Amazon Web Service における Cisco ISE

- Amazon Web Service における Cisco ISE （1 ページ）
- AWS における Cisco ISE 評価インスタンス （3 ページ）
- Cisco ISE AWS インスタンスを作成するための前提条件 （3 ページ）
- AWS での Cisco ISE の使用に関する既知の制限事項 （4 ページ）
- 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 （6 ページ）
- Cloud Formation テンプレートを使用した Cisco ISE の起動 （9 ページ）
- Cisco ISE AMI の起動 （12 ページ）
- インストール後の注意事項とタスク （16 ページ）
- AWS における Cisco ISE の互換性情報 （17 ページ）
- AWS でのパスワードの回復とリセット （18 ページ）

Amazon Web Service 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。

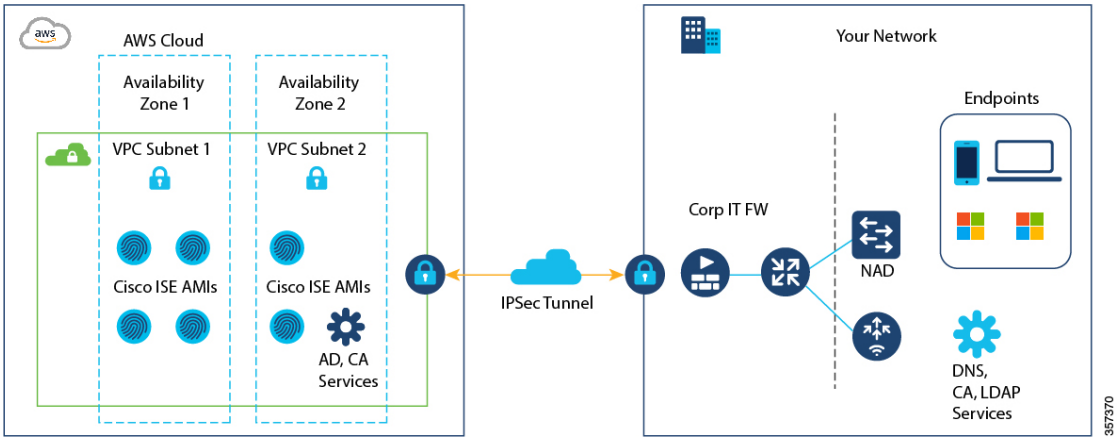
AWS CloudFormation テンプレート（CFT）または Amazon マシンイメージ（AMI）を通じて Cisco ISE を AWS に設定し、起動できます。次のリストのいずれかの方法で CFT を使用することをお勧めします。AWS で Cisco ISE を起動するには、、次のいずれかの手順を実行します。

- 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 （6 ページ）
- Cloud Formation テンプレートを使用した Cisco ISE の起動 （9 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 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。

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。「Configure A Cisco ISE Release 3.1 Repository With AWS S3」を参照してください。

AWS における Cisco ISE 評価インスタンス

Cisco ISE を初めて使用する場合は、評価インスタンス t3.xlarge を使用して Cisco ISE 機能を評価できます。90 日間有効な評価ライセンスは、Cisco ISE の新しいインスタンスの起動時に自動的に有効になります。 t3.xlarge インスタンスは、評価モードで Cisco ISE をサポートします。評価モードでは、Cisco ISE は 100 の同時アクティブエンドポイントをサポートし、すべての Cisco ISE 機能に 90 日間アクセスできます。

インスタンス タイプ	CPU コア	RAM（GB）
t3.xlarge	4	16

t3.xlarge インスタンスは、評価モードの Cisco ISE のみをサポートします。適切なライセンスを使用して Cisco ISE をネットワークに完全に展開する場合は、C または M のインスタンスタイプを使用して、Cisco ISE をインストールおよび設定する必要があります。t3.xlarge インスタンスは、Cisco ISE リリース 3.1 パッチ 1 以降のリリースをサポートします。

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。Cisco ISE ポート リファレンス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。Cisco ISE AWS インスタンスでデータを復元すると、データは Cisco ISE リリース 3.1 バージョンにアップグレードされます。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 admin 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。
- Cisco ISE AMI を使用して設定された Cisco ISE プライマリサーバーは、Cisco TrustSec AAA サーバーとして、誤ったホスト名と IP アドレス値で自動的に Cisco ISE に登録されます。正しい詳細情報を使用して Cisco ISE サーバーを登録し、Cisco TrustSec AAA サーバーのリストから、自動的に追加されたサーバーを削除する必要があります。Cisco TrustSec AAA サーバーの詳細については、『*Cisco ISE Administrator Guide*』[英語] の「Segmentation」の章にある「Configure Cisco TrustSec AAA Servers」を参照してください。
- 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。

（注）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。また、CFT を介して IPv6 DNS または NTP サーバーの設定もできません。IPv6 サーバーを設定するには、Cisco ISE CLI を使用します。

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。

始める前に

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。

ステップ 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。

ステップ 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。

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

ステップ 4 製品名をクリックします。

ステップ 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。

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

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 11 [作成（Launch）] をクリックします。

ステップ 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。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 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 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。

  （注） 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。

  （注） 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。

  （注） 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。

  （注） 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。

- [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。

（注） 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。

- [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。

ステップ 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。

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。また、CFT を介して IPv6 DNS または NTP サーバーの設定もできません。IPv6 サーバーを設定するには、Cisco ISE CLI を使用します。

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。

始める前に

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。

ステップ 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。

ステップ 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。

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

ステップ 4 製品名をクリックします。

ステップ 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。

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

ステップ 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。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 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。

  （注） 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。

  （注） 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。

  （注） 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。

  （注） 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。

- [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。

（注） 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。

- [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。

  （注） 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。

ステップ 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

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

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

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

ステップ 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。

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

ステップ 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。

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

ステップ 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。次のインスタンスタイプがサポートされています。

- c5.4xlarge
- m5.4xlarge
- c5.9xlarge

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

ステップ 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。

ステップ 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*>

dnsdomain=<*example.com*>

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

timezone=<*timezone*>

username=<*admin*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

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。
- 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）。
- 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。
- username：設定するデフォルトのユーザー名は **admin** である必要があります。**admin** 以外のユーザー名を設定すると、AMI の起動時に Cisco ISE CLI にアクセスできなくなります。
- 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（admin または nimda）、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。

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

ステップ 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。

（注） 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。

ステップ 14 [Next: Add Tags] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 20 [作成（Launch）] をクリックします。

ステップ 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）]

（注） SSH を使用して Cisco ISE にログインするには、ユーザー名が **admin** 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。

ステップ 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 admin@<*Cisco ISE Private IP Address*>

3. ログインプロンプトで、ユーザー名として **admin** 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. インストール後のタスクの一覧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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [接続（Connect）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 9 **application reset-passwd ise admin** コマンドを使用して、admin 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。

ステップ 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、このキーペアの作成を参照してください。

ステップ 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。

ステップ 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、手順 4 に進みます。

ステップ 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。

ステップ 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。

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。