Azure Cloud Services 上の Cisco ISE

- Azure Cloud 上の Cisco ISE （1 ページ）
- Microsoft Azure Cloud Services での Cisco ISE の既知の制限事項 （3 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 （6 ページ）
- 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 （10 ページ）
- インストール後の作業 （13 ページ）
- Azure Cloud 上の Cisco ISE の互換性情報 （13 ページ）
- Azure Cloud でのパスワードの回復とリセット （14 ページ）

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 （10 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 （6 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 *1 : 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。

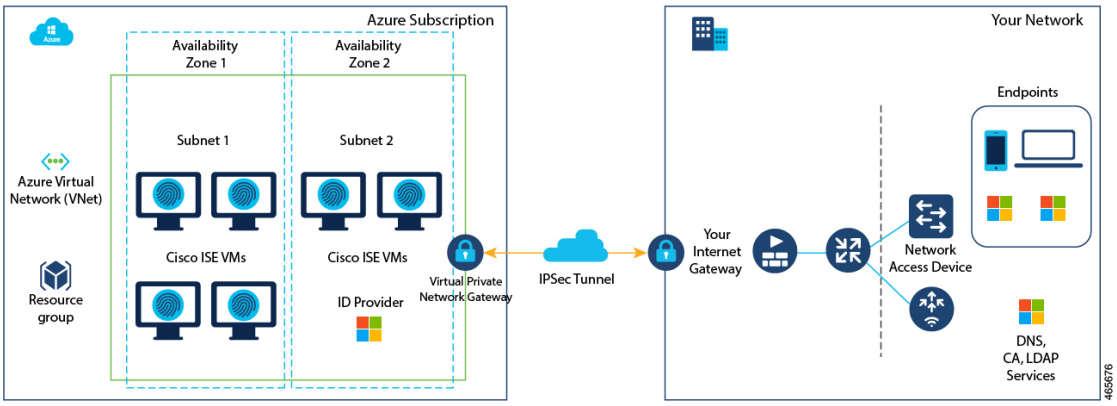
Dsv4 シリーズは、PAN または MnT ノード、またはその両方としての使用に最適な汎用の Azure VM サイズであり、データ処理タスクとデータベース操作を目的としています。

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 *1 : 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 仮想マシンを使用して Cisco ISE 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。

- 順序が不正なフラグメンテーションの問題：Azure では、ネットワーキング仮想ネットワークスタックは、デフォルトで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、サイト間 VPN ソリューションや Azure ExpressRoute などのオンプレミス接続モードを使用します。これは、フラグメンテーションの問題が発生しやすい傾向にあります。このようなシナリオでは、Cisco ISE は完全な RADIUS パケットを受信しないため、認証エラーが発生する場合があります。

  Microsoft では、Azure VPN Gateway、Azure ExpressRoute（FastPath が無効）、および Azure vWAN において、順序が不正なフラグメントのドロップを防止するオプションを有効にで

きません。その結果、順序が不正なフラグメントの受信と処理が適切に行われない場合があります。

回避策として、シスコは、オンプレミス展開から VPN トンネルを終端するための Azure 仮想マシンとして、Cisco Catalyst 8000V などのサードパーティ VPN ゲートウェイを検証しました。サードパーティ VPN ゲートウェイでは、次の設定を行う必要があります。

- サードパーティゲートウェイで ip virtual-reassembly を有効にします。これにより、受信パケットの順序が正しくない場合でも、サードパーティ VPN ゲートウェイは、フラグメント化されたパケットを正しい順序で再構成して送信できます。
- Microsoft Azure Portal の内部および外部ネットワーク インターフェイスで IP 転送を有効にします。
- Microsoft Azure Portal のルーティングテーブルが、サードパーティ VPN ゲートウェイを介してオンプレミスのリソースに接続するために必要な仮想ネットワークを許可するように適切に設定されていることを確認します。

サードパーティ VPN ゲートウェイの設定に加えて、次のいずれかを実行して、順序が不正な UDP パケットが適切に処理されるようにします。

- Microsoft Azure Cloud ですでに修正が実装されている次のリージョンを選択します。カナダ中部（CanadaCentral）、インド中部（CentralIndia）、スウェーデン中部（SwedenCentral）、アラブ首長国連邦中部（UAECentral）、東アジア（eastasia）、カナダ東部（CanadaEast）、米国東部（eastus）、東日本（japaneast）、ドイツ北部（GermanyNorth）、EU 北部（EUNorth）、南アフリカ北部（SouthAfricaNorth）、ブラジル南部（brazilsouth）、オーストラリア南東部（australiasoutheast）、インド南部（SouthIndia）、英国南部（uksouth）、米国中西部（westcentralus）、ドイツ中西部（GermanyWestCentral）、英国西部（ukwest）。

  Cisco ISE のお客様は、Microsoft Azure サポートチケットを発行して、順序が不正なフラグメントをドロップするのではなく送信先に到達させるオプションを有効にする必要があります。

- その他のリージョンでは、Microsoft Azure サポートチケットを発行して次の設定を更新する必要があります。
  - 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。
  - 順序が不正なフラグメントを許可するオプションを有効にします。

- 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

始める前に

- 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。

（注） 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。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [Virtual Machine] をクリックします。

ステップ 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。

ステップ 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 （1 ページ） 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。

（注）
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。

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

ステップ 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。

（注）
[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。

ステップ 9 [Next: Networking] をクリックします。

ステップ 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。

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

ステップ 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。

ステップ 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*>

重要
Cisco ISE リリース 3.4 以降、

1. [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。
2. 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。
3. [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。
4. [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。

ステップ 14 [次へ：タグ（Next: Tag）] をクリックします。

ステップ 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。

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

ステップ 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）。

次のタスク

（注） 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

始める前に

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。

（注） 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。

手順

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

ステップ 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。

ステップ 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。

ステップ 4 [Azure Application] をクリックします。

ステップ 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。

ステップ 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。

（注）
[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。

ステップ 7 **[Next]** をクリックします。

ステップ 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) （任意）[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。

（注）
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。

（注）
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。

（注）
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。

（注）
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。

ステップ 9 **[Next]** をクリックします。

ステップ 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。

（注）
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。

ステップ 11 **[Next]** をクリックします。

ステップ 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。

ステップ 13 **[Next]** をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

インストール後の作業

Cisco ISE インスタンスを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 Load Balancer 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 Load Balancer 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 PSN に送信できます。

Azure Load Balancer 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 Load Balancer 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

以下のタスクを使用して、Cisco ISE 仮想マシンのパスワードをリセットまたは回復できます。必要なタスクを選択し、詳細な手順に従います。

（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

手順

ステップ 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。

ステップ 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。

ステップ 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。

Azure Cloud Shell が新しいウィンドウに表示されます。

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。

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。

1. 左側のメニューから、[ブート診断（Boot diagnostics）] をクリックします。
2. [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。
3. 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。

ステップ 4 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。

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

次の手順に従って、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。

手順

ステップ 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。

ステップ 2 Azure Cloud 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、『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。

ステップ 4 新しい公開キーをインポートするには、次のコマンドを使用します。

crypto key import <public key filename> repository <repository name>

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。

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。