2022年5月	Oracle Cloud Infrastructure IAMサービスの最新の変更に合わせて大幅に更新
2021年8月	新しいテンプレートに更新して編集
2018年3月	初版発行

目次

概要

このテクニカル・ペーパーでは、Oracle Cloud Infrastructure (OCI)でソリューションを計画、設計、デプロイする際にOCIのIdentity and Access Management (IAM)サービスを使用するためのベスト・プラクティスについて説明します。

IAMサービスを利用すると、クラウド・リソースにアクセスできるユーザーを制御することができます。あるグループのユーザーがどのリソースに対してどのようなアクセス権を持つかを制御できます。このサービスを利用することにより、デフォルトでは最小権限の付与というセキュリティ原則を徹底させることができます。新規ユーザーは、適切な権限が付与されるまで、いかなるリソースに対しても一切アクションを実行できません。

IAMサービスでは、すべてのOCIサービスにわたって、1つの認証/認可モデルを使用できます。IAMを使用すれば、1つのプロジェクトに取り組んでいる1人のユーザーから、多数のグループが多数のプロジェクトに同時に取り組んでいる大規模な企業まで、あらゆる規模の組織におけるアクセスを1つのアカウント内で簡単に管理できます。

IAMはスケーラビリティに優れているため、何億ものユーザーの管理が可能になります。IAMは、強力な多要素認証(MFA)、アダプティブ・セキュリティ、アイデンティティ・ライフサイクル管理、サードパーティ・アプリケーションへのシングル・サインオン(SSO)、ハイブリッド環境とオンプレミス環境のサポートなどの機能により、従業員、消費者、開発者のユースケースに対応した堅牢なIdentity-as-a-Serviceソリューションを提供します。

IAMサービスのコンポーネント

IAMサービスは複数の主要コンポーネントで構成されています。これらのコンポーネントは、リソースへのアクセスを制御し、アプリケーション管理、SSOおよびアイデンティティ・ライフサイクル管理用にアイデンティティ・ドメインを構成するのに役立ちます。このセクションでは、次のIAMコンポーネントの基本的な定義を示します。

- **リソース:**組織の従業員がOCIを操作して作成/使用するクラウド・オブジェクトです。リソースには、Computeインスタンス、ブロック・ストレージ・ボリューム、仮想クラウド・ネットワーク(VCN)、サブネット、ルーティングテーブルが含まれます。
- **コンパートメント:**関連するリソースの集まりです。コンパートメントは、クラウド・リソースを編成/分離するためのOCIの基本コンポーネントです。使用状況の測定や課金、アクセス(ポリシーを使用)、および分離(あるプロジェクトやビジネス・ユニットのリソースを他のプロジェクトやビジネス・ユニットから分離)の目的で、コンパートメントを使用してリソースを明確に分離します。一般的なアプローチとしては、組織の主要事業部ごとにコンパートメントを作成するという使い方があります。
- **テナンシー:**組織のすべてのOCIリソースが含まれているルート・コンパートメントです。組織のテナンシーは自動的に作成されます。テナンシーの下にはデフォルトのアイデンティティ・ドメインがあり、ユーザー、グループ、ダイナミック・グループ、MFAおよびアプリケーション・カタログが含まれています。テナンシーにはコンパートメントといくつかのポリシーも含まれています。テナンシー内のコンパートメントにポリシーを追加できます。その他のタイプのクラウド・リソース(インスタンス、仮想ネットワーク、ブロック・ストレージ・ボリュームなど)は、お客様が作成したコンパートメント内に配置します。
- **ポリシー:**誰がどのリソースにどのようにアクセスできるのかを指定するドキュメントです。アクセス権は、グループ・レベルとコンパートメント・レベルで付与されます。そのため、特定のコンパートメント内またはテナンシー自体に対する特定のタイプのアクセス権をグループに付与するポリシーを記述できます。テナンシーへのアクセス権をグループに付与すると、そのグループには、テナンシー内のすべてのコンパートメントに対する同じタイプのアクセス権が自動的に付与されます。*ポリシー*という単語には複数の意味があります。ポリシー言語で記述された個別のステートメントのこともあれば、Oracle Cloud ID (OCID)が割り当てられた1つの名前付きポリシー・ドキュメント内のステートメントの集まりのこともあります。また、リソースへのアクセスを制御するために使用されるポリシーの全体的な内容を意味する場合もあります。

- **アイデンティティ・ドメイン**:ユーザー、グループおよびダイナミック・グループの管理を目的とするコンテナの役割を果たすOCIリソースです。ユーザーのフェデレーションとプロビジョニング、セキュア・アプリケーション統合のためのSSOの構成、アダプティブ認証とMFAの構成、SAMLおよびOAuthベースのアイデンティティ・プロバイダの管理を行います。すべてのOCIサービスにわたるアクセス・コントロール・プレーンと複雑なハイブリッドID環境向けの堅牢なエンタープライズIAMとして機能します。

  あるアイデンティティ・ドメインのリソースは他のアイデンティティ・ドメインのリソースから分離されます。ユーザーは常にアイデンティティ・ドメインにサインインし、権限に基づいて、Oracle Cloudコンソールから複数のドメインを管理できます。

- **デフォルト・ドメイン**:各テナンシーにデフォルトのアイデンティティ・ドメインが付属しています。デフォルト・ドメインの管理者はテナンシーの*スーパー管理者*であり、シードされた"テナント管理者"ポリシー(変更不可)からその権限を獲得します。そのため、デフォルト・ドメイン管理者やテナント管理者を日常業務に使用しないようにしてください。かわりに、デフォルト・ドメイン管理者が、特定のリソースを管理するための管理者を作成する必要があります。

- **セカンダリ・ドメイン:**デフォルト・ドメイン以外のアイデンティティ・ドメインです。デフォルト・ドメインとセカンダリ・ドメインには、ソリューションを設計する際に考慮すべき違いがあります。詳細については、次のセクション「コンパートメントとアイデンティティ・ドメイン」を参照してください。

- **ホーム・リージョン:**IAMリソースとドメインが存在するリージョンです。デフォルト・ドメインのすべてのIAMリソースをすべてのリージョンで利用できますが、各定義のマスター・セットは1つのリージョンであるホーム・リージョンに存在します。IAMリソースはホーム・リージョン内でのみ変更できます。

次の図は、US East (Ashburn) (us-ashburn-1)リージョンにおけるIAMサービスの主要コンポーネントを説明したものです。デフォルト・ドメインはルート・コンパートメントに存在し、ProductionDomainとConsumerDomainの2つのセカンダリ・ドメインは本番コンパートメントと消費者コンパートメントに存在しています。この図は、ドメイン管理者にアクセス権を付与する3つのポリシー・ステートメントも示しています。

us-ashburn-1リージョン

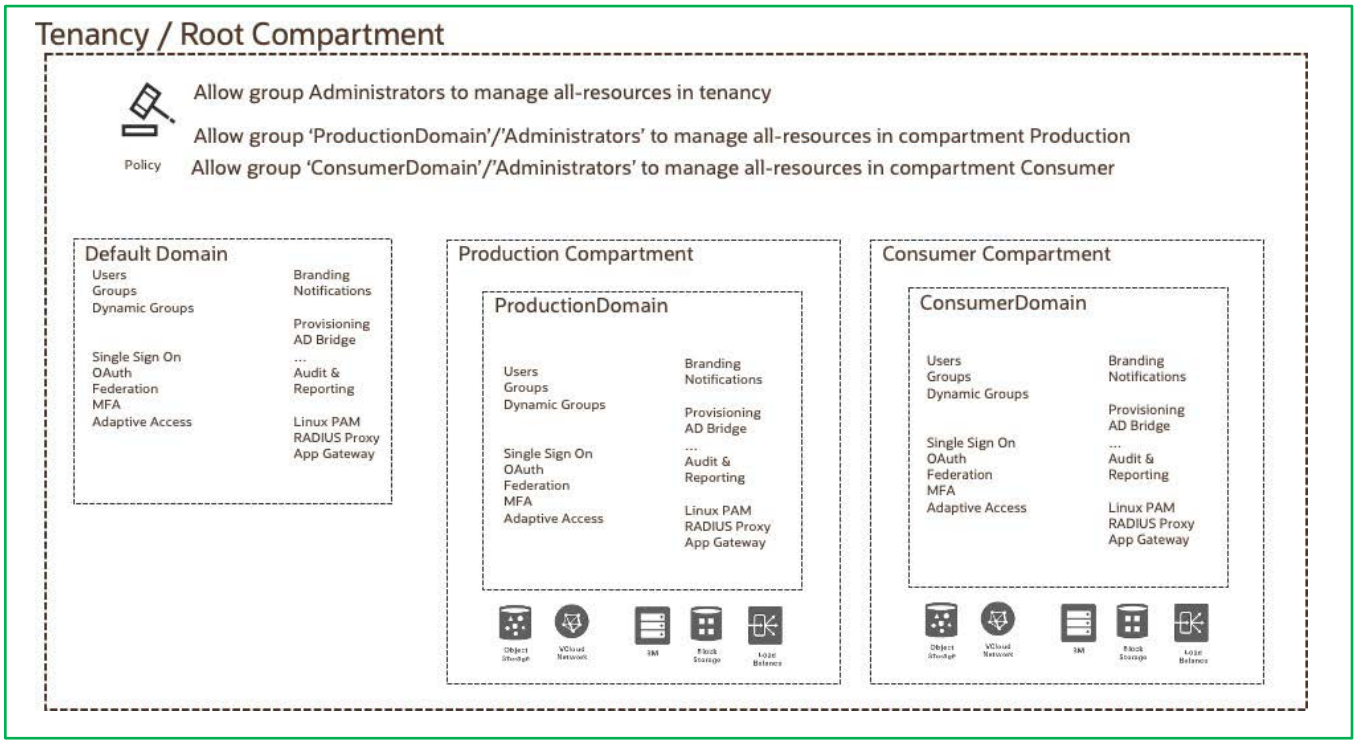

図1:Oracle Cloud Infrastructure IAMサービスのコンポーネント

コンパートメントとアイデンティティ・ドメイン

コンパートメントを使用してクラウド・リソースを編成/分離することで、クラウド・リソースへのアクセスの管理と保護が容易になります。Oracle Cloud Infrastructureの使用を開始するにあたっては、コンパートメントに関して次の点を慎重に検討してください。

- Computeインスタンス、ブロック・ストレージ・ボリューム、VCN、サブネットなどのリソースを作成する際には、それらをコンパートメント内に配置する必要があります。
- コンパートメントはすべてのリージョンのテナンシー全体で使用できます。コンパートメントを作成すると、テナンシーがサブスクライブしているすべてのリージョンでそのコンパートメントが使用可能になります。
- コンパートメントは論理的なエンティティであり、物理エンティティではありません。そのため、関連するリソース・コンポーネントを異なるコンパートメントに配置することもできます。たとえば、インターネット・ゲートウェイにアクセスするクラウド・ネットワーク・サブネットを別個のコンパートメントに配置して、同じクラウド・ネットワーク内の他のサブネットから保護することができます。
- リソースは一度に1つのコンパートメントにのみ存在できます。
- ポリシー・ルールを記述してユーザーのグループにリソースへのアクセス権を付与する際には、アクセス・ルールの適用先となるコンパートメントを指定します。リソースを複数のコンパートメントに分散させる場合は、それらのリソースにアクセスする必要があるユーザーの各コンパートメントに、適切な権限を付与する必要があります。
- コンパートメントは6レベルの深さまでネストさせることができます。ネストしたコンパートメントは親コンパートメントのポリシーを継承します。たとえば、CompartmentParentにCompartmentChildという子コンパートメントがあるとします。次のポリシーは、groupAがCompartmentChild内のネットワークを管理することを許可します。

  ```
  allow group domainA/groupA to manage virtual-network-family in compartment A
  ```

  このトピックの詳細については、「権限の管理」のセクションを参照してください。
- コンパートメントを計画する際には、使用状況データや監査データをどのように集計するのかを検討してください。これは後で重要な問題になってくる可能性があります。
- リソースは、いくつかの例外(リソースに依存関係がある場合)を除き、コンパートメント間で移動できます。リソースを別のコンパートメントに移動すると、そのコンパートメントを制御するポリシーがただちに適用され、リソースへのアクセスに影響が出ます。コンパートメントの構造によっては、編成、測定、請求およびアラームも影響を受ける可能性があります。コンパートメントを移動すると、ポリシーやタグ付けにも影響が出ます。詳細については、「コンパートメントの管理」をお読みください。

アイデンティティ・ドメインは、OCIのユーザー群とそれに関連付けられた構成およびセキュリティ設定を表します。
アイデンティティ・ドメインの使用を開始する際には、次の点を考慮してください。

- アイデンティティ・ドメインを含むIAMは、様々なIAMユースケースに対処するために使用できる、自己完結型のアイデンティティおよびアクセス管理サービスです。
- アイデンティティ・ドメインはOCIのリソースであり、ドメインに対する権限を付与するIAMポリシーを記述できます。ユーザーは常にドメインにサインインします。権限によっては、1人の管理者が1つのドメインにサインインしたまま、複数のドメインを管理できます。
- アイデンティティ・ドメイン内のリソースは他のアイデンティティ・ドメインから分離されます。開発者環境、テスト環境、本番前環境、本番環境を分離するために、別個のアイデンティティ・ドメインを作成することを検討してください。
- 消費者の管理用と従業員の管理用に別々のアイデンティティ・ドメインを作成するなど、ユーザー群ごとに別個のアイデンティティ・ドメインを作成することを検討してください。異なるパスワード・ポリシーや消費者の自己登録の有効化など、消費者のユースケースと従業員のユースケースに対応するアプリケーションおよび構成を各ドメインに持たせることができます。

- 各アイデンティティ・ドメインにタイプが関連付けられており、そのアイデンティティ・ドメインで使用できる制限や機能はタイプによって決まります。タイプには、Free Tier、Oracle Apps、Oracle Apps Premium、Premium、Externalがあります。アイデンティティ・ドメインはあるタイプから別のタイプに変換できます。ユースケースに基づいてドメインのタイプを選択してください。詳細については、「IAMアイデンティティ・ドメインのタイプ」を参照してください。
- 各テナンシーに、テナンシーのホーム・リージョン内の無料のデフォルト・ドメインが付属しています。デフォルト・ドメイン管理者はスーパー管理者であり、テナンシー内のすべてのリソース(アイデンティティ・ドメインを含む)を管理できます。
- デフォルト・ドメインは常にルート・コンパートメントに存在します。削除することはできません。
- デフォルト・ドメインのホーム・リージョンは、テナンシーの作成時に選択します。セカンダリ・ドメインのホーム・リージョンは、セカンダリ・ドメインの作成時に選択します。これはOracle Cloudコンソールで選択するリージョンです。ドメインのホーム・リージョンは変更できません。
- 選択したホーム・リージョンに複数のセカンダリ・ドメインを作成できます。セカンダリ・ドメイン管理者は、セカンダリ・ドメイン内のリソースしか管理できません。セカンダリ・ドメインの外部にあるリソースを管理するには、追加の権限が必要です。
- テナンシーで新しいリージョンをサブスクライブすると、デフォルト・ドメインは新しいリージョンに自動的にレプリケートされます。デフォルト・ドメインを使用する場合、組織のデータ所在地要件を考慮してください。セカンダリ・ドメインについては、ドメインを別のリージョンに明示的にレプリケートする必要があります。

以上の考慮事項を踏まえて、次のことをお薦めします。

- アイデンティティ・ドメイン管理者ロールを持つデフォルト・ドメイン管理者グループおよびユーザーを日常業務に使用しないでください。かわりに、OCIの特定のリソースを管理するための管理者を別途作成してください。
- デフォルト・ドメイン管理者グループに属するのは誰か、デフォルト・ドメインでアイデンティティ・ドメイン管理者ロールを持つのは誰かを定期的にチェックしてください。この2つのグループに属するユーザーはスーパー管理者であり、OCIのすべてのリソースを管理できます。
- デフォルト・ドメインは最初に作成するドメインとして使用してください。デフォルト・ドメインのユーザーがOCIのリソースのアクセスや管理を行えるだけでなく、セカンダリ・ドメインのユーザーもすべてのOCIリソースにアクセスして管理できます。
- アイデンティティの区分(消費者と従業員)、環境の分離(開発、テスト、本番)、データの所在地要件(特定の地理的地域にドメインを作成)などの様々なユースケース用には、他のセカンダリ・ドメインを作成してください。

コンパートメントとアイデンティティ・ドメインをどう設計するかは、組織のユースケースや、リソースの編成/分離ニーズに応じて決まってきます。以下のシナリオはその例です。

概念実証:サンドボックス・コンパートメント

組織の規模が小さい場合や、OCIの評価がまだ概念実証段階である場合は、すべてのリソースをルート・コンパートメントまたはテナンシーに配置することを検討してください。このアプローチにより、すべてのリソースをすばやく簡単に表示/管理することができます。この方法でも、ポリシーを記述してグループを作成すれば、特定のリソースに対する権限を必要なユーザーだけに制限することは可能です。

ユーザーおよびグループの作成とアプリケーションおよびMFAの管理にはデフォルト・ドメインを使用できます。独立した"サンドボックス"コンパートメントを設定して、ユーザーが機能を試すための専用の場所を提供することをお薦めします。サンドボックス・コンパートメントでは、サンドボックス・ドメインを作成して、リソースの作成/管理権限をユーザーに付与することができます。そのため、サンドボックス・ドメインの管理者は、ユーザーがアイデンティティ・ドメインの様々な機能(MFA、SSO、OAuthなど)をより柔軟に試せるようにする一方で、テナンシーの(ルート)コンパートメントとデフォルト・ドメインのリソースに対する権限を厳格化することができます。

次の図に示すように、サンドボックス・ドメインの管理者が管理できるのはサンドボックス・コンパートメントのすべてのリソースのみで、デフォルト・ドメイン管理者がテナンシー内のすべてのリソースを管理する権限を持ちます。

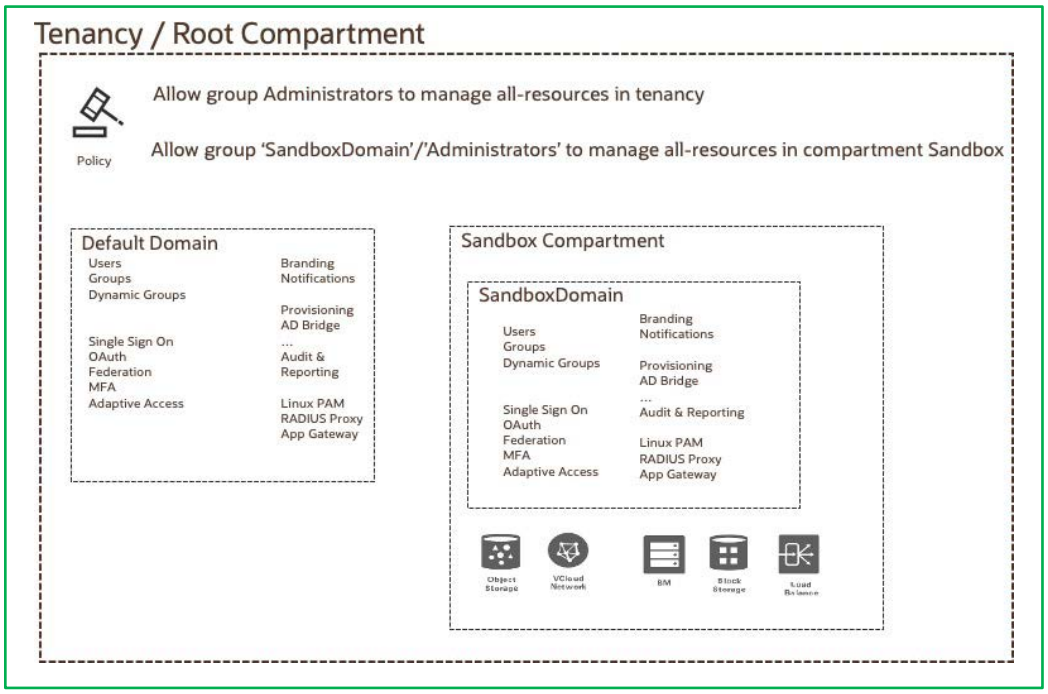

図2:サンドボックス・ドメインを含むサンドボックス・コンパートメント

本番環境での使用

本番環境では、リソースへのアクセスを制限し、リソースをどのようにコンパートメントの中で編成するかを検討してください。ユーザー、グループ、アプリケーションおよびリソースを追加する前に、テナンシーとコンパートメントのプランを作成します。プランには、リソースを編成するためのコンパートメント階層と、リソースにアクセスする必要があるユーザー・グループの定義を含めてください。ユーザー、グループおよびアプリケーションはアイデンティティ・ドメイン内に構成されます。コンパートメント階層とアイデンティティ・ドメインは、アクセスを管理するポリシーをどのように記述するかに影響を与えるため、両方一緒に検討してください。

別々に管理したい事業部が複数ある場合や、別々の方が管理しやすいプロジェクトがある場合は、事業部やプロジェクトの分離ニーズに応じてコンパートメント構造を設計することをお薦めします。このアプローチを使用すれば、コンパートメントまたはプロジェクトごとに専任の管理者グループを追加して、担当のプロジェクトに対してのみ、アクセス・ポリシーを設定できるようにすることができます。ユーザー、グループ、ダイナミック・グループおよびアプリケーションはアイデンティティ・ドメインから管理されます。たとえば、あるグループに対し、担当するすべてのリソースの制御権限を付与しながらも、ルート・コンパートメントやその他のプロジェクトについては、管理者権限を付与しないようにすることができます。これにより、組織内の各グループが担当のリソース用のサブクラウドを設定し、それらを個別に管理できるようになります。

次のシナリオは、コンパートメントの設計方法と関連ポリシーの定義方法について説明したものです。

ACME社にはA、B、Cという3つの主要事業部があります。また、複数のタイプの管理者が配置されています。データベース、ネットワーク、ストレージ、セキュリティです。各事業部に、その事業部のデータベースを管理するデータベース管理者がいます。ネットワーク管理者、ストレージ管理者、セキュリティ管理者は、3つの事業部すべてに対応するネットワーク、ストレージ、セキュリティ関連リソースにアクセスし、管理する必要があります。

ACMEにはMuShopという消費者対応アプリケーションもあり、消費者のアイデンティティと従業員のアイデンティティを分離したいと考えています。たとえば、同社の本番ドメインでは、従業員のアイデンティティとFidelityやJiraなどのアプリケーションがホストされています。消費者ドメインには、消費者のアイデンティティと消費者向け小売アプリケーションのMuShopがあります。

消費者ドメインの管理者は従業員のアイデンティティ・ストアに存在しており、消費者のアイデンティティとアプリケーションを管理する必要があります。

これらのニーズに対応するには、ACMEの事業部構造に合わせて5つのコンパートメントを作成する必要があります。その後、本番用と消費者用に1つずつ、2つのドメインを作成します。各タイプの管理者に対応するグループを定義します。最後に、誰がどのリソースにアクセスできるかを制御するためのポリシーを定義します。

次の図は、このシナリオで考えられるコンパートメント、アイデンティティ・ドメインおよびポリシーの設計を示したものです。

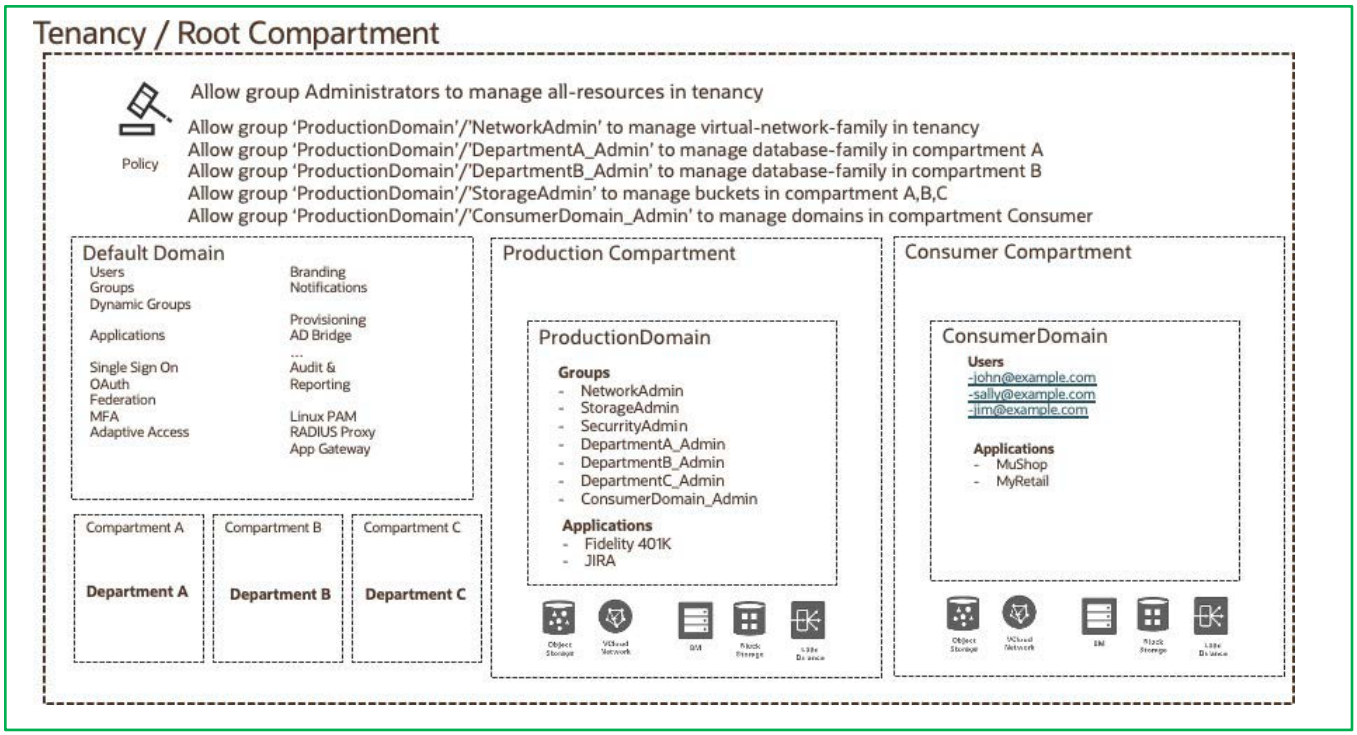

図3:本番環境の例

図に記載されているポリシーをいくつか説明しましょう。

- `Allow group Administrators to manage all-resources in tenancy`

  このポリシーは標準のテナント管理者ポリシーであり、変更できません。Administratorsグループにはドメイン名の接頭辞が付いていません。つまり、Administratorsグループはデフォルト・ドメインに属しています。そのため、デフォルト・ドメインのAdministratorsグループに属するユーザーは、テナンシー内のすべてのリソースを管理する権限を持ちます。

  デフォルト・ドメイン管理者を日常業務に使用することはお薦めしません。そのため、図に示すように、OCIの様々なリソースを管理するための管理者グループを本番ドメインに追加で作成しました。

- `Allow group 'ProductionDomain'/'NetworkAdmin' to manage virtual-network-family in tenancy`

  このポリシーは、本番ドメインのNetworkAdminグループに属するユーザーがテナンシー内のネットワークを管理することを許可します。

- `Allow group 'ProductionDomain'/'DepartmentA_Admin' to manage database-family in compartment A`

  このポリシーは、本番ドメインのDepartmentA_Adminグループに属するユーザーがコンパートメントAのデータベースを管理することを許可します。

- `Allow group 'ProductionDomain'/'ConsumerDomain_Admin' to manage domains in compartment Consumer where request.domain.name='ConsumerDomain'`

  このポリシーは、本番ドメインのConsumerDomain_Adminグループに属するユーザーが消費者ドメインを管理することを許可します。これが可能なのは、ドメインがOCIのリソースであり、ポリシーで適切な権限が付与されれば、他のドメインのユーザーが他のドメインを管理できるためです。

ユーザー管理

アイデンティティ・ドメインのユーザーとグループは複数の方法で管理できます。アイデンティティ・ドメインのユーザーを管理する際には、次の点を考慮してください。

考慮事項	推奨事項とオプション
どのようなタイプのユーザーを管理するのか。従業員か消費者ユーザーか。	通常、消費者ユーザーにはセルフサービス機能が必要です。IAMの自己登録機能を使用するか、System for Cross-domain Identity Management (SCIM) APIを使用してカスタム・ソリューションを構築します。 従業員ユーザーは、Fusion Human Capital Management (HCM)やActive Directoryなど、様々なシステムに属している可能性があります。「外部ソースからのユーザーの取り込み」のセクションを参照してください。
ユーザー管理は自動か手動か。	簡単なテストやサンドボックスのユースケースの場合は、Oracle Cloudコンソールを使用して手動でユーザーを作成します。 Oracle Cloudコンソールを使用して多数のユーザーやグループをインポートするには、CSVのエクスポート/インポート・オプションを使用します。
IAMにユーザーを取り込む際にパスワードを同期する必要があるか。	REST APIを使用し、CSVのインポート・ジョブを使用してハッシュ・パスワードをIAMにインポートします。
非アクティブ状態のユーザーを作成する必要があるか。非アクティブ状態のユーザーを後でアクティブにする必要があるか。	REST APIを使用するか、アクティブ状態をFalseに設定してCSVインポートを使用します。

コンソールを使用したユーザーのローカル管理

ユーザーを管理するには、次の権限のうち1つ以上が必要です。

- アイデンティティ・ドメインの管理者グループに属していること。アイデンティティ・ドメインの管理者グループは、ドメインのすべてのリソース(ユーザーとグループを含む)を管理できます。
- ユーザーを管理する権限があること。ポリシー管理者は、次の例のようなポリシーを記述することにより、ユーザーとグループの管理をさらに委任できます。

  ```
  allow group <domain1>/<group1> to manage users in tenancy where request.domain.name=domain
  ```

- ユーザー管理者ロールまたはユーザー・マネージャ管理者ロールに属していること。

ユーザーとグループの権限管理には、管理者ロールではなくIAMポリシーを使用できます。詳細については、「管理者ロールとIAMポリシーの比較」のセクションを参照してください。

新規ユーザーは、テナンシーまたはコンパートメントに対してのグループ権限を付与するポリシーが少なくとも1つあるグループに配置されるまで、何の権限も付与されません。

最初に新規ユーザーの役割を明確に分類し、その後、適切なポリシーが適用されたグループにユーザーを配置することをお薦めします。たとえば、ユーザーがデータベース管理者の場合、対応するコンパートメントの`database-family`リソース・タイプの管理権限を付与するポリシーが適用されたデータベース管理者グループにユーザーを配置できます。

外部ソースからのユーザーの取り込み

自動化を使用して外部ソースからIAMにユーザーを取り込むには、ユースケースによっていくつかの方法があります。IAMは次の方法をサポートしています。

- **アプリケーション・カタログ**:Oracle Human Capital Management (HCM)、Oracle Unified Directory、Oracle Internet Directoryなどのアプリケーションからユーザーを取り込むための充実したプロビジョニング・アプリケーション・カタログがあります。
- **SCIM API**:ユーザーのライフサイクルを管理するには、IAM SCIM APIを使用します。
- **ブリッジ・コンポーネント**:IAMは、Active Directoryブリッジおよびプロビジョニング・ブリッジのソフトウェア・コンポーネントを提供します。これは、お客様がユーザーの同期とプロビジョニングのためにローカルにインストールするものです。
- **ジャストインタイム(JIT)**:ジャストインタイム・プロビジョニングを使用したフェデレーション認証の一環としてユーザーをインポートします。

アイデンティティ・ドメインのユーザーを管理する際には、次の点を考慮してください:

- ブリッジ・コンポーネントは、IAMで使用するためにダウンロードしてインストールと構成を行う必要のあるソフトウェアです。
- Active Directoryブリッジは Active Directoryでのみ機能しますが、ユーザーがActive Directoryの資格証明を使用してIAMに直接サインインできる委任認証にも使用されます。
- プロビジョニング・ブリッジは、Oracle Unified DirectoryやOracle E-Business Suiteなど、特定のアプリケーション・テンプレートで使用されます。このブリッジは、すべてのプロビジョニング・テンプレートに必要なわけではありません。たとえば、Fusion Applicationsテンプレートはブリッジを必要としません。
- プロビジョニング・テンプレートに用意されているフィルタを使用して、どのグループとユーザーをインポートするかを検討してください。
- パスワードをIAMに同期するには、REST APIによるCSVインポートを使用することを検討してください。

権限管理

Oracle Cloud Infrastructureでの権限管理は、ポリシーを通じて行われます。ポリシーが適用されたグループでは、特定のコンパートメントやテナンシー内にある特定のタイプのリソースを、特定の方法で操作することができます。ポリシーは、個別のユーザーではなく、ユーザーのグループにアクセス権を付与するものです。ユーザーは、グループに属することで、アクセス権を取得することができます。

ポリシーはアクセスを*許可する*目的にのみ使用されます。アクセスを明示的に禁止することはできません。特定のユーザーのアクセスを制限する必要がある場合は、そのユーザーを当該のグループから削除するか、IAMサービスから完全に削除することで対処できます。

各ポリシーは、次の基本構文に従った1つ以上のポリシー・ステートメントで構成されます。

```
Allow group <domain name>/<group name> to <verb> <resource-type> in compartment <compartment name>
```

- `<domain name>`は、グループが存在するドメインです。
- `<verb>`は、アクセスのタイプを示します。タイプには`inspect`、`read`、`use`、`manage`があります。これらの各アクセス・タイプには、先行するタイプのアクセス権がそれぞれ含まれています。たとえば、inspectが指定されたグループのユーザーは、リソースを一覧表示することができますが、リソース内の機密情報やユーザー固有のメタデータにアクセスすることはできません。readには、inspectの権限に加えて、ユーザー固有のメタデータと、実際のリソース自体を取得する権限が含まれます。
- `<resource-type>`では、集約(ファミリー)リソースか、個別のリソースを指定することができます。たとえば、`database-family`は集約リソース・タイプで、`db-systems`や`db-nodes`はそのファミリー内の個別のリソース・タイプです。

最初にできるだけ具体的なポリシーを定義し、その後、ユースケースに応じてそれらを徐々に更新していくことをお薦めします。詳細については、IAMサービス・ドキュメントの「ポリシーの仕組み」を参照してください。

次の例に示すように、ドメイン名に接頭辞を付けない場合は、デフォルト・ドメインを意味します。以下の2つの例は同等です。

```
Allow group NetworkAdmin to manage virtual-network-family in compartment AcmeCorp

Allow group 'Default'/'NetworkAdmin' to manage virtual-network-family in compartment AcmeCorp
```

デフォルト・ドメインのグループを対象としたポリシーを記述する場合は、グループ名にdefaultの接頭辞を付けてポリシー・ステートメントを読みやすくすることをお薦めします。次の図に示すように、ポリシー・ビルダー・ツールを使用すると、ポリシーをすばやく簡単に作成できます。

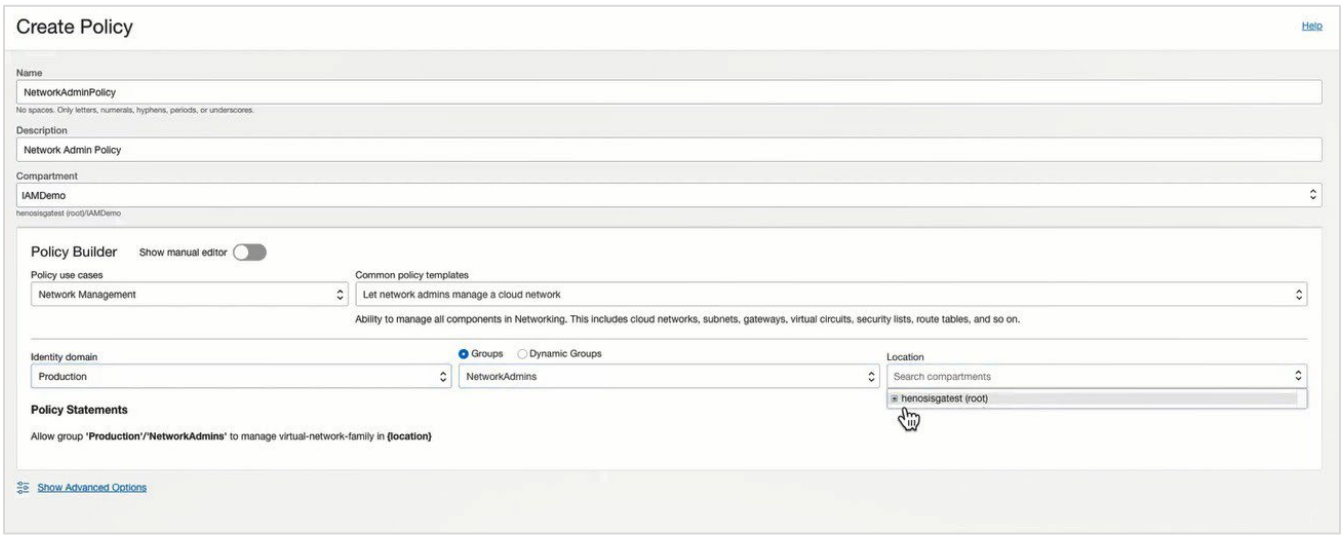

図4:ポリシー・ビルダーを使用したポリシーの作成

ポリシーのアタッチと継承

ポリシーを作成する前に、ポリシーのアタッチと継承について理解しておく必要があります。ポリシーを作成する際にはコンパートメントの下に作成し、作成したポリシーはそのコンパートメントにアタッチされます。どこにポリシーをアタッチするかによって、そのポリシーの変更や削除を行えるユーザーが決まります。また、コンパートメントは親コンパートメントのポリシーを継承します。

次の例では、ポリシー1はルート・コンパートメントに、ポリシー2は親コンパートメントに、ポリシー3は子コンパートメントにアタッチされています。したがって、これらのコンパートメントのポリシーを管理する権限を持つユーザーは、これらのポリシーの更新や削除を行うことができます。

ポリシー1は、デフォルト・ドメインの管理者がテナンシー(ルート・コンパートメント)内のすべてのリソースを管理することを許可します。この例では、コンパートメントの階層はルート>親>子です。したがって、ポリシーの継承により、ポリシー1は管理者が親コンパートメントと子コンパートメントのすべてのリソースを管理することも許可します。

同様に、ポリシー2は、Domain1とGroup1が親コンパートメントと子コンパートメントのネットワークを管理することを許可します。親>子というコンパートメント階層があるためです。

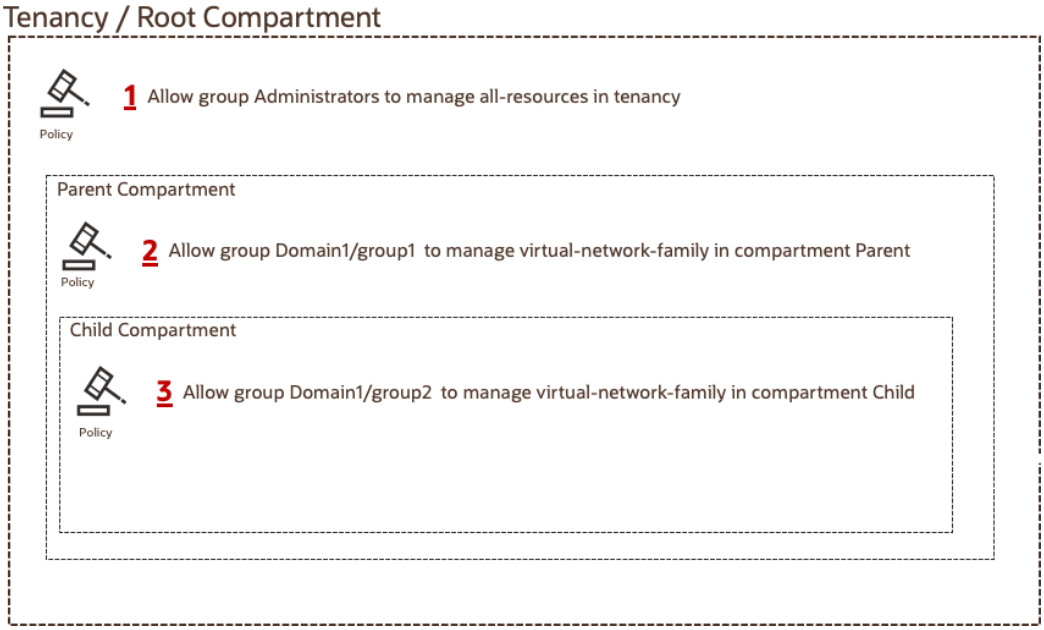

図5:親コンパートメントからの子コンパートメントのポリシー継承

次のことをお薦めします。

- プロジェクトに基づいて、誰がポリシー管理者になるかを検討し、ポリシーをアタッチするコンパートメントを決定してください。
- ポリシーを作成するためのアクセス権を持つ管理者の数を制限してください。
- 次のポリシーのmanage all-resourcesは、ポリシーを管理することも意味します。

  ```
  allow group domain/group to manage all-resources in compartment A
  ```

  かわりに、manage policiesやmanage virtual-network-familiesなどの具体的な権限を使用することをお薦めします。
- 追加のポリシー管理者を作成する必要がある場合は、特定のコンパートメントのポリシー管理者にすることで、最小限の範囲に制限してください。この制限により、リソースを管理するためのポリシーの作成を許可できますが、ポリシー管理者が記述できるのはそのコンパートメント内のリソースのみを管理するためのポリシーです。
- ポリシーが誤って削除されるのを防ぐため、ポリシーの削除権限は付与しないでください。たとえば、次のポリシーでは、manageキーワードによって作成、読み取り、更新、削除(CRUD)の操作をすべて許可しています。

  ```
  allow group domain1/group1 to manage policies in compartment
  ```

  かわりに、次のポリシーを使用してください。

  ```
  allow group domain1/group1 to manage policies in compartment demo where
  request.permission = any {'POLICY_CREATE', 'POLICY_UPDATE'}
  ```

最小権限の徹底

最小権限を徹底するポリシーを記述し、必要に応じて徐々に権限を追加していくことをお薦めします。いくつかの例を基に、このようなポリシーの記述方法を理解しましょう。

ポリシーの定義	説明

ポリシーA
`Allow dynamic-group AuditDG to manage objects in compartment AcmeCorp`
ポリシーB
`Allow dynamic-group AuditDG to manage objects in compartment AcmeCorp where all {target.bucket.name = 'audit_logs_bucket', request.permission='OBJECT_CREATE'}`
	ポリシーAでは、最小権限を徹底していません。コンパートメントAcmeCorp内のすべてのバケットのオブジェクトを管理することを許可しています。
	ポリシーBでは、オブジェクトを管理するためのアクセスを次の方法で制限しています。
	• バケット名を指定することで、アクセスを1つのバケットのみに制限する。
	`target.bucket.name='audit_logs_bucket'`
	• 作成権限のみを与えることで、更新と削除のためのアクセスを制限する。
	`request.permission='OBJECT_CREATE'`

`Allow dynamic-group AuditDG to read secret-family in compartment AcmeCorp where target.secret.name = 'audit-secret'`	このポリシーでは、グループへの読み取り専用アクセスを指定しています。グループを使用するには読み取りアクセスが必要であるためです。

ポリシーA
`Allow group XYZ to manage groups in tenancy where request.permission != 'GROUP_DELETE'`
ポリシーB
`Allow group XYZ to manage groups in tenancy where any {request.permission='GROUP_INSPECT', request.permission='GROUP_CREATE', request.permission='GROUP_UPDATE'}`
ポリシーC
`Allow group XYZ to manage groups in tenancy where any {request.operation='ListGroups', request.operation='GetGroup', request.operation='CreateGroup', request. operation='UpdateGroup'}`
	グループXYZは、グループを一覧表示、取得、作成、更新できる必要がありますが、削除できる必要はありません。
	ポリシーA、BおよびCは同じ結果になりますが、次の違いを考慮してください。
	• **ポリシーA**:サービスによって将来追加される可能性のある新しい権限は、GROUP_DELETEのみを除き、グループXYZに自動的に付与されます。
	• **ポリシーB**:許可される権限が明示的に指定されています。この方法をお薦めします。
	• **ポリシーC**:この方法では、特定のAPI操作に基づいた条件が記述されています。

`Allow group DomainA/GroupA to manage object-family in tenancy where request.networkSource.name='corpnet'`	このポリシーでは、ネットワーク・ソースに基づいてアクセスを制限しています。
`Allow DomainA/Contractors to use instances in compartment contractors where all {request.utc-timestamp after '<TIME>', request.utc-timestamp before '<TIME>'}`	このポリシーでは、時間ベースの変数を使用して、ポリシーで付与されるアクセス権を特定の時間枠のみに制限しています。

タグベースのアクセス制御

Oracle Cloud Infrastructure Taggingを使用すると、リソースにメタデータを追加でき、キーと値を定義してリソースに関連付けることが可能になります。このタグは、組織のビジネス・ニーズに基づいてリソースを編成し一覧表示するために使用できます。

ポリシー・ステートメントでタグを使用することで、OCIのリソースのアクセスを制御できます。タグベースのアクセス制御(TBAC)では、複数のコンパートメント、グループおよびリソースにわたるアクセス・ポリシーをタグを使って定義できるので、ポリシーの柔軟性が高まります。アクセス制御は、リクエスト側のリソース(グループ、ダイナミック・グループ、コンパートメントなど)に存在するタグ、またはリクエストのターゲット(リソースやコンパートメントなど)に存在するタグに基づいて行うことができます。

Oracle Cloudコンソール、APIまたはCLIを使用して説明、タグまたはわかりやすい名前をクラウド・リソースに割り当てる際には、機密情報を入力することは避けてください。

次の例を使って、TBACを使用する際の主な考慮事項を確認しましょう。この例は、様々な値でタグ付けされた2つのComputeインスタンスを示しています。

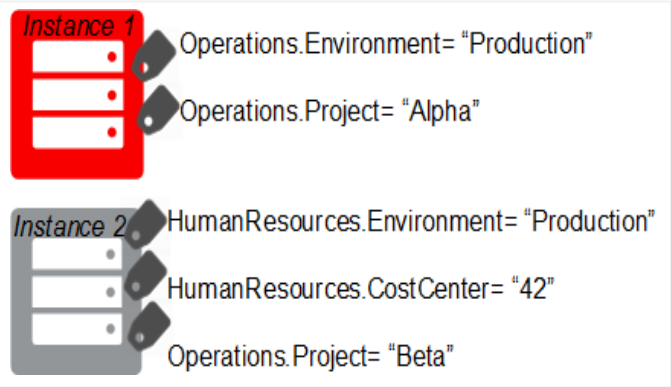

図6:タグ付けされた値を持つComputeインスタンスの例

タグが付いている場合、次のベスト・プラクティスをお薦めします。

- 誰がリソースにタグを適用できるかを制御します。たとえば、次のポリシーを使用すると、GroupAに属するユーザーが適用できるタグを“Operations.Environment”のみに制限できます。

  ```
  Allow group DomainA/GroupA to use tag-namespaces in tenancy where all{target.tag-namespace.name='Operations'}
  ```

- タグを使用してポリシーを記述するポリシー管理者は、タグが付いたリソースおよびリクエスタをすべて把握し、タグを使用してポリシーを記述した場合の影響を考慮する必要があります。たとえば、管理者が次のポリシーを記述するとします。

  ```
  Allow group DomainA/ProductionAdmins to manage instance in compartment Production where target.resource.tag.Operations.Project= 'Alpha'
  ```

  ポリシー管理者は、ポリシーを記述する前に、`project = alpha`でタグ付けされたすべてのインスタンスを把握するか、`Operations.Project`タグを適用するためのアクセス権を持つのは誰かを把握し、記述しようとしているポリシーを使用してアクセスできるのは誰かを知っておく必要があります。

TBACの詳細については、OCIのドキュメントをお読みください。

管理者ロールとIAMポリシーの比較

各アイデンティティ・ドメインには、アイデンティティ・ドメイン管理者が各種タスクおよびリソースへの様々なレベルのアクセス権を持てるようにする管理者ロールがあります。このセクションでは、各管理者ロールの権限について説明します。

ロールは、ドメイン内のユーザーにのみ適用され、ドメイン内のアプリケーション、またはドメインと統合されたデータ・プレーンへのきめ細かなアクセスを可能にしますが、コンパートメントへの範囲指定はできません。ポリシーは、より広範に適用できますが、対象となるのはコントロール・プレーンのみで、コンパートメントへの範囲指定が可能です。

管理者ロールとポリシーの使用に関しては、次の推奨事項とオプションを考慮してください。

管理者ロール	権限	推奨事項とオプション
アイデンティティ・ドメイン管理者	IAMのアイデンティティ・ドメインに対するスーパーユーザー権限を持ちます。 アイデンティティ・ドメイン管理者は次のことを実行できます。 • ユーザー、グループ、アプリケーション、システム構成およびセキュリティ設定を管理する • ユーザーを様々な管理ロールに割り当てて、委任管理を実行する • MFAを有効/無効にする、MFA設定を構成する、認証要素を構成する • 自己登録プロファイルを作成して、様々なユーザー、承認ポリシーおよびアプリケーションのセットを管理する	ドメインの作成時にドメイン管理者を指定すると、IAMにより、そのユーザーにアイデンティティ・ドメイン管理者ロールが割り当てられます。 ドメインの作成時にドメイン管理者を割り当てることは必須ではありません。管理者を指定せずにドメインを作成し、ユーザーにドメイン管理権限を付与するポリシーを後から記述することもできます。そのようなポリシーの例を次に示します。 `Allow group 'Domain1'/'Group1' to manage domains in compartment A where request.domain.name=Domain2` したがって、個々のユーザーにアイデンティティ・ドメイン管理者ロールを割り当てるかわりに、ポリシーを使用してドメインを管理できます。
ユーザー管理者、ユーザー・マネージャおよびヘルプデスク管理者	アイデンティティ・ドメインのユーザー、グループおよびグループのメンバーシップを管理します。	この管理者ロールを使用するかわりに、ユーザー・グループおよびグループのメンバーシップの管理権限を付与するポリシーを記述できます。

管理者アカウント

管理者アカウントは、アカウントが乗っ取られた場合に悪用される可能性のある特権的アクセス権を持ちます。管理者アカウントについては、次の要件を満たしてください。

- すべての管理者アカウントに対して、FIDO2セキュリティ・キーやモバイル・アプリのプッシュ通知など、よりセキュアな要素を使用したMFAを有効にします。モバイル・アプリでは、通知に応答する前に、電話の生体認証を使用した構成可能なロック解除が必要になるため、SMSや電子メールで送信されたワンタイム・パスワード(OTP)よりもセキュアです。
- 管理者の資格証明をユーザー間で共有するかわりに、追加の管理者アカウントを作成して、誰が何を変更したかを監査ログに記録できるようにします。
- すべての管理者アカウントのアクセスを定期的にモニターします。
- アイデンティティ・ドメイン管理者(IDA)ロールが付与されたアイデンティティ・ドメイン内のアプリケーションをチェックします。IDAロールはドメイン管理者であり、ドメイン内のすべてのリソースを管理できます。IDAロールを持つアプリケーションは、APIを呼び出したり、管理者が実行可能な操作をコンソールから変更したりすることができます。
- 管理者アカウントのアダプティブ・アクセスを有効にし、リスク・スコアが高い場合に認証の強化やアクセスの拒否ができるようにすることを検討します。

Break Glass (緊急用)アカウント

誰もOracle Cloudコンソールにアクセスできない場合に使用する緊急用のBreak Glassアカウントを作成してください。Break Glassアカウントを作成する際には、次の要素を考慮してください。

- デフォルト・ドメイン管理者グループに属するユーザーはすべてグローバル管理者であり、OCIのすべてのリソースを管理できます。
- テナント管理者は、OCIの特定のリソースを管理するための管理者を追加作成し、Break Glassアカウントを作成した後、デフォルト・ドメイン管理者グループとアイデンティティ・ドメイン管理者ロールから自分自身を削除して、自分の権限レベルを下げる必要があります。
- コンソールでアカウントを作成する際、電子メール・アドレスを指定する必要があります。アカウントの設定用には、アカウントを作成する管理者の電子メール・アドレスを選択できます。管理者は、Break Glassアカウントのパスワードを設定した後、その電子メール・アドレスを削除し、無効な電子メール・アドレスでプロファイルを更新する必要があります。これにより、パスワードをリセットしようとしてもできなくなります。
- Break Glassアカウントのモニタリングを有効にし、このアカウントが使用されたら必ず他の管理者に通知します。
- Break Glassアカウントは高度な権限を持つアカウントであるため、Break Glassアカウントに対してMFAを有効にするとともに、緊急時に使用できない可能性のあるユーザーやデバイスにBreak Glassアカウントが関連付けられていないことを確認してください。非同期でないMFA要素(既知の場所に安全に格納されたFast ID Online (FIDO)セキュリティ・キーなど)を使用するBreak Glassアカウントを少なくとも1つ用意することを検討してください。
- このアカウントがデフォルト・ドメインのもので、管理者グループのみに属しているか、テナンシー内のすべてのリソースを管理する権限を持っていることを確認します。
- デフォルト・ドメインのサインイン・ポリシーに明示的なdenyが含まれていないことを確認します。これにより、`Break Glass`アカウントでのサインインを防止できます。

シングル・サインオンの有効化

アプリケーションおよびサービスへのアクセス時に、複数のURL、ユーザー名およびパスワードを追跡するようユーザーに求めることができます。オンプレミスとクラウド両方のアプリケーションおよびサービス全体にわたってIAMのシングル・サインオン(SSO)機能を有効にすることをお薦めします。

- SAML、OpenIDおよびプロビジョニング・アプリケーションからなる、充実したIAMアプリケーション・カタログを使用します。
- カタログに載っていないアプリケーションには、SAML、OAuthまたはOpenIDアプリケーション・ウィザードを使用します。
- SAML、OpenIDまたはOAuthプロトコルを使用することで、標準ベースの統合を使用します。
- オープン標準プロトコルをサポートしていないアプリケーションには、IAMアプリケーション・ゲートウェイのヘッダーベースの認証を使用し、そのようなアプリケーションはいずれSAML、OpenIDまたはOAuthをサポートするようにアップグレードします。
- IAMアイデンティティ・プロバイダのポリシーは、どのアイデンティティ・プロバイダ(IdP)が認証に使用されるかを制御します。IdPポリシーは認証の前に適用されます。
- ルール、条件および実行順序を使用して、IdPポリシーを使用した複雑なサインイン要件を調整します。たとえば、管理者は、パスワードレス・グループに属するユーザーに対して発するパスワードレス・ルールや、ユーザー名がexampledomain.comで終わる場合には必ず外部IdPを使用して認証するルールを構成することができます。

多要素認証とアダプティブ・セキュリティの実施

多要素認証(MFA)は、組織にとって、きわめて重要なセキュリティ層となります。MFAは、エンドユーザーの資格証明と、オンプレミスおよびSoftware-as-a-Service (SaaS)のアプリケーションに対する管理者のアクセスを保護します。

IAMでは、サインオン・ポリシーを使用してMFAを実施します。サインイン・ポリシーを使用すると、管理者は、アプリケーションへのアクセス・ルールを構成し、認証、MFAおよびアダプティブ・リスク・スコアリングを強化してアクセスをチャレンジまたは拒否することができます。

コンテキストに基づいたサインイン・エクスペリエンスを作成することをお薦めします。たとえば、ユーザーが財務アプリケーションにアクセスする場合はMFAを要求し、仮想ビデオ会議アプリケーションにアクセスしてプロファイル設定を変更する場合はMFAを要求しないようにすることができます。

使用可能な次の条件、リスク・イベントおよびアクションを考慮し、アプリケーションのユーザー、アプリケーションの使用方法、アプリケーションのコンプライアンス要件、およびユーザーが期待するユーザー・エクスペリエンスのタイプに基づいて、認証とMFAを設計してください。

条件	リスク・イベント	アクション
ユーザー グループ アプリケーション 認証方式 信頼できるデバイス ネットワーク境界 リスク・スコア	MFAイベントの失敗が多すぎる ロケーション間を移動できない 疑わしいIPアドレスからのアクセス 不明なデバイスからのアクセス サインインの失敗が多すぎる 見知らぬロケーションからのアクセス	許可 拒否 再認証 MFA • 必須または任意 • *n*時間または*n*日ごと • FIDO2などの特定の要素 • 信頼できるデバイスの場合はスキップ

リスク・イベントが条件で直接使用されることはありません。リスク・スコアはポリシー条件で使用され、リスク・スコアリングはアダプティブ・セキュリティの画面で構成されます。次の図に示すように、リスク・スコアの生成方法に影響を与える個々のリスク・イベントに重みを定義します。

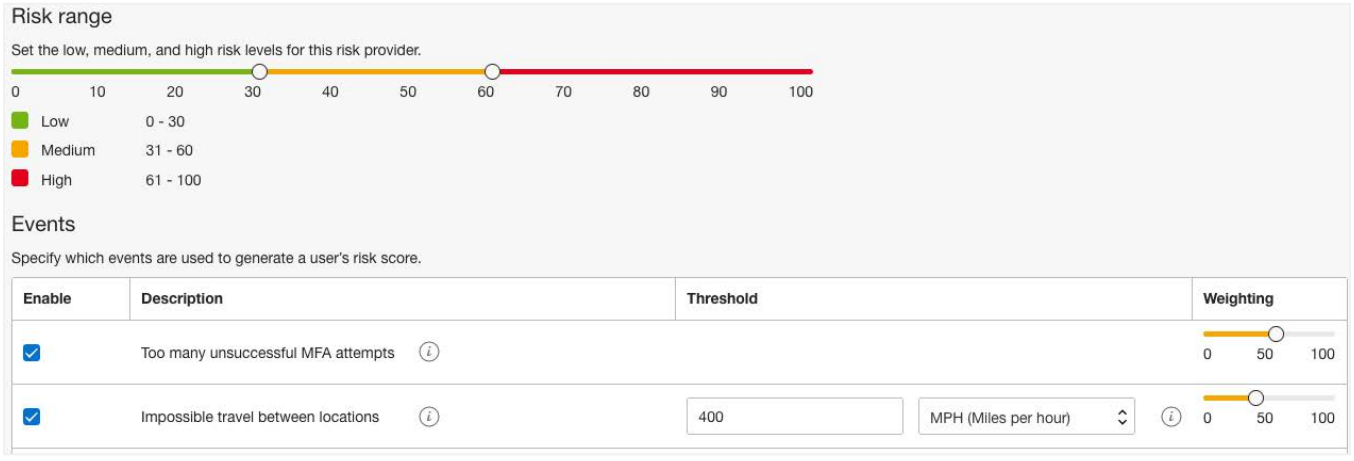

図7:リスク範囲チャート(イベントと重みを含む)

レプリケーション、ディザスタ・リカバリおよび高可用性

このセクションでは、IAMでのレプリケーション、ディザスタ・リカバリおよび高可用性について、お客様とOracle Cloud Infrastructureのどちらが責任を負うかを明確化します。

レプリケーション

各アイデンティティ・ドメインにはホーム・リージョンが割り当てられており、さらにドメインをテナンシーがサブスクライブしている他のリージョンにレプリケートすることができます。ドメインを別のリージョンにレプリケートすると、すべてのアイデンティティ・リソースがそのリージョンにレプリケートされ、IAMはそのリージョンのリソースに対してユーザーを認可できるようになります。

認証とアイデンティティ・リソースの編集はすべて、常にドメインのホーム・リージョンで行われます。そのため、このレプリケーションは高可用性やディザスタ・リカバリのソリューションではありません。ただし、レプリケーションを使用した高可用性読み取り専用および高可用性読み書きのサポートが追加される予定です。

レプリケーションが1つの要因となるのは、テンシーが複数のリージョンをサブスクライブしている場合のみです。デフォルト・ドメインは、テナンシーがサブスクライブしているすべてのリージョンを自動的にサブスクライブしますが、この自動サブスクリプションは変更できません。お客様は、テナンシーがサブスクライブしているリージョンのいずれかにセカンダリ・ドメインをレプリケートすることを選択できます。

データの所在地要件に対応するにはセカンダリ・ドメインを使用することをお薦めします。セカンダリ・ドメインがあれば、ドメインをレプリケートする地理的地域を選択できます。

レプリケーションの責任はOCIとお客様が共有します。

ディザスタ・リカバリ

ディザスタ・リカバリとは、災害に備えてドメインのデータのバックアップを別のリージョンに作成することを指します。この独立した操作は、レプリケーションやIAMの高可用性とは関係ありません。

OCIリージョン全体が使用できなくなった場合、ディザスタ・リカバリ・リージョンにトラフィックをルーティングすることによって、サービスの復旧を迅速化し、可能な限り多くのデータを保持することができます。リージョンとディザスタ・リカバリ・リージョンのペアはオラクルによって自動的に作成されます。お客様がディザスタ・リカバリ・リージョンを選択することはできません。リージョンのマッピングは、各国の法規制に基づいて決定を下すOCIコンプライアンス・チームから入手できます。

詳細については、「ディザスタ・リカバリ・リージョンのペアの作成」および「ディザスタ・リカバリとアイデンティティ・ドメイン」を参照してください。

ディザスタ・リカバリの責任はOCIが負います。お客様は、ディザスタ・リカバリ・リージョンからのトラフィックを許可するようにファイアウォールを更新しなければならない場合があります。

高可用性

IAMはホーム・リージョン内の高可用性を提供します。OCIリージョン内では、単一の可用性ドメインにフォルト・ドメインがあるか、複数の可用性ドメインかのいずれかです。どちらでも同じ機能が得られますが、フォルト・ドメイン同士の方が可用性ドメイン同士よりも物理的な距離は近くなります。IAMは、各リージョンに二重にインストールする(可用性ドメインまたはフォルト・ドメイン全体で2つ)デプロイ方式を取り、リージョン内での高可用性を提供します。

高可用性の責任はOCIが負います。お客様は、カスタム・サインイン・ページなどのアプリケーションを高可用性に対応させる責任を負います。

インスタンス・プリンシパルとダイナミック・グループ

IAMのインスタンス・プリンシパル機能を使用すると、IAMユーザーを作成したり、各インスタンスの資格証明を管理したりしなくても、IAMで保護されたAPIをOracle Cloud Infrastructure Computeインスタンス(仮想マシンまたはベア・メタル)から呼び出すことができます。

たとえば、Computeインスタンスで実行されているアプリケーションから、Object Storageサービスにアクセスする必要があるとします。その場合、インスタンス・プリンシパルを使用しないのであれば、特定のユーザーを作成した後、Object Storageサービス内のバケットに対する読み取り権限と書き込み権限を付与するポリシーを作成して、そのポリシーをユーザーに割り当てる必要があります。その後、アプリケーションでユーザーの資格証明を使用してオブジェクト・バケットにアクセスすることになります。このアプローチの問題点は、ユーザーの秘密鍵をアプリケーションから使用できるようにするために、通常はその鍵を構成ファイル内に格納する必要があるという点です。秘密鍵を取得して構成ファイルに格納するプロセスは複雑で、セキュリティ・リスクが生じる可能性もあります。

インスタンス・プリンシパルを使用する場合は、ダイナミック・グループを作成します。ダイナミック・グループを使用すると、Computeインスタンスをプリンシパル・アクターとしてグループ化し、ユーザー・グループと同様に扱うことができます。その後、OCIサービスに対するAPI呼び出しをインスタンスに許可するポリシーを作成することができます。ダイナミック・グループを作成する際には、変更不可能なダイナミック・グループ名を指定します。この名前は、テナンシー内のすべてのグループ間で一意である必要があります。

注意:インスタンスへのアクセス権を持つユーザーは、そのインスタンスに付与された権限を自動的に継承します。この機能を使用してインスタンスに権限を付与する前に、インスタンスにアクセスできるユーザーを確認し、インスタンスに付与する権限をそれらのユーザーに許可する必要があるかどうかを判断してください。

フェデレーション

IAMでは、SAML 2.0とOpenID Connectを使用したフェデレーションがサポートされています。フェデレーションはアイデンティティ・ドメイン・レベルで行われます。各テナンシーが複数のドメインを持つことができ、アイデンティティ・ドメインは、SAML 2.0またはOpenID Connectをサポートする外部アイデンティティ・プロバイダ(IdP)のいずれかとフェデレートします。

フェデレーションを設定する際には、次の要素を考慮してください。

- アイデンティティ・ドメインは、IdPとサービス・プロバイダの役割を果たすことができます。
- サービス・プロバイダを追加するには、アイデンティティ・ドメインのアプリケーション・カタログを使用します。テンプレートにアプリケーションが見つからない場合は、アプリケーション・テンプレート・ウィザードを使用します。
- 一般的なソーシャルIdPテンプレートがすべて使用できます。OpenID Connectは「ソーシャルIDPの追加」メニューから使用できます。
- IdPポリシーを使用すると、様々な条件に基づいて実行時にIdPを選択できます。IdPがポリシーに1つしかない場合は、IAMのサインイン画面は表示されず、そのIdPに直接移動します。たとえば、ユーザーが消費者ユーザー・グループに属する場合はソーシャルIdPに対して認証するIdPポリシーを作成できます。
- フェデレーションが機能するためには、IAMと外部IdPの間でユーザーを同期するか、SAML JITプロビジョニングを使用する必要があります。

パスワード管理の有効化

パスワードのリセットをセルフサービスで行えると、ユーザーの不満とヘルプデスクの負担が軽減されます。IAMでは、ユーザーがセルフサービスで自分のパスワードをリセットしたり、MFAデバイスを登録したりすることができます。

IAMのパスワード・ポリシーには簡易、標準、カスタムの3種類があり、包括的なパスワード・ルールが用意されています。パスワード・ポリシーの作成については、次のベスト・プラクティスをお薦めします。

- デフォルトのパスワード・ポリシーに頼らないでください。かわりに、カスタム・ポリシー・テンプレートを使用してパスワード・ポリシーを作成すれば、組織のコンプライアンス要件に合わせてカスタマイズできます。
- 別個のパスワード･ポリシーが必要なグループを特定し、管理者アカウントには強力なパスワード･ポリシーを実施します。
- ユースケースに応じて、最小限の権限を持つグループのための自動アカウント・ロック解除や異なるロックしきい値を検討してください。
- パスワード･ポリシーの優先順位を設定する際には、次のシナリオを検討してください。ユーザーに複数のグループが割り当てられている場合、優先順位が最も高いパスワード・ポリシーはそのユーザーに割り当てられたパスワード・ポリシーです。

結論

このテクニカル・ペーパーでは、Oracle Cloud Infrastructure IAMサービスを使用して、クラウド・リソースへのアクセスを安全に管理/制御するためのベスト・プラクティスについて説明しました。以下にこれらのベスト・プラクティスの要点をまとめます。

- ユーザーやリソースを追加する前に、テナンシーとコンパートメントを計画しましょう。
- コンパートメントは、組織の事業部やプロジェクトの構造に合わせて設計しましょう。
- 最初にユーザーの役割を分類し、その後、適切なポリシーが適用されたグループにユーザーを配置するようにしましょう。
- ユーザーには最小限の権限を付与し、必要に応じて、徐々に権限を増やしていくようにしましょう。
- 強力なパスワード・ポリシーを実施し、パスワードを定期的に更新するようにしましょう。
- OCIサービスをComputeインスタンスから呼び出す場合は、インスタンス・プリンシパルとダイナミック・グループを使用しましょう。

Oracle Cloud Infrastructureには新しい機能が継続的に追加されています。oracle.com/cloud/のオンライン・ドキュメントやトレーニングを通じて、常に最新の情報を確認するようにしてください。