ORACLE

Exadata Cloud@Customer向け Oracle Operator Access Control

Exadata Cloud@Customer向けクロス・テナント・アクセス管理サービス

2021年7月13日、バージョン3

本書の目的

本書では、Operator Access Control（OpCtl）サービスの機能の概要と強化された点について説明しています。本書は、OpCtlの機能を使用することで得られるビジネス上の利点の評価と、ITプロジェクトの計画立案を支援することのみを目的としています。

免責事項

本書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。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないでください。本書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上、コードが大幅に不安定化するリスクなしに、本書に記載されているすべての機能を安全に含めることができない場合があります。

目次

画像一覧

表一覧

概要

Oracle Operator Access Control（OpCtl）は、Oracle Cloud Infrastructure（OCI）のアクセス制御サービスです。お客様が規制の厳しい業界の一般的な要件を満たせるように、オラクルのスタッフがExadata Cloud@Customer（ExaC@C）インフラストラクチャにどうアクセスすべきか、その方法をより的確に制御するための技術的なメカニズムを提供します。制御方法に関する本書の説明は、Operator Access Controlの製品ドキュメントをまとめた内容であり、お客様のセキュリティ・スタッフがExaC@Cを採用する上で、OpCtlサービスを補完的なコントロール機能になり得るかどうかを評価できるよう支援することを目的としています。

ExaC@Cを使用するには、以下のサービス提供要件に同意する必要があります。

- オラクルが、ExaC@Cインフラストラクチャに接続できるスタッフを選択する。

  ExaC@Cインフラストラクチャにアクセスするスタッフの**ID**プロバイダはオラクルである。

- ExaC@Cインフラストラクチャへのアクセスを許可されたオラクルのスタッフは、オラクル提供のソフトウェアとハードウェアを使ってインフラストラクチャにアクセスする。

OpCtlは、以下を実行するためのインタフェースを提供します。

- ExaC@Cインフラストラクチャにオラクルのスタッフがアクセスするべきタイミングと頻度を制御する。
- ExaC@Cインフラストラクチャに対してオラクルのスタッフが実行するOracleオペレータ・コマンドとキーストロークを観察および記録する。
- Oracleオペレータの接続をお客様の裁量で終了する。

OpCtlを評価するセキュリティ・スタッフは、ExaC@CサービスとOracle Cloud Infrastructureコントロール・プレーンのその他のコントロール機能を説明する以下に示すような関連ドキュメントも確認する必要があります。

- Exadata Cloud@Customerシステム・セキュリティ・ガイド
- Exadata Cloud@Customer Security Controls
- Oracle Cloud Infrastructure Security Architecture

はじめに

クラウド・コンピューティングは従来のオンプレミス・コンピューティングとは根本的に異なります。従来モデルの場合、通常、組織はオンプレミスにあるテクノロジー・インフラストラクチャを完全に制御しています（ハードウェアの物理的な制御、本番環境のテクノロジー・スタックの完全制御など）。クラウドの場合、クラウド・サービス・プロバイダの管理下にあるリソースとプラクティスを利用する必要があります。クラウドでのセキュリティとプライバシーの管理は実質的に、クラウドのお客様とクラウド・サービス・プロバイダ間の共有責任となります。

Infrastructure as a Service（IaaS）クラウド・モデルとPlatform as a Service（PaaS）クラウド・モデルでは、クラウド・サービス・プロバイダが、インフラストラクチャなどのシステムの一部を管理し（クラウド・プロバイダ・テナンシー）、お客様が仮想マシン、アプリケーション、データベースなどのシステムの他の一部を管理します（お客様のテナンシー）。一定の規制フレームワークにより、お客様は、クラウド・プロバイダ・テナンシーのクラウド・プロバイダのスタッフが実行するアクションなど、システムへのアクセス時に実行するアクションに責任を負い、制御する必要があります。お客様がこれらの要件を満たせるよう、オラクルではOracle Operator Access Control（OpCtl）とExadata Cloud@Customer（ExaC@C）、ExaC@C上のAutonomous Database Dedicated（ADB-D）を併せて使用できるようになっています。

OpCtlは、Exadata Cloud@Customer（ExaC@C）向けOracle Cloud Infrastructure（OCI）テナント間アクセス管理サービスです。OpCtlではお客様のテナンシーにお客様用のソフトウェア・インタフェースを提供しています。このインタフェースを使用すると、ExaC@Cサービスのオラクル・テナンシーのオラクルが管理するインフラストラクチャに対するOracle Cloud Operations（Cloud Ops）スタッフによるアクセスのタイミングと方法を制御し、管理できます。これらのコントロール機能は、ExaC@Cサービスの標準搭載機能の一部であり、オラクルのお客様は無償で利用できます。

OpCtlは、ミッション・クリティカルなアプリケーションと規制の厳しい業界に影響するポリシー、法律、規制の要件を満たしながら、クラウド実装の運用と財務面の価値を求めるお客様のユースケースを対象に設計されています。たとえば、OpCtlは、銀行や金融サービスのアプリケーション、公益事業、防衛、リスク管理がアプリケーションの成功において重要な柱となる他のアプリケーションに最適です。これらの業界で事業を営み、クラウド戦略の追及に感心があるお客様は、選択したクラウド・プロバイダが、標準提供しているサービス内でこれらの機能を包括的にサポートしていることを確認する必要があります。

OpCtlサービスは、お客様がアクセス権を付与し、オラクルが作業を実行する職務分掌を実現します。OpCtlの予防的セキュリティ・コントロール機能は次のとおりです。

- オラクルのスタッフは、お客様から許可され、オラクルの特定の作業リクエストがあるときにだけアクセスします。
- オラクルのスタッフによるアクセスは、指定された特定の作業リクエストに関連する明示的に承認されたコンポーネントに制限されます。
- オラクルのスタッフによるアクセスは一時的であり、許可された作業の完了後、自動的に取り消されます。
- オラクルのスタッフがインフラストラクチャにアクセスできるタイミングはお客様が制御します。
- オラクルのスタッフによる権限のエスカレーションはソフトウェアが管理します。

OpCtlの検知可能なセキュリティ・コントロール機能は次のとおりです。

- オラクルのスタッフがインフラストラクチャにアクセスする必要がある場合、お客様に通知
- オラクルのスタッフが実行したすべてのコマンドとキーストロークの個別識別が可能な監査ロギング
- オラクルのスタッフが入力したすべてのコマンドとキーストロークをお客様がセキュリティ監視
- 実行したコマンドに対してリクエストがあった場合、オラクルのスタッフのIDを記載したレコードをオラクルが提供
- オラクルのセキュリティ・スタッフがOracle Cloud Opsスタッフの全アクティビティを監視

OpCtlの即応的セキュリティ・コントロール機能は次のとおりです。

- お客様は、オラクルのスタッフによるアクセスと、オラクルのスタッフが開始した全プロセスをいつでも制御して終了できます。
- オラクルのセキュリティ・スタッフは、オラクルのスタッフによるアクセスと、オラクルのスタッフが開始した全プロセスをいつでも制御して終了できます。

サービスの範囲

OpCtlを使用すると、オラクルのスタッフ（人間）が保守を委託されているリソース（ExaC@Cインフラストラクチャなど）への同スタッフのアクセス権を管理できます。OpCtlでは、お客様がExaC@Cインフラストラクチャへのソフトウェアによる自動アクセスを制御したり、お客様が管理するリソースにアクセスしたりすることはできません。

サービス・アーキテクチャ

図1は、第2世代ExaC@Cサービス提供ネットワーク・アーキテクチャを示します。

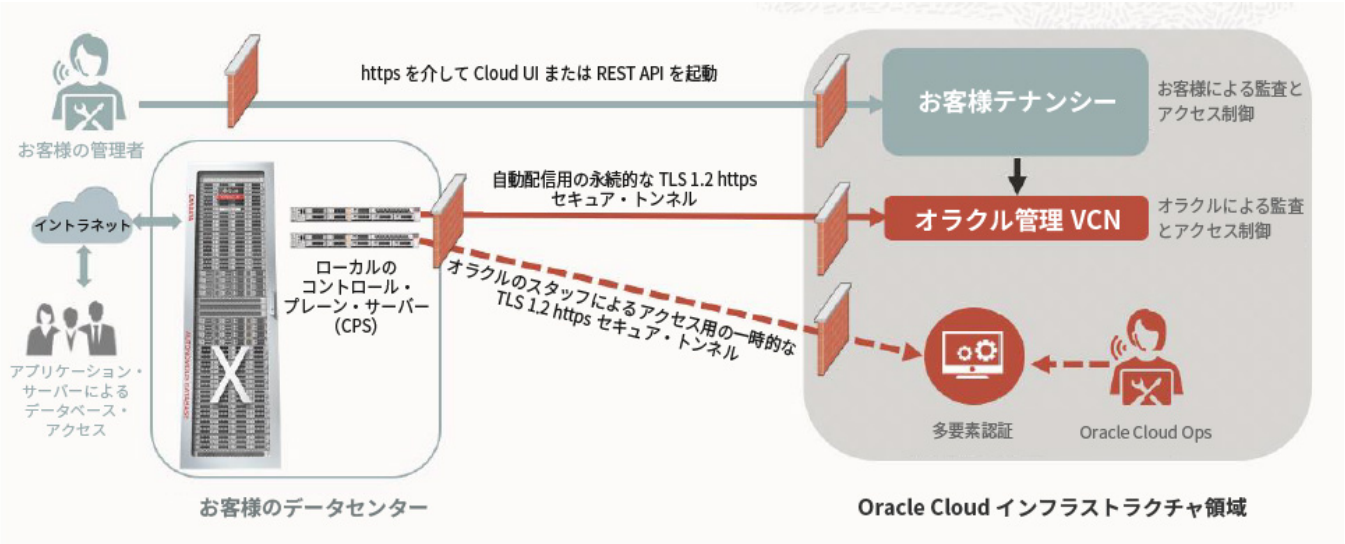

図1：第2世代ExaC@Cネットワーク・アーキテクチャの概要

以下に示す実装の詳細は、図1に示すセキュリティ・モデルに関連しています。

- お客様は、httpsプロトコルを介してお客様管理下の資格証明で自身のテナンシーへの認証を行います。OCI Identity and Access Management（IAM）サービスは、テナンシーへのお客様の認証とアクセスを管理します。詳細は以下に記載されています。
  https://docs.oracle.com/ja-jp/iaas/Content/Identity/Concepts/overview.htm
- お客様のテナンシーはOCIセキュリティ・アーキテクチャによって保護されます。詳細は以下に記載されています。
  https://www.oracle.com/jp/a/ocom/docs/oracle-cloud-infrastructure-security-architecture-ja.pdf
- ExaC@Cサービスは、OCIセキュリティ・アーキテクチャとExaC@Cサービスのその他のソフトウェアによって保護されます。詳細は以下に記載されています。
  https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/exadata-cloud-at-customer-security-controls.pdf
- お客様はOpCtl管理ポリシーを自身のExaC@Cインフラストラクチャ・リソースに適用して、ExaC@CインフラストラクチャへのOracle Cloud Opsのアクセスを管理します。このプロセスはOCI IAMによって保護および制御されます。詳細は以下に記載されています。
  https://docs.oracle.com/ja-jp/iaas/Content/Identity/Concepts/overview.htm
- ExaC@Cラックに設置されたローカルのコントロール・プレーン・サーバー（CPS）が、TLS 1.2で保護されたOCI WebSocket Serviceへの永続的なアウトバウンド・セキュア・トンネル（レイヤー7のWebSocket）を保持して、お客様のテナンシーおよびOracle Admin Virtual Cloud Network（VCN）からローカルCPSへのREST APIコマンドの伝送をサポートします。
- お客様がExaC@CインフラストラクチャへのOracle Cloud Opsのアクセスを許可すると、REST APIコマンドが永続的なセキュア・トンネルを介してExaC@Cインフラストラクチャのエージェントに送信されて、一時的なセキュア・オペレーター・トンネル（レイヤー7のstunnel）が、インフラストラクチャ・コンポーネントからOCIのセ

キュア・トンネル・サービスに向けて確立されます。

- Oracle Cloud Opsスタッフはこの一時的なオペレータ・トンネルを使ってssh接続を確立します。この接続により、Oracle Cloud Opsスタッフは指定ユーザーとして、Oracleが管理するデバイスからハードウェアの多要素認証を介して、お客様が許可したインフラストラクチャ・コンポーネントへの認証を行います。

図2は、お客様がアクセスを承認し、OpCtlソフトウェアが一時的な資格証明をインフラストラクチャ・コンポーネントのchroot jailにデプロイした後で生じる、OpCtl sshアクセス・フローの主要コンポーネントを詳述します。

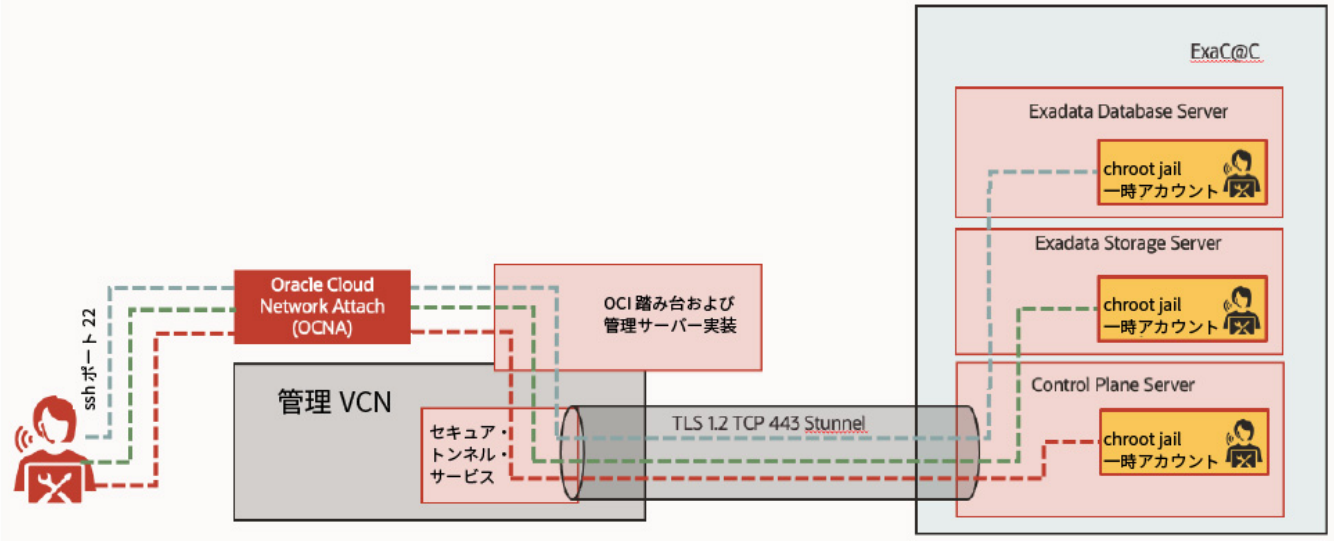

図2：chroot jailにデプロイされた一時アカウントへのssh経由の一時的なセキュア・トンネルを使用するオラクルのオペレータ

ExaC@Cインフラストラクチャへのオラクルのアクセスには、オラクルが実行する次のコントロール機能が含まれます。

- Cloud Opsスタッフは自身のハードウェアYubikey（FIPS 140-2レベル3ハードウェアの多要素認証）を使ってOracle Cloud Network Attachに接続する必要があります。VPN認証後、エンドユーザーのデバイスが次のスキャン基準について自動的にスキャンされ、この基準を満たしていないとアクセスは拒否されます。
  - ウイルス・スキャン・ソフトウェア基準など、Oracleエンドポイント/デバイスの要件への準拠（https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.htmlを参照）
  - オラクルの地理的アクセス制御基準への準拠（『OCI Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure』（PDF）を参照）
  - 役割に基づくアクセスの認可要件への準拠（https://www.oracle.com/corporate/security-practices/corporate/access-control.htmlを参照）
- Cloud OpsスタッフはExaC@Cインフラストラクチャへのssh接続を確立するために、OCI踏み台および管理サーバーへのアクセス権を得る必要があります。
  - このアクセスは、オラクルの企業ID管理（OIM）と内部OCI権限サービスによってオラクル社内で制御されます。
  - アクセス権はジョブ・コードに関連付けられており、最小権限アクセス・モデルで実装されています。詳細は以下のサイトで公開されています。
    https://www.oracle.com/corporate/security-practices/corporate/access-control.html
- Cloud Opsスタッフはオラクルが提供した各人のノートパソコンとYubikeyを使って、各人のノートパソコンからExaC@Cインフラストラクチャへのssh接続の認証を行います。
- Cloud Opsスタッフはハードウェアyubikeyを所有する必要があり、アクセス・リクエストを作成して一時アカウントへの認証を行うためのハードウェアYubikeyへのパスコードを把握している必要があります。

サービスの役割と責任

OpCtlサービスでオラクルのスタッフによるアクセスを制御する際、お客様には次の責任があります。

- システムにアクセスできるルールを決定するポリシーを作成および適用する。
- お客様の基準に従って通知とロギングを構成する。
- セキュリティと監査のため、オラクルのスタッフによるコマンドとキーストロークを監視する。
- ビジネスとセキュリティのニーズに応じてインフラストラクチャへのアクセスを取り消すか拒否する。
- OpCtlアクセス・リクエストに適切なタイミングで応答する[1]。

お客様がオラクルのスタッフによるアクセスをOpCtlサービスで制御する際、オラクルは次の操作を実行します。

- オラクルのスタッフがOpCtlで制御されているインフラストラクチャにアクセスする必要があるときに、アクセス・リクエストを発行する必要がある。
- OpCtlコントロール機能が課す技術的な制限内で必要な作業のみを実行できる。
- 識別可能なオラクルの従業員を、OpCtlで管理されるシステム上でオラクルの従業員が入力したすべてのコマンドまたはキーストロークに関連付ける。

サービスのサポートと可用性に関する示唆

OpCtlポリシーの事前承認済みアクセスの場合、オラクルのスタッフはサービス維持のためにアクセスが許可され、サービスの標準的な除外以外の他の除外はありません。明示的なアクセスの承認の場合、お客様がCloud Opsアクセス・リクエストを承認するまで、オラクルのスタッフはサービスにアクセスできません。アクセス・リクエストの処理中にお客様がその要求を取り消すと、保守アクションは完了しません。

Oracle Cloud Opsスタッフは、お客様のためにExaC@Cサービスの可用性と品質のサポート作業を行います。お客様がOpCtlを実装してOracle Cloud Opsの作業を管理する場合は、自社の業務プロセスとテクノロジーの更新作業を担って、OpCtlアクセス・リクエストへのタイムリーな対応と承認を確実に行う必要があります。Oracle Cloud Opsは、OpCtlアクセス・リクエストの重大度レベルを1～5で表します。重大度1の発行は緊急であることを示し、サービスの可用性または品質に大きく影響するため、できるだけ早く（ASAP）承認する必要があります。重大度5は、お客様ができるだけ早期に実施する必要がある、緊急性のない保守を示します。お客様の計画策定を支援するため、表1に、ExaC@Cサービスの品質と可用性を確保するために、どのくらい迅速にOpCtlアクセス・リクエストを承認する必要があるかを示します。

[1] サービスの可用性を維持するために、Cloud Opsアクセス・リクエストに即座に対応する必要があり、これは事前承認ポリシーを実施することで達成できます。実際のユースケースでは15分のレスポンス時間で十分ですが、それより長いとサービス停止が生じる可能性があります。

表1：OpCtlアクセス・リクエストに対するお客様の推奨レスポンス時間

OpCtlの重大度	問題の範囲と緊急性	お客様のレスポンス時間
1	差し迫ったサービス停止リスクにより即座に問題が発生するか、サービスがすでに停止している。サービス停止を回避するか、サービスをオンラインに戻すため即座に問題を解決する必要がある	できるだけ早く手動で対応する
2	サービス停止の可能性が高い、緊急の問題。サービス停止を回避するには、素早く対応する必要がある	15分未満
3	切迫している、または発生する可能性が高いサービス停止を回避するために解決する必要がある重要な問題	4時間未満
4	サービス品質を維持または改善するために解決する必要がある小さい問題	24時間未満
5	サービス品質を改善する軽微な問題	72時間未満

セキュリティとアクセス制御

OpCtlでは、多数の予防的、発見的、即応的なセキュリティ・コントロール機能を提供しています。

- **予防的**コントロール機能は、インフラストラクチャへのログインの可否とタイミング、インフラストラクチャにアクセスできる時間の長さ、実行できるコマンド、アクセスできる対象ファイルとデバイスなど、Oracle Cloud Opsスタッフが実行できるアクションの範囲を制限します。
- **発見的**コントロール機能は、Oracle Cloud Opsスタッフが行っている作業を示し、それには、実行しているコマンドと入力しているキーストロークが含まれます。
- **即応的**コントロール機能は、Oracle Cloud Opsスタッフによる現時点以降の作業の実行を停止し、それには、Oracle Cloud Opsスタッフが開始したTCP接続とプロセスの終了が含まれます。

これらの3つのタイプのコントロール機能を利用することで、お客様はExaC@Cインフラストラクチャへのアクセスを管理し、インフラストラクチャにアクセスしたときに実行されたスタッフ全員の作業範囲を示し、不正アクセスを検出して終了させることができます。

予防的コントロール機能

このセクションでは、ExaC@Cインフラストラクチャへのアクセス管理用としてOpCtlがお客様に提供する予防的コントロール機能について詳述します。

インフラストラクチャへのアクセス制御

デフォルトでは、OpCtlを使ってインフラストラクチャへのアクセスを管理する際にリモート・ログインを許可するアカウントはインフラストラクチャ上にありません。そのためお客様はOpCtlアクセス・リクエストの監視と対応を行って、Oracle Cloud Opsがサービスの品質と可用性の維持に必要な作業を実行できるようにする必要があります。お客様がOracle Cloud Opsアクセス・リクエストを拒否するか、タイムリーに対応しないと、サービス停止が生じるおそれがあります。

お客様がOpCtlアクセスを許可すると、アクセス・リクエストを作成したOracle Cloud Opsスタッフによるターゲット・インフラストラクチャへのアクセスを許可するために、OpCtlソフトウェアが一時的な資格証明のデプロイを調整します。当人以外によるこの資格証明の使用を技術的に防ぐ予防的コントロール機能が、Cloud Opsスタッフのハードウェアyubikeyになります。この認証制御の場合、ssh接続を確立するスタッフは、アクセス・リクエストの作成とハードウェアYubikeyのパスコードの入手に使う物理的なYubikeyを所有する必要があります。

インフラストラクチャ内のアクセス制御

Cloud OpsスタッフがExaC@Cインフラストラクチャへのアクセスを許可されて認証された後、Oracle Linuxのchroot jailが、Cloud Opsスタッフによるアクセスが可能なインフラストラクチャを管理します。

chroot jailによって、プロセスとその子を実行するための明確なルート・ディレクトリが変更されます。ユーザーは、/以外のルート・ディレクトリでプログラムを実行できます。プログラムは、指定のディレクトリ・ツリー以外のファイルを認識したり、ファイルにアクセスしたりすることはできません。このような人工ルート・ディレクトリは、chroot jailと呼ばれており、その目的は、潜在的な攻撃者によるディレクトリへのアクセスを制限することです。chroot jailによって、使用している特定のプロセスや任意のユーザーIDがロックダウンされるため、表示されるのはプロセスが実行されているディレクトリだけになります。プロセス側からは、実行されているディレクトリはルート・ディレクトリとして認識されます。Oracle Linux 7のchroot jailの詳細は、以下に記載されています。 https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-s3-syssec 。

OpCtlによるchroot jailの実装はOpCtlアクションといい、詳細は『Enforcement of Actions in Operator Access Control』製品ドキュメントに記載されています。OpCtlアクションは、Exadata Database Server Infrastructure（Dom0）、Exadata Storage Server（セル/セル・サーバー）、コントロール・プレーン・サーバー（CPS）などのExaC@Cインフラストラクチャに対してオペレータが実行できる操作を定義します。OpCtlアクションはExaC@Cインフラストラクチャ全体（指定のExaC@Cラック内の全Exadata Database Server、Storage Server、CPS）を対象としているため、お客様がインフラストラクチャ内の個々のコンポーネントへのアクセスを指定することはありません。OpCtlには、お客様VM（DomU）にアクセスするための一時アカウントをデプロイする方法はありません。

OpCtlアクションは、Oracle Linuxの権限をターゲットのExaC@Cシステム上で変換します。これらの権限は、ファイル・システム権限、コマンド実行権限、およびsu権限またはsudo権限に分類されます。OpCtlアクションは、ExaC@Cシステムでオペレータが実行できる変更の性質に従って分類されます。OpCtlでは、4種類のアクションを提供します。

- システム診断：INFRA_DIAGとして識別され、ExaC@Cインフラストラクチャ・レイヤーでの問題の診断に使用します。
- 再起動権限付きシステム・メンテナンス：INFRA_UPDATE_RESTARTとして識別され、システム構成の変更やシステムの再起動が必要なオペレータのアクセス・シナリオで使用します。
- ハイパーバイザ・アクセス/VMコントロール権限付きシステム・メンテナンス：INFRA_HYPERVISORとして識別され、Exadata Database ServerでのVM管理が必要な診断およびメンテナンスのシナリオで使用します。
- フル・システム・アクセス：INFRA_FULLとして識別され、使用されるとしても極めてまれであり、複雑な状況または異常な状況に対処するために、オラクルのオペレータに最大限の柔軟性を提供するためだけに用います。

OpCtlアクション：システム診断

INFRA_DIAGとして識別されるシステム診断は、ExaC@Cインフラストラクチャ・レイヤーでの問題の診断に使用します。

診断には、ログの読取り、診断の実行、コマンドの監視が含まれます。このアクションは、ExaC@Cシステム内の診断エージェントで問題を修正することも目的としています。修正には、変更された可能性のあるパラメータでの診断デーモンの再起動が伴います。表2に、一時アカウントのアクセスと権限を管理するchroot jail構成を詳しく示します。

注：

- システム診断アクションによって、お客様のデータが漏洩のリスクにさらされたり、可用性低下のリスクが生じたりすることはありません。
- システム診断アクションによって、次のことが実現します。
  - オペレータはcat、grepなどを使って、オペレーティング・システム、インフラストラクチャ・ソフトウェア、クラウド・オーケストレーション・ソフトウェアのログ・ファイルを読み取ることができます。
  - オペレータはtopやnetstatなどのOracle Linux診断コマンドを実行できます。
  - オペレータはExadata Storage Serverでcellcliコマンドを実行して診断情報を取得できます。

- オペレータはコントロール・プレーン・サーバーで全デーモンを再起動する機能により、コントロール・プレーン・サーバー上のクラウド・オーケストレーション・インフラストラクチャにアクセスして管理することができます。

表2：診断アクションの権限

アクション名	アクションの識別子	オペレータの権限
システム診断	INFRA_DIAG	Oracle Linuxユーザーの権限：非root suを使ってrootへの切替えが可能：非対応 chrootケージ内：対応 読取り可能なディレクトリ： Exadata Storage Server： /opt、/proc、/sys、/tmp、/var、/var/log、/usr/lib64、/usr/bin、/usr/etc、/usr/include、/usr/lib、/usr/libexec、/usr/local、/ usr/share、/usr/java、/opt/cellconf、/home/cellmonitor/ Exadata Database Server Infrastructure： /bin、/lib64、/lib、/opt、/proc、/sys、/tmp、/var、/usr/lib64、/usr/bin、/usr/etc、/usr/include、/usr/lib、/usr/libexec、/us r/local、/usr/share コントロール・プレーン・サーバー： /opt、/proc、/sys、/tmp、/var、/usr/lib64、/usr/bin、/usr/etc、/usr/include、/usr/lib、/usr/libexec、/usr/local、/usr/share 読取り可能なファイル： /var/log/* 書込み可能なディレクトリ： Exadata Storage Server：/var/db、/opt/oracle Exadata Database Server Infrastructure：/var/db コントロール・プレーン・サーバー：/var/db 実行可能なコマンド一覧： 以下の全コマンド /bin、/usr/bin、/usr/local/bin、/sbin/ifconfig、/sbin/ip、/sbi n/lspci cellcli（Exadata Storage Server上） suを使って以下への切替えが可能： セル：cellmonitor Exadata Database Server Infrastructure：dbmmonitor コントロール・プレーン・サーバー：ecra、exawatcher、dbmsvc rootとして実行：

		cat head tail /var/log/*内のファイルのcp [CPS]: systemctl Exadata Storage Serverの権限：cell monitorとして動作 ネットワーク権限：SSHを実行して、すべてのExadata Database Server Infrastructure、Exadata Storage Server、コントロール・プレーン・サーバーに接続することが可能。ユーザー名はこれらすべてのサーバーに対して同じです。

OpCtlアクション：再起動権限付きシステム・メンテナンス

再起動権限付きシステム・メンテナンスは、INFRA_UPDATE_RESTARTとして識別され、システム構成の変更やシステムの再起動が必要なオペレータのアクセス・シナリオで使用します。

INFRA_UPDATE_RESTARTは通常、メンテナンスのシナリオで使われます。ただし、再起動が必要とされる診断のシナリオにも使われます。システム構成の変更には、ネットワーク構成の変更、ハードウェア構成の変更、オペレーティング・システム構成の変更（mounts、inodes、ulimitsなど）、またはクラウド・オーケストレーション・ソフトウェア構成の変更があります。システムの再起動により、オラクルのオペレータはオペレーティング・システムを再起動することで（Exadata Database Server、Exadata Storage Server）、ネットワークなどの特定のサブシステムを再起動し、セル・ディスクを再起動することができます。

表3に、一時アカウントのアクセスと権限を管理するchroot jail構成を詳しく示します。

注：

- 再起動権限付きシステム・メンテナンスのアクションを実行すると、システムに対し、サービスの可用性の大きなリスクが生じることがあるので注意してください。ただし、データがリスクにさらされることはありません。
- 再起動権限付きシステム・メンテナンスのアクション：
  - オラクルのオペレータはroot権限でシステム・メンテナンス作業を実行できます。オペレータはrootにはなれませんが、rootとしてメンテナンス・コマンドを実行できます。
  - オペレータは監査パラメータを変更したり、監査ログにアクセスしたりすることはできませんが、このアクションにより、ExaC@Cシステム全体をオフラインにすることができます。
  - オペレータは永続的な変更を通してオペレーティング・システムの構成を変更できます。たとえば、オラクルのオペレータは/etc/パラメータを変更できます。
  - オラクルのオペレータはデーモン・プロセスを開始でき、Exadata Storage Server上でcellcliのcell admin権限を使ってセル・ディスクを管理できます。
  - オラクルのオペレータはコントロール・プレーン・サーバーで全デーモンを再起動する機能により、コントロール・プレーン・サーバー上のクラウド・オーケストレーション・インフラストラクチャにアクセスして管理することができます。

継承：システム診断の全権限

表3：再起動権限付きシステム・メンテナンス

アクション名	アクションの識別子	オペレータの権限
再起動権限付きシステム・メンテナンス	INFRA_UPDATE_RESTART	システム診断と同じ権限に加えて、次の権限があります。 suを使ってrootへの切替えが可能：非対応

		chrootケージ内：対応suを使って以下への切替えが可能： exawatcher、dbmsvc、dbmadmin、dbmmonitor（Exadata Database Server Infrastructure上） rootとして実行：restart、ip、ifconfig、lspci Exadata Storage Serverの権限：celladmin（Exadata Storage Server内） ネットワーク権限：SSHを実行して、すべてのExadata Database Server Infrastructure、Exadata Storage Server、コントロール・プレーン・サーバーに接続することが可能 ユーザー名はこれらすべてのレイヤー全体で同じです。

OpCtlアクション：ハイパーバイザ・アクセス権限付きシステム・メンテナンス

ハイパーバイザ・アクセス権限付きシステム・メンテナンスはINFRA_HYPERVISORとして識別され、Exadata Database ServerでのVM管理が必要な診断およびメンテナンスのシナリオで使用します。

VMコントロール権限付きシステム・メンテナンスのアクションは、Exadata Database ServerでのVM管理が必要な診断およびメンテナンスのシナリオで使用します。お客様VM上のデータはお客様のデータとして扱われます。VM管理では、VMデータにアクセスできるため、このアクションはデータをリスクにさらす可能性があります。ただし、ExaC@Cデータベースで作成されるお客様のデータはすべてTDEで暗号化され、このアクションでは、Exadata Storage Serverに保存されたデータのTDEキーへのアクセス権は付与されません。VMソフトウェア・インフラストラクチャに問題がある場合、またはVM構成の変更が必要な場合は、VM管理が必要です。
構成には、接続したネットワーク、接続したディスク、または割り当てられたリソース（CPU、メモリ）など、VMの外部の要素が含まれます。表4に、一時アカウントのアクセスと権限を管理するchroot jail構成を詳しく示します。

注：

- VMコントロール権限付きシステム・メンテナンスのアクションによって、お客様はデータと可用性の大きなリスクにさらされます。データのリスクは、お客様VMファイル・システムにはVMディスクのアクセスを介してアクセス可能という事実から露呈し、可用性のリスクは、オペレータがVMを制御できるという事実から露呈します。
- VMコントロール権限付きシステム・メンテナンスのアクション：
    - オペレータはroot権限でXen/KVM管理コマンドを実行できます。オペレータはrootにはなれません。このアクションはExadata Database Serverのみが対象です。
    - "再起動権限付きシステム・メンテナンス"のアクションから権限を継承します。
    - オペレータはExadata Database ServerまたはExadata Storage Serverのオペレーティング・システムのパラメータを変更することはできません。ただし、お客様VMを停止し、その構成を大きく変更することは許可されています。
    - オペレータは、Oracle Linux 監査サービスの構成を変更することはできません。

継承：再起動権限付きシステム・メンテナンスの全権限

表4：ハイパーバイザ・アクセス権限付きシステム・メンテナンス

アクション名	アクションの識別子	オペレータの権限
データ・アクセス/VMコントロール権限付きシステム・メンテナンス	INFRA_HYPERVISOR	"再起動権限付きシステム・メンテナンス"と同じ権限に加えて、次の権限があります。 Oracle Linuxユーザーの権限：非root

		suを使ってrootへの切替えが可能：非対応 chrootケージ内：対応 読取り可能なディレクトリ： /EXAVMIMAGES（Exadata Database Server Infrastructure上） /home/celladmin/（Exadata Storage Server上） 実行可能なコマンド一覧： /usr/sbin/xm /usr/sbin/xentop（Exadata Database Server Infrastructure上） cellcli（Exadata Storage Server上） suを使って以下への切替えが可能：celladmin（Exadata Storage Server内） rootとして実行： /usr/sbin/xm /usr/sbin/xentop /usr/sbin/virsh Exadata Storage Serverの権限：celladmin ネットワーク権限：SSHを実行して、すべてのExadata Database Server Infrastructure、Exadata Storage Server、コントロール・プレーン・サーバーに接続することが可能。ユーザー名はこれらすべてのサーバーに対して同じです。

OpCtlアクション：フル・システム・アクセス

フル・システム・アクセスはEXACC_SYS_ADMIN_FULL_ACCESSとして識別され、使用されるとしても極めてまれです。フル・システム・アクセスのアクションは、ExaC@Cインフラストラクチャのフル・アクセスが必要な場合に使用するものです。アクセスは常に、お客様の以外のVMレイヤーに制限されています。フル・アクセスとは、お客様VM以外の、ExaC@Cシステム上の各オペレーティング・システム・インスタンスへのroot権限のことです。

表5に、一時アカウントのアクセスと権限を管理するchroot jail構成を詳しく示します。

注：

- フル・システム・アクセスのアクションによって、可用性とデータ漏洩のリスクが生じ、永続的に続くことがあります。このアクションでは、システムから監査ログのエクスポートを防ぐ機能も使えます。
- OCI Bastionサーバーを介したオラクルの監査ロギングは、監査ログがExaC@Cインフラストラクチャで改ざんされるリスクを軽減する補完的なコントロール機能を提供します。

表5：フル・システム・アクセスの権限

アクション名	アクションの識別子	オペレータの権限
フル・システム・アクセス	EXACC_SYS_ADMIN_FULL_ACCESS	Linuxユーザーの権限：非root suを使ってrootへの切替えが可能：対応 chrootケージ内：非対応 読取り可能なディレクトリ：すべて

		読取り可能なファイル：すべて 書込み可能なディレクトリ： 書込み可能な全ファイル：すべて 実行可能なコマンド一覧：すべて suを使って以下への切替えが可能：sudoを使ってrootへ切替え sudoユーザーおよびコマンド一覧：制限なし Exadata Storage Serverの権限：rootとcelladmin ネットワーク権限：SSHを実行して、すべてのExadata Database Server Infrastructure、Exadata Storage Server、コントロール・プレーン・サーバーに接続することが可能。ユーザー名はこれらすべてのサーバーに対して同じです。また、exasshを使って、Exadata Database Server Infrastructure、Exadata Storage Server上のrootに直接接続できます。

発見的コントロール機能

OpCtlは、インフラストラクチャ・コンポーネント上で実行されているOracle Linux（OL）監査サービスを介してオペレータのコマンドとキーストロークのロギングを実現します。お客様は次の2つのインタフェースを通じてOL監査サービスからの情報を入手できます。

- OCI Loggingサービス
- お客様指定のIPアドレスやホスト名またはお客様管理のsyslogサーバーに監査ログがsyslog形式で直接送信されます。これは、お客様のSecurity Information Event Management（SIEM）システムに監査ログを伝送する場合に役立ちます。

OL監査サービスの内容は通常、コマンド実行後30秒以内にOCI Loggingサービス内で取得できます。

OCI Loggingサービスのドキュメントは、https://docs.oracle.com/ja-jp/iaas/Content/Logging/Concepts/loggingoverview.htmで公開されています。OCI LoggingサービスはOCI Streamingサービスと統合されて、OpCtl監査ログ情報を、OCI Streamingサービスでサポートされている任意のエンドポイントに送信できます。OCI Streamingサービスの詳細は、https://docs.oracle.com/ja-jp/iaas/Content/Streaming/Concepts/streamingoverview.htmで公開されています。

SplunkへのOCIログのストリーミング方法を紹介するチュートリアルを、https://docs.oracle.com/ja/solutions/logs-stream-splunk/index.html#GUID-8D87CAA4-CD41-4E90-A333-5B04E23DBFAAおよびhttps://blogs.oracle.com/cloud-infrastructure/announcing-the-oracle-cloud-infrastructure-logging-plugin-for-splunkで公開しています。

即応的コントロール機能

不正なアクションが疑われる場合、お客様はOpCtlインタフェースを使って、特定のアクセス・リクエストに対するCloud Opsアクセスを取り消すことができます。不正なアクションが疑われるときには、常にセキュリティに関するサポート・リクエスト（SR）を申請することをお勧めします。アクセスが取り消されると、OpCtlソフトウェアは次のアクションを実行します。

- オペレータが開始したすべてのシェルを特定し、終了させる。
- オペレータが開始したすべてのプロセス、およびオペレータが開始したプロセスによって開始されたすべての子プロセスを特定し、終了させる。
- sshセッションで使われたTCP接続を終了させる。
- オペレータが使用した一時アカウントをすべてのインフラストラクチャ・コンポーネントから削除する。

お客様のアクションによりアクセスを取り消した後、Cloud Opsスタッフがその他の作業を実行するための資格証明はなくなり、Cloud Opsスタッフが実行していた作業は終了します。その結果、Cloud Opsスタッフが実行していた作業がサービス停止の防止やサービス品質の維持に必要だった場合は、サービス停止、サービス品質の低下、または不完全なサービス・メンテナンス作業（ほぼ満杯のファイル・システムのクリーンアップなど）が発生する可能性があります。

運用の概念

OpCtlの運用は共有責任であり、お客様とオラクルが連携して、アクセスをリクエスト、承認、監視する必要があります。このセクションの目的は、権限を有するお客様のスタッフを対象に、承認プロセスとOpCtlテクノロジーの統合に必要な計画策定プロセスとテクノロジーの最新情報を提供することです。

運用フローのブロック図

図3に、OpCtl運用フローを示します。オラクルのスタッフのアクションとオラクルの内部インタフェースは赤色で示しています。お客様の管理スタッフのアクションとお客様のOCIインタフェースは灰色で示しています。お客様のセキュリティ・スタッフのアクションとインタフェースは緑色で示しています。お客様はOCI Identity and Access Management（IAM）のフレームワークとインタフェースを使って、図に示されていない責任分担を自社スタッフに委任することができます。

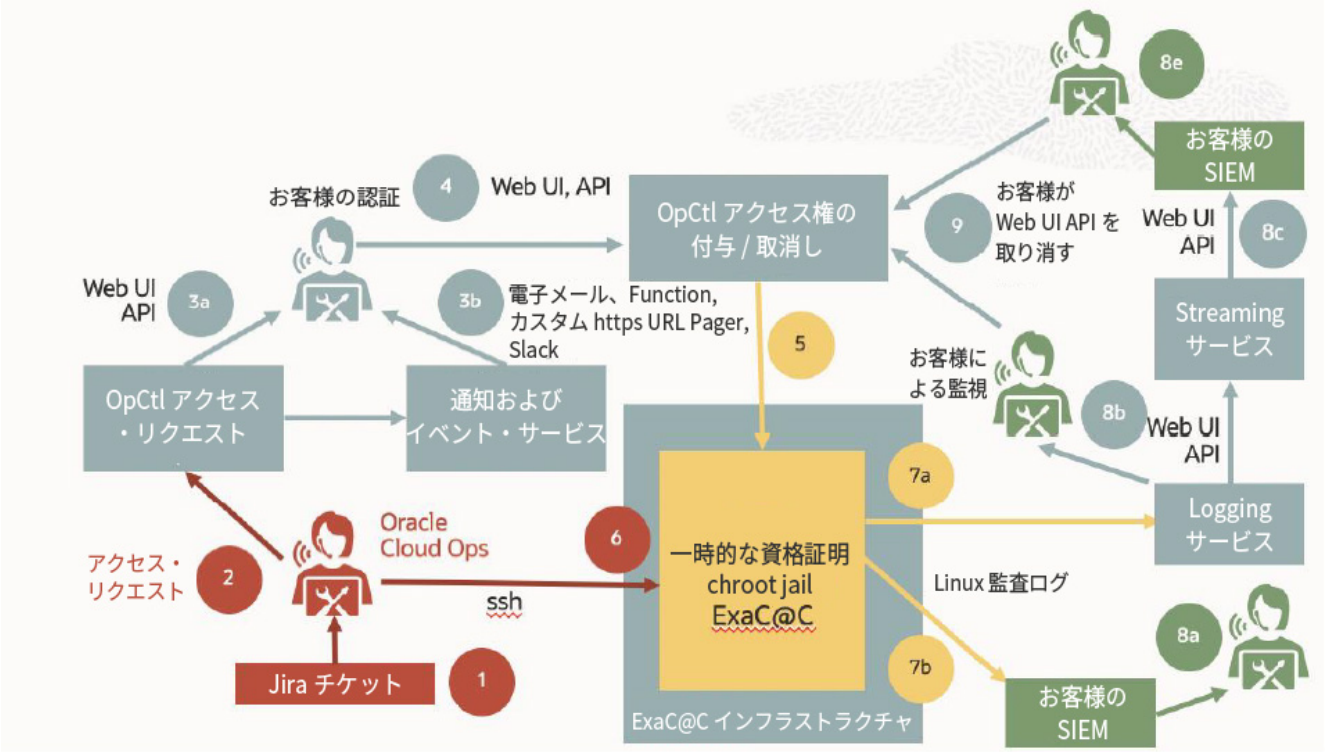

図3：OpCtl運用フロー

アクセス権のリクエスト、付与、監視、取消しのプロセスは次のとおりです。

1) ExaC@Cインフラストラクチャでのイベント処理や予防的システム・メンテナンスなどのオラクルの内部プロセスでは、特定のExaC@CインフラストラクチャでCloud Opsスタッフが作業を実行するための、OCIDで識別されるJiraチケットが作成されます。

2) Jiraチケットが割り当てられたOracle Cloud OpsスタッフはFIPS 140-2ハードウェアMFAデバイス（Yubikey）を使って、特定のプロファイル（chroot jail構成）へのOpCtlアクセス・リクエストを作成します。アクセス・リクエストは識別可能なオラクルのスタッフに帰属し、アクセス・リクエストを行うCloud Opsスタッフの秘密鍵に関連付けられた公開鍵がOpCtlサービス・ソフトウェアによって記録されます。

3) お客様はアクセス・リクエストを受け取ります。

   3a）お客様はOCIのOpCtlインタフェース（Web UI、OCI CLI、REST API）からアクセス・リクエストを確認できます。

3b） お客様はOCI通知サービスでアクセス・リクエストの通知を受信できます。アクセス・リクエスト通知は、OCI API対応のお客様のシステムに統合できます。

4) お客様はWeb UI、OCI CLI、REST APIなどのOpCtlインタフェースを使ってアクセス権を付与します。アクセス権付与は、OCI APIインタフェース対応のお客様のシステムに統合できます。

5) OpCtlソフトウェアは、要求されたOCIDで識別される指定の一時ユーザー・アカウントをExaC@Cインフラストラクチャの指定のchroot jailにデプロイするプロセスを調整します。指定の一時ユーザー・アカウントへのアクセスは、一時アカウントの~/.ssh/authorized_keysファイルに、アクセス・リクエストの作成に使われる秘密鍵に関連付けられた公開鍵をシード処理することで制御します。chroot jailは、~/.ssh/authorized_keysファイルの改ざんを防ぎます。

6) Oracle Cloud Opsスタッフは、sshを介して一時ExaC@Cインフラストラクチャにアクセスします。認証は、FIPS 140-2対応ハードウェアMFAを使って実行され、接続への認可は、初期アクセス・リクエストに関連付けられた秘密鍵に対して付与されます。

7) Linux監査サービスは、Oracle Cloud Opsが入力したコマンドとキーストロークを記録し、パブリッシュします。
7a） 監査ログはOCI Loggingサービスから取得できます。
7b） コントロール・プレーン・サーバー（CPS）からお客様のSIEMにsyslog形式で直接送信されます。

8) お客様は、Cloud Opsのアクションを以下のシステムやサービスから監視します。

8a） CPSから監査情報を受け取る自社のローカルSIEM

8b） OCI Loggingサービス

8c） OCI Streamingサービス

8e） OCI Streamingサービスと統合された、お客様の他のSIEM

本書の「即応的コントロール機能」のセクションに説明されているように、お客様はWeb UIやREST APIなどのOpCtlインタフェースからいつでもアクセス権を取り消すことができます。

アクセス承認ポリシー

OpCtlポリシーには、アクションごとに2つの承認設定があります。

- 事前承認
- 明示的承認

OpCtlアクションを実行するためのアクセス権を事前承認するようにポリシーを構成した場合、Oracle Cloud Opsがお客様にアクセス・リクエストを送信すると、OpCtlソフトウェアは自動的に一時的な資格証明を生成し、chroot jailをデプロイします。事前承認されたアクセスの場合、明示的承認と比較すると、予防的（chroot jail）、発見的（ロギング）、または即応的（アクセス権の取消し/終了）コントロール機能への変更はありません。管理負担の軽減とサービス品質向上という有用性に比べて、特定のchroot jailへの事前承認アクセスのビジネス、セキュリティのリスクが小さい場合、事前承認は、管理負担を軽減し、サービスの品質と可用性を改善する上で最適です。

OpCtlアクションを実行するためのアクセス権を事前承認するようにポリシーを構成しない場合、お客様はOCIインタフェースにアクセスして、一時的な資格証明の生成、chroot jailのデプロイに必要なアクセス・リクエストを明示的に承認する必要があります。事前承認されたアクセス権と違って、予防的（chroot jail）、発見的、または即応的コントロール機能への変更はありません。明示的承認は、ビジネスまたはセキュリティ上の理由によってシステムへのアクセスを許可できない場合に、システムへのアクセスのリスクを軽減する上で最適です。明示的承認の場合、お客様はシステムへのアクセス権をタイムリーに付与する必要があり[2]、タイムリーに付与できなかった場合、サービス停止やサービス品質の低下が生じる可能性があります。

[2] 実際のユースケースでは15分のレスポンス時間で十分ですが、それより長いとサービス停止が生じる可能性があります。

OpCtlでは、お客様は特定のアクションを選択的に事前承認してアクションのリスクとメリットのバランスをとることができます。また、サービスの品質/可用性とアクセス制御要件のバランスをとれるように、各種アクションを事前承認または明示的に承認する一定の時間枠を選択することもできます。

お客様のインタフェース

OpCtlはOCIコンソール（Web UI）またはOCI APIから構成し、管理することができます。OCIコンソールはシンプルで直感的なインタフェースで、ユーザーはOpCtlサービスと容易にやり取りしてポリシーを構成したり、ポリシーをインフラストラクチャに適用したり、アクセス権の付与、監視、取消しを行ったりすることができます。OCIコンソールのドキュメントは、https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/console.htmで公開されています。OCI APIインタフェースはOCIコンソールと同じ機能に対して、プログラムで規定されたアクセスを提供し、お客様はこのインタフェースを使ってOpCtl管理をチケット発行や変更管理システムなど、OCI APIインタフェースと相互運用する自社システムやプロセスに統合できます。https://docs.oracle.com/en-us/iaas/Content/API/Concepts/devtoolslanding.htmで公開されているOCI Developer Toolsのドキュメントでは、OCI APIフレームワークとの統合方法を説明しています。

お客様への通知

OpCtlアクセス・リクエストは、OpCtlインタフェースでお客様に発行されます。許可する保留中のアクセス・リクエストがある場合、お客様はOCIコンソールとOCI APIインタフェースからこれらのインタフェースにいつでもアクセスできます。アクセス・リクエストについてOpCtlインタフェースをポーリングすることを計画していて、ポリシーで明示的承認を構成している場合は、アクセス・リクエストの処理の遅れ、サービス停止やサービス品質低下のリスクを避けるために、頻繁なポーリング（5分未満）を必ず実行する必要があります。

OCI EventsサービスとOCI Notificationサービスを介して通知をプッシュするよう選択できます。次のOpCtlイベントをパブリッシュするようにOCI Eventsサービスを構成できます。

- アクセス・リクエスト – 承認
- アクセス・リクエスト – 自動認証
- アクセス・リクエスト – 作成
- アクセス・リクエスト – クローズ
- アクセス・リクエスト – 期限切れ
- アクセス・リクエスト – 延長
- アクセス・リクエスト – 却下
- アクセス・リクエスト – 取消し
- アクセス・リクエスト共有オペレータ – 作成
- オペレータ・コントロールの割当て – 作成
- オペレータ・コントロールの割当て – 削除
- オペレータ・コントロールの割当て – 更新
- オペレータ – ログイン
- オペレータ – ログアウト
- オペレータ・コントロール – 作成
- オペレータ・コントロール – 削除
- オペレータ・コントロール – 更新

お客様は処理のために、これらのイベントの任意の組合せを通知サービスにプッシュできます。OCI Eventsサービスの詳細は、https://docs.oracle.com/ja-jp/iaas/Content/Events/Concepts/eventsoverview.htmで公開されています。

OCI Notifications Serviceにより、お客様は次の形式でイベント通知にサブスクライブできます。

- 電子メール
- 機能
- HTTPS（カスタムURL）
- PagerDuty
- Slack
- SMS

OCI Notifications Serviceの製品ドキュメントは、https://docs.oracle.com/ja-jp/iaas/Content/Notification/Concepts/notificationoverview.htmで公開されています。

OpCtlサービス統合のお客様側のテストと検証

管理対象サービスのSLAを維持するには、オラクルのアクセス・リクエストを承認する、お客様のタイムリーな対応が必要です。お客様はOpCtlアクセス・リクエスト処理を既存のプロセスとシステムにOCIインタフェースを介して統合でき、そのような統合には、テストをして運用がうまくいくことを確認する必要があります。テストの遂行には4つのステップが必要です。

- お客様がOracle Cloud Opsにアクセス・リクエストを作成するように通知する。
- Oracle Cloud Opsがアクセス・リクエストを上げる。
- お客様がアクセス・リクエストを承認する。
- Oracle Cloud Opsがアクセス・リクエストを処理する。

Cloud Ops OpCtlテストを開始する際、お客様はサービス・リクエスト（SR）を開いて、SRに記述されているとおりに標準アクセス・リクエスト・テストを実行することをOracle Cloud Opsに通知できます。お客様が自社システムへのアクセス・リクエスト処理の統合を検証できるように、Oracle Cloud Opsは最大限の対応をしてアクセス・リクエスト・テストを実行します。

標準アクセス・リクエスト・テストでは、お客様がOpCtlロギング機能、および他のサービスへのOpCtl監査ログのさらなる統合を検証できるように、事前定義された一連のコマンドを実行します。

アクセス・リクエスト・テストを依頼する前に、お客様には以下を準備する必要があります。

- ExaC@CインフラストラクチャのOCID
- 診断、再起動権限付きメンテナンス、VM/データ・アクセス権付きメンテナンス、またはフル・アクセスのテストの1つとして、どのアクセス・リクエスト・テストを実行するかを選択

アクセス・リクエスト・テストの実行プロセスは次のとおりです。

1. My Oracle Support（MOS）にログインして、「Create Technical SR」を選択します。
2. 「Problem Summary」、「Problem Description」に有用なメタデータを入力します。
3. Where is the Problem?の「Cloud」タブを選択します。
4. 「Service Type」フィールドに“Gen 2 Exadata Cloud at Customer”と入力します。
5. Problem Typeでは「Infrastructure (Dom0)」を選択し、次に「Operator Access Control Test (Limited Availability)」を選択します。
6. 重大度レベル2[3]を選択します。

[3] 重大度2のサービス・リクエストでは、Cloud Opsオンコール・スタッフが自動的に呼び出され、アクションの通知が届くため、オラクルはお客様のOpCtl統合に対してタイムリーに対応します。重大度3～5のサービス・リクエストが開くと、アクセス・リクエスト・テストに対するレスポンス時間はより長くかかります。

7. 「Next」をクリックします。
8. ターゲットOCIDを「OCID」フィールドに入力します（Webから簡単にコピーして貼り付けることができます）。
9. 希望するテストのラジオ・ボタンをクリックします（ほとんどの統合テスト作業の場合、Diagnostics Accessで十分です）。
10. リクエストを送信します。
11. OpCtlアクセス・リクエストを承認します。
12. アクセス・リクエストのログを監視します（任意）。
13. アクセス・リクエスト・テストが完了したことを確認します。
14. SRをクローズします。

Oracle Cloud Opsスタッフ配置の更新

Cloud Opsアクセス・リクエストに関連付けられた一時アカウントを使用できるOracle Cloud OpsスタッフのIDを変更すること可能性のあるユースケースが3つあります。

- OpCtlアクセス・リクエストを承認するお客様のレスポンス時間が、リクエストを発行したCloud Opsスタッフのシフト勤務時間を超過した。
- アクセス・リクエストに記載された作業が、Cloud Opsスタッフのシフト勤務時間の残り時間より長くかかり、作業を完了するために作業リクエストを別のCloud Opsスタッフに割り当てた。
- 問題を解決するには、スペシャリストがもう1人必要だった。
- スタッフ変更の技術的プロセスは、3つ全部のケースで同じです。以下にそのプロセスを説明します。
- 別のCloud Opsスタッフが、ハードウェアYubikeyで認証される“Add Shared Operator – Create”リクエストを発行する。
- OpCtlソフトウェアが“Add Shared Operator – Create”イベントをお客様のテナンシーに発行して、お客様に変更を伝える。
- OpCtlソフトウェアが、元のアクセス・リクエストと同じルール（同じchroot jailと同じバウンド・アクセス）が課せられた追加分の一意の一時アカウントを、別のCloud Opsスタッフのハードウェアによる認証を使ってデプロイする。
- 別のOpCtlスタッフが新しい一時的な資格証明に対して認証を行い、作業リクエストを処理する。

OpCtlがデプロイした一時的な資格証明へのログインで実行された各コマンドとキーストロークにはタイムスタンプが付けられ、一時的な資格証明への認証に使われた特定のYubikeyと関連付けることができるため、オラクルは常に、ExaC@Cインフラストラクチャ上で入力されたコマンドに関連付けられた一意のスタッフを示すことができます。お客様がアクセス・リクエストを取り消すと、そのアクセス・リクエストに関連付けられたすべての資格証明が取り消されます。

Exadataインフラストラクチャ・ソフトウェアの更新

ExaC@Cインフラストラクチャの更新は、指定のメンテナンス期間に実行されるようにお客様がスケジューリングした自動プロセスです。お客様は、メンテナンス期間の管理機能をOCIインタフェースから利用でき、管理機能はお客様管理下のOCI IAM資格証明を介して実行されます。ExaC@Cインフラストラクチャの更新中にサービス品質を確保するには、OpCtlを使用するExaC@Cのお客様は、自社が承認したメンテナンス期間中の全システム・アクセス・プロファイル（診断、メンテナンス更新、ハイパーバイザ、およびフル）を事前承認することで、Oracle Cloud Opsスタッフが即座にアクセスして、ソフトウェア更新プロセス中に見つかった予期しない問題や障害を解決できるようにする必要があります。メンテナンス期間後、事前承認されたアクセスが取り消され、お客様が以前適用したアクセス制御が再び使えるようなります。

例外ワークフロー

OpCtlサービスは、複数の重要なユースケースで例外ワークフローを実行できるようにするプロセスと技術的コントロールを実現します。これらのユースケースは次のとおりです。

- 別のOracle Cloud Opsスタッフが作業処理を続行または完了させるためにインフラストラクチャにアクセスする必要がある場合の、Cloud Opsスタッフ配置の更新
- Cloud Opsスタッフがお客様VMにアクセスする場合（作業処理でこのアクセスが必要なとき）
- OpCtlソフトウェアの障害またはリモート・アクセスの障害からのリカバリ

このセクションでは、お客様が必要な補完的なコントロールを準備できるように、これらの例外ケースの処理の仕組みを説明します。

お客様VMへのオラクルのアクセス

通常の運用状況の場合、ExaC@Cサービスは、お客様VMへのアクセスをオラクルのスタッフに許可しません。お客様VMで障害が発生して、オラクルのスタッフが問題解決のためにアクセスする必要がある例外的なケースがあります。オラクルのスタッフによるお客様VMへのアクセス方法を管理するプロセスと技術的コントロールは、お客様がお客様VMにアクセスできるかどうかによって決まります。

ケース1：お客様がお客様VMにログインできる場合

お客様がお客様VMにアクセスできる場合、お客様VMへのオラクルのスタッフのアクセス許可にOpCtlは使用されません。
代わりに、お客様のスタッフが自社資格証明を使ってお客様VMにアクセスする必要があります。アクセス後、お客様のスタッフは共有画面テクノロジー（Zoom、Webex、Skypeなど）を使ってお客様VMへのアクセスを共有できます。プロセスは次のとおりです。

- お客様が、障害を示すサービス・リクエスト（SR）を開く。
- お客様またはオラクルが共有セッションを開き、SRのセッション情報を提供する。
- オラクルとお客様のスタッフがSRから共有セッション情報にアクセスする。
- お客様が自社資格証明を使ってお客様VMにアクセスする。
- 問題解決のために、お客様がオラクルのスタッフの指示に従ってコマンドを入力するか、お客様がVMセッションのキーボード入力の管理をオラクルのスタッフに許可する。
- お客様が診断情報でSRを更新する。
- オラクルのスタッフが解決に関する情報でSRを更新する。

ケース2：お客様がお客様VMにログインできない場合

お客様がお客様VMにアクセスできない場合、OpCtlを使って、インフラストラクチャからお客様VMにアクセスすることをオラクルのスタッフに許可します。このアクセスはSRプロセス、および問題解決のためにフル・アクセスOpCtlケージの使用を許可するお客様が制御します。プロセスは次のとおりです。

- お客様が次の文言のサービス・リクエスト（SR）をオープンする。
    - SRのタイトル：「SR granting Oracle explicit permission to access DomU of ExaCC with serial number AKXXXXXXXXX」

      (「シリアル番号AKXXXXXXXXXのExaCCのDomUにアクセスするために、オラクルに明示的権限を付与するSR」)
    - SRの内容：「We are opening this SR to grant explicit permission to Oracle to access our DomU in order for support to help resolve issue described in SR# XXXXXXXX. We acknowledge that by providing this permission, we understand that Oracle will have access to ALL FILES in DomU and agree that there are no confidential files stored in any of the file systems in DomU. In addition, we also agree that customer security team has authorized Oracle to have access to customer DomU in order to resolve the issue described in the above SR.」

      （SR番号XXXXXXXXに記載されている問題の解決を支援するため、このSRを開いて、当社のDomUにアクセスするための明示的権限をオラクルに付与します。この権限を付与することで、オラクルがDomUの全ファイルへのアクセス権を持てるようになることを承認し、DomUのいずれのファイル・システムにも機密ファイルが保存されていないことに同意します。さらに、上記のSRに記載の問題を解決するために、お客様のセキュリティ・チームがオラクルにお客様DomUへのアクセス権を許可していることにも同意します）

- オラクルがターゲット・インフラストラクチャに対するOpCtlハイパーバイザまたはフル・アクセス・リクエストを開く。
- お客様がアクセス・リクエストを許可する。
- オラクルまたはお客様が共有セッションを開いて、SRの共有セッション情報を提供する。
- オラクルとお客様の双方が共有セッションにアクセスしている状態で、オラクルはOpCtlを使って、問題解決に必要なコンポーネントにアクセスする。

OpCtlソフトウェア障害からのリカバリ

OpCtlサービスは、あらゆる単一ハードウェア・コンポーネント障害から保護する高可用性（HA）デリバリ・モデルに実装されます。お客様がすべてのリモート・アクセスを完全に制御できるようにするため、OpCtlソフトウェアは、OpCtlソフトウェアの障害を軽減するための、手動による代替リモート・アクセス方法をオラクルに提供しません（アクセス・リクエスト処理、chroot jailのデプロイなど）。OpCtlソフトウェアに障害が発生し、手動によるshellアクセスを行って問題を解決する必要がある場合、お客様がオラクルにアクセス権を付与してOpCtlソフトウェアの障害からリカバリさせるプロセスは次のとおりです。

- オラクルがお客様指定の連絡方法でお客様に連絡して問題を伝える。
- オラクルのスタッフが物理的機器がある現場に赴く。
- お客様が指名したスタッフがオラクルのスタッフを物理的機器の場所に案内する。
- オラクルのスタッフが物理的機器にアクセスし、分析とリカバリを実行する。

OpCtlの機能が復旧したら、さらに修復を行うためのアクセスがOpCtlサービスを介して実行されます。

セキュリティ・インシデントのレポートと通信

セキュリティ・インシデントが発生した場合、オラクルは適用法、およびインシデントへの対応と管理に関わるオラクルのグローバル・セキュリティ・ポリシーに従います。オラクルの企業セキュリティ慣行とインシデント対応の詳細は、https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.htmlで公開されています。不正アクセスまたはアクションの疑いがある場合は、オラクル・サービス・リクエスト（SR）プロセスで報告する必要があります。それには、セキュリティ・サービス・リクエスト（SR）を開いて、疑わしい不正アクセスまたはアクションの詳細を記載してください。

まとめ

OpCtlサービスは、オラクルのスタッフによるインフラストラクチャ・コンポーネントへのアクセスに関するポリシーと規制要件を満たせるようにお客様を支援でき、Oracle Cloud Opsサポートとお客様のテクノロジー変更管理およびセキュリティ・スタッフを緊密に連携させます。予防的、発見的、即応的コントロール機能は、オラクルのスタッフによるアクセスを管理、制御するため、およびオラクルのスタッフに対するアクセス制御の管理をお客様の変更管理システムとSIEMシステムに統合するためのOCIインタフェースを提供します。お客様がオラクルのスタッフによるアクセスを管理する場合、お客様はオラクルのアクセス・リクエストに対してタイムリーにアクセス権を付与する必要があります。したがってお客様は、アクセス・リクエストを事前承認するか、OpCtlアクセス・リクエスト処理を24時間365日稼働する既存の自社オンコール・サポート・システムに統合することを計画して、ExaC@Cサービスの可用性と品質を確保することができます。