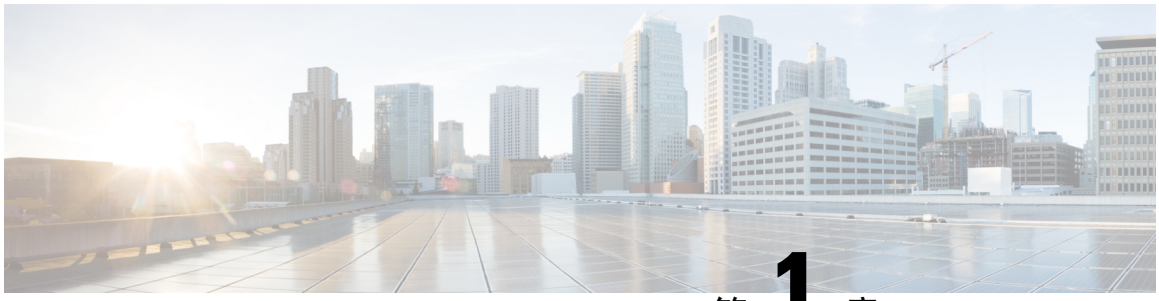
クラウドプラットフォームへの Cisco Identity Services Engine のネイティブな展開

First Published: 2022-08-16

Last Modified: 2024-09-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



第 1 章

クラウド上の Cisco ISE

クラウド上の Cisco ISE の概要

Cisco Identity Services Engine（ISE）がクラウド サービス プロバイダーからネイティブに利用可能になったことにより、変化するビジネスニーズに合わせて、Cisco ISE 展開をすばやく簡単に拡張できるようになりました。Cisco ISE は Infrastructure as Service ソリューションとして利用できるため、場所を問わずネットワークアクセスを迅速に展開し、サービスを制御できます。

ホームネットワークの Cisco ISE ポリシーを、次のクラウドプラットフォーム上の新しいリモート展開に安全に拡張できます。

- Amazon Web Services：Cisco ISE リリース 3.1 以降
- Azure Cloud Services：Cisco ISE リリース 3.2 以降
- Oracle Cloud Infrastructure：Cisco ISE リリース 3.2 以降

クラウドプラットフォームでの Cisco ISE 展開のパフォーマンスと拡張性については、『Performance and Scalability Guide for Cisco Identity Services Engine』の「Cisco ISE on Cloud」のセクションを参照してください。

Cisco ISE の詳細については、『Cisco Identity Services Engine End-User Documentation』を参照してください。

サポートされているクラウドプラットフォームによってホストされているクラウドネイティブのイメージまたはインスタンスを介して起動される Cisco ISE の場合：

- すべてのクラウドプラットフォームで、インスタンスのセットアップ時に設定するパスワードはプレーンテキストとして保存されます。ただし、プレーンテキストのパスワードはセキュリティリスクをもたらす可能性があります。そのため、クラウドプラットフォームから起動される Cisco ISE では、Cisco ISE GUI に最初にアクセスするときにログインパスワードをリ

セットする必要があります。次に、エラーを回避するために、更新されたパスワードで API ベースの自動化スクリプトも更新する必要があります。

- クラウドプラットフォームを介して起動される Cisco ISE インスタンスのデフォルトのユーザー名は **iseadmin** です。ユーザーデータに別のユーザー名を入力した場合でも、Cisco ISE インスタンスはユーザー名 **iseadmin** で作成されます。

（注） AWS を介して起動される Cisco ISE リリース 3.1 インスタンスの場合、デフォルトのユーザー名は **admin** です。

クラウドプラットフォームでの Cisco ISE ライセンス

Cisco ISE は、クラウドプラットフォームで利用可能な所有ライセンス持ち込み（BYOL）ソリューション利用しています。共通 VM ライセンスを使用して、使用する Cisco ISE 機能に必要な他の Cisco ISE ライセンスに加えて、クラウドプラットフォームで Cisco ISE を有効にします。Cisco ISE ライセンスについては、『Cisco ISE Ordering Guide』を参照してください。

ハイブリッド展開のアップグレードガイドライン

Cisco ISE アップグレードワークフローは、AWS、Microsoft Azure、または OCI 上 の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。

オンプレミスにインストールされた PAN を使用したハイブリッド展開のアップグレード

プライマリ管理ノード（PAN）がオンプレミスにインストールされ、セカンダリノードのいずれかまたは一部がクラウドにインストールされているハイブリッド展開をアップグレードするには、次の手順を実行します。

Procedure

Step 1 Cisco ISE 展開から、クラウドにインストールされているセカンダリノードの登録を解除します。

すべてのセカンダリノードがクラウドにインストールされている場合、ダウンタイムが発生する可能性があります。

Step 2 オンプレミス展開をより上位のリリースにアップグレードします。

詳細については、ご使用のリリースの『Cisco Identity Services Engine Upgrade Journey』[英語] の「Perform the Upgrade」セクションを参照してください。

Step 3 必要な数のスタンドアロン Cisco ISE ノードを、上位のリリースでクラウドにインストールします。

NAD の設定変更を回避するために、同じ IP アドレスを使用してノードをインストールして設定する必要があります。インストールプロセスの詳細については、ご使用のリリースの『*Cisco Identity Services Engine Installation Guide*』[英語] を参照してください。

Step 4 これらのスタンドアロンノードを、アップグレードしたオンプレミス展開に登録します。

Cisco ISE に新しく展開されたノードにシステム証明書をインポートする必要があります。システム証明書を Cisco ISE ノードにインポートする方法の詳細については、ご使用のリリースの『Cisco Identity Services Engine Administrator Guide 』[英語] の「Basic Setup」章にある「Import a System Certificate」セクションを参照してください。

クラウドにインストールされた PAN を使用したハイブリッド展開のアップグレード

PAN がクラウドにインストールされているハイブリッド展開をアップグレードするには、次の手順を実行します。

Procedure

Step 1 Cisco ISE の構成設定と既存の展開からの運用ログのバックアップを作成します。

Step 2 展開内のすべてのノードをシャットダウンします。

Step 3 必要な数のスタンドアロン Cisco ISE ノードを、クラウドとオンプレミスに上位のリリースでインストールします。

NAD の設定変更を回避するために、同じ IP アドレスを使用してノードをインストールして設定する必要があります。インストールプロセスの詳細については、ご使用のリリースの『*Cisco Identity Services Engine Installation Guide*』[英語] を参照してください。

Step 4 バックアップデータから Cisco ISE の設定を復元します。詳細については、ご使用のリリースの『*Cisco Identity Services Engine Upgrade Journey*』[英語] の「Backup and Restore Upgrade Process」セクションを参照してください。

Step 5 すべてのノードを展開に戻します。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。

- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

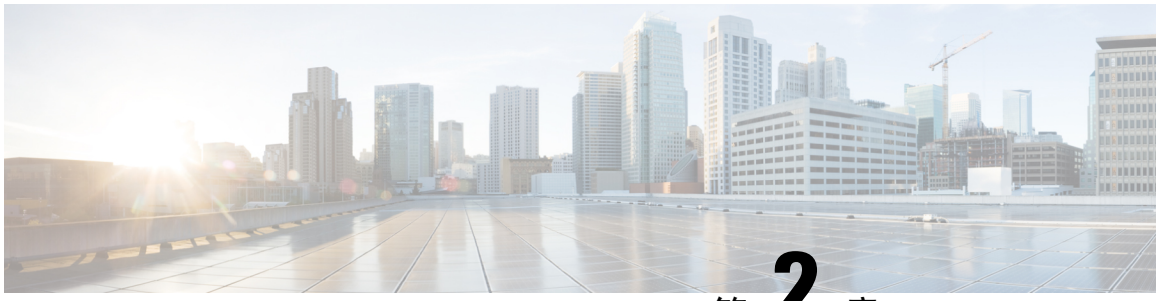
シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

その他の参考資料

Cisco ISE を使用するときに活用できるその他のリソースについては、『Cisco ISE End-User Resources』[英語] を参照してください。



第 2 章

Amazon Web Service における Cisco ISE

Amazon Web Services における Cisco ISE

ホームネットワークの Cisco ISE ポリシーを、Amazon Web Services（AWS）を使用して、新しいリモート展開へと安全に拡張します。

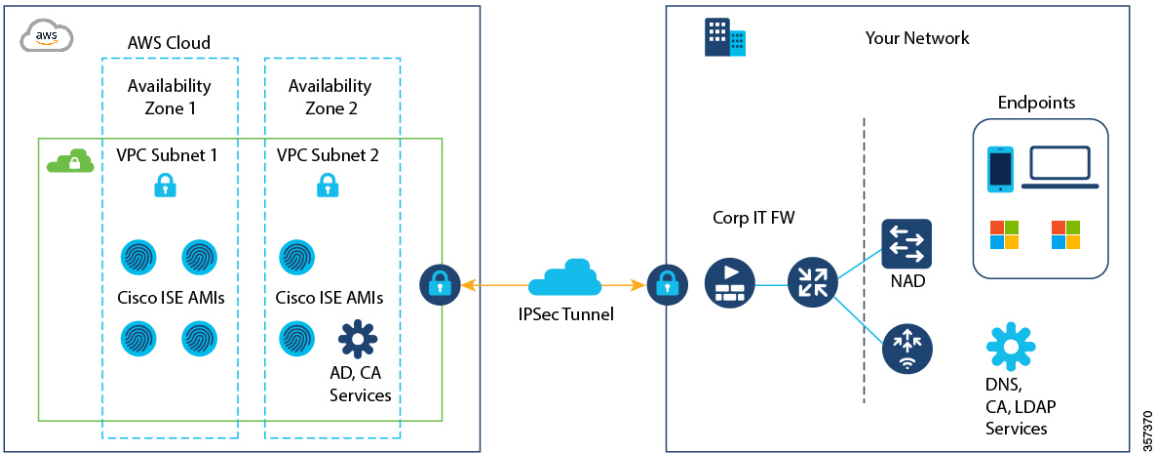
AWS CloudFormation テンプレート（CFT）または Amazon マシンイメージ（AMI）を通じて Cisco ISE を AWS に設定し、起動できます。次のリストのいずれかの方法で CFT を使用することをお勧めします。AWS で Cisco ISE を起動するには、、次のいずれかの手順を実行します。

- AWS マーケットプレイスからの Cisco ISE CloudFormation テンプレートの起動 （10 ページ）
- Cloud Formation テンプレートを使用した Cisco ISE の起動 （13 ページ）
- Cisco ISE AMI の起動

CFT は、クラウドの導入を簡単に作成および管理できる AWS ソリューションです。AWS 内で仮想プライベートクラウドを作成してネットワークをクラウドに拡張し、IPsec トンネルを介して組織のネットワークと通信できるように、仮想プライベートゲートウェイを設定します。

次の図はあくまでも一例です。組織の要件に応じて、認証局（CA）、Active Directory（AD）、ドメインネームシステム（DNS）サーバー、Lightweight Directory Access Protocol（LDAP）などの共通サービスを、オンプレミスまたは AWS に配置できます。

図 *1 : AWS* クラウドに接続された展開の例



AWS での CFT の使用については、『AWS CloudFormation ユーザーガイド』を参照してください。

次の表に、現在使用可能な Cisco ISE インスタンスの詳細を示します。次のいずれかのインスタンスを使用するには、Cisco ISE VM ライセンスを購入する必要があります。特定の要件に対応する EC2 インスタンスの価格設定については、「Amazon EC2 オンデマンド料金」を参照してください。

表 *1 : Cisco ISE* インスタンス

Cisco ISE インスタンスタイプ	CPU コア	RAM（GB）
t3.xlarge このインスタンスは、Cisco ISE 評価ユースケースをサポートしており、Cisco ISE リリース 3.1 パッチ 1 以降のリリースでサポートされています。100 の同時アクティブエンドポイントがサポートされています。	4	16
m5.2xlarge	8	32
c5.4xlarge	16	32
m5.4xlarge	16	64
c5.9xlarge	36	72
m5.8xlarge	32	128
m5.16xlarge	64	256

c5.4xlarge や c5.9xlarge などの計算に最適化されたインスタンスは、コンピューティング集約型のタスクまたはアプリケーションを対象としており、ポリシーサービスノード（PSN）での使用に適しています。

m5.4xlarge、m5.8xlarge、m5.16xlarge などの汎用インスタンスは、データ処理タスクとデータベース操作を対象としており、ポリシー管理ノード（PAN）またはモニタリングとトラブルシューティング（MnT）ノード、あるいはその両方としての使用に適しています。

汎用インスタンスをPSNとして使用する場合、パフォーマンスの数値は、PSNとしてのコンピューティング最適化インスタンスのパフォーマンスよりも低くなります。

m5.2xlarge インスタンスは、極小規模 PSN としてのみ使用する必要があります。

AWSインスタンスのスケールとパフォーマンスデータの詳細については、『*Cisco ISE Performance and Scale*』ガイド [英語] を参照してください。

AWS インスタンスタイプのスケールおよびパフォーマンスデータについては、『*Performance and Scalability Guide for Cisco Identity Services Engine*』を参照してください。

AWS S3 ストレージサービスを活用して、バックアップおよび復元ファイル、モニターリングおよびトラブルシューティング レポートなどを簡単に保存できます。

上記の手順に加えて、シスコが開発した次のソリューションを使用して、AWS にマルチノード Cisco ISE 展開をインストールして自動的に作成することもできます。

- 小規模展開向けのCisco ISE AWS パートナーソリューション 。
- あらゆる規模の展開向けの シスコが開発した Terraform スクリプト。

Cisco ISE AWS インスタンスを作成するための前提条件

- Amazon Elastic Compute Cloud（EC2）インスタンスや Amazon Elastic Block Store（EBS）ボリュームなどの AWS ソリューション、およびリージョン、可用性ゾーン、セキュリティグループ、仮想プライベートクラウド（VPC）などの概念に精通している必要があります。これらのソリューションの詳細については、AWS のドキュメントを参照してください。

  また、AWS サービスクォータの管理に精通している必要があります。

- AWS で VPC を設定する必要があります。

  「VPC with public and private subnets and AWS Site-to-Site VPN access」を参照してください。

- 暗号化 EBS ボリュームを作成するには、AWS Identity and Access Management（IAM）ポリシーでキー管理サービス（KMS）リソースへのアクセスを許可する必要があります。「Policies and permissions in IAM」を参照してください。

- Cisco ISE インスタンスを設定する前に、AWS でセキュリティグループ、サブネット、およびキーペアを作成します。

  Cisco ISE のセキュリティグループを作成する場合は、使用する Cisco ISE サービスのすべてのポートとプロトコルのルールを作成する必要があります。ご使用のリリースの『*Cisco ISE Installation Guide*』の「Cisco ISE Ports Reference」の章を参照してください。

- ネットワーク インターフェイスの IPv6 アドレスを設定するには、サブネットには AWS で有効になっている IPv6 Classless Inter-Domain Routing（CIDR）プールが必要です。

- Cisco ISE CloudFormation テンプレートの [管理ネットワーク（Management Network）] フィールドに入力する IP アドレスは、AWS にネットワーク インターフェイス オブジェクトとして存在する IP アドレスであってはなりません。
- 展開では、静的 IP をプライベート IP として設定できます。ただし、スタティック IP は DNS 解決可能なホスト名で設定する必要があります。

AWS での Cisco ISE の使用に関する既知の制限事項

AWS で Cisco ISE を使用する場合の既知の制限事項は次のとおりです。

- Cisco ISE インスタンスの Amazon EBS スナップショットは取得できません。そのスナップショットを使用して別の EBS ボリュームを作成できません。
- Amazon VPC は、レイヤ 3 機能のみをサポートします。AWS インスタンス上の Cisco ISE ノードは、レイヤ 1 およびレイヤ 2 の機能に依存する Cisco ISE 機能をサポートしません。たとえば、Cisco ISE CLI を使用する DHCP SPAN プロファイラプローブおよび CDP プロトコルとの連携動作は、現在サポートされていません。
- NIC ボンディングはサポートされていません。
- デュアル NIC は、2 つの NIC のみ（ギガビットイーサネット 0 とギガビットイーサネット 1 のみ）でサポートされます。Cisco ISE インスタンスでセカンダリ NIC を設定するには、まず AWS でネットワーク インターフェイス オブジェクトを作成し、Cisco ISE インスタンスの電源をオフにしてから、このオブジェクトを Cisco ISE にアタッチします。AWS に Cisco ISE をインストールして起動したら、Cisco ISE CLI を使用して、ネットワーク インターフェイス オブジェクトの IP アドレスをセカンダリ NIC として手動で設定します。
- Cisco ISE アップグレードワークフローは、AWS 上 の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。ハイブリッド Cisco ISE 展開のアップグレードについては、『Upgrade Guidelines for Hybrid Deployments』を参照してください。
- パスワードベースの認証を使用した Cisco ISE CLI への SSH アクセスは、AWS ではサポートされていません。キーペアを介してのみ Cisco ISE CLI にアクセスでき、このキーペアは安全に保存する必要があります。

  秘密キー（または PEM）ファイルを使用しており、そのファイルを失うと、Cisco ISE CLI にアクセスできなくなります。

  パスワードベースの認証方式を使用して Cisco ISE CLI にアクセスする統合は、サポートされていません（たとえば、Cisco DNA Center リリース 2.1.2 以前）。
- Cisco ISE がアイドル状態のときに、「仮想マシンリソースが不十分（`Insufficient Virtual Machine Resources`）」というアラームを受信する場合があります。CPU 周波数は、効果的な電力節約のために必要なベースライン周波数（2 GHz）より低く維持されるため、このアラームは無視できます。

- ソフトウェアバージョンが Cisco ISE 3.1 の場合、AWS 経由で起動した Cisco ISE インスタンスを介して **show inventory** コマンドを実行すると、AWS 上の Cisco ISE のインスタンスタイプはコマンド出力に表示されません。この問題は、Cisco ISE 3.1 パッチ 1 以降のソフトウェアバージョンでは発生しません。
- AWS を介して Cisco ISE を起動する場合、IPv6 サーバーは NTP サーバーとして設定できません。
- 初期管理者ユーザーアカウント名 iseadmin がデフォルトで生成されます。このユーザーアカウント名は、インストールプロセスの完了後に Cisco ISE への SSH アクセスと GUI アクセスの両方に使用されます。
- EC2 インスタンスのサイズは変更できません。
- Cisco ISE ディスク EBS ボリュームは AMI として変換できません。その後、その AMI では別の EC2 インスタンスを再起動できません。
- 正常に作成されたインスタンスの IP アドレスまたはデフォルトゲートウェイは変更できません。
- オンプレミスにある外部アイデンティティソースを統合できます。ただし、遅延のため、オンプレミスのアイデンティティソースを使用した場合の Cisco ISE パフォーマンスは、AWS でホストされるアイデンティティソースまたは Cisco ISE の内部ユーザーデータベースを使用した場合の Cisco ISE パフォーマンスと同等ではありません。
- 次の展開タイプがサポートされていますが、ノード間遅延が 300 ミリ秒未満であることを確認する必要があります。
  - オンプレミス上の一部の Cisco ISE ノードと AWS の一部のノードを使用したハイブリッド展開。
  - VPC ピアリング接続によるリージョン間展開。
- Amazon EC2 ユーザーデータスクリプトはサポートされていません。
- 設定する Cisco ISE CFT で、ボリュームサイズを GB 単位で定義します。ただし、AWS は EBS ストレージボリュームをギビバイト（GiB）で作成します。したがって、Cisco ISE CFT でボリュームサイズとして 600 を入力すると、AWS は 600 GiB（または 644.25 GB）の EBS ボリュームを作成します。
- Cisco ISE CLI または GUI を使用して設定データのバックアップ中に復元操作を実行する場合は、ADE-OS パラメータを含めないでください。
- ユーザーデータの取得は、メタデータ V1（IMDSv1）でのみ機能し、V2 では機能しません。

（注）
- オンプレミスデバイスから VPC への通信は安全である必要があります。
- Cisco ISE リリース 3.1 パッチ 3 では、Cisco ISE は IP アドレス 169.254.169.254 を介して AWS クラウドにトラフィックを送信して、インスタンスの詳細を取得します。これは、それがクラウドインスタンスであるかどうかを確認するためのものであり、オンプレミスの展開では無視できます。

AWS マーケットプレイスからの Cisco ISE CloudFormation テンプレートの起動

この方法では、スタンドアロンの Cisco ISE インスタンスのみを起動できます。Cisco ISE 展開を作成するには、お使いのリリースの『*Cisco ISE Administrator Guide*』[英語] の「Deployment」の章を参照してください。

Note
- CFT を介して複数の DNS または NTP サーバーは追加できません。Cisco ISE インスタンスの作成後に、Cisco ISE CLI を使用して DNS または NTP サーバーを追加できます。ただし、Cisco ISE リリース 3.4 以降では、CFT を使用してセカンダリおよびターシャリ DNS または NTP サーバーを追加できます。
- CFT を介して IPv6 DNS または NTP サーバーを設定することはできません。IPv6 サーバーを設定するには、Cisco ISE CLI を使用できます。

Cisco ISE CFT は、汎用 SSD（gp2）ボリュームタイプのインスタンスを作成します。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Before you begin

AWS では、Cisco ISE CFT の設定に含めるセキュリティグループと管理ネットワークを作成します。

Procedure

Step 1 https://console.aws.amazon.com/ でAmazon 管理コンソールにログインし、[マーケットプレイス サブスクリプション（AWS Marketplace Subscriptions）] を検索します。

Step 2 表示された [サブスクリプション管理（Manage Subscriptions）] ウィンドウで、左ペインの [製品の検出（Discover Products）] をクリックします。

Step 3 検索バーに [Cisco Identity Services Engine（ISE）] と入力します。

Step 4 製品名をクリックします。

Step 5 表示された新しいウィンドウで [引き続き登録する（Continue to Subscribe）] をクリックします。

Step 6 [設定を続行 (Continue to Configuration)] をクリックします。

Step 7 [このソフトウェアを設定する（Configure this software）] 領域で、[詳細情報（Learn More）] をクリックし、[CloudFormation テンプレートのダウンロード（Download CloudFormation Template）]をクリックして、Cisco ISE CFT をローカルシステムにダウンロードします。このテンプレートを使用して、必要に応じて他の Cisco ISE インスタンスの設定を自動化できます。

[詳細情報（Learn More）] ダイアログボックスの [テンプレートを表示（View Template）] をクリックして、AWS CloudFormation Designer の CFT も表示できます。

Step 8 [ソフトウェアバージョン（Software Version）] および [AWSリージョン（AWS Region）] ドロップダウンリストから必要な値を選択します。

Step 9 [続行して起動する（Continue to Launch）] をクリックします

Step 10 [アクションの選択（Choose Action）] ドロップダウンリストから、[CloudFormationの起動（Launch CloudFormation）] を選択します。

Step 11 [作成（Launch）] をクリックします。

Step 12 [スタックの作成（Create Stack）] ウィンドウで、[テンプレートの準備完了（Template Is Ready）] および [Amazon S3 URL] オプションボタンをクリックします。

Step 13 [次へ（Next）] をクリックします。

Step 14 新しいウィンドウで、[スタック名（Stack Name）] フィールドに値を入力します。

Step 15 [パラメータ（Parameters）] 領域の次のフィールドに必要な詳細情報を入力します。

- [ホスト名（Hostname）]：この領域では、英数字とハイフン（-）のみがサポートされます。ホスト名の長さは 19 文字までです。
- **[Instance Key Pair]**：SSH を介して Cisco ISE インスタンスにアクセスするには、AWS で作成した、ユーザー名が iseadmin（Cisco ISE Release 3.1 の場合はユーザー名が admin）の PEM ファイルを選択します。まだ設定していない場合は、AWS で PEM キーペアを作成します。このシナリオの SSH コマンドの例：**ssh -i mykeypair.pem iseadmin@myhostname.compute-1.amazonaws.com**
- [管理セキュリティグループ（Management Security Group）]：ドロップダウンリストからセキュリティグループを選択します。この CFT を設定する前に、AWS でセキュリティグループを作成する必要があります。

  Note
  この手順では、1 つのセキュリティグループのみを追加できます。インストール後に Cisco ISE にセキュリティグループを追加できます。起動時に Cisco ISE で使用できるようにするネットワーク トラフィック ルールは、ここで追加するセキュリティグループで設定する必要があります。

- [管理ネットワーク（Management Network）]：Cisco ISE インターフェイスに使用するサブネットを選択します。IPv6 アドレスを有効にするには、IPv6 CIDR ブロックを VPC およびサブネットに関連付ける必要があります。まだ設定していない場合は、AWS でサブネットを作成します。
- [管理プライベートIP（Management Private IP）]：前に選択したサブネットの IPv4 アドレスを入力します。このフィールドを空白のままにすると、AWS DHCP が IP アドレスを割り当てます。

  Cisco ISE インスタンスが作成されたら、[インスタンス概要（Instance Summary）] ウィンドウからプライベート IP アドレスをコピーします。次に、DNS サーバーで IP とホスト名をマッピングしてから、Cisco ISE 展開を作成します。
- [タイムゾーン（Timezone）]：ドロップダウンリストからタイムゾーンを選択します。
- [インスタンスタイプ（Instance Type）]：ドロップダウンリストから Cisco ISE のインスタンスタイプを選択します。
- [EBS暗号化（EBS Encryption）：ドロップダウンリストから [True] を選択して暗号化を有効にします。このフィールドのデフォルト値は [False] です。このフィールドのデフォルト値は [False] です。Cisco ISE リリース 3.3 以降のリリースでは、[EBS Encryption] フィールドのデフォルト値は [True] です。
- （オプション）[KMS Key]：データ暗号化のための **KMS キー** または Amazon リソースネームまたはエイリアスを入力します。

  Note
  これは、Cisco ISE リリース 3.3 以降のリリースに適用されるオプションのフィールドです。[KMS Key] が指定されている場合は、データ暗号化に使用されます。[KMS Key] が指定されていない場合は、デフォルトのキーがデータ暗号化に使用されます。

- [ボリュームサイズ（Volume Size）]：ボリュームサイズを GB 単位で指定します。許容範囲は 300 ー 2400 GB です。実稼働環境では 600 GB が推奨されます。600 GB 未満のボリュームサイズは評価目的でのみ設定します。インスタンスを終了すると、ボリュームも削除されます。

  Note
  AWS は EBS ストレージボリュームをギビバイト（GiB）で作成します。[ボリュームサイズ（Volume Size）] フィールドに 600 と入力すると、AWS は 600 GiB（または 644.25 GB）の EBS ボリュームを作成します。

- [DNSドメイン（DNS Domain）]：このフィールドで使用できる値は、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）です。
- [ネームサーバーIP（Name Server IP）] ：正しい構文でネームサーバーの IP アドレスを入力します。

  Note
  この手順では、1 つの DNS サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して DNS サーバーを追加できます。Cisco ISE リリース 3.4 以降では、この手順でセカンダリおよびターシャリ DNS サーバーも追加できます。[Secondary DNS Server] フィールドが空白の場合、[Tertiary DNS Server] オプションは使用できません。

- [NTPサーバー（NTP Server）]：NTP サーバーの IP アドレスまたはホスト名を正しいシンタックスで入力します（例：**time.nist.gov**）。入力内容は送信時に検証されません。誤った構文を使用すると、Cisco ISE サービスが起動時に表示されないことがあります。

Note
ここで入力した IP アドレスまたはホスト名が正しくない場合、Cisco ISE は NTP サーバーと同期できません。SSH ターミナルを使用して Cisco ISE にログインし、Cisco ISE CLI を使用して正しい NTP サーバーを設定します。

この手順では、1 つの NTP サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して NTP サーバーを追加できます。Cisco ISE リリース 3.4 以降では、この手順でセカンダリおよびターシャリ NTP サーバーを追加することもできます。[Secondary NTP Server] フィールドが空白の場合、[Tertiary NTP Server] オプションは使用できません。

- [ERS]：Cisco ISE の起動時に External RESTful Services（ERS）サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- [OpenAPI]：Cisco ISE の起動時に OpenAPI サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- ERS：Cisco ISE の起動時に ERS サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- [pxGridクラウド（pxGrid Cloud）]：このフィールドのデフォルト値は [いいえ（no）] です。
- [パスワードの入力（Enter Password）]：GUI に使用する必要がある管理パスワードを入力します。パスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。パスワードは、AWS コンソールのインスタンス設定ウィンドウの [ユーザーデータ（User Data）] 領域に、プレーンテキストで表示されます。ご使用のリリースの『Cisco ISE Administrator Guide』[英語] の「Basic Setup」の章にある「User Password Policy」のセクションを参照してください。
- [パスワードの確認（Confirm Password）]：管理パスワードを再入力します。

Step 16 [次へ（Next）] をクリックし、インスタンス作成プロセスを開始します。

Cloud Formation テンプレートを使用した Cisco ISE の起動

この方法では、スタンドアロンの Cisco ISE インスタンスのみを起動できます。Cisco ISE 展開を作成するには、お使いのリリースの『*Cisco ISE Administrator Guide*』[英語] の「Deployment」の章を参照してください。

Note

- CFT を介して複数の DNS または NTP サーバーは追加できません。Cisco ISE インスタンスの作成後に、Cisco ISE CLI を使用して DNS または NTP サーバーを追加できます。ただし、Cisco ISE リリース 3.4 以降では、CFT を使用してセカンダリおよびターシャリ DNS または NTP サーバーを追加できます。
- CFT を介して IPv6 DNS または NTP サーバーを設定することはできません。IPv6 サーバーを設定するには、Cisco ISE CLI のみを使用できます。

Cisco ISE CFT は、汎用 SSD（gp2）ボリュームタイプのインスタンスを作成します。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Before you begin

AWS では、Cisco ISE CFT の設定に含めるセキュリティグループと管理ネットワークを作成します。

Procedure

Step 1 https://console.aws.amazon.com/ でAmazon 管理コンソールにログインし、[マーケットプレイス サブスクリプション（AWS Marketplace Subscriptions）] を検索します。

Step 2 表示された [サブスクリプション管理（Manage Subscriptions）] ウィンドウで、左ペインの [製品の検出（Discover Products）] をクリックします。

Step 3 検索バーに [Cisco Identity Services Engine（ISE）] と入力します。

Step 4 製品名をクリックします。

Step 5 表示された新しいウィンドウで [引き続き登録する（Continue to Subscribe）] をクリックします。

Step 6 [設定を続行 (Continue to Configuration)] をクリックします。

Step 7 [このソフトウェアを設定する（Configure this software）] 領域で、[詳細情報（Learn More）] をクリックし、[CloudFormation テンプレートのダウンロード（Download CloudFormation Template）]をクリックして、Cisco ISE CFT をローカルシステムにダウンロードします。このテンプレートを使用して、必要に応じて他の Cisco ISE インスタンスの設定を自動化できます。

[詳細情報（Learn More）] ダイアログボックスの [テンプレートを表示（View Template）] をクリックして、AWS CloudFormation Designer の CFT も表示できます。

Step 8 AWS 検索バーを使用して、[CloudFormation] を検索します。

Step 9 [スタックの作成（Create Stack）] ドロップダウンリストから、[新しいリソースで（標準（With new resources（standard））] を選択します。

Step 10 [スタックの作成（Create Stack）] ウィンドウで、[テンプレートの準了（Template Is Ready）] と [テンプレートファイルのアップロード（Upload a Template File）] を選択します。

Step 11 [ファイルの選択（Choose File）] をクリックし、ステップ 7 でダウンロードした CFT ファイルをアップロードします。

Step 12 [次へ（Next）] をクリックします。

Step 13 新しいウィンドウで、[スタック名（Stack Name）] フィールドに値を入力します。

Step 14 [パラメータ（Parameters）] 領域の次のフィールドに必要な詳細情報を入力します。

- [ホスト名（Hostname）]：この領域では、英数字とハイフン（-）のみがサポートされます。ホスト名の長さは 19 文字までです。

- [インスタンスキーペア（Instance Key Pair）]：SSH を介して Cisco ISE インスタンスにアクセスするには、AWS で作成したユーザー名 admin の PEM ファイルを選択します。まだ設定していない場合は、AWS で PEM キーペアを作成します。このシナリオの SSH コマンドの例：**ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com**

- [管理セキュリティグループ（Management Security Group）]：ドロップダウンリストからセキュリティグループを選択します。この CFT を設定する前に、AWS でセキュリティグループを作成する必要があります。

  Note
  この手順では、1 つのセキュリティグループのみを追加できます。インストール後に Cisco ISE にセキュリティグループを追加できます。インスタンスの起動時に Cisco ISE で使用できるようにするネットワーク トラフィック ルールは、ここで追加するセキュリティグループで設定する必要があります。

- [管理ネットワーク（Management Network）]：Cisco ISE インターフェイスに使用するサブネットを選択します。IPv6 アドレスを有効にするには、IPv6 CIDR ブロックを VPC およびサブネットに関連付ける必要があります。まだ設定していない場合は、AWS でサブネットを作成します。

- [管理プライベート IP（Management Private IP）]：前に選択したサブネットの IPv4 アドレスを入力します。このフィールドを空白のままにすると、AWS DHCP が IP アドレスを割り当てます。

  Cisco ISE インスタンスが作成されたら、[インスタンス概要（Instance Summary）] ウィンドウからプライベート IP アドレスをコピーします。次に、DNS サーバーで IP アドレスとホスト名をマッピングしてから、Cisco ISE 展開を作成します。

- [タイムゾーン（Timezone）]：ドロップダウンリストからタイムゾーンを選択します。

- [インスタンスタイプ（Instance Type）]：ドロップダウンリストから Cisco ISE のインスタンスタイプを選択します。

- [EBS暗号化（EBS Encryption）：ドロップダウンリストから [True] を選択して暗号化を有効にします。このフィールドのデフォルト値は [False] です。Cisco ISE リリース 3.3 以降のリリースでは、[EBS Encryption] フィールドのデフォルト値は [True] です。

- （オプション）[KMS Key]：データ暗号化のための **KMS キー** または Amazon リソースネームまたはエイリアスを入力します。

  Note
  これは、Cisco ISE リリース 3.3 以降のリリースに適用されるオプションのフィールドです。[KMS Key] が指定されている場合は、データ暗号化に使用されます。[KMS Key] が指定されていない場合は、デフォルトのキーがデータ暗号化に使用されます。

- [ボリュームサイズ（Volume Size）]：ボリュームサイズを GB 単位で指定します。許容範囲は 300 ー 2400 GB です。実稼働環境では 600 GB が推奨されます。600 GB 未満のボリュームサイズは評価目的でのみ設定します。インスタンスを終了すると、ボリュームも削除されます。

  Note
  AWS は EBS ストレージボリュームをギビバイト（GiB）で作成します。[ボリュームサイズ（Volume Size）] フィールドに 600 と入力すると、AWS は 600 GiB（または 644.25 GB）の EBS ボリュームを作成します。

- [DNSドメイン（DNS Domain）]：このフィールドで使用できる値は、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）です。
- [ネームサーバー（Name Server）]：正しいシンタックスでネームサーバーの IP アドレスを入力します。

Note
この手順では、1 つの DNS サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して DNS サーバーを追加できます。

Cisco ISE リリース 3.4 以降では、この手順でセカンダリおよびターシャリ NTP サーバーを追加することもできます。[Secondary DNS Server] フィールドが空白の場合、[Tertiary DNS Server] オプションは使用できません。

- [NTPサーバー（NTP Server）]：NTP サーバーの IP アドレスまたはホスト名を正しいシンタックスで入力します（例：**time.nist.gov**）。入力内容は送信時に検証されません。誤った構文を使用すると、Cisco ISE サービスが起動時に表示されないことがあります。

Note
ここで入力した IP アドレスまたはホスト名が正しくない場合、Cisco ISE は NTP サーバーと同期できません。SSH ターミナルを使用して Cisco ISE にログインし、Cisco ISE CLI を使用して正しい NTP サーバーを設定します。

この手順では、1 つの NTP サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して NTP サーバーを追加できます。

Cisco ISE リリース 3.4 以降では、この手順でセカンダリおよびターシャリ NTP サーバーを追加することもできます。[Secondary NTP Server] フィールドが空白の場合、[Tertiary NTP Server] オプションは使用できません。

- [ERS]：Cisco ISE の起動時に ERS サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- [OpenAPI]：Cisco ISE の起動時に OpenAPI サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- ERS：Cisco ISE の起動時に ERS サービスを有効にするには、[はい（yes）] と入力します。このフィールドのデフォルト値は [いいえ（no）] です。
- [pxGridクラウド（pxGrid Cloud）]：このフィールドのデフォルト値は [いいえ（no）] です。

Note
補完的な製品リリースには依存関係があるため、pxGrid クラウド機能は現在使用できません。[pxGrid クラウド（pxGrid Cloud）] サービスは有効にしないでください。

- [パスワードの入力（Enter Password）]：GUI に使用する必要がある管理パスワードを入力します。パスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。パスワードは、AWS コンソールのインスタンス設定ウィンドウの [ユーザーデータ（User Data）] エリアに、プレーンテキストで表示されます。ご使用のリリースの『Cisco ISE Administrator Guide』[英語] の「Basic Setup」の章にある「User Password Policy」のセクションを参照してください。

- [パスワードの確認（Confirm Password）]：管理パスワードを再入力します。

Step 15 [次へ（Next）] をクリックし、インスタンス作成プロセスを開始します。

Cisco ISE AMI の起動

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Procedure

Step 1 https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールにログインします。

Step 2 左側のペインで [インスタンス（Instances）] をクリックします。

Step 3 **[Instances]** ウィンドウで、**[Launch Instances]** をクリックします。

Step 4 **[Step 1: Choose AMI]** ウィンドウで、左側のメニューから **[AWS Marketplace]** をクリックします。

Step 5 検索バーに [Cisco Identity Services Engine] と入力します。

Step 6 **[Cisco Identity Services Engine（ISE）]** オプションで、**[Select]** をクリックします。

AMI のさまざまな詳細を含む [Cisco Identity Services Engine（ISE）] ダイアログボックスが表示されます。

Step 7 情報を確認し、[続行（Continue）] をクリックして続行します。

Step 8 **[Step 2: Choose an Instance Type]** ウィンドウで、使用するインスタンスタイプの横にあるラジオボタンをクリックします。

Step 9 [Next: Configure Instance Details] をクリックします。

Step 10 [ステップ3：インスタンスの詳細を設定（Step 3: Configure Instance Details）] ウィンドウで、次のフィールドに必要な詳細情報を入力します。

- [インスタンスの数（Number of Instances）]：このフィールドには **1** を入力します。
- [ネットワーク（Network）]：ドロップダウンリストから、Cisco ISE インスタンスを起動する VPC を選択します。
- [サブネット（Subnet）]：ドロップダウンリストから、Cisco ISE インスタンスを起動するサブネットを選択します。
- [ネットワーク インターフェイス（Network Interfaces）]：ドロップダウンリストには、デフォルトで**新しいネットワーク インターフェイス**が表示されます。これは、接続された DHCP サーバーによって IP アドレスが Cisco ISE に自動的に割り当てられることを意味します。このフィールドに IP アドレスを入力して、Cisco ISE に固定 IP アドレスを割り当てることができます。[ネットワーク インターフェイス（Network Interfaces）] ドロップダウンリストで、同じサブネットから既存のネットワーク イン

ターフェイスを選択することもできます。セットアッププロセス中に設定できるインターフェイスは 1 つだけです。Cisco ISE のインストール後、Cisco ISE を介してインターフェイスを追加できます。

Step 11 [詳細設定（Advanced Details）] エリアの [ユーザーデータ（User Data）] エリアで、[テキスト形式（As Text）] オプションボタンをクリックして、次の形式でキーと値のペアを入力します。

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

tertiarynameserver=<*IPv4 address of tertiary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important
Cisco ISE リリース 3.4 以降、

a. [ntpserver] フィールド名が [primaryntpserver] に変更されました。[ntpserver] を使用すると、Cisco ISE サービスは起動しません。

b. OpenAPI はデフォルトで有効になっています。したがって、[openapi=<yes/no>] フィールドは必須ではありません。

c. [secondarynameserver] フィールドを空白のままにして、[tertiarynameserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

d. [secondaryntpserver] フィールドを空白のままにして、[tertiaryntpserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

ユーザーデータエントリを使用して設定する各フィールドには、正しいシンタックスを使用する必要があります。[ユーザーデータ（User Data）] フィールドに入力した情報は、入力時に検証されません。誤った構文を使用すると、Cisco ISE サービスが AMI の起動時に表示されないことがあります。次に、[ユーザーデータ（User Data）] フィールドを使用して送信する設定のガイドラインを示します。

- hostname：英数字とハイフン（-）のみを含むホスト名を入力します。ホスト名の長さは 19 文字以下で、下線（_）を含めることはできません。

- プライマリネームサーバー：プライマリネームサーバーの IP アドレス。サポートされているのは IPv4 アドレスだけです。Cisco ISE リリース 3.4 以降では、インストール時に [secondarynameserver] および [tertiarynameserver] フィールドを使用して、secondarynameserver および tertiarynameserver を設定できます。
- dnsdomain：DNS ドメインの FQDN を入力します。エントリには、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）を含めることができます。
- ntpserver：同期に使用する NTP サーバーの IPv4 アドレスまたは FQDN を入力します（例：time.nist.gov）。Cisco ISE リリース 3.4 以降では、インストール中に [secondaryntpserver] および [tertiaryntpserver] フィールドを使用して、セカンダリおよびターシャリ NTP サーバーを設定できます。
- timezone：タイムゾーンを入力します（例：Etc/UTC）。すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されるようにします。
- password：Cisco ISE への GUI ベースのログインのパスワードを設定します。入力するパスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。パスワードは 6 ～ 25 文字で、少なくとも 1 つの数字、1 つの大文字、および 1 つの小文字を含める必要があります。パスワードは、ユーザー名またはその逆（iseadmin または nimdaesi）、cisco、または ocsic を含めたりそれらと同じにすることはできません。使用できる特殊文字は @~*!,+=_- です。ご使用のリリースの『*Cisco ISE Administrator Guide*』の「Basic Setup」章にある「User Password Policy」セクションを参照してください。
- ersapi：ERS を有効にするには **yes** と入力し、ERS を拒否するには **no** と入力します。
- openapi：OpenAPI を有効にするには **yes** と入力し、OpenAPI を拒否するには **no** と入力します。
- pxGrid：pxGrid を有効にするには **yes** と入力し、pxGrid を拒否するには **no** と入力します。
- pxgrid_cloud：pxGrid Cloud を有効にするには **yes** と入力し、pxGrid Cloud を拒否するには **no** と入力します。pxGrid クラウドを有効にするには、pxGrid を有効にする必要があります。pxGrid を拒否して、pxGrid Cloud を有効にすると、pxGrid Cloud サービスは起動時に有効になりません。

Step 12 [次：ストレージの追加（Next: Add Storage）] をクリックします。

Step 13 [ステップ4 ：ストレージの追加（Step 4：Add Storage）] ウィンドウで、次の手順を実行します。

a) [サイズ（GiB）（Size (GiB)）] 列に値を入力します。

このフィールドの有効な範囲は 279.4 ー 2235.2 GiB です。実稼働環境では、558.8 GiB 以上のストレージを設定する必要があります。558.8 GiB 未満のストレージは、評価環境のみをサポートします。Cisco ISE は GB 単位で定義されたストレージで作成されることに注意してください。ここで入力した GiB 値は、Cisco ISE イメージの作成プロセス中に自動的に GB 値に変換されます。GB 単位の有効なストレージ範囲は 300 ー 2400 GB で、実稼働環境の Cisco ISE の最小値は 600 GB です。

b) [ボリュームタイプ（Volume Type）] ドロップダウンリストから [汎用 SSO（gp2）（General Purpose SSO (gp2)）] を選択します。

c) EBS 暗号化を有効にするには、[暗号化（Encryption）] ドロップダウンリストから暗号化キーを選択します。

Note

このウィンドウに表示される [新しいボリュームの追加（Add New Volume）] ボタンはクリックしないでください。

Step 14 [Next: Add Tags] をクリックします。

Step 15 （オプション）[ステップ5：タグの追加（Step 5：Add Tags）] ウィンドウで、[タグの追加（Add Tag）] をクリックし、[キー（Key）] フィールドと [値（Value）] フィールドに必要な情報を入力します。[インスタンス（Instances）]、[ボリューム（Volumes）]、および [ネットワーク インターフェイス（Network Interfaces）] カラムのチェックボックスは、デフォルトでオンになっています。[ステップ3 ：インスタンスの詳細の設定（Step 3：Configure Instance Details）] ウィンドウで特定のネットワーク インターフェイスを選択した場合は、このウィンドウで追加する各タグの [ネットワーク インターフェイス（Network Interfaces）] チェックボックスをオフにする必要があります。

Step 16 [次へ：セキュリティグループの設定（Next: Configure Security Group）] をクリックします。

Step 17 [ステップ6：セキュリティグループの設定（Step 6: Configure Security Group）] ウィンドウの [セキュリティグループ領域の割り当て（Assign a security group area）] 領域で、新しいセキュリティグループを作成するか、または対応するオプションボタンをクリックして、既存のセキュリティグループを選択できます。

a) [新しいセキュリティグループの作成（Create a new security group）] を選択した場合は、[タイプ（Type）]、[プロトコル（Protocol）]、[ポート範囲（Port Range）]、[送信元（Source）]、および [詳細（Description）] フィールドに必要な詳細情報を入力します。

b) [既存のセキュリティグループを選択（Select an existing security group）] を選択した場合は、追加するセキュリティグループの横にあるチェックボックスをオンにします。

Step 18 [確認して起動する（Review and Launch）] をクリックします。

Step 19 [ステップ7：インスタンス起動の確認（Step 7: Review Instance Launch）] ウィンドウで、このワークフローで作成したすべての構成を確認します。これらのセクションの値を編集するには、対応する [編集（Edit）] リンクをクリックします。

Step 20 [作成（Launch）] をクリックします。

Step 21 **[Select an existing key pair or create a new key pair]** ダイアログボックスで、ドロップダウンリストから次のいずれかのオプションを選択します。

- [既存のキーペアの選択（Choose an existing key pair）]
- [新しいキーペアの作成（Create a new key pair）]

Note
SSH を使用して Cisco ISE にログインするには、ユーザー名が **iseadmin** のキーペアを使用します。キーペアはそのままにしておく必要があります。キーペアが失われたり破損したりすると、新しいキーペアを既存のインスタンスにマッピングできないため、Cisco ISE を回復できません。

Step 22 確認応答ステートメントのチェックボックスをオンにして、[インスタンスの起動（Launch Instances）] をクリックします。

[起動ステータス（Launch Status）] ウィンドウに、インスタンス作成の進行状況が表示されます。

インストール後の注意事項とタスク

インスタンス起動のステータスを確認するには、AWS コンソールの左ペインで [インスタンス（Instances）] をクリックします。インスタンスの [ステータスのチェック（Status Check）] カラムには、インスタンスの設定中に [初期化中（Initializing）] が表示されます。インスタンスの準備が整い、使用可能になると、カラムに [xチェック完了（x checks done）] が表示されます。

Cisco ISE GUI または CLI には、Cisco ISE EC2 インスタンスが構築されてから約 30 分後にアクセスできます。AWS からインスタンスに提供される IP アドレスを使用して Cisco ISE の CLI および GUI にアクセスし、Cisco ISE 管理ポータルまたはコンソールにログインできます。

Cisco ISE インスタンスの準備が整い、使用可能になったら、次のステップを実行します。

1. AWS でキーペアを作成すると、キーペアをローカルシステムにダウンロードするように求められます。キーペアをダウンロードするのは、それに SSH ターミナルから Cisco ISE インスタンスへの正常なログインのために更新する必要がある、特定の権限が含まれているからです。

   Linux または MacOS を使用している場合は、CLI から次のコマンドを実行します。

   sudo chmod 0400 mykeypair.pem

   Windows を使用している場合：

   1. ローカルシステムのキーファイルを右クリックします。
   2. **[プロパティ（Properties）] > [セキュリティ（Security）] > [詳細設定（Advanced）]** の順に選択します。
   3. [権限（Permissions）] タブで、対応するオプションをクリックして適切なユーザーにフルコントロールを割り当て、[継承の無効化（Disable Inheritance）] をクリックします。
   4. [継承のブロック（Block Inheritance）] ダイアログボックスで、[継承された権限をこのオブジェクトの明示的な権限に変換する（Convert inherited permissions into explicit permissions on this object）] を選択します。
   5. [権限（Permissions）] タブの [権限エントリ（Permissions entries）] 領域で、対応するエントリをクリックしてシステムユーザーと管理者ユーザーを選択し、[削除（Remove）] をクリックします。
   6. **[適用（Apply）]** をクリックして、**[OK]** をクリックします。

2. CLI アプリケーションで次のコマンドを実行して、Cisco ISE CLI にアクセスします。

   ssh -i mykeypair.pem iseadmin@<*Cisco ISE Private IP Address*>

3. ログインプロンプトで、ユーザー名として **iseadmin** と入力します。
4. システム プロンプトで、**show application version ise** と入力し、Enter を押します。
5. Cisco ISE プロセスの状態を調べるには、**show application status ise** と入力し、Enter を押します。

アプリケーションサーバーが実行状態にあると出力に表示される場合は、Cisco ISE は使用可能です。

6. その後、Cisco ISE GUI にログインできます。
7. ご使用のリリースの『*Cisco ISE インストールガイド*』の「Installation Verification and Post-Installation Tasks」の章の「List of Post-Installation Tasks」に記載されているインストール後のタスクを実行します。

AWS における Cisco ISE の互換性情報

このセクションでは、AWS 上の Cisco ISE に固有の互換性情報について詳しく説明します。Cisco ISE の詳細については、『Cisco Identity Services Engine Network Component Compatibility, Release 3.1』を参照してください。

Cisco DNA Center の統合サポート

Cisco ISE を Cisco DNA Center リリース 2.2.1 以降のリリースに接続できます。

ロードバランサ統合のサポート

RADIUS トラフィックのロードバランシングのために、AWS ネイティブ ネットワーク ロード バランサ（NLB）を Cisco ISE と統合できます。ただし、次の注意事項が適用されます。

- 認可変更（CoA）機能は、NLB でクライアント IP の保存を有効にした場合にのみサポートされます。
- NLB は送信元 IP アフィニティのみをサポートし、発信側ステーション ID ベースのスティッキセッションをサポートしないため、不均等なロードバランシングが発生する可能性があります。
- NLB は RADIUS ベースの正常性チェックをサポートしていないため、RADIUS サービスがノードでアクティブでない場合でも、トラフィックを Cisco ISE PSN に送信できます。

TACACS トラフィックのロードバランシングのために、AWS ネイティブ ネットワーク ロード バランサ（NLB）を Cisco ISE と統合できます。ただし、NLB は TACACS+ サービスに基づくヘルスチェックをサポートしないため、ノードで TACACS サービスがアクティブでない場合でも、Cisco ISE PSN にトラフィックが送信されることがあります。

NIC ジャンボフレームサポート

Cisco ISE はジャンボフレームをサポートしています。Cisco ISE の最大伝送ユニット（MTU）は 9,001 バイトですが、ネットワーク アクセス デバイスの MTU は通常 1,500 バイトです。Cisco ISE は、標準フレームとジャンボフレームの両方を問題なくサポートし、受信します。コンフィギュレーション モードで Cisco ISE CLI を使用して、Cisco ISE MTU を必要に応じて再設定できます。

AWS での廃止された Amazon マシンイメージの取得

Amazon マシンイメージ（AMI）は、AWS で公開された日から 2 年後が自動で廃止日に設定されます。AWS は、廃止日以降のすべての AMI ID を非表示にします。つまり、AMI カタログまたは EC2 コンソールでイメージを確認することはできませんが、AMI ID で明示的に参照される場合は引き続き使用できます。廃止された AMI は、AWS Marketplace から、または AWS CLI を使用して取得できます。

AWS CLI を使用して廃止された AMI を取得する方法については、『Describe deprecated AMIs』を参照してください。

AWS Marketplace から廃止された AMI を取得するには、次の手順に従います。

Procedure

Step 1 AWS Marketplace にログインします。

Step 2 検索バーを使用して **ISE** を検索します。

Step 3 検索結果から [Cisco Identity Services Engine (ISE)] を選択します。

Step 4 **[引き続きサブスクライブする（Continue to Subscribe）]** をクリックして登録します。

Step 5 [設定を続行 (Continue to Configuration)] をクリックします。

Step 6 [Fulfillment Option] ドロップダウンリストで、[Amazon Machine Image] を選択します。

Step 7 [Software version] ドロップダウンリストから、必要なソフトウェアバージョンを選択します。

Step 8 [Region] ドロップダウンリストから必要なリージョンを選択します。

Step 9 [Continue to Launch] をクリックします

Step 10 [Choose Action] ドロップダウンリストから、[Launch through EC2] を選択します。

Step 11 [Launch] をクリックします。

新しいタブが開き、必要なリージョンと、インスタンスの起動に使用できる EC2 コンソールが表示されます。

Step 12 [Application and OS Images (Amazon Machine Image)] セクションの [AMI from catalog] タブから、選択したリージョンの廃止された AMI ID をコピーします。

AWS でのパスワードの回復とリセット

次のタスクでは、Cisco ISE 仮想マシンのパスワードをリセットするために役立つタスクについて説明します。必要なタスクを選択し、詳細な手順を実行します。

シリアルコンソールを介した Cisco ISE GUI パスワードの変更

Procedure

Step 1 AWS アカウントにログインし、EC2 ダッシュボードに移動します。

Step 2 左側のメニューから [インスタンス（Instances）] をクリックします。

Step 3 パスワードを変更する必要があるインスタンス ID をクリックします。パスワードがわかっている場合は、このタスクの手順 5 に進みます。

Step 4 シリアルコンソールにログインするには、インスタンスのインストール時に設定された元のパスワードを使用する必要があります。設定されたパスワードを表示するには、次の手順を実行します。

a) [アクション（Actions）] をクリックします。
b) [インスタンス設定（Instance Settings）] を選択します。
c) [ユーザーデータの編集（Edit user data）] をクリックします。

パスワードを含む現在のユーザーデータが表示されます。

Step 5 [接続（Connect）] をクリックします。

EC2 シリアルコンソールタブが表示されます。

Step 6 [接続（Connect）] をクリックします。

Step 7 新しいブラウザタブが表示されます。画面が黒い場合は、Enter を押してログインプロンプトを表示します。

Step 8 シリアルコンソールにログインします。手順4で表示されたパスワードが機能しない場合は、「パスワードの回復」セクションを参照してください。

Step 9 **application reset-passwd ise iseadmin** コマンドを使用して、iseadmin アカウントの新しい Web UI パスワードを設定します。

新しい公開キーペアの作成

このタスクを通じて、追加のキーペアをリポジトリに追加します。Cisco ISE インスタンスの設定時に作成された既存のキーペアは、新しく作成する公開キーに置き換えられません。

Procedure

Step 1 AWS で新しい公開キーを作成します。公開キーペアを作成する方法については、『Amazon EC2 インスタンスのキーペアを作成する』を参照してください。

Step 2 前のタスクで説明したように、AWS シリアルコンソールにログインします。

Step 3 公開キーを保存する新しいリポジトリを作成するには、プライベートリポジトリの作成を参照してください。

CLI を介してアクセスできるリポジトリがすでにある場合は、次の手順に進みます。

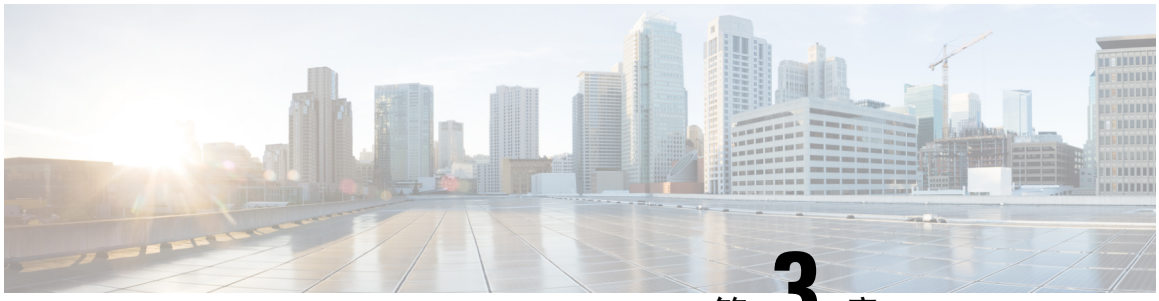
Step 4 新しい公開キーをインポートするには、コマンド **crypto key import <public key filename> repository <repository name>** を使用します。

Step 5 インポートが完了すると、新しい公開キーを使用して SSH 経由で Cisco ISE にログインできます。

パスワードの回復

AWS には Cisco ISE のパスワード回復のメカニズムはありません。新しい Cisco ISE インスタンスを作成し、設定データのバックアップと復元を実行する必要が生じる場合があります。

AWS で EC2 インスタンスのユーザーデータを編集しても、セットアップスクリプトが実行されないため、シリアルコンソールへのログインに使用される CLI パスワードは変更されません。Cisco ISE 仮想インスタンスは影響を受けません。



第 3 章

Azure Cloud Services 上の Cisco ISE

Azure Cloud 上の Cisco ISE

Cisco ISE は Azure Cloud Services で利用できます。Azure Cloud で Cisco ISE を設定してインストールするには、Azure Cloud の機能とソリューションについてよく理解しておく必要があります。開始する前に理解しておく必要がある Azure Cloud の概念は次のとおりです。

- サブスクリプションとリソースグループ
- Azure 仮想マシン：インスタンス、イメージ、SSH キー、タグ、VM のサイズ変更を参照してください。

Azure アプリケーションまたは AWS 仮想マシンを使用して、Cisco ISE をMicrosoft Azure に展開できます。Azure アプリケーションまたは Azure 仮想マシンを使用して Cisco ISE を展開しても、コストや Cisco ISE の機能に相違はありません。Azure アプリケーションは、Azure 仮想マシンと比較して次の利点があるため、Azure アプリケーションを使用することをお勧めします。

- Azure アプリケーションを使用すると、Azure 仮想マシン設定でのユーザーデータフィールドの代わりに、UI を使用して Cisco ISE 固有の選択肢を直接、簡単に設定できます。
- Azure アプリケーションの初期設定では、300 ～ 2400 GB の範囲の OS ディスクボリュームを選択できます。しかしながら、Azure 仮想マシンの初期設定中に、OS ディスクボリュームを、Azure ポータルのドロップダウンメニューによって示される固定値のセットに変更することはできます。仮想マシンを再設定するには、Cisco ISE をインストールして起動した後に、さらに手順を実行する必要があります。
- Cisco ISE がサポートする特定の Azure VM サイズから直接選択できます。

- 初期設定時に静的プライベート IPアドレスを設定できます。

次の場合に Azure 仮想マシンを使用できます。

- Cisco ISE を展開するために Azure ポータル UI を使用しない場合。
- Azure 仮想マシンの設定ワークフローで使用可能な追加設定のいずれかを使用する必要がある場合。

次のタスクフローでは、 Azure アプリケーションまたは Azure 仮想マシンを使用して Microsoft Azure に Cisco ISE を展開する手順を示します。

- Azure アプリケーションを使用した Cisco ISE インスタンスの作成 （35 ページ）
- Azure 仮想マシンを使用した Cisco ISE インスタンスの作成 （31 ページ）

Cisco ISE は、次の Azure VM サイズのいずれかを使用してインストールできます。

表 *2 : Cisco ISE* でサポートされる *Azure VM* サイズ

Azure VM サイズ	vCPU	RAM（GB）
Standard_D4s_v4 （このインスタンスは、Cisco ISE 評価のユースケースをサポートしています。100 の同時アクティブエンドポイントがサポートされています）	4	16
Standard_D8s_v4	8	32
Standard_F16s_v2	16	32
Standard_F32s_v2	32	64
Standard_D16s_v4	16	64
Standard_D32s_v4	32	128
Standard_D64s_v4	64	256

Fsv2 シリーズの Azure VM サイズはコンピューティングに最適化され、コンピューティング集約型のタスクやアプリケーションの PSN として使用するのに最適です。

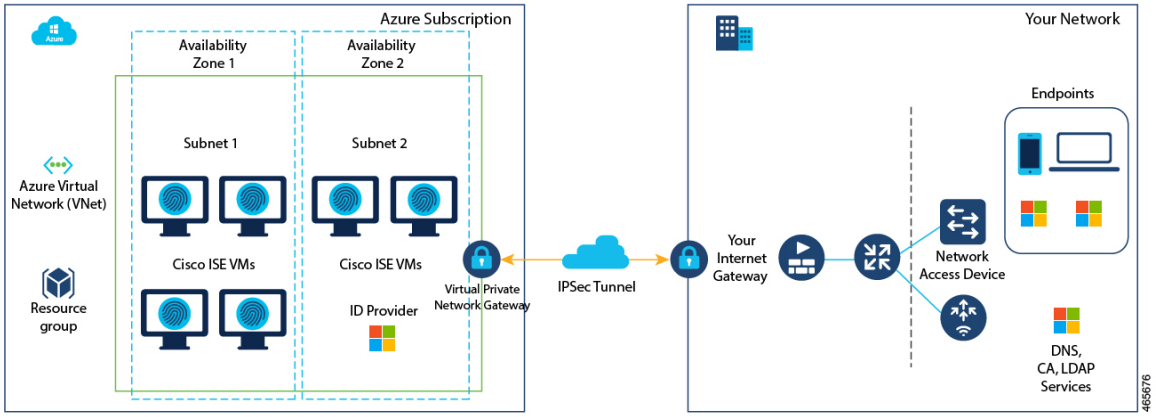
Dsv4 シリーズは、PAN または MnT ノード、またはその両方としての使用に最適な汎用の Azure VM サイズであり、データ処理タスクとデータベース操作を目的としています。

汎用インスタンスをPSNとして使用する場合、パフォーマンスの数値は、PSNとしてのコンピューティング最適化インスタンスのパフォーマンスよりも低くなります。

Standard_D8s_v4 VM サイズは、極小規模の PSN としてのみ使用する必要があります。

Azure VM サイズのスケールおよびパフォーマンスデータについては、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

図 *2 : Azure Cloud* に接続された展開の例



（注） Cisco ISE インスタンスを作成するために、既存の Azure Cloud イメージを複製しないでください。

上記の手順に加えて、シスコが開発した次のソリューションを使用して、Azure にマルチノード Cisco ISE 展開をインストールして自動的に作成することもできます。

- シスコが開発した Terraform スクリプト

Microsoft Azure Cloud Services での Cisco ISE の既知の制限事項

- Azure アプリケーションを使用した Cisco ISE インスタンスの作成 を作成すると、Microsoft Azure はデフォルトで DHCP サーバーを介して VM にプライベート IP アドレスを割り当てます。Microsoft Azure で Cisco ISE 展開を作成する前に、Microsoft Azure によって割り当てられた IP アドレスを使用して、フォワードおよびリバース DNS エントリを更新する必要があります。

  または、Cisco ISE をインストールした後、Microsoft Azure でネットワーク インターフェイス オブジェクトを更新して、VM に静的 IP アドレスを割り当てます。

  1. VM を停止します。
  2. VM の [プライベートIPアドレス設定（Private IP address settings）] エリアの [割り当て（Assignment）] エリアで、[静的（Static）] をクリックします。
  3. VM を再起動します。
  4. Cisco ISE シリアルコンソールで、IP アドレスを Gi0 として割り当てます。
  5. Cisco ISE アプリケーションサーバーを再起動します。

- デュアル NIC は、2 つの NIC のみ（ギガビットイーサネット 0 とギガビットイーサネット 1 のみ）でサポートされます。Cisco ISE インスタンスでセカンダリ NIC を設定するには、まず Azure でネットワーク インターフェイス オブジェクトを作成し、Cisco ISE インスタンスの電源をオフにしてから、このオブジェクトを Cisco ISE にアタッチします。Azure に Cisco ISE をインストールして起動したら、Cisco ISE CLI を使用して、ネットワーク インターフェイス オブジェクトの IP アドレスをセカンダリ NIC として手動で設定します。

- Cisco ISE アップグレードワークフローは、Microsoft Azure 上 の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。ハイブリッド Cisco ISE 展開のアップグレードについては、『Upgrade Guidelines for Hybrid Deployments』を参照してください。

- パブリッククラウドはレイヤ 3 機能のみをサポートします。Microsoft Azure 上の Cisco ISE ノードは、レイヤ 2 の機能に依存する Cisco ISE 機能をサポートしません。たとえば、Cisco ISE CLI を介した DHCP SPAN プロファイラプローブおよび CDP プロトコル機能の使用は、現在サポートされていない機能です。

- 設定データの復元およびバックアップ機能を実行する場合、バックアップ操作が完了した後、まず CLI から Cisco ISE を再起動します。次に、Cisco ISE GUI から復元操作を開始します。Cisco ISE のバックアップおよび復元プロセスの詳細については、お使いのバージョンのリリースの『Cisco ISE Administrator Guide』の「Maintain and Monitor」の章を参照してください。

- パスワードベースの認証を使用した Cisco ISE CLI への SSH アクセスは、Azure ではサポートされていません。キーペアを介してのみ Cisco ISE CLI にアクセスでき、このキーペアは安全に保存する必要があります。

  秘密キー（または PEM）ファイルを使用していてそのファイルを失った場合、Cisco ISE CLI にアクセスできなくなります。

  パスワードベースの認証方式を使用して Cisco ISE CLI にアクセスする統合は、サポートされていません（たとえば、Cisco DNA Center リリース 2.1.2 以前）。

- Gen 8 の Azure の VPN ゲートウェイは、フラグメンテーションの結果として使用できません。これは、Azure のファースト パーティ ゲートウェイの制限です。

- Azure では、ネットワーキング仮想ネットワークスタックは、順序が不正なフラグメントを仮想マシンのエンドホストに転送せずにドロップします。この設計は、『Azure and fragmentation』[英語] で文書化されているように、ネットワークセキュリティの脆弱性である FragmentSmack に対処することを目的としています。

  Azure での Cisco ISE 展開では、通常、Dynamic Multipoint Virtual Private Network（DMVPN; ダイナミックマルチポイント仮想プライベートネットワーク）やソフトウェア定義型ワイドエリアネットワーク（SD-WAN）などの VPN ソリューションを利用します。これらのネットワークでは、IPsec トンネルのオーバーヘッドによって MTU とフラグメンテーションの問題が発生する可能性があります。このようなシナリオでは、Cisco ISE は完全な RADIUS パケットを受信せず、認証エラーが発生しても障害のエラーログが生成されません。

  この既知の問題により、次のいずれかを実行してください。

1. Azure Cloud がすでに修正を実装しているリージョンである東アジア（eastasia）と米国中西部（westcentralus）を選択します。
2. Cisco ISE のお客様は、Azure サポートチケットを作成する必要があります。Microsoftは、次の措置を講じることに同意しています。
    1. サブスクリプションを固定し、そのサブスクリプションのすべてのインスタンスが第 7 世代ハードウェアに展開されるようにします。
    2. [allow out-of-order fragment] オプションを有効にします。これにより、フラグメントはドロップされるのではなく、宛先にパススルーされます。

- Azure クラウドでの Cisco ISE 展開では、Accelerated Networking 機能はサポートされていません。Cisco ISE 展開のいずれかの段階でこの機能を有効にすると、ノードの登録や登録解除などの操作が失敗する可能性があります。

Azure 仮想マシンを使用した Cisco ISE インスタンスの作成

Before you begin

- SSH キー ペアを生成します。
- 必要な VN のゲートウェイ、サブネット、およびセキュリティグループを作成します。
- Cisco ISE で使用するサブネットは、インターネットにアクセスできる必要があります。Microsoft Azure の [Public Route Table] ウィンドウで、サブネットの次のホップをインターネットとして設定します。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Procedure

Step 1 https://portal.azure.com に移動して Microsoft Azure アカウントにログインします。

Step 2 ウィンドウの上部にある検索フィールドを使用して、**マーケットプレイス**を検索します。

Step 3 [マーケットプレイスの検索（Search the Marketplace）] 検索フィールドを使用して、**Cisco Identity Services Engine**（**ISE**）を検索します。

Step 4 [Virtual Machine] をクリックします。

Step 5 表示される新しいウィンドウで、[作成（Create）] をクリックします。

Step 6 [基本（Basics）] タブで次の手順を実行します。

a) [プロジェクトの詳細（Project details）]エリアで、[サブスクリプション（Subscription）]および[リソースグループ（Resource group）] ドロップダウンリストから必要な値を選択します。

b) [インスタンスの詳細（Instance details）] エリアで、[仮想マシン名（Virtual Machine name）] フィールドに値を入力します。

c) [イメージ（Image）] ドロップダウンリストから、Cisco ISE イメージを選択します。

d) [サイズ（Size）] ドロップダウンリストから、Cisco ISE をインストールするインスタンスサイズを選択します。Azure Cloud 上の Cisco ISE, on page 27 のセクションの **Cisco ISE でサポートされる Azure Cloud インスタンス**というタイトルの表にリストされているように、Cisco ISE でサポートされるインスタンスを選択します。

e) [管理者アカウント（Administrator account）]>[認証タイプ（Authentication type）]エリアで、[SSH公開キー（SSH Public Key）] オプションボタンをクリックします。

f) [ユーザー名（Username）] フィールドに **iseadmin** と入力します。

Note
許可されているユーザー名は **iseadmin** のみです。他のユーザー名の使用はサポートされていません。

g) [SSH公開キーソース（SSH public key source）] ドロップダウンリストから、[Azureに保存されている既存のキーを使用（Use existing key stored in Azure）] を選択します。

h) [保存されたキー（Stored keys）] ドロップダウンリストから、このタスクの前提条件として作成したキーペアを選択します。

i) [受信ポートの規則（Inbound port rules）] エリアで、[選択されたポートを許可する（Allow selected ports）] オプションボタンをクリックします。

j) [受信ポートの選択（Select inbound ports）] ドロップダウンリストから、アクセスを許可するすべてのプロトコルポートを選択します。

k) [ライセンス（Licensing）]エリアの[ライセンスタイプ（Licensing type）] ドロップダウンリストから、[その他（Other）] を選択します。

Step 7 [次へ：ディスク（Next: Disks）] をクリックします。

Step 8 [Disks] タブで、[OS Disk Size] ドロップダウンリストからディスク サイズを選択するか、デフォルト値をそのまま使用します。

Note
[Key Management] フィールドでは、ディスク暗号化にカスタマーマネージドキーを使用することをお勧めします。デフォルトでは、プラットフォーム管理キーが使用されます。キーの作成の詳細については、『About encryption key management』[英語]を参照してください。

残りの必須フィールドについては、デフォルト値をそのまま使用できます。

Step 9 [Next: Networking] をクリックします。

Step 10 [ネットワークインターフェイス（Network Interface）]エリアで、[仮想ネットワーク（Virtual network）]、[サブネット（Subnet）]、および [ネットワークセキュリティグループの設定（Configure network security group）] ドロップダウンリストから、作成した仮想ネットワークとサブネットを選択します。

パブリック IP アドレスを持つサブネットは、オンラインおよびオフラインのポスチャフィードの更新を受信しますが、プライベート IP アドレスを持つサブネットは、オフラインのポスチャフィードの更新のみを受信することに注意してください。

Step 11 [次へ：管理（Next: Management）] をクリックします。

Step 12 [管理（Management）] タブで、必須フィールドのデフォルト値をそのままにして、[次へ：詳細設定（Next: Advanced）] をクリックします。

Step 13 [ユーザーデータ（User data）] エリアで、[ユーザーデータを有効にする（Enable user data）] チェックボックスをオンにします。

[ユーザーデータ（User data）] フィールドに次の情報を入力します。

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

tertiarynameserver=<*IPv4 address of tertiary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important
Cisco ISE リリース 3.4 以降、

a. [ntpserver] フィールド名が [primaryntpserver] に変更されました。[ntpserver] を使用すると、Cisco ISE サービスは起動しません。

b. OpenAPI はデフォルトで有効になっています。したがって、[openapi=<yes/no>] フィールドは必須ではありません。

c. [secondarynameserver] フィールドを空白のままにして、[tertiarynameserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

d. [secondaryntpserver] フィールドを空白のままにして、[tertiaryntpserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

ユーザーデータエントリを使用して設定する各フィールドには、正しいシンタックスを使用する必要があります。[ユーザーデータ（User Data）] フィールドに入力した情報は、入力時に検証されません。誤った構文を使用すると、イメージの起動時に Cisco ISE サービスが表示されないことがあります。次に、[ユーザーデータ（User Data）] フィールドを使用して送信する設定のガイドラインを示します。

- hostname：英数字とハイフン（-）のみを含むホスト名を入力します。ホスト名の長さは 19 文字以下で、下線（_）を含めることはできません。
- プライマリネームサーバー：プライマリネームサーバーの IP アドレス。サポートされているのは IPv4 アドレスだけです。

  この手順では、1 つの DNS サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して DNS サーバーを追加できます。ただし、Cisco ISE リリース 3.4 以降では、インストール時に [secondarynameserver] および [tertiarynameserver] フィールドを使用して、セカンダリおよびターシャリネームサーバーを設定できます。
- dnsdomain：DNS ドメインの FQDN を入力します。エントリには、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）を含めることができます。
- ntpserver：同期に使用する NTP サーバーの IPv4 アドレスまたは FQDN を入力します（例：time.nist.gov）。

  この手順では、1 つの NTP サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して NTP サーバーを追加できます。ただし、Cisco ISE リリース 3.4 以降では、インストール中に [secondaryntpserver] および [tertiaryntpserver] フィールドを使用して、セカンダリおよびターシャリ NTP サーバーを設定できます。
- timezone：タイムゾーンを入力します（例：Etc/UTC）。すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されるようにします。
- password：Cisco ISE への GUI ベースのログインのパスワードを設定します。入力するパスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。パスワードは 6 ～ 25 文字で、少なくとも 1 つの数字、1 つの大文字、および 1 つの小文字を含める必要があります。パスワードは、ユーザー名またはその逆（iseadmin または nimdaesi）、cisco、または ocsic と同じにすることはできません。使用できる特殊文字は @~*!,+=_- です。ご使用のリリースの『Cisco ISE Administrator Guide』の「Basic Setup」章にある「User Password Policy」セクションを参照してください。
- ersapi：ERS を有効にするには **yes** と入力し、ERS を拒否するには **no** と入力します。
- openapi：OpenAPI を有効にするには **yes** と入力し、OpenAPI を拒否するには **no** と入力します。
- pxGrid：pxGrid を有効にするには **yes** と入力し、pxGrid を拒否するには **no** と入力します。
- pxgrid_cloud：pxGrid Cloud を有効にするには **yes** と入力し、pxGrid Cloud を拒否するには **no** と入力します。pxGrid クラウドを有効にするには、pxGrid を有効にする必要があります。pxGrid を無効にして pxGrid クラウドを有効にすると、pxGrid クラウドサービスは起動時に有効になりません。

Step 14 [次へ：タグ（Next: Tag）] をクリックします。

Step 15 リソースを分類し、複数のリソースとリソースグループを統合できる名前と値のペアを作成するには、[名前（Name）] フィールドと [値（Value）] フィールドに値を入力します。

Step 16 [次へ：確認して作成（Next: Review + Create）] をクリックします。

Step 17 これまでに提供した情報を確認し、[作成（Create）] をクリックします。

[展開が進行中です（Deployment is in progress）] ウィンドウが表示されます。Cisco ISE インスタンスが作成されて使用できるようになるまで、約 30 分かかります。Cisco ISE VM インスタンスが [仮想マシン（Virtual Machines）] ウィンドウに表示されます（ウィンドウを見つけるには、メインの検索フィールドを使用します）。

What to do next

Note このセクションは、Cisco ISE VM のディスクサイズが 300 GB の場合にのみ適用されます。他のディスクサイズを選択した場合、これらの手順は適用されません。

Microsoft Azure のデフォルト設定により、作成した Cisco ISE VM は 300 GB のディスクサイズのみで設定されます。通常、Cisco ISE ノードには 300 GB を超えるディスクサイズが必要です。Microsoft Azure から Cisco ISE を初めて起動したときに、**仮想メモリ不足**のアラームが表示される場合があります。

Cisco ISE VM の作成が完了したら、Cisco ISE 管理ポータルにログインして、Cisco ISE が設定されていることを確認します。その後、Microsoft Azure ポータルで、[Virtual Machines] ウィンドウで次の手順を実行して、ディスクサイズを編集します。

1. Cisco ISE インスタンスを停止します。
2. 左ペインで [ディスク（Disk）] をクリックし、Cisco ISE で使用しているディスクをクリックします。
3. 左ペインで [サイズとパフォーマンス（Size + performance）] をクリックします。
4. [カスタムディスクサイズ（Custom disk size）] フィールドに、必要なディスクサイズを GiB 単位で入力します。

Azure アプリケーションを使用した Cisco ISE インスタンスの作成

Before you begin

リソースグループ、仮想ネットワーク、サブネット、SSH キーなど、必要な Azure リソースを作成します。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になります。したがって、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Procedure

Step 1 https://portal.azure.com に移動し Azure ポータルにログインします。

Step 2 ウィンドウの上部にある検索フィールドを使用して、**マーケットプレイス**を検索します。

Step 3 [マーケットプレイスの検索（Search the Marketplace）] 検索フィールドを使用して、**Cisco Identity Services Engine（ISE）**を検索します。

Step 4 [Azure Application] をクリックします。

Step 5 表示される新しいウィンドウで、[作成（Create）] をクリックします。
5 つの手順のワークフローが表示されます。

Step 6 [基本（Basics）] タブで次の手順を実行します。

a) [リソースグループ（Resource Group）] ドロップダウンリストから、Cisco ISE に関連付けるオプションを選択します。

b) [リージョン（Region）] ドロップダウンリストから、リソースグループが配置されているリージョンを選択します。

c) [ホスト名（Hostname）] フィールドに、ホスト名を入力します。

d) [タイムゾーン（Time Zone）] ドロップダウンリストから、タイムゾーンを選択します。

e) [VMサイズ（VM Size）] ドロップダウンリストから、Cisco ISE に使用する Azure VM サイズを選択します。

f) [Disk Encryption Key] ドロップダウンリストから、ディスク暗号化のキーを選択します。

Note
[Disk Encryption Key] フィールドでは、ディスク暗号化にカスタマーマネージドキーを使用することをお勧めします。デフォルトでは、プラットフォーム管理キーが使用されます。このフィールドは、Cisco ISE リリース 3.3 以降で使用できます。詳細については、『About encryption key management』[英語]を参照してください。

g) [ディスクストレージタイプ（Disk Storage Type）] ドロップダウンリストからオプションを選択します。

h) [ボリュームサイズ（Volume Size）] フィールドに、Cisco ISE インスタンスに割り当てるボリュームを GB 単位で入力します。600 GB がデフォルト値です。

Step 7 **[Next]** をクリックします。

Step 8 [ネットワーク設定（Network Settings）] タブで次の手順を実行します。

a) [仮想ネットワーク（Virtual Network）] ドロップダウンリストで、選択したリソースグループで使用可能な仮想ネットワークのリストからオプションを選択します。

b) [サブネット（Subnet）] ドロップダウンリストで、選択した仮想グループに関連付けられたサブネットのリストからオプションを選択します。

c) (Optional) [ネットワークセキュリティグループ（Network Security Group）] ドロップダウンリストで、選択したリソースグループのセキュリティグループのリストからオプションを選択します。

d) [SSH公開キーソース（SSH public key source）] ドロップダウンリストから、対応するオプションをクリックして、新しいキーペアを作成するか、既存のキーペアを使用するかを選択します。

e) 前の手順で [Azureに保存されている既存のキーを使用（Use existing key stored in Azure）] オプションを選択した場合は、[保存されたキー（Stored Keys）] ドロップダウンリストから、使用するキーを選択します。

f) 静的 IP アドレスを Cisco ISE に割り当てるには、[プライベートIPアドレス（Private IP address）] フィールドに IP アドレスを入力します。この IP アドレスが、選択したサブネット内の他のリソースによって使用されていないことを確認してください。

g) [パブリックIPアドレス（Public IP Address）] ドロップダウンリストで、Cisco ISE で使用するアドレスを選択します。このフィールドを空白のままにすると、パブリック IP アドレスが Azure DHCP サーバーによってインスタンスに割り当てられます。

h) [DNS名（DNS Name）] フィールドに DNS ドメイン名を入力します。

この手順では、1 つの DNS サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して DNS サーバーを追加できます。

i) [ネームサーバー（Name Server）] フィールドに、ネームサーバーの IP アドレスを入力します。

Note
Cisco ISE リリース 3.4 以降、[Name Server] フィールドの名前が [Primary Name Server] に変更されました。

[Secondary Name Server] フィールドには、セカンダリネームサーバーの IP アドレスまたはホスト名を入力します。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。

[Tertiary Name Server] フィールドには、ターシャリネームサーバーの IP アドレスを入力します。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。このフィールドを使用してアプリケーションを正常に起動するには、[Secondary Name Server] フィールドを空白のままにしないでください。

Note
入力した IP アドレスが正しくない、または到達不能な場合、Cisco ISE サービスが起動しない可能性があります。

j) [NTPサーバー（NTP Server）] フィールドに、NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。

Note
Cisco ISE リリース 3.4 以降、[NTP Server] フィールドの名前が [Primary NTP Server] に変更されました。

[Secondary NTP Server] フィールドには、セカンダリ NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。

[Tertiary NTP Server] フィールドに、ターシャリ NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。このフィールドを使用してアプリケーションを正常に起動するには、[Secondary NTP Server] フィールドを空白のままにしないでください。

Note
入力した IP アドレスが正しくない、または到達不能な場合、Cisco ISE サービスが起動しない可能性があります。

この手順では、1 つの NTP サーバーのみを追加できます。インストール後に、Cisco ISE CLI を使用して NTP サーバーを追加できます。

Step 9 **[Next]** をクリックします。

Step 10 [サービス（Service）] タブで次の手順を実行します。

a) [ERS] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

b) [オープンAPI（Open API）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

Note
Cisco ISE リリース 3.4 以降、OpenAPI はデフォルトで有効になっています。したがって、このフィールドは使用できません。

c) [pxGrid] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

d) [pxGridクラウド（pxGrid Cloud）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

Step 11 **[Next]** をクリックします。

Step 12 [ユーザーの詳細（User Details）] タブで次の手順を実行します。

a) [iseadminのパスワードの入力（Enter Password for iseadmin）] および [パスワードの確認（Confirm Password）] フィールドに、Cisco ISE のパスワードを入力します。パスワードは Cisco ISE のパスワードポリシーに準拠し、最大 25 文字である必要があります。

Step 13 **[Next]** をクリックします。

Step 14 [確認して作成（Review + create）] タブで、インスタンスの詳細を確認します。

Step 15 [作成（Create）] をクリックします。

[概要（Overview）] ウィンドウに、インスタンス作成プロセスの進行状況が表示されます。

Step 16 検索バーを使用して、[仮想マシン（Virtual Machines）] ウィンドウに移動します。作成した Cisco ISE インスタンスがウィンドウにリストされ、[ステータス（Status）] は [作成中（Creating）] になります。Cisco ISE インスタンスの作成には約 30 分かかります。

インストール後のタスク

Cisco ISE インスタンスを正常に作成した後に実行する必要があるインストール後のタスクについては、お使いのバージョンの Cisco ISE リリースの『Cisco ISE Installation Guide』の「Installation Verification and Post-Installation Tasks」の章を参照してください。

Azure Cloud 上の Cisco ISE の互換性情報

このセクションでは、Azure Cloud 上の Cisco ISE に固有の互換性情報について詳しく説明します。Cisco ISE の一般的な互換性の詳細については、お使いのバージョンのリリースの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

ロードバランサ統合のサポート

RADIUS トラフィックのロードバランシングのために、Azure ロードバランサを Cisco ISE と統合できます。ただし、次の注意事項が適用されます。

- 認可変更（CoA）機能は、Azure portal のロードバランシングルールでセッションの永続性のプロパティを設定するときにクライアント IP の保存を有効にしている場合にのみサポートされます。
- Azure ロードバランサは送信元 IP アフィニティのみをサポートし、発信側ステーションの ID ベースのスティッキセッションをサポートしないため、不均等なロードバランシングが発生する可能性があります。
- Azure ロードバランサは RADIUS ベースの正常性チェックをサポートしていないため、RADIUS サービスがノードでアクティブでない場合でも、トラフィックを Cisco ISE PSN に送信できます。

Azure ロードバランサの詳細については、『What is Azure Load Balancer?』を参照してください。

TACACS トラフィックのロードバランシングのために、Azure ロードバランサを Cisco ISE と統合できます。ただし、Azure ロードバランサは TACACS+ サービスに基づく正常性チェックをサポートしないため、ノードで TACACS サービスがアクティブでない場合でも、Cisco ISE PSN にトラフィックが送信されることがあります。

Azure Cloud でのパスワードの回復とリセット

次のタスクでは、Cisco ISE 仮想マシンのパスワードをリセットまたは回復するために役立つタスクについて説明します。必要なタスクを選択し、詳細な手順を実行します。

（注） Azure ポータルの [Help] > [Reset Password] オプションは、Cisco ISE Azure VM ではサポートされていません。

シリアルコンソールを介した Cisco ISE GUI パスワードのリセット

Procedure

Step 1 Azure Cloud にログインし、Cisco ISE 仮想マシンを含むリソースグループを選択します。

Step 2 リソースのリストから、パスワードをリセットする Cisco ISE インスタンスをクリックします。

Step 3 左側のメニューの **[Help]** セクションで、[Serial console] をクリックします。

Step 4 ここでエラーメッセージが表示された場合は、次の手順を実行してブート診断を有効にする必要がある場合があります。

a) 左側のメニューから、[ブート診断（Boot diagnostics）] をクリックします。

b) [カスタムストレージアカウントで有効にする（Enable with custom storage account）] をクリックします。

c) ストレージアカウントを選択し、[保存（Save）] をクリックします。

Step 5 左側のメニューの **[Help]** セクションで、[Serial console] をクリックします。

Step 6 Azure Cloud Shell が新しいウィンドウに表示されます。

Step 7 画面が黒い場合は、Enter を押してログインプロンプトを表示します。

Step 8 シリアルコンソールにログインします。

シリアルコンソールにログインするには、インスタンスのインストール時に設定された元のパスワードを使用する必要があります。このパスワードを覚えていない場合は、「パスワードの回復」セクションを参照してください。

Step 9 **application reset-passwd ise iseadmin** コマンドを使用して、iseadmin アカウントの新しい GUI パスワードを設定します。

SSH アクセスのための新しい公開キーペアの作成

このタスクを通じて、追加のキーペアをリポジトリに追加します。Cisco ISE インスタンスの設定時に作成された既存のキーペアは、新しく作成する公開キーに置き換えられません。

Procedure

Step 1 Azure Cloud で新しい公開キーを作成します。『Generate and store SSH keys in the Azure portal』を参照してください。

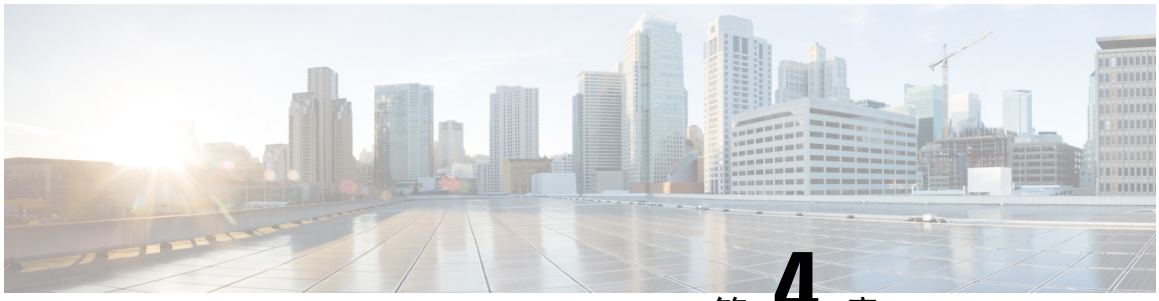
Step 2 前のタスクで説明したように、Azure Cloud シリアルコンソールにログインします。

Step 3 公開キーを保存する新しいリポジトリを作成するには、『Azure Repos documentation』を参照してください。

CLI を介してアクセスできるリポジトリがすでにある場合は、手順 4 に進みます。

Step 4 新しい公開キーをインポートするには、コマンド **crypto key import <public key filename> repository <repository name>** を使用します。

Step 5 インポートが完了すると、新しい公開キーを使用して SSH 経由で Cisco ISE にログインできます。



第 4 章

Oracle Cloud Infrastructure（OCI）上の Cisco ISE

Oracle Cloud Infrastructure（OCI）上の Cisco ISE

Cisco ISE は Oracle Cloud Infrastructure（OCI）で使用できます。OCI で Cisco ISE を設定してインストールするには、OCI のいくつかの機能とソリューションについてよく理解しておく必要があります。開始する前に理解しておく必要がある概念には、コンパートメント、可用性ドメイン、イメージとシェイプ、ブートボリュームなどがあります。OCI のコンピューティングリソースの単位は、Oracle CPU（OCPU）です。1 つの OCPU は、2 つの vCPU に相当します。

『Oracle Cloud Infrastructure Documentation』を参照してください。

Cisco ISE は、イメージとスタックの 2 つの形式で OCI で利用できます。Cisco ISE ユーザーが使いやすいようにカスタマイズされていることから、スタックタイプを使用して Cisco ISE をインストールすることをお勧めします。

- Terraform スタックファイルを使用した OCI での Cisco ISE インスタンスの作成（49 ページ）
- OCI での Cisco ISE インスタンスの作成（45 ページ）

表 *3 : Cisco ISE* でサポートされる *OCI* インスタンス

OCI インスタンス	OCPU	OCI インスタンスメモリ（GB 単位）

Oracle Cloud Infrastructure（OCI）上の Cisco ISE

Standard3.Flex （このインスタンスは、Cisco ISE 評価のユースケースをサポートしています。100 の同時アクティブエンドポイントがサポートされています）	2	16
Optimized3.Flex	8	32
	16	64
Standard3.Flex	4	32
	8	64
	16	128
	32	256

Optimized3.Flex シェイプはコンピューティングに最適化され、コンピューティング集約型のタスクやアプリケーションの PSN として使用するのに最適です。

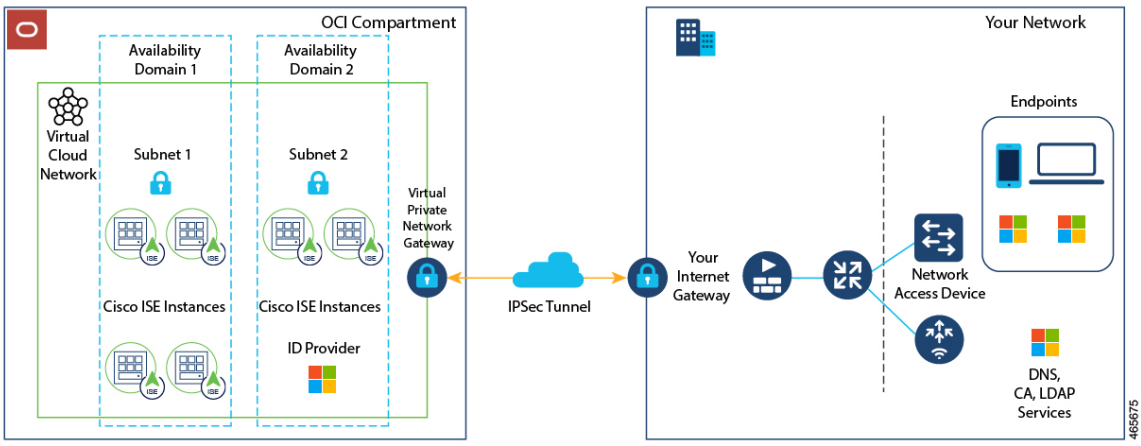
Standard3.Flex シェイプは、PAN または MnT ノード、またはその両方としての使用に最適な汎用のシェイプであり、データ処理タスクとデータベース操作を目的としています。

汎用インスタンスを PSN として使用する場合、パフォーマンスの数値は、PSN としてのコンピューティング最適化インスタンスのパフォーマンスよりも低くなります。

Standard3.Flex（4 OCPU、32 GB）シェイプは、極小規模の PSN としてのみ使用する必要があります。

OCI インスタンスタイプのスケールおよびパフォーマンスデータについては、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

図 *3 : Oracle Cloud* に接続された展開の例



（注） Cisco ISE インスタンスを作成するために既存の OCI イメージを複製しないでください。

OCI 上の Cisco ISE の使用に関する既知の制限事項

- Cisco ISE アップグレードワークフローは、OCI 上 の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。ハイブリッド Cisco ISE 展開のアップグレードについては、『Upgrade Guidelines for Hybrid Deployments』を参照してください。
- パブリッククラウドはレイヤ 3 機能のみをサポートします。OCI 上の Cisco ISE ノードは、レイヤ 2 の機能に依存する Cisco ISE 機能をサポートしません。たとえば、Cisco ISE CLI を介した DHCP SPAN プロファイラプローブおよび CDP プロトコル機能の使用は、現在サポートされていない機能です。
- Cisco ISE で IPv6 アドレスを有効にするには、Cisco ISE の OCI ポータルで IPv6 アドレスを設定し、インターフェイス ギガビット イーサネット 0 を再起動します。Cisco ISE シリアルコンソールに管理者としてログインし、次のコマンドを実行します。

```
#configure terminal
Entering configuration mode terminal
(config)#interface GigabitEthernet 0
(config-GigabitEthernet-0)#shutdown
(config-GigabitEthernet-0)#no shutdown
(config-GigabitEthernet-0)#exit
(config)#exit
```

- 設定データの復元およびバックアップ機能を実行する場合、バックアップ操作が完了した後、まず CLI から Cisco ISE を再起動します。次に、Cisco ISE GUI から復元操作を開始します。Cisco ISE のバックアップおよび復元プロセスの詳細については、お使いのバージョンのリリースの『Cisco ISE Administrator Guide』の「Maintain and Monitor」の章を参照してください。
- パスワードベースの認証を使用した Cisco ISE CLI への SSH アクセスは、OCI ではサポートされていません。キーペアを介してのみ Cisco ISE CLI にアクセスできます。このキーペアを安全に保管してください。

  秘密キー（または PEM）ファイルを使用していてそのファイルを失った場合、Cisco ISE CLI にアクセスできません。

  パスワードベースの認証方式を使用して Cisco ISE CLI にアクセスする統合は、サポートされていません（たとえば、Cisco DNA Center リリース 2.1.2 以前）。

OCI での Cisco ISE インスタンスの作成

Before you begin

- 次のタスクの手順 3 を開始する前に、コンパートメント、カスタムイメージ、シェイプ、仮想クラウドネットワーク、サブネット、およびサイト間 VPN を作成します。

Cisco ISE インスタンスを作成するのと同じコンパートメントに仮想クラウドネットワークとサブネットを作成します。

- Cisco ISE で使用する仮想クラウドネットワークを作成するときは、[Create VCN with Internet Connectivity] VCN タイプを選択することをお勧めします。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Procedure

Step 1 OCI アカウントにログインします。

Step 2 検索フィールドを使用して、**マーケットプレイス**を検索します。

Step 3 [リストの検索（Search for listings...）] の検索フィールドで、**Cisco Identity Services Engine**（**ISE**）と入力します。

Step 4 **イメージ**タイプの Cisco ISE オプションをクリックします。

Step 5 表示される新しいウィンドウで、[インスタンスの起動（Launch Instances）] をクリックします。

Step 6 左ペインの [リストスコープ（List Scope）] エリアで、[コンパートメント（Compartment）] ドロップダウンリストからコンパートメントを選択します。

Step 7 右ペインで [インスタンスの作成（Create Instance）] をクリックします。

Step 8 [Create Compute Instance] ウィンドウの [Name] フィールドに、Cisco ISE インスタンスの名前を入力します。

Step 9 [コンパートメントに作成（Create in Compartment）] ドロップダウンリストから、Cisco ISE インスタンスを作成する必要があるコンパートメントを選択します。Cisco ISE で使用する仮想クラウドネットワークやサブネットなどの他のリソースを作成したコンパートメントを選択する必要があります。

Step 10 [配置（Placement）]エリアで可用性ドメインをクリックします。ドメインによって利用可能なコンピューティングシェイプが決められます。

Step 11 [イメージとシェイプ（Image and Shape）] エリアで次の手順を実行します。

a) [イメージの変更（Change Image）] をクリックします。
b) [イメージソース（Image Source）] ドロップダウンリストから、[カスタムイメージ（Custom Image）] を選択します。
c) 必要なカスタムイメージ名の横にあるチェックボックスをオンにします。
d) [イメージの選択（Select Image）] をクリックします。
e) [イメージとシェイプ（Image and Shape）] エリアから、[シェイプの変更（Change Shape）] をクリックします。
f) [シェイプシリーズ（Shape Series）]エリアから、[Intel] をクリックします。使用可能なシェイプのリストが表示されます。
g) 必要なシェイプ名の横にあるチェックボックスをオンにします。[シェイプの選択（Select Shape）] をクリックします。

Step 12 [ネットワーク（Networking）] エリアで次の手順を実行します。

a) [プライマリネットワーク（Primary Network）] エリアで、[既存の仮想クラウドネットワークを選択（Select existing virtual cloud network）] オプションボタンをクリックします。

b) ドロップダウンリストから仮想クラウドネットワークを選択します。

c) [サブネット（Subnet）] エリアで、[既存のサブネットを選択（Select existing subnet）] オプションボタンをクリックします。

d) ドロップダウン リストからサブネットを選択します。表示されるサブネットは、同じコンパートメントで作成されたサブネットです。

Step 13 [SSHキーの追加（Add SSH Keys）] エリアで、対応するオプションボタンをクリックして、キーペアを生成するか、既存の公開キーを使用できます。

Step 14 [ブートボリューム（Boot Volume）]エリアで、[カスタムブートボリュームサイズの指定（Specify a custom boot volume size）] チェックボックスをオンにして、必要なブートボリュームを GB 単位で入力します。Cisco ISE 実稼働環境に必要な最小ボリュームは 600 GB です。この手順でブートボリュームが指定されていない場合、インスタンスに割り当てられるデフォルトのボリュームは 250 GB です。

Note
[Encrypt this volume with a key that you manage] フィールドでは、暗号化にカスタマーマネージドキーを使用することをお勧めします。デフォルトでは、Oracle マネージドキーが使用されます。キーの作成の詳細については、『Key Management』[英語] を参照してください。

Step 15 [詳細オプションの表示（Show advanced options）] をクリックします。

Step 16 [管理（Management）] タブで、[クラウド初期化スクリプトの貼り付け（Paste cloud-init script）] オプションボタンをクリックします。

Step 17 [Cloud-init script] テキストボックスに、必要なユーザーデータを入力します。

[ユーザーデータ（User data）] フィールドに次の情報を入力します。

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

tertiarynameserver=<*IPv4 address of tertiary nameserver*>（Cisco ISE 3.4 以降のリリースに適用）

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*>（Cisco ISE 3.4 以降のリリースに適用）

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important
Cisco ISE リリース 3.4 以降、

a. [ntpserver] フィールド名が [primaryntpserver] に変更されました。[ntpserver] を使用すると、Cisco ISE サービスは起動しません。

b. OpenAPI はデフォルトで有効になっています。したがって、[openapi=<yes/no>] フィールドは必須ではありません。

c. [secondarynameserver] フィールドを空白のままにして、[tertiarynameserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

d. [secondaryntpserver] フィールドを空白のままにして、[tertiaryntpserver] フィールドのみを使用した場合、Cisco ISE サービスは起動しません。

ユーザーデータエントリを使用して設定する各フィールドには、正しいシンタックスを使用する必要があります。[ユーザーデータ（User Data）] フィールドに入力した情報は、入力時に検証されません。誤った構文を使用すると、イメージの起動時に Cisco ISE サービスが表示されないことがあります。次に、[ユーザーデータ（User Data）] フィールドを使用して送信する設定のガイドラインを示します。

- hostname：英数字とハイフン（-）のみを含むホスト名を入力します。ホスト名の長さは 19 文字以下で、下線（_）を含めることはできません。
- プライマリネームサーバー：プライマリネームサーバーの IP アドレス。サポートされているのは IPv4 アドレスだけです。Cisco ISE リリース 3.4 以降では、インストール時に [secondarynameserver] および [tertiarynameserver] フィールドを使用して、セカンダリおよびターシャリネームサーバーを設定できます。
- dnsdomain：DNS ドメインの FQDN を入力します。エントリには、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）を含めることができます。
- ntpserver：同期に使用する NTP サーバーの IPv4 アドレスまたは FQDN を入力します（例：time.nist.gov）。Cisco ISE リリース 3.4 以降では、インストール中に [secondaryntpserver] および [tertiaryntpserver] フィールドを使用して、セカンダリおよびターシャリ NTP サーバーを設定できます。
- timezone：タイムゾーンを入力します（例：Etc/UTC）。すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。これにより、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。
- password：Cisco ISE への GUI ベースのログインのパスワードを設定します。入力するパスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。パスワードは 6 ～ 25 文字で、少なくとも 1 つの数字、1 つの大文字、および 1 つの小文字を含める必要があります。パスワードは、ユーザー名またはその逆（iseadmin または nimdaesi）、cisco、または ocsic を含めたりそれらと同じにすることはできません。使用できる特殊文字は @~*!,+=_- です。パスワードに特殊文字を使用する場合は、バックスラッシュ（\）でエスケープする必要があります。ご使用のリリースの『Cisco ISE Administrator Guide』[英語] の「Basic Setup」の章にある「User Password Policy」のセクションを参照してください。

- ersapi：ERS を有効にするには **yes** と入力し、ERS を拒否するには **no** と入力します。
- openapi：OpenAPI を有効にするには **yes** と入力し、OpenAPI を拒否するには **no** と入力します。
- pxGrid：pxGrid を有効にするには **yes** と入力し、pxGrid を拒否するには **no** と入力します。
- pxgrid_cloud：pxGrid Cloud を有効にするには **yes** と入力し、pxGrid Cloud を拒否するには **no** と入力します。pxGrid クラウドを有効にするには、pxGrid を有効にする必要があります。pxGrid を無効にして pxGrid クラウドを有効にすると、pxGrid クラウドサービスは起動時に有効になりません。

Step 18 [作成（Create）] をクリックします。インスタンスが作成されて使用できるようになるまで、約 30 分かかります。

Cisco ISE インスタンスを表示するには、[Instances] ウィンドウに移動します（このウィンドウは検索フィールドを使用して探すことができます）。Cisco ISE インスタンスがこのウィンドウにリストされます。

Terraform スタックファイルを使用した OCI での Cisco ISE インスタンスの作成

Before you begin

OCI Terraform を利用して、Cisco ISE インスタンスを作成します。OCI の Terraform については、https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm を参照してください。

OCI で、SSH キー、仮想クラウドネットワーク（VCN）、サブネット、ネットワーク セキュリティ グループなど、Cisco ISE インスタンスを作成するために必要なリソースを作成します。

Note Cisco ISE リリース 3.4 以降、OpenAPI サービスは自動的に有効になるため、インスタンスの起動時に OpenAPI 関連のオプションを送信する必要はありません。

Procedure

Step 1 OCI アカウントにログインします。

Step 2 検索フィールドを使用して、**マーケットプレイス**を検索します。

Step 3 [リストの検索（Search for listings...）] の検索フィールドで、**Cisco Identity Services Engine**（**ISE**）と入力します。

Step 4 [Cisco Identity Services Engine（ISE）スタック（Cisco Identity Services Engine (ISE) Stack）] をクリックします。

Step 5 表示される新しいウィンドウで、[スタックの作成（Create Stack）] をクリックします。

Step 6 [スタック情報（Stack Information）] ウィンドウで次の手順を実行します。

a) [マイ設定（My Configuration）] オプションボタンをクリックします。
b) [コンパートメントに作成（Create in Compartment）] ドロップダウンリストから、Cisco ISE インスタンスを作成するコンパートメントを選択します。

Step 7 **[Next]** をクリックします。

Step 8 [変数の構成（Configure Variables）] ウィンドウで、次の手順を実行します。

a) [ホスト名（Hostname）] フィールドに、ホスト名を入力します。
b) [シェイプ（Shape）] ドロップダウンリストから、使用する OCI シェイプを選択します。[VM.Optimized3.Flex] を選択した場合は、[Flex OCPU] ドロップダウンリストから必要な値を選択します。[Flexメモリ（GB）（Flex Memory in GB）] フィールドには、対応する値が自動的に表示されます。他のシェイプでは値は事前に設定され、これらのフィールドはスタック形式に表示されません。
c) [Boot Volume Size] フィールドには、前の手順で選択したシェイプに基づいて必要な値が自動的に表示されます。

   1. [Vault] フィールドで、ブートボリューム暗号化キーの Vault を選択します。
   2. [Volume Encryption Key] フィールドで、ブートボリュームを暗号化するキーを選択します。

   Note
   [Volume Encryption Key] フィールドと [Vault] フィールドでは、カスタマーマネージドキーを暗号化に使用することをお勧めします。デフォルトでは、**Oracle マネージドキー**が使用されます。これらのフィールドは、Cisco ISE リリース 3.3 以降で使用できます。キーの作成の詳細については、『Key Management』[英語] を参照してください。

d) [SSHキー（SSH Key）] エリアで、対応するオプションボタンをクリックして、SSH キーファイルをアップロードするか、SSH キーコードを貼り付けることができます。
e) [タイムゾーン（Time Zone）] ドロップダウンリストから、タイムゾーンを選択します。
f) [可用性ドメイン（Availability Domain）] ドロップダウンリストで、リージョンのドメインのリストからオプションを選択します。
g) [仮想クラウドネットワーク（Virtual Cloud Network）] ドロップダウンリストで、手順 6b で選択したコンパートメントの VCN のリストからオプションを選択します。
h) [サブネット（Subnet）] ドロップダウンリストで、手順 8g で選択した VCN に関連付けられたサブネットのリストからオプションを選択します。
i) (Optional) [ネットワークセキュリティグループ（Network Security Group）] ドロップダウンリストで、前に選択したコンポーネントに関連付けられているセキュリティグループのリストからオプションを選択します。
j) [パブリックIPアドレスの割り当て（Assign Public IP Address）] チェックボックスはデフォルトでオンになっています。Cisco ISE インスタンスにプライベート IP アドレスのみを割り当てる場合は、チェックボックスをオフにすることができます。
k) [プライベートIPアドレス（Private IP Address）] フィールドに、選択したサブネットで定義されている IP アドレス範囲に準拠する IP アドレスを入力します。このフィールドを空白のままにすると、OCI DHCP サーバーが Cisco ISE に IP アドレスを割り当てます。
l) [DNS名（DNS Name）] フィールドにドメイン名を入力します。
m) [ネームサーバー（Name Server）] フィールドに、ネームサーバーの IP アドレスを入力します。

   Note

Cisco ISE リリース 3.4 以降、[Name Server] フィールドの名前が [Primary Name Server] に変更されました。

[Secondary Name Server] フィールドには、セカンダリネームサーバーの IP アドレスまたはホスト名を入力します。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。

[Tertiary Name Server] フィールドには、ターシャリネームサーバーの IP アドレスを入力します。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。[Secondary Name Server] フィールドが空白の場合、[Tertiary Name Server] オプションは使用できません。

Note
入力した IP アドレスのイベントが使用不可または到達不能な場合、Cisco ISE サービスが起動しない可能性があります。

n) [NTPサーバー（NTP Server）] フィールドに、NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。Cisco ISE リリース 3.4 以降、このフィールド名は [Primary NTP Server] に変更されました。

[Secondary NTP Server] フィールドには、セカンダリ NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。

[Tertiary NTP Server] フィールドに、ターシャリ NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。このフィールドは、Cisco ISE リリース 3.4 以降で使用できます。[Secondary NTP Server] フィールドが空白の場合、[Tertiary NTP Server] オプションは使用できません。

Note
入力した IP アドレスが使用できない、または到達できない場合、Cisco ISE サービスが起動しない可能性があります。

o) [ERS] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
p) [オープンAPI（Open API）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
q) [pxGrid] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
r) [pxGridクラウド（pxGrid Cloud）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
s) [パスワード（Password）] および [パスワードの再入力（Re-enter Password）] フィールドに Cisco ISE のパスワードを入力します。パスワードは Cisco ISE のパスワードポリシーに準拠し、最大 25 文字である必要があります。

Step 9 **[Next]** をクリックします。

[レビュー（Review）] ウィンドウに、スタックで定義されているすべての設定の概要が表示されます。

Step 10 情報を確認し、変更がある場合は [前へ（Previous）] をクリックして変更します。

Step 11 [作成したスタックで適用を実行（Run Apply on the created stack?）] エリアで、[適用を実行（Run Apply）] チェックボックスをオンにすると、[作成（Create）] をクリックしたときにスタックビルドが実行されます。[適用を実行（Run Apply）] を選択していない場合、[作成（Create）] をクリックしたときにスタック

情報が保存されます。後で[スタック（Stacks）] ウィンドウからスタックを選択し、[適用（Apply）] をクリックしてビルドを実行できます。

Step 12 [作成（Create）] をクリックします。

Step 13 OCI の [インスタンス（Instances）] ウィンドウに移動します。インスタンスは、スタック形式で指定したホスト名とともにリストされます。ホスト名をクリックすると、設定の詳細が表示されます。

Step 14 Cisco ISE インスタンスは、約 30 分で OCI で起動できるようになります。

インストール後のタスク

Cisco ISE インスタンスを正常に作成した後に実行する必要があるインストール後のタスクについては、お使いのバージョンの Cisco ISE リリースの『Cisco ISE Installation Guide』の「Installation Verification and Post-Installation Tasks」の章を参照してください。

OCI 上の Cisco ISE の互換性情報

このセクションでは、OCI 上の Cisco ISE に固有の互換性情報について詳しく説明します。Cisco ISE の一般的な互換性の詳細については、お使いのバージョンのリリースの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

ロードバランサ統合のサポート

RADIUS トラフィックのロードバランシングのために、OCI ネイティブ ネットワーク ロードバランサ（NLB）を Cisco ISE と統合できます。ただし、次の注意事項が適用されます。

- 認可変更（CoA）機能は、ネットワークロードバランサを作成するときに、送信元や宛先のヘッダー（IP、ポート）の保存セクションでクライアント IP の保存を有効にしている場合にのみサポートされます。
- NLB は送信元 IP アフィニティのみをサポートし、発信側ステーション ID ベースのスティッキセッションをサポートしないため、不均等なロードバランシングが発生する可能性があります。
- NLB は RADIUS ベースのヘルスチェックをサポートしていないため、RADIUS サービスがノードでアクティブでない場合でも、トラフィックを Cisco ISE PSN に送信できます。

OCI ネイティブ ネットワーク ロード バランサの詳細については、『Introduction to Network Load Balancer』を参照してください。

TACACS トラフィックのロードバランシングのために、OCI ネイティブ ネットワーク ロード バランサ（NLB）を Cisco ISE と統合できます。ただし、NLB は TACACS+ サービスに基づくヘルスチェックをサポートしないため、ノードで TACACS サービスがアクティブでない場合でも、Cisco ISE PSN にトラフィックが送信されることがあります。

NIC ジャンボフレームサポート

Cisco ISE はジャンボフレームをサポートしています。Cisco ISE の最大伝送ユニット（MTU）は 9,001 バイトですが、ネットワーク アクセス デバイスの MTU は通常 1,500 バイトです。Cisco ISE は、標準フレームとジャンボフレームの両方を問題なくサポートし、受信します。コンフィギュレーション モードで Cisco ISE CLI を使用して、Cisco ISE MTU を必要に応じて再設定できます。

OCI でのパスワードの回復とリセット

次のタスクでは、Cisco ISE 仮想マシンのパスワードをリセットするために役立つタスクについて説明します。必要なタスクを選択し、詳細な手順を実行します。

シリアルコンソールを介した Cisco ISE GUI パスワードのリセット

Procedure

Step 1 OCI にログインし、[コンピューティング（Compute）] の [インスタンス（Instances）] ウィンドウに移動します。

Step 2 インスタンスのリストから、パスワードを変更する必要があるインスタンスをクリックします。

Step 3 左ペインの [リソース（Resource）] メニューから、[コンソール接続（Console connection）] をクリックします。

Step 4 [Cloud Shell接続の起動（Launch Cloud Shell connection）] をクリックします。

Step 5 新しい画面に Oracle Cloud Shell が表示されます。

Step 6 画面が黒い場合は、Enter を押してログインプロンプトを表示します。

Step 7 シリアルコンソールにログインします。

シリアルコンソールにログインするには、インスタンスのインストール時に設定された元のパスワードを使用する必要があります。OCI は、この値をマスクされたパスワードとして保存します。このパスワードを覚えていない場合は、「パスワードの回復」セクションを参照してください。

Step 8 **application reset-passwd ise iseadmin** コマンドを使用して、iseadmin アカウントの新しい Cisco ISE GUI パスワードを設定します。

新しい公開キーペアの作成

このタスクを通じて、追加のキーペアをリポジトリに追加します。Cisco ISE インスタンスの設定時に作成された既存のキーペアは、新しく作成する公開キーに置き換えられません。

Procedure

Step 1 OCI で新しい公開キーを作成します。『Creating a Key Pair』を参照してください。

Step 2 前のタスクで説明したように、OCI シリアルコンソールにログインします。

Step 3 公開キーを保存する新しいリポジトリを作成するには、『Creating a Repository』を参照してください。

CLI を介してアクセスできるリポジトリがすでにある場合は、手順 4 に進みます。

Step 4 新しい公開キーをインポートするには、コマンド **crypto key import <public key filename> repository <repository name>** を使用します。

Step 5 インポートが完了すると、新しい公開キーを使用して SSH 経由で Cisco ISE にログインできます。

パスワードの回復

OCI には Cisco ISE のパスワード回復のメカニズムはありません。新しい Cisco ISE インスタンスを作成し、設定データのバックアップと復元を実行する必要が生じる場合があります。

OCI スタックの変数を編集すると、設定や構成を保存せずに Cisco ISE インスタンスが破棄され、新しい Cisco ISE インスタンスとして再作成されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。