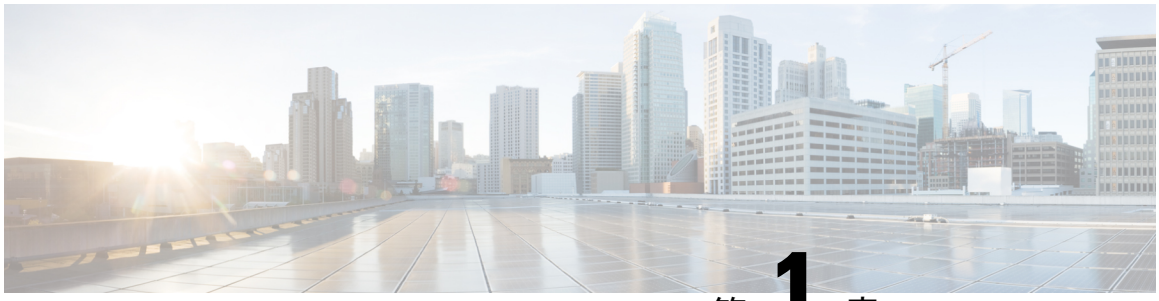
Cisco Identity Services Engine リリース 3.0 インストール ガイド

初版：2022 年 8 月 10 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

Cisco ISE のネットワーク デプロイメント

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

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、シスコサービス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、シスコサポート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 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 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

シスコのテクニカルドキュメント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。

Cisco ISE ネットワークアーキテクチャ

Cisco ISE アーキテクチャには、次のコンポーネントが含まれます。

- ノードおよびペルソナの種類
  - Cisco ISE ノード：Cisco ISE ノードは管理、ポリシー サービス、モニターリング、または pxGrid のペルソナのいずれかまたはすべてを担当することができます。
- ネットワーク リソース
- エンドポイント

ポリシー情報ポイントは、外部の情報がポリシー サービス ペルソナに伝送されるポイントを表します。たとえば、外部情報は Lightweight Directory Access Protocol（LDAP）属性になります。

Cisco ISE 展開の用語

このガイドでは、Cisco ISE デプロイメント シナリオについて説明する際に次の用語を使用します。

用語	定義
サービス	ネットワーク アクセス、プロファイリング、ポスチャ、セキュリティ グループ アクセス、モニターリング、およびトラブルシューティングなど、ペルソナが提供する特定の機能。
ノード	個別の物理または仮想 Cisco ISE アプライアンス。
ノード タイプ	Cisco ISE ノードは、管理、ポリシー サービス、モニターリングのペルソナのいずれかを担当することができます。
ペルソナ	ノードによって提供されるサービスを決定します。Cisco ISE ノードは、 のペルソナのいずれかまたはすべてを担うことができます。管理ユーザー インターフェイスで使用できるメニュー オプションは、ノードが担当するロールおよびペルソナによって異なります。
ロール	ノードがスタンドアロン、プライマリ、セカンダリ ノードのいずれであるかを決定し、管理ノードとモニターリング ノードだけに適用されます。

分散デプロイメント環境のノードタイプおよびペルソナ

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。デプロイメントの各ノードは、管理、ポリシー サービス、pxGrid、およびモニターリングのペルソナのいずれかを担当することができます。分散デプロイメントでは、ネットワーク上で次の組み合わせのノードを使用できます。

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理ノード
- 自動フェールオーバー用の 1 組のモニターリング ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード
- pxGrid サービスの 1 つ以上の pxGrid ノード

管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。このノードは、認証、認可、およびアカウンティングなどの機能に関するすべてのシステム関連の設定を扱います。分散デプロイメント環境では、最大2つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、セカンダリのロールを担当できます。

ポリシー サービス ノード

ポリシー サービス ペルソナの Cisco ISE ノードは、ネットワーク アクセス、ポスチャ、ゲスト アクセス、クライアント プロビジョニング、およびプロファイリング サービスを提供します。このペルソナはポリシーを評価し、すべての決定を行います。複数のノードがこのペルソナを担当できます。通常、1つの分散デプロイメントに複数のポリシー サービス ノードが存在します。同じ高速ローカル エリア ネットワーク（LAN）またはロード バランサの背後に存在するポリシー サービス ノードはすべて、グループ化してノード グループを形成することができます。ノード グループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。

モニターリング ノード

モニターリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシー サービス ノードからのログを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度なモニターリングおよびトラブルシューティング ツールを提供します。このペルソナのノードは収集したデータを集約して関連付けを行い、有意義なレポートを提供します。Cisco ISE では、このペルソナを持つノードを最大2つ使用することができます。これらのノードは、ハイ アベイラビリティ用のプライマリ ロールまたはセカンダリ ロールを担うことができます。プライマリ モニターリング ノードおよびセカンダリ モニターリング ノードの両方が、ログ メッセージを収集します。プライマリ モニターリング ノードがダウンした場合は、セカンダリ モニターリング ノードが自動的にプライマリ モニターリング ノードになります。

分散セットアップでは、少なくとも1つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニターリング ペルソナとポリシー サービス ペルソナを有効にしないことをお勧めします。最適なパフォーマンスを実現するために、モニターリング ノードはモニターリング専用とすることをお勧めします。

pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッション ディレクトリからの状況依存情報を、ISE エコ システムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。pxGrid フレームワークは、Cisco ISE とサード パーティのベンダー

間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用できます。また、その他の情報交換にも使用できます。Cisco pxGrid によって、サードパーティ システムは適応型のネットワーク制御アクション（EPS）を呼び出し、ネットワークまたはセキュリティ イベントに応じてユーザーまたはデバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイント プロファイルは、エンドポイント プロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング（IP-SGT マッピング）を発行および受信登録できます。SXP バインディングの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Source Group Tag Protocol」のセクションを参照してください。

ハイ アベイラビリティ設定で、Cisco pxGrid サーバーは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバーは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバーの PAN をアクティブにするには、手動で昇格する必要があります。

ISE のスタンドアロン デプロイメント環境と分散デプロイメント環境

単一の Cisco ISE ノードがあるデプロイメント環境は「スタンドアロン デプロイメント」と呼ばれます。このノードは、管理、ポリシーサービス、およびモニターリングのペルソナを実行します。

複数の Cisco ISE ノードがあるデプロイメント環境は「分散デプロイメント」と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散デプロイメント環境では、管理およびモニターリング アクティビティは一元化され、処理はポリシー サービス ノード間で分配されます。パフォーマンスのニーズに応じて、デプロイメント環境の規模を変更できます。Cisco ISE ノードは、管理、ポリシーサービス、およびモニターリングのペルソナのいずれかまたはすべてを担当することができます。

分散デプロイメント環境のシナリオ

- 小規模のネットワーク デプロイメント
- 中規模のネットワーク デプロイメント
- 大規模のネットワーク デプロイメント

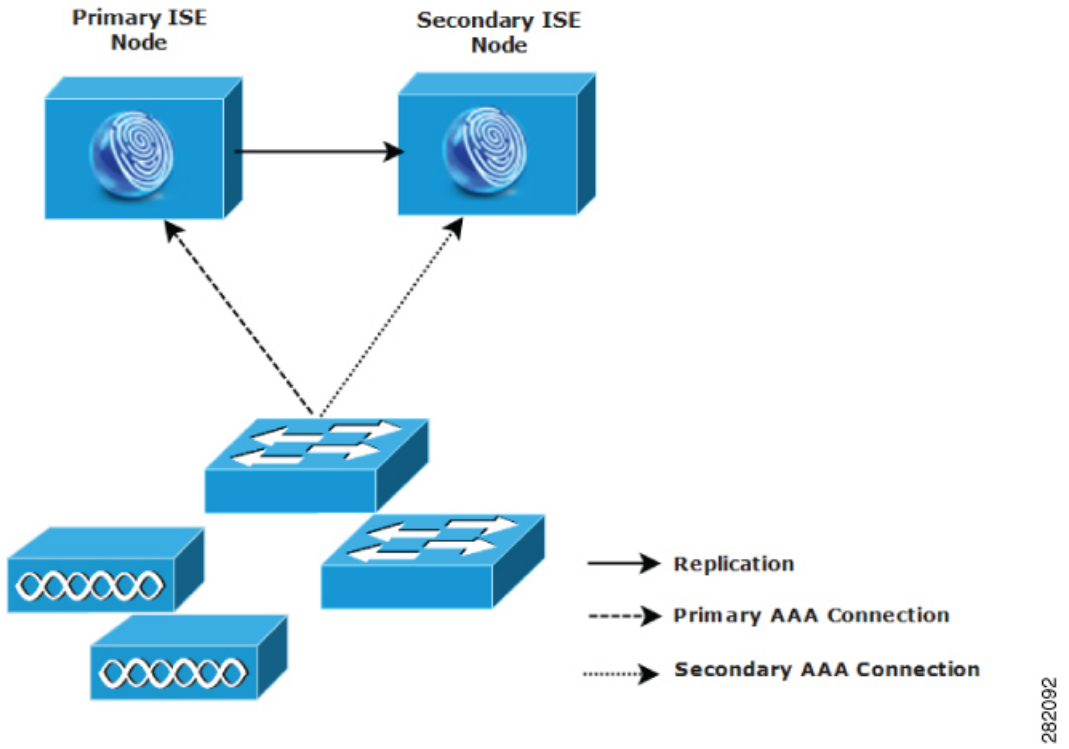
小規模のネットワーク デプロイメント

最も小規模な Cisco ISE デプロイメント環境は、2 つの Cisco ISE ノードから構成されます（小規模なネットワークでは 1 つの Cisco ISE ノードがプライマリ アプライアンスとして動作します）。

プライマリ ノードは、このネットワーク モデルに必要なすべての設定、認証、およびポリシー機能を提供し、セカンダリ Cisco ISE ノードはバックアップ ロールで稼働します。セカンダリ ノードはプライマリ ノードをサポートし、プライマリ ノードとネットワーク アプライアンス、ネットワーク リソース、または RADIUS との間で接続が失われたときにネットワークを稼働し続けます。

クライアントとプライマリ Cisco ISE ノード間の一元化された認証、認可、アカウンティング（AAA）操作は RADIUS プロトコルを使用して行われます。Cisco ISE は、プライマリ Cisco ISE ノードに存在するすべてのコンテンツをセカンダリ Cisco ISE ノードに同期（複製）します。したがって、セカンダリ ノードは、プライマリ ノードの状態と同じになります。小規模なネットワーク デプロイメントでは、このような設定モデルにより、このタイプのデプロイメントまたは同様の方法を使用して、すべての RADIUS クライアントでプライマリ ノードとセカンダリ ノードの両方を設定することが可能です。

図 *1 : Cisco ISE* ノードの小規模なネットワークデプロイメント



ネットワーク環境で、デバイス、ネットワーク リソース、ユーザー、および AAA クライアントの数が増えた場合、基本的な小規模モデルからデプロイメント環境の設定を変更し、分割または分散されたデプロイメント モデルを使用する必要があります。

分割デプロイメント

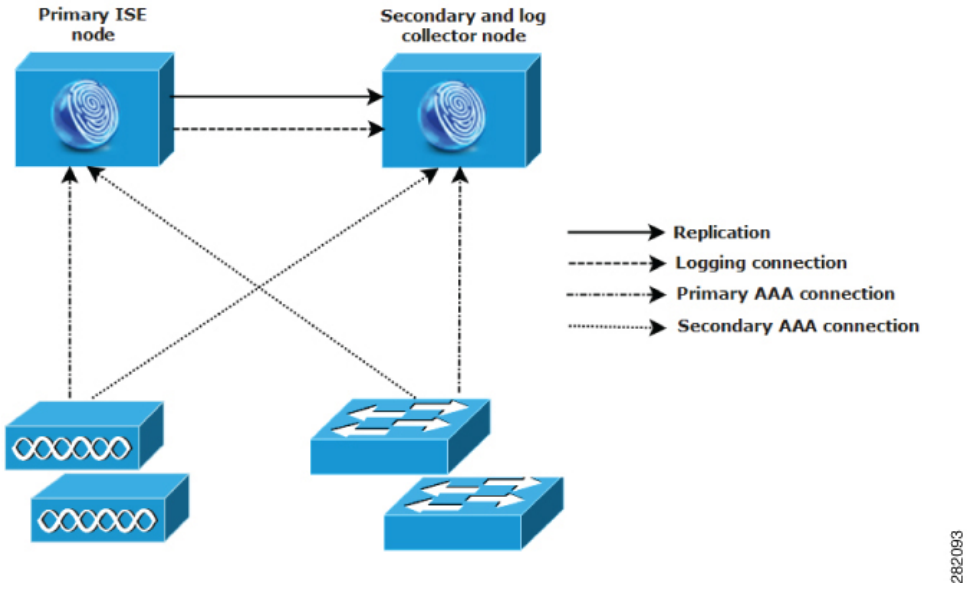
分割 Cisco ISE デプロイメント環境でも、小規模な Cisco ISE デプロイメント環境で説明したように、プライマリ ノードとセカンダリ ノードを維持することができます。ただし、AAA ロードは、AAA ワークフローを最適化するためにこの 2 つの Cisco ISE ノード間で分割されます。AAA 接続で問題がある場合は、各 Cisco ISE アプライアンス（プライマリまたはセカンダリ）がすべてのワークロードを処理できる必要があります。通常のネットワーク運用では、プライマリ ノードとセカンダリ ノードのどちらもすべての AAA 要求を処理することはできません。これは、このワークロードがこの 2 つのノード間で分散されているためです。

このようにロードを分割できるため、システムの各 Cisco ISE ノードに対する負荷は減少します。また、負荷の分割により優れた負荷の制御が実現する一方で、通常のネットワーク運用中のセカンダリ ノードの機能ステータスはそのまま保持されます。

分割された Cisco ISE のデプロイメント環境では、各ノードが、ネットワーク アドミッションやデバイス管理などの独自の固有操作を実行でき、障害発生時でもすべての AAA 機能を引き続き実行することができます。認証要求を処理し、アカウンティング データを AAA クライアントから収集する 2 つの Cisco ISE ノードがある場合は、Cisco ISE ノードのいずれかがログ コレクタとして動作するよう設定することを推奨します。

また、分割 Cisco ISE デプロイメント環境の設計は、拡張に対応しているため、メリットがもたらされます。

図 *2 : Cisco ISE* での分割ネットワークデプロイメント



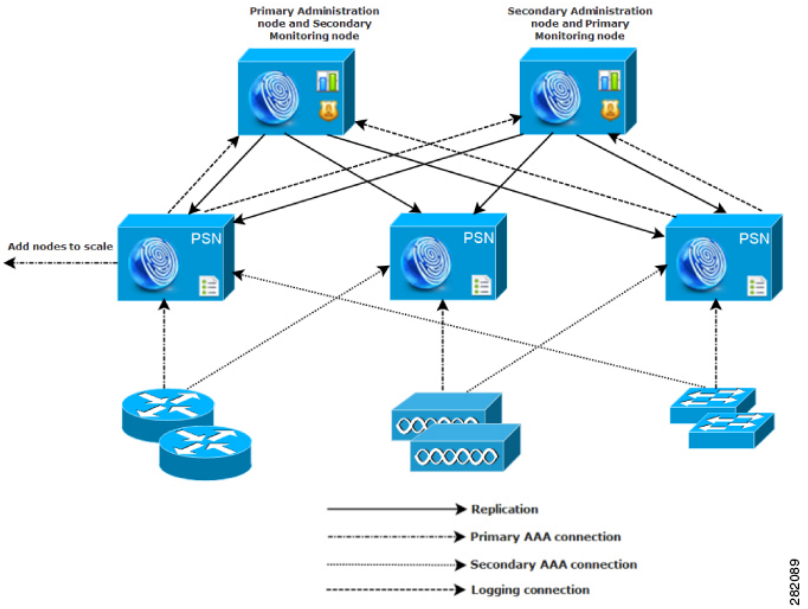
中規模のネットワーク デプロイメント

小規模なネットワークが大きくなった場合に、Cisco ISE ノードを追加して中規模なネットワークを作成することで、素早くネットワークの拡大に対応できます。中規模なネットワーク デプロイメントでは、新規ノードをすべての AAA 機能専用とし、元のノードを設定およびロギング機能のために使用します。

（注） 中規模のネットワーク デプロイメントでは、管理ペルソナ、モニターリング ペルソナ、またはその両方を実行しているノードでポリシー サービス ペルソナを有効にできません。専用のポリシー サービス ノードが必要です。

ネットワークでログ トラフィックの量が増加した場合は、セカンダリ Cisco ISE ノードの 1 つまたは 2 つを、ネットワークでのログ収集に使用することを選択できます。

図 *3 : Cisco ISE* での中規模のネットワークデプロイメント



大規模のネットワーク デプロイメント

集中ロギング

大規模な Cisco ISE ネットワークには集中ロギングを使用することをお勧めします。集中ロギングを使用するには、大規模で通信量の多いネットワークが生成することがある大きな syslog

トラフィックを処理するモニターリング ペルソナ（モニターリングおよびロギング用）として動作する、専用ロギング サーバーを最初に設定する必要があります。

syslog メッセージは発信ログ トラフィックに対して生成されるため、どの RFC-3164 準拠 syslog アプライアンスでも、発信ロギング トラフィックのコレクタとして動作できます。専用ロギング サーバーでは、すべての Cisco ISE ノードをサポートするために Cisco ISE で使用できるレポート機能およびアラート機能を使用できます。

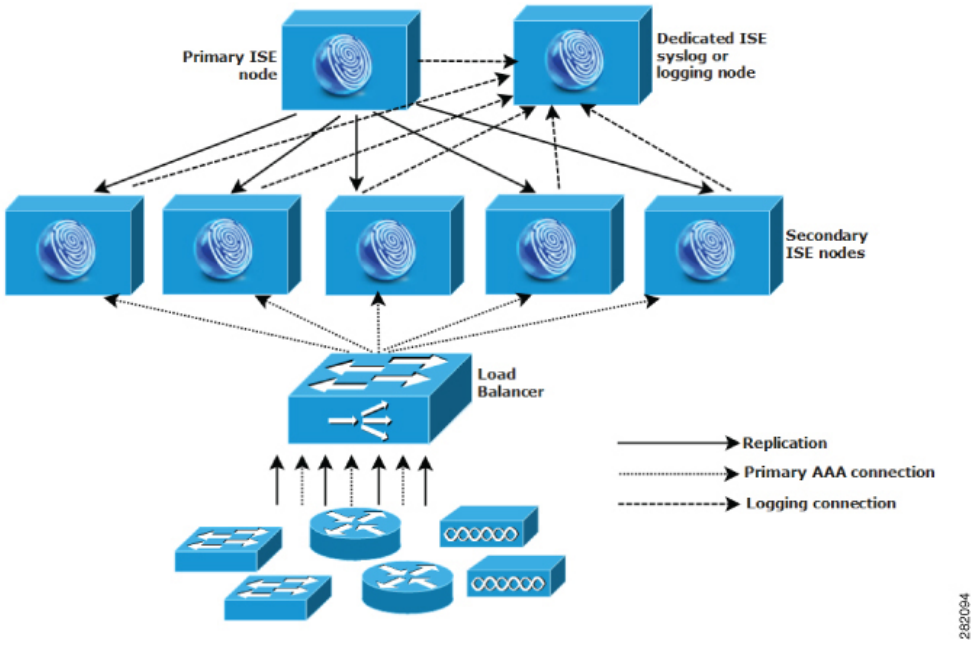
また、アプライアンスが Cisco ISE ノードの監視ペルソナと汎用 syslog サーバーの両方にログを送信するよう設定することもできます。汎用 syslog サーバーを追加することにより、Cisco ISE ノード上の監視ペルソナがダウンした場合に冗長なバックアップが提供されます。

集中型ネットワークでのロードバランサの使用

大規模な集中ネットワークでは、ロード バランサを使用する必要があります。これにより、AAA クライアントのデプロイメントが簡素化されます。ロードバランサを使用するには、AAA サーバーのエントリが 1 つだけ必要です。ロード バランサは、利用可能なサーバーへの AAA 要求のルーティングを最適化します。

ただし、ロード バランサが 1 つだけしかないと、シングル ポイント障害が発生する可能性があります。この問題を回避するために、2 つのロードバランサをデプロイし、冗長性とフェールオーバーを実現します。この構成では、各 AAA クライアントで 2 つの AAA サーバー エントリを設定する必要があります（この設定は、ネットワーク全体で同じになります）。

図 *4 :* ロードバランサを使用した *Cisco ISE* での大規模なネットワークデプロイメント

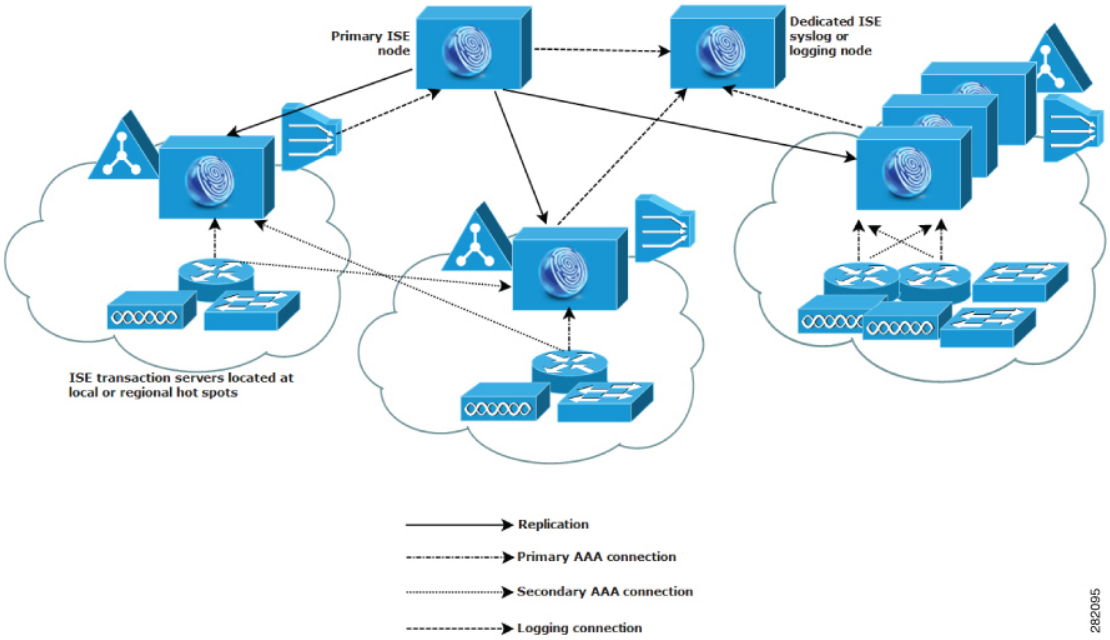


Cisco ISE での分散ネットワークデプロイメント

分散 Cisco ISE ネットワーク デプロイメントは、主要な拠点があり、他の場所に地域、全国、またはサテライトの拠点がある組織に最も役に立ちます。主要な拠点は、プライマリ ネットワークが存在し、追加の LAN に接続される小規模～大規模な場所であり、異なる地域や距離が離れた場所のアプライアンスとユーザーをサポートします。

大規模なリモート サイトでは最適な AAA パフォーマンスのために独自の AAA のインフラストラクチャを持つことができます。集中管理モデルにより、同一の同期された AAA ポリシーが保持されます。集中設定モデルでは、プライマリ Cisco ISE ノードとセカンダリ Cisco ISE ノードを使用します。Cisco ISE ノードで個別の監視ペルソナを使用することを推奨しますが、リモートの場所それぞれで独自の固有なネットワーク要件を満たす必要があります。

図 *5 : Cisco ISE* での分散ネットワークデプロイメント



複数のリモート サイトがあるネットワークを計画する際の考慮事項

- Microsoft Active Directory や Lightweight Directory Access Protocol（LDAP）などの中央または外部データベースが使用されているかどうかを確認します。AAA のパフォーマンスを最適化するために、各リモート サイトでは Cisco ISE がアクセスできる外部データベースの同期されたインスタンスが必要です。
- AAA クライアントの場所は重要です。ネットワーク遅延の影響と WAN 障害により引き起こされるアクセス損失の可能性を減らすために、Cisco ISE ノードを AAA クライアントのできるだけ近くに配置する必要があります。

- Cisco ISE では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトでターミナルを使用して、各ノードへのネットワーク アクセスをバイパスする直接的で安全なコンソール アクセスを行うことができます。
- 小規模な場合は、リモート サイトが近くにあるため、他のサイトに信頼できる WAN 接続を行えます。また、冗長性を提供するために、ローカル サイトのバックアップとして Cisco ISE ノードを使用できます。
- 外部データベースに確実にアクセスできるようにするために、すべての Cisco ISE ノードでドメイン ネーム システム（DNS）を適切に設定する必要があります。

Cisco ISE の各デプロイメントモデルでサポートされるセッションの最大数

次の表に、各デプロイメント モデルでサポートされるセッションの最大数を示します。

表 *1:* デプロイメント モデルごとにサポートされる最大セッション数

デプロイメント モデル	プラットフォーム	最大セッション数
スタンドアロン（単一ノード上のすべてのペルソナ）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
基本的な 2 ノード デプロイメント（冗長）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
ハイブリッド分散型デプロイメント（同一アプライアンス上の Admin および MnT、専用アプライアンスのポリシー サービス）	PAN と MnT としての 3615	10,000
	PAN と MnT としての 3655	25,000
	PAN と MnT としての 3695	50,000
	PAN と MnT としての 3515	7,500
	PAN と MnT としての 3595	20,000

デプロイメント モデル	プラットフォーム	最大セッション数
専用（PAN、MnT、PXG、および PSN ノード）	PAN と MnT としての 3595	500,000
	PAN と MnT としての 3655	500,000
	PAN/MnT としての 3695	2,000,000

表 *2:* 最大アクティブ セッション数（*PSN* あたり）

PSN[1]	最大アクティブ セッション数
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3515	7,500
SNS 3595	40,000

[1] 専用ポリシー ノードごとのスケーリング（合計デプロイメント サイズでゲートされる最大セッション数）

SNS 3500/3600 シリーズ アプライアンスのデプロイメント規模およびスケーリングについての推奨事項

表 *3 : SNS 3500/3600* シリーズ アプライアンスの *RADIUS* 最大スケーリング

デプロイメント モデル	プラットフォーム	専用 PSN の最大数	最大 RADIUS セッション数（1 デプロイメントあたり）
スタンドアロン	3515	0	7500
	3595	0	20,000
	3615	0	10,000
	3655	0	25,000
	3695	0	50,000

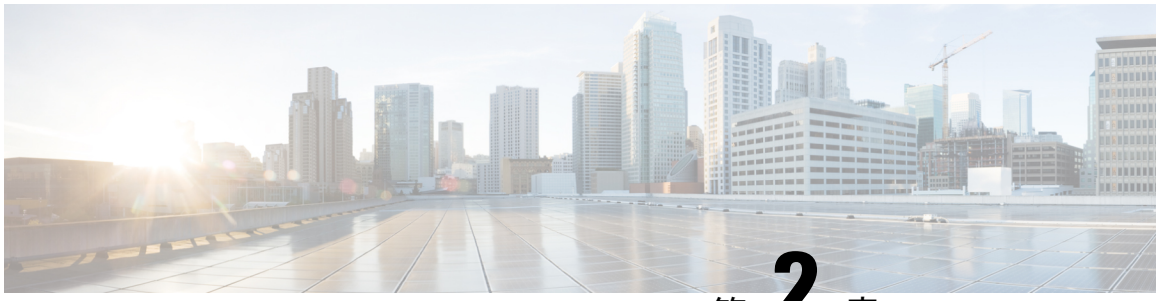
デプロイメントモデル	プラットフォーム	専用 PSN の最大数	最大 RADIUS セッション数（1 デプロイメントあたり）
同一ノードおよび専用 PSN 上の PAN と MnT	PAN と MnT としての 3515	6	7,500
	PAN と MnT としての 3595	6	20,000
	PAN と MnT としての 3615	6	10,000
	PAN と MnT としての 3655	6	25,000
	PAN と MnT としての 3695	6	50,000
専用（PAN、MnT、PXG、および PSN ノード）	PAN と MnT としての 3595	50	500,000
	PAN と MnT としての 3655	50	500,000
	PAN と MnT としての 3695	50	2,000,000

Cisco ISE のサポートに必要なスイッチおよびワイヤレス LAN コントローラの設定

Cisco ISE がネットワーク スイッチと相互運用することができ、Cisco ISE の機能がネットワーク セグメント全体で正常に使用できるよう保証するためには、ご使用のネットワーク スイッチを、必要とされる特定のネットワーク タイム プロトコル（NTP）、RADIUS/AAA、IEEE 802.1X、MAC 認証バイパス（MAB）などの設定を使用して設定する必要があります。

ISE Community Resource

WLC 付き Cisco ISE の設定については、Cisco ISE with WLC Setup Video を参照してください。



第 2 章

Cisco Secured Network Server 3500/3600 シリーズ アプライアンスおよび仮想マシンの要件

Cisco ISE 用のハードウェアおよび仮想アプライアンスの要件

Cisco Identity Services Engine（ISE）は、Cisco SNS のハードウェアまたは仮想アプライアンスにインストールできます。Cisco ISE ハードウェア アプライアンスと同等のパフォーマンスと拡張性を実現するには、仮想マシンに Cisco SNS 3500 または 3600 シリーズ アプライアンスと同等のシステム リソースが割り当てられている必要があります。このセクションでは、Cisco ISE のインストールに必要なハードウェア、ソフトウェア、および仮想マシンの要件を示します。

（注） 仮想環境を強化し、すべてのセキュリティ更新が最新の状態であることを確認します。シスコは、ハイパーバイザで検出されたセキュリティ上の問題については責任を負いません。

Cisco Secured Network Server 3500 および 3600 シリーズ アプライアンス

Cisco Secured Network Server（SNS）ハードウェアアプライアンスの仕様については、『Cisco Secure Network Server Data Sheet』の「Table 1, Product Specifications」を参照してください。

Cisco SNS 3500 シリーズ アプライアンスについては、『Cisco SNS-3500 Series Appliance Hardware Installation Guide』を参照してください。

Cisco SNS 3600 シリーズ アプライアンスについては、『Cisco SNS-3600 Series Appliance Hardware Installation Guide』を参照してください。

Cisco ISE 用の VMware 仮想マシンの要件

Cisco ISE は次の VMware サーバーとクライアントをサポートしています。

- ESXi 5.*x*（5.1 U2 以上）の VMware バージョン 8（デフォルト）
- ESXi 6.*x*VMware バージョン 11（デフォルト）
- ESXi 7.*x* の VMware バージョン 13（デフォルト）

Cisco ISE では、仮想マシン（VM）インスタンス（任意のペルソナを実行）のホスト間での移行を可能にする、VMware コールドマイグレーション機能がサポートされます。該当のコールドマイグレーション機能が動作するには、次の条件を満たす必要があります。

- Cisco ISE は、シャットダウンして電源をオフにする必要があります。 Cisco ISE では、移行中にデータベース操作を停止または一時停止できません。このような操作は、データ破損の問題につながる可能性があります。したがって、移行中は Cisco ISE が実行されておらずアクティブでないことを確認します。

（注）
- データベースの破損の問題を防ぐために、halt コマンドを使用する前、または VM の電源をオフにする前に、application stop コマンドを使用する必要があります。
- Cisco ISE VM はホットマイグレーション（vMotion）をサポートしていません。

vMotion の要件の詳細については、VMware のドキュメントを参照してください。

注意 VM でスナップショット機能が有効になっていると、VM 設定が破損する可能性があります。この問題が発生した場合、VM のイメージを再作成し、VM のスナップショットを無効にする必要があります。

（注） Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。VMware スナップショットを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。ISE ノードを起動するには、再起動が必要です。

Cisco ISE は、仮想マシン（VM）に Cisco ISE をインストールし、デプロイするために使用できる、次の OVA テンプレートを提供します。

- ISE-3.0.0.*xxx*-virtual-SNS3615-SNS3655-300.ova
- ISE-3.0.0.*xxx*-virtual-SNS3615-SNS3655-600.ova
- ISE-3.0.0.*xxx*-virtual-SNS3655-SNS3695-1200.ova
- ISE-3.0.0.*xxx*-virtual-SNS3695-2400.ova

300 GB OVA テンプレートは、専用のポリシーサービスや pxGrid ノードとして動作する Cisco ISE ノードには十分です。

600 GB および 1.2 TB OVA テンプレートは、管理またはモニターリング ペルソナを実行する ISE ノードの最小要件を満たすために推奨されています。ディスク容量要件の詳細については、「#unique_31」を参照してください。

ディスク サイズ、CPU、またはメモリ配賦をカスタマイズする必要がある場合、標準の .iso イメージを使用して手動で Cisco ISE をデプロイできます。ただし、このドキュメントで指定されている最小要件およびリソース予約を確認することが重要です。OVA テンプレートは、各プラットフォームに必要な最小のリソースを自動的に適用することにより、ISE の仮想アプライアンスのデプロイメントを簡素化します。

表 *4 : OVA* テンプレートの予約

OVA テンプレートタイプ	CPU の数	CPU の予約（MHz）	メモリ（GB）	メモリ予約（GB）
評価	4	予約なし	16	予約なし
小	16	16,000	32	32
中規模	24	24,000	96	96
大	24	24,000	256	256

リソースの割り当てに合わせてCPUとメモリのリソースを予約することを強くお勧めします。これを行わない場合は ISE のパフォーマンスと安定性に大きく影響することがあります。

サポートされているオペレーティングシステムについては、『Supported Operating System for Virtual Machines』を参照してください。

Cisco SNS アプライアンスの製品仕様については、『Cisco Secure Network Server データシート』を参照してください。

次の表に、VMware 仮想マシンの要件を示します。

表 *5 : VMware* 仮想マシンの要件

要件のタイプ	仕様
CPU	• **評価** • クロック速度：2.0 GHz 以上 • CPU コア数：4 CPU コア • **本稼働** • クロック速度：2.0 GHz 以上 • コア数： • **SNS 3500 シリーズ アプライアンス**： • 小規模：12 • 中規模：16 • 大規模：16 （注） コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3500 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3515 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。 • **SNS 3600 シリーズ アプライアンス**： • 小規模：16 • 中規模：24 • 大規模：24 （注） コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3600 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3615 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。

要件のタイプ	仕様

メモリ	• **評価**：16 GB
	• **本稼働**
	  • 小規模：SNS 3515 の場合は 16 GB、SNS 3615 の場合は 32 GB
	  • 中規模：SNS 3595 の場合は 64 GB、SNS 3655 の場合は 96 GB
	  • 大規模：SNS 3695 の場合は 256 GB

ハード ディスク	• **評価**：300 GB • **本稼働** 300 GB ～ 2.4 TB のディスクストレージ（サイズは展開とタスクによって異なります）。 以下のリンクで VM の推奨ディスク容量を参照してください：「ディスク領域に関する要件」。 VM ホスト サーバーでは、最小速度が 10,000 RPM のハードディスクを使用することをお勧めします。 （注） Cisco ISE に対して仮想マシンを作成する場合は、ストレージ要件を満たす単一の仮想ディスクを使用します。ディスク領域要件を満たしている複数の**仮想**ディスクを使用する場合、インストーラがすべてのディスク領域を認識しない可能性があります。
ストレージおよびファイル システム	Cisco ISE 仮想アプライアンスのストレージ システムには、50 MB/秒の最小書き込みパフォーマンスと 300 MB/秒の読み取りパフォーマンスが必要です。これらのパフォーマンス基準を満たし、VMware サーバーでサポートされているストレージ システムをデプロイします。 Cisco ISE は、ストレージ システムが Cisco ISE のインストール前、インストール中、インストール後にこれらの最小要件を満たしているかどうかを確認するためのさまざまな方法を提供します。詳細については、「#unique_32」を参照してください。 ここでは、最も広範にテストされているという理由で VMFS ファイル システムを推奨しますが、上記の要件を満たせば、その他のファイル システム、転送、およびメディアもデプロイできます。

要件のタイプ	仕様
ディスク コントローラ	Paravirtual（64 ビット RHEL 7 のデフォルト）または LSI Logic Parallel 最適なパフォーマンスと冗長性のために、キャッシュ RAID コントローラが推奨されます。RAID 10（1+0）などのコントローラ オプションは、たとえば RAID 5 よりも全体のパフォーマンスと冗長性が優れている可能性があります。さらに、バッテリバックアップ式コントローラ キャッシュは書き込み操作の効率をかなり高めることができます。 （注） ISE VM のディスク SCSI コントローラを別のタイプから VMware Paravirtual に更新すると、ブートできなくなる可能性があります。
NIC	1 つの NIC インターフェイスが必要（複数の NIC が推奨されます。6 つの NIC がサポートされます）。Cisco ISE は E1000 および VMXNET3 アダプタをサポートしています。 （注） デフォルトで正しいアダプタ順序を確保するために、E1000 を選択することをお勧めします。VMXNET3 を選択した場合、ISE のアダプタ順序と同期させるために ESXi アダプタを再マップしなければならない場合があります。
VMware 仮想ハードウェア バージョンまたはハイパーバイザ	ESXi 5.*x*（5.1 U2 以上）と 6.x の VMware 仮想マシンのハードウェアバージョン 8 以降。

Cisco ISE 用の Linux KVM の要件

表 *6 : Linux KVM* 仮想マシンの要件

要件のタイプ	最小要件
CPU	

要件のタイプ	最小要件
	• 評価 • クロック速度：2.0 GHz 以上 • コア数：4 CPU コア • 本稼働 • クロック速度：2.0 GHz 以上 • コア数： • SNS 3500 シリーズ アプライアンス： • 小規模：12 • 中規模：16 • 大規模：16 （注） コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3500 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3515 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。 • SNS 3600 シリーズ アプライアンス： • 小規模：16 • 中規模：24 • 大規模：24 （注） コアの数は、ハイパースレッディン

要件のタイプ	最小要件
	グにより、Cisco Secure Network Server 3600 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3615 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。

メモリ	• **評価**：16 GB
	• **本稼働**
	  • 小規模：SNS 3515 の場合は 16 GB、SNS 3615 の場合は 32 GB
	  • 中規模：SNS 3595 の場合は 64 GB、SNS 3655 の場合は 96 GB
	  • 大規模：256 GB

要件のタイプ	最小要件
ハードディスク	• **評価**：300 GB • **本稼働** 300 GB ～ 2.4 TB のディスクストレージ（サイズは展開とタスクによって異なります）。 以下のリンクで VM の推奨ディスク容量を参照してください：「ディスク領域に関する要件」。 VM ホスト サーバーでは、最小速度が 10,000 RPM のハードディスクを使用することをお勧めします。 （注） Cisco ISE に対して仮想マシンを作成する場合は、ストレージ要件を満たす単一の仮想ディスクを使用します。ディスク領域要件を満たしている複数の**仮想**ディスクを使用する場合、インストーラがすべてのディスク領域を認識しない可能性があります。
KVM ディスク デバイス	ディスク バス：virtio、キャッシュ モード：なし、I/O モード：ネイティブ 事前割り当て済みの RAW ストレージ形式を使用します。
NIC	1 つの NIC インターフェイスが必要（複数の NIC が推奨されます。6 つの NIC がサポートされます）。Cisco ISE は VirtIO ドライバをサポートします。パフォーマンスを向上させるには、VirtIO ドライバを推奨します。
ハイパーバイザ	QEMU 1.5.3-160 上の KVM

Cisco ISE 用の Microsoft Hyper-V の要件

表 *7: Microsoft Hyper-V* 仮想マシンの要件

要件のタイプ	最小要件
CPU	• **評価** • クロック速度：2.0 GHz 以上 • コア数： 4 CPU コア • **本稼働** • クロック速度：2.0 GHz 以上 • **コア数**： • **SNS 3500 シリーズ アプライアンス**： • 小規模：12 • 中規模：16 • 大規模：16 コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3500 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3515 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。 • **SNS 3600 シリーズ アプライアンス**： • 小規模：16 • 中規模：24 • 大規模：24 （注） コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3600 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3615 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。

要件のタイプ	最小要件
メモリ	• **評価**：16 GB • **本稼働** • 小規模：SNS 3515 の場合は 16 GB、SNS 3615 の場合は 32 GB • 中規模：SNS 3595 の場合は 64 GB、SNS 3655 の場合は 96 GB • 大規模：256 GB
ハードディスク	• **評価**：300 GB • **本稼働** 300 GB ～ 2.4 TB のディスクストレージ（サイズは展開とタスクによって異なります）。 以下のリンクで VM の推奨ディスク容量を参照してください：「ディスク領域に関する要件」。 VM ホスト サーバーでは、最小速度が 10,000 RPM のハードディスクを使用することをお勧めします。 （注） Cisco ISE に対して仮想マシンを作成する場合は、ストレージ要件を満たす単一の仮想ディスクを使用します。ディスク領域要件を満たしている複数の**仮想**ディスクを使用する場合、インストーラがすべてのディスク領域を認識しない可能性があります。
NIC	1 つの NIC インターフェイスが必要（複数の NIC が推奨されます。6 つの NIC がサポートされます）。
ハイパーバイザ	Hyper-V（Microsoft）

Cisco ISE に関する Nutanix AHV の要件

Cisco ISE は、標準の Cisco ISE .iso イメージを使用して Nutanix AHV に展開する必要があります。OVA テンプレートを使用した Cisco ISE の展開は、Nutanix AHV ではサポートされていません。

次の表に、Nutanix AHV でのさまざまな展開タイプに推奨されるリソース予約を示します。

タイプ	CPU の数	CPU の予約（MHz）	メモリ（GB）	メモリ予約（GB）	ハードディスク
評価	4	予約なし	16	予約なし	200 GB
小	16	16,000	32	32	600 GB

中規模	24	24,000	96	96	1.2 TB
大	24	24,000	256	256	2.4 TB（4*600 GB として分割）

Cisco ISE のインストールを進める前に、Nutanix AHV で次の設定を行う必要があります。

- Nutanix AHV で仮想マシン（VM）を作成し、VM の電源をオフのままにします。
- ssh ログインを使用して Nutanix CVM にアクセスし、次のコマンドを実行します。
  - $acli
  - <acropolis> vm.serial_port_create <*Cisco ISE VM Name*> type=kServer index=0
  - <acropolis> vm.update <*Cisco ISE VM Name*> disable_branding=true
  - <acropolis> vm.update <*Cisco ISE VM Name*> extra_flags=”enable_hyperv_clock=False”
- Acropolis CLI を終了し、VM の電源をオンにして、standard.iso イメージを使用してCisco ISE のインストールを続行します。

表 *8 : Nutanix AHV* の要件

要件のタイプ	最小要件
CPU	• **評価**： • クロック速度：2.0 GHz 以上 • コア数：2 CPU コア • **実稼動**： • クロック速度：2.0 GHz 以上 • **コア数** • 小規模：12 プロセッサ（ハイパースレッディングが有効の 6 コア） • 大規模：16 プロセッサ（ハイパースレッディングが有効の 8 コア） 6 コア、2.0 GHz 以上。 Cisco ISE はハイパースレッディングをサポートしています。可能であれば、ハイパースレッディングをイネーブルにすることを推奨します。 （注） ハイパースレッディングによって全体のパフォーマンスが向上する場合にも、仮想マシンアプライアンスごとにサポートされるスケーリング制限は変更されません。また、CPU リソースは、論理プロセッサの数ではなく、必要な物理コアの数に基づいて割り当てる必要があります。

要件のタイプ	最小要件
メモリ	• **評価**： • 基本：4 GB（ゲスト アクセスと基本的なアクセス ポリシー フローの評価用） • 拡張：16 GB（pxGrid、内部 CA、SXP、デバイス管理、パッシブ アイデンティティ サービスなどの高度な機能の評価用） • **実稼動**： • 小規模：16 GB • 大規模：64 GB
ハード ディスク	• **評価**：200 GB • **実稼動**： 200 GB ～ 2 TB のディスク ストレージ（サイズは展開とタスクによって異なります）。 VM ホスト サーバでは、最小速度が 10,000 RPM のハードディスクを使用することをお勧めします。 （注） 2.4 TB のハードディスクサポートには 4 *600 GB を使用する必要があります。
KVM ディスク デバイス	ディスクバス：SCSI
NIC	1 GB の NIC インターフェイスが必要（複数の NIC が推奨されます。6 つの NIC がサポートされます）。Cisco ISE は VirtIO ドライバをサポートします。パフォーマンスを向上させるには、VirtIO ドライバを推奨します。
ハイパーバイザ	AOS - 5.20.1.1 LTS、Nutanix AHV - 20201105.2096

Amazon Web サービスの VMware クラウドおよび Azure VMware ソリューションにおける Cisco ISE のサポート

VMware クラウドに Cisco ISE をインストールするプロセスは、VMware 仮想マシンに Cisco ISE をインストールするプロセスとまったく同じです。

- Amazon Web サービス（AWS）の VMware クラウドに展開された Cisco ISE 仮想マシン：Cisco ISE は、AWS の VMware クラウドが提供するソフトウェア定義型データセンター（SDDC）でホストできます。オンプレミス展開、必要なデバイスとサービスへの到達可能性を有効にするために、セキュリティ グループ ポリシーが VMware クラウドで設定されていることを確認します（[ネットワーキングとセキュリティ（Networking and Security）] > [セキュリティ（Security）] > [ゲートウェイ ファイアウォール設定（Gateway Firewall Settings）]）。
- Azure VMware ソリューション（AVS）に展開された Cisco ISE 仮想マシン：AVS は Microsoft Azure で VMware ワークロードをネイティブに実行します。Cisco ISE は VMware 仮想マシンとしてホストできます。

Cisco ISE の仮想マシンアプライアンスサイズについての推奨事項

Cisco ISE 2.4 では、モニターリング ノードに大規模 VM が導入されました。大規模な VM にモニターリングペルソナを展開すると、ライブログのクエリとレポートの完了に迅速に対応できるという点からパフォーマンスが向上します。

（注） このフォーム ファクタは、リリース 2.4 以降での VM としてのみ使用可能で、大規模 VM ライセンスが必要です。

仮想マシン（VM）アプライアンスの仕様は、実稼働環境で動作している物理アプライアンスと同等である必要があります。

アプライアンスのリソースを割り当てる際は、次のガイドラインに留意してください。

- 指定したリソースの割り当てに失敗すると、パフォーマンスの低下やサービスの障害が発生する可能性があります。専用の VM リソースをデプロイする（複数のゲスト VM 間でリソースを共有またはオーバーサブスクライブしない）ことを強くお勧めします。OVF テンプレートを使用して Cisco ISE 仮想アプライアンスをデプロイすると、十分なリソースが各 VM に割り当てられます。OVF テンプレートを使用しない場合は、ISO イメージを使用して Cisco ISE を手動でインストールするときに、必ず同等のリソース予約を割り当てるようにしてください。

（注） 推奨する予約なしで Cisco ISE を手動でデプロイする場合は、密接にアプライアンスのリソース使用率を監視し、必要に応じてリソースを増やすことに責任を負い、Cisco ISE デプロイメントの適切な状態および機能を確保する必要があります。

（注） OVF テンプレートは Linux KVM には適用できません。OVF テンプレートは VMware 仮想マシンに対してのみ使用できます。

- インストールに OVA テンプレートを使用している場合は、インストールが完了した後に次の設定を確認します。
  - [CPU/メモリの予約（CPU/Memory Reservation）] フィールド（[設定の編集（Edit Settings）] ウィンドウの [仮想ハードウェア（Virtual Hardware）] タブの下）の Cisco ISE 用の VMware 仮想マシンの要件 （16 ページ） のセクションに指定されているリソースの予約を割り当てて、Cisco ISE 導入環境の正しい状態と機能が維持されるようにします。
  - [CPU の制限（CPU Limit）] フィールド（[設定の編集（Edit Settings）] ウィンドウの [仮想ハードウェア（Virtual Hardware）] タブの下）の CPU 使用率が [無制限（Unlimited）] に設定されていることを確認します。CPU 使用率の制限を設定すると（CPU 使用率の制限を 12000 MHz に設定するなど）、システムのパフォーマンスに影響します。制限が設定されている場合は、VM クライアントをシャットダウンし、その制限を削除して、VM クライアントを再起動する必要があります。
  - [メモリの制限（Memory Limit）] フィールド（[設定の編集（Edit Settings）] ウィンドウの [仮想ハードウェア（Virtual Hardware）] タブの下）の メモリ使用率が [無制限（Unlimited）] に設定されていることを確認します。メモリ使用率の制限を設定すると（制限を 12000 MB に設定するなど）、システムのパフォーマンスに影響します。
  - [共有（Shares）] オプションが、[ハードディスク（Hard Disk）] 領域（[設定の編集（Edit Settings）] ウィンドウの [仮想ハードウェア（Virtual Hardware）] タブの下）で [高（High）] に設定されていることを確認します。

    管理者ノードと MnT ノードは、ディスクの使用率に大きく依存しています。共有ディスクストレージ VMware 環境を使用すると、ディスクのパフォーマンスに影響する可能性があります。ノードのパフォーマンスを向上させるには、ノードに割り当てられているディスク共有数を増やす必要があります。

- VM のポリシー サービス ノードは管理またはモニターリング ノードよりも少ないディスク領域でデプロイできます。すべての実稼働 Cisco ISE ノードの最小ディスク領域は 300 GB です。各種 Cisco ISE ノードとペルソナに必要なディスク領域の詳細については、「#unique_31」を参照してください。

- VM は 1 ～ 6 つの NIC を使用して設定できます。2 つ以上の NIC を使用できるようにすることをお勧めします。追加のインターフェイスは、プロファイリングやゲストサービス、RADIUS などのさまざまなサービスをサポートするために使用できます。

（注） VM での RAM と CPU の調整では、再イメージ化は必要ありません。

Cisco ISE デプロイメントにおける VM のディスク容量の要件

次の表に、実稼働デプロイメントで仮想マシンを実行するために推奨される Cisco ISE ディスク領域の割り当てを示します。

（注） 2 TB 以上の GPT パーティションをブートするには、VM 設定のブート モードでファームウェアを **BIOS** から **EFI** に変更する必要があります。

表 *9:* 仮想マシンに推奨されるディスク領域

Cisco ISE ペルソナ	評価環境での最小ディスク容量	実稼働環境での最小ディスク容量	実稼働環境用に推奨されるディスク領域	最大ディスク領域
スタンドアロン Cisco ISE	300 GB	600 GB	600 GB ～ 2.4 TB	2.4 TB
分散型 ISE：管理専用	300 GB	600 GB	600 GB	2.4 TB
分散型 Cisco ISE：モニターリングのみ	300 GB	600 GB	600 GB ～ 2.4 TB	2.4 TB
分散型 Cisco ISE：ポリシーサービスのみ	300 GB	300 GB	300 GB	2.4 TB
分散型 Cisco ISE、pxGrid のみ	300 GB	300 GB	300 GB	2.4 TB
分散型 Cisco ISE：管理およびモニターリング（およびオプションで pxGrid）	300 GB	600 GB	600 GB ～ 2.4 TB	2.4 TB
分散型 Cisco ISE：管理、モニターリング、およびポリシーサービス（およびオプションで pxGrid）	300 GB	600 GB	600 GB ～ 2.4 TB	2.4 TB

（注） 追加のディスク領域は、プライマリ管理ノードが一時的にモニターリングノードになるときに、ローカルデバッグログ、ステージングファイルを格納し、アップグレード中にログデータを処理するために必要です。

Cisco ISE のディスク容量に関するガイドライン

Cisco ISE のディスク容量を決定するときは、次のガイドラインに留意してください。

- Cisco ISE は、仮想マシンの単一のディスクにインストールする必要があります。
- ディスク割り当ては、ロギングの保持要件によって異なります。モニターリングペルソナが有効になっている任意のノードでは、VMディスク領域の60パーセントがログストレージ用に割り当てられます。25,000 のエンドポイントがあるデプロイメントでは、1 日あたり約 1 GB のログが生成されます。

  たとえば、600 GB の VM ディスク領域があるモニターリング ノードがある場合、360 GB がログストレージ用に割り当てられます。100,000 のエンドポイントが毎日このネットワークに接続する場合、1 日あたり約 4 GB のログが生成されます。この場合、リポジトリに古いデータを転送し、モニターリングデータベースからそのデータをパージすれば、モニターリング ノードのログを 76 日を保存することができます。

追加のログ ストレージ用に、VM ディスク領域を増やすことができます。追加するディスクスペースの 100 GB ごとに、ログ ストレージ用に 60 GB が追加されます。

最初のインストール後に仮想マシンのディスクサイズを増やす場合、Cisco ISE の新規インストールを実行します。新規インストールは、ディスク割り当て全体を適切に検出して利用するのに役立ちます。

次の表に、割り当てられたディスク領域とネットワークに接続するエンドポイントの数に基づいて、モニターリング ノードで RADIUS ログを保持できる日数を示します。数値は、次の前提に基づいています：ログ抑制が有効になっているエンドポイントごとに 1 日あたり 10 個以上の認証。

表 *10 :* ノード ログ記憶域のモニターリング：*RADIUS* の保持日数

エンドポイント数	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258

エンドポイント数	300 GB	600 GB	1024 GB	2048 GB
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

次の表に、割り当てられたディスク領域とネットワークに接続するエンドポイントの数に基づいて、モニターリング ノードでTACACS+ログを保持できる日数を示します。数値は、次の前提に基づいています：スクリプトはすべての NAD に対して実行され、1 日あたり 4 セッション、セッションあたり 5 コマンド。

表 *11 :* ノード ログ記憶域のモニターリング：*TACACS+* の保持日数

エンドポイント数	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

ディスク サイズを増やす

コンテキストと可視性の機能が低速であるか、ログの空き領域が不足している場合は、ディスク容量の割り当てを増やす必要があります。

ログストレージの追加を計画するには、100 GB のディスク容量を追加するごとに 60 GB をログストレージ用に使用できます。

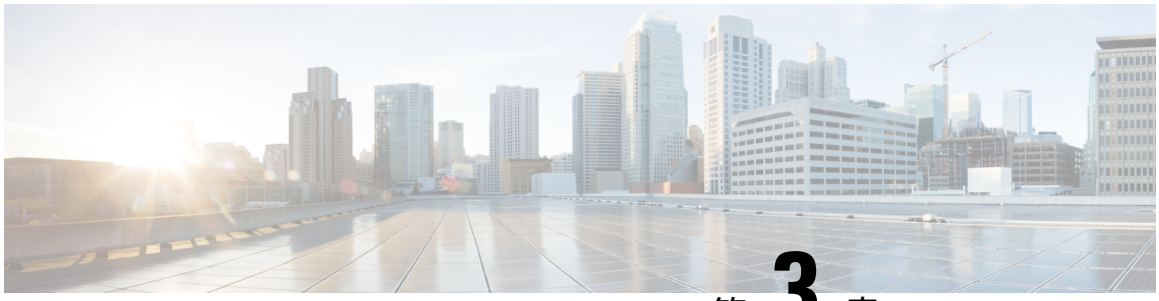
ISE を検出して新しいディスクの割り当てを利用するために、ノードの登録を解除し、VM の設定を更新し、ISEを再インストールする必要があります。これを行う1つの方法は、新しい、より大きいノードにISEをインストールし、ハイ アベイラビリティとしてのデプロイメントにそのノードを追加することです。ノードの同期後、新しいVMをプライマリにして元のVMの登録を解除します。

ディスクサイズの縮小

VM に Cisco ISE をインストールした後は、VM の予約分を減らさないでください。VM のメモリを Cisco ISE サービスが必要とするメモリよりも少なくすると、リソースが不足するため、Cisco ISE サービスが起動しません。

Cisco ISE をインストールした後、VM を再設定する必要がある場合は、次の手順を実行します。

1. Cisco ISE のバックアップを実行します。
2. 必要に応じて、変更された VM 設定で Cisco ISE を再イメージ化します。
3. Cisco ISE を復元します。



第 3 章

Cisco ISE のインストール

CIMC を使用した Cisco ISE のインストール

このセクションでは、Cisco ISE を簡単にインストールするための基本的なインストール手順を提供します。

始める前に

- 本書で指定されているとおりに「システム要件」を満たしていることを確認します。
- （オプション：Cisco ISE を仮想マシンにインストールする場合にのみ必要）仮想マシンを正常に作成したことを確認します。詳細については、次のトピックを参照してください。
  - #unique_43
  - #unique_44
  - Hyper-V での Cisco ISE 仮想マシンの作成 （66 ページ）
- （オプション：Cisco ISE を SNS ハードウェア アプライアンスにインストールするときにのみ必要）Cisco Integrated Management Interface（CIMC）設定ユーティリティを設定して、アプライアンスを管理し、BIOS を設定していることを確認します。詳細については、次のマニュアルを参照してください。
  - SNS3500 シリーズ アプライアンスについては、『Cisco SNS-3500 Series Appliance Hardware Installation Guide』を参照してください。
  - SNS-3600 シリーズ アプライアンスについては、『Cisco SNS-3600 Series Appliance Hardware Installation Guide』を参照してください。

ステップ 1 Cisco ISE を次のものにインストールするには、

- Cisco SNS アプライアンス：ハードウェア アプライアンスをインストールします。サーバー管理用の CIMC に接続します。
- 仮想マシン：VM が正しく設定されていることを確認します。

ステップ 2 Cisco ISE ISO イメージをダウンロードします。

a) http://www.cisco.com/go/ise にアクセスします。このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルが事前に必要です。

b) [ソフトウェアダウンロード（Download Software for this Product）] をクリックします。

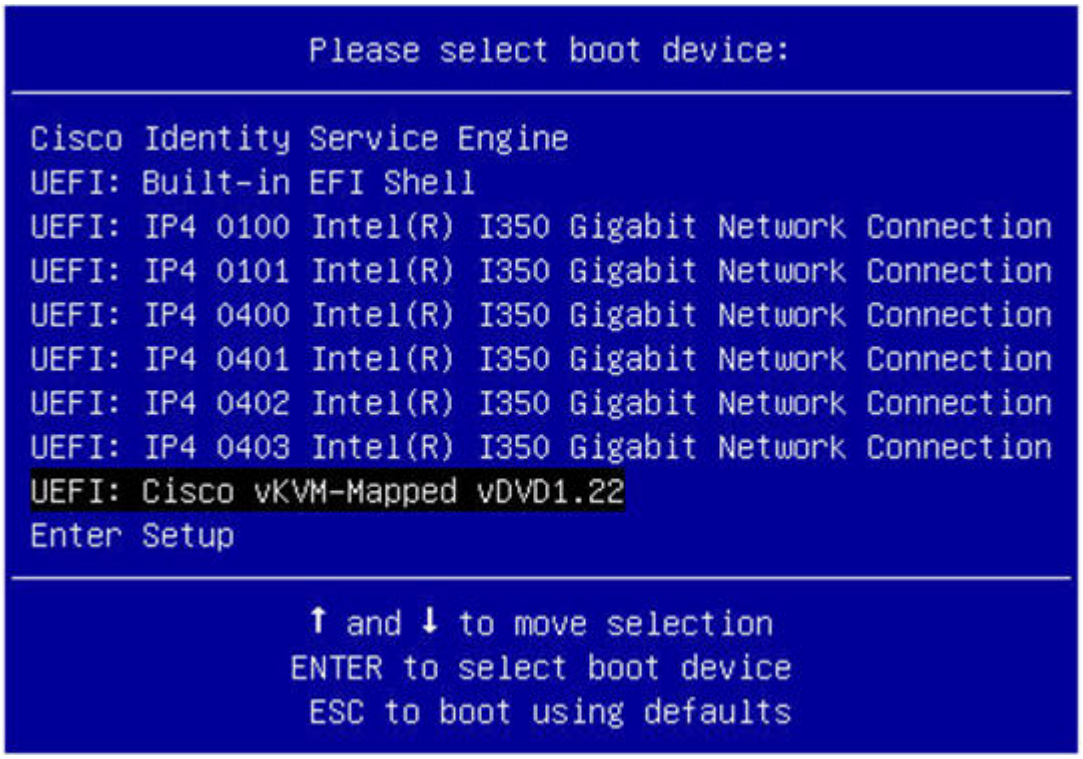
Cisco ISE イメージには、90 日間の評価ライセンスがすでにインストールされた状態で付属しているため、インストールおよび初期設定が完了すると、すべての Cisco ISE サービスのテストを開始できます。

ステップ 3 アプライアンスまたは仮想マシンを起動します。

- Cisco SNS アプライアンス。

1. CIMC に接続し、CIMC クレデンシャルを使用してログインします。
2. KVM コンソールを起動します。
3. [仮想メディア（Virtual Media）] > [仮想デバイスのアクティブ化（Activate Virtual Devices）] の順に選択します。
4. [仮想メディア（Virtual Media）] > [CD/DVDのマッピング（Map CD/DVD）] の順に選択し、ISE ISO イメージを選択して [デバイスのマッピング（Map Device）] をクリックします。
5. [マクロ（Macros）] > [静的マクロ（Static Macros）] > [Ctrl-Alt-Del] の順に選択して、ISE ISO image でアプライアンスを起動します。
6. F6 を押して、ブート メニューを起動します。次のような画面が表示されます。

図 *6:* ブートデバイスの選択



（注） SNS アプライアンスがリモート ロケーション（データ センターなど）に配置されている場合で、その場所に対する物理的なアクセス権がなく、リモート サーバーから CIMC インストールを実行する必要がある場合、インストールに時間がかかることがあります。インストールプロセスを高速化するために、USB ドライブに ISO ファイルをコピーし、そのリモートの場所で使用することをお勧めします。

- 仮想マシン。

1. CD/DVD を ISO イメージにマッピングします。次のような画面が表示されます。次のメッセージとインストール メニューが表示されます。

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 3.0.0.xxx


Available boot options:

Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

ステップ 4 シリアル コンソールを使用して Cisco ISE をインストールするには、ブート プロンプトで **1** および Enter キーを押します。

キーボードとモニターを使用する場合は、矢印キーを使用して、[Cisco ISE のインストール（シリアル コンソール）（Cisco ISE Installation (Serial Console)）] オプションを選択します。次のメッセージが表示されます。

```
*******************************************
Please type 'setup' to configure the appliance
*******************************************
```

ステップ 5 プロンプトで、**setup** と入力し、セットアップ プログラムを起動します。セットアップ プログラム パラメータの詳細については、「Cisco ISE のセットアッププログラムの実行 （40 ページ）」を参照してください。

ステップ 6 セットアップ モードでネットワーク設定パラメータを入力すると、アプライアンスが自動的に再起動し、シェル プロンプト モードに戻ります。

ステップ 7 シェル プロンプト モードを終了します。アプライアンスが起動します。

ステップ 8 「Cisco ISE インストールプロセスの確認 （45 ページ）」に進みます。

Cisco ISE のセットアッププログラムの実行

ここでは、ISE サーバーを設定するためのセットアップ プロセスについて説明します。

セットアップ プログラムでは、必要なパラメータの入力を求める、対話型のコマンドライン インターフェイス（CLI）が起動されます。管理者は、コンソールまたはダム端末とセットアップ プログラムを使用して、ISE サーバーの初期ネットワークを設定し、初期管理者資格情報を設定します。このセットアップ プロセスは一度だけ実行する設定作業です。

（注） Active Directory（AD）と統合する場合は、ISE 専用に作成された専用サイトから IP アドレスとサブネット アドレスを使用することをお勧めします。インストールと設定を行う前に、AD を担当する組織のスタッフに相談し、ISE ノードの関連する IP アドレスとサブネット アドレスを取得します。

（注） システムが不安定になる可能性があるため、Cisco ISE のオフラインインストールの試行は推奨しません。Cisco ISE のインストールスクリプトをオフラインで実行すると、次のエラーが表示されます。

NTP サーバーとの同期に失敗しました。時刻が正しくないと、再インストールされるまで、システムは使用できなくなる可能性があります。（Sync with NTP server failed' Incorrect time could render the system unusable until it is re-installed.）再試行? はい/いいえ [はい]（Y/N [Y]:）

[はい（Yes）] を選択してインストールを続けます。NTP サーバーとの同期を再試行するには、[いいえ（No）] を選択します。

インストールスクリプトの実行中に、NTP サーバーと DNS サーバーの両方とのネットワーク接続を確立することを推奨します。

セットアップ プログラムを実行するには、次の手順を実行します。

ステップ 1 インストール用に指定されているアプライアンスをオンにします。

次のセットアップ プロンプトが表示されます。

```
Please type 'setup' to configure the appliance
localhost login:
```

ステップ 2 ログイン プロンプトで **setup** と入力し、Enter を押します。

コンソールにパラメータのセットが表示されます。次の表の説明に従って、パラメータ値を入力する必要があります。

（注） IPv6 アドレスをもつドメイン ネーム サーバーまたは NTP サーバーを追加する場合は、ISE の eth0 インターフェイスを IPv6 アドレスで静的に設定する必要があります。

表 *12 : Cisco ISE* セットアップ プログラム パラメータ

プロンプト	説明	例
Hostname	19 文字以下にする必要があります。有効な文字には、英数字（A–Z、a–z、0–9）、およびハイフン（-）などがあります。最初の文字は文字である必要があります。 （注） Cisco ISE の証明書認証が、証明書による検証のわずかな違いの影響を受けないようにするために小文字を使用することをお勧めします。ノードのホスト名として「localhost」を使用することはできません。	isebeta1
(eth0) Ethernet interface address	ギガビットイーサネット 0（eth0）インターフェイスの有効な IPv4 アドレス またはグローバル IPv6 アドレスでなければなりません。	10.12.13.14/2001: 420: 54ff: 4:: 458: 121: 119
Netmask	有効な IPv4 または IPv6 のネットマスクでなければなりません。	255.255.255.0/2001: 420: 54ff: 4:: 458: 121: 119/122
Default gateway	デフォルトゲートウェイの有効な IPv4 アドレスまたはグローバル IPv6 アドレスでなければなりません。	10.12.13.1/2001: 420: 54ff: 4:: 458: 1
DNS domain name	IP アドレスは入力できません。有効な文字には、ASCII 文字、任意の数字、ハイフン（-）、およびピリオド（.）が含まれます。	example.com
Primary name server	プライマリ ネーム サーバーの有効な IPv4 アドレスまたはグローバル IPv6 アドレスでなければなりません。	10.15.20.25 /2001: 420: 54ff: 4:: 458: 118

プロンプト	説明	例
Add/Edit another name server	プライマリ ネーム サーバーの有効な IPv4 アドレスまたはグローバル IPv6 アドレスでなければなりません。	（オプション）複数のネーム サーバーを設定できます。これを行うには、**y** を入力して続行します。
Primary NTP server	有効なネットワーク タイム プロトコル（NTP）サーバーの IPv4 アドレスまたはグローバル IPv6 アドレスまたはホスト名でなければなりません。 （注） プライマリ NTP サーバーがアクセス可能であることを確認してください。	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	有効な NTP ドメインでなければなりません。	（オプション）複数の NTP サーバーを設定できます。これを行うには、**y** を入力して続行します。

プロンプト	説明	例
System Time Zone	有効な時間帯でなければなりません。たとえば、太平洋標準時（PST）では、システム時間帯はPST8PDT です（つまり、協定世界時（UTC）から 8 時間を差し引いた時間）。 （注） システム時刻とタイムゾーンが CIMC またはハイパーバイザ ホストの OS 時刻およびタイムゾーンと一致していることを確認します。タイムゾーン間に不一致がある場合、システムパフォーマンスが影響を受ける可能性があります。 サポートされているタイムゾーンのすべてのリストについては、Cisco ISE CLI から **show timezones** コマンドを実行できます。 （注） すべての Cisco ISE ノードを UTC タイム ゾーンに設定することをお勧めします。このタイムゾーンの設定により、デプロイメント環境におけるさまざまなノードからのレポート、ログ、およびポスチャ エージェントのログ ファイルが、タイムスタンプで常に同期されるようになります。	UTC（デフォルト）

プロンプト	説明	例
Username	Cisco ISE システムへの CLI アクセスに使用される管理者ユーザー名を特定します。デフォルト（admin）を使用しない場合は、新しいユーザー名を作成する必要があります。ユーザー名は、3 ～ 8 文字の長さで、有効な英数字（A ～ Z、a ～ z、または 0 ～ 9）で構成される必要があります。	admin（デフォルト）
Password	Cisco ISE システムへの CLI アクセスに使用される管理者パスワードを特定します。デフォルト パスワードは存在しないため、続行するにはパスワードを作成する必要があります。パスワードの長さは 6 文字以上で、少なくとも 1 つの小文字（a–z）、1 つの大文字（A-Z）、および 1 つの数字（0–9）を含める必要があります。	MyIseYPass2

（注） CLI でインストール中またはインストール後に管理者のパスワードを作成する際に、パスワードの最後の文字の場合を除いて文字「$」を使わないでください。この文字が最初または後続の文字にあると、パスワードは受け入れられますが、CLI へのログインには使用できません。

誤ってこのようなパスワードを作成した場合は、コンソールにログインし、CLI コマンドを使用するか、ISE CD または ISO ファイルを取得して、パスワードをリセットします。ISO ファイルを使用してパスワードをリセットする手順は、次のドキュメントで説明されています。
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

セットアップ プログラムを実行すると、システムが自動的に再起動します。

これで、セットアップ プロセスで設定したユーザー名とパスワードを使用して Cisco ISE にログインできるようになります。

Cisco ISE インストールプロセスの確認

インストール プロセスが正しく完了したことを確認するには、次の手順を実行します。

ステップ 1 システムが再起動したら、ログイン プロンプトでセットアップ時に設定したユーザー名を入力し、Enter を押します。

ステップ 2 新しいパスワードを入力します。

ステップ 3 アプリケーションが適切にインストールされていることを確認するために、**show application** コマンドを入力し、Enter を押します。
コンソールに次のメッセージが表示されます。

```
ise/admin# show application
<name>          <Description>
ise             Cisco Identity Services Engine
```

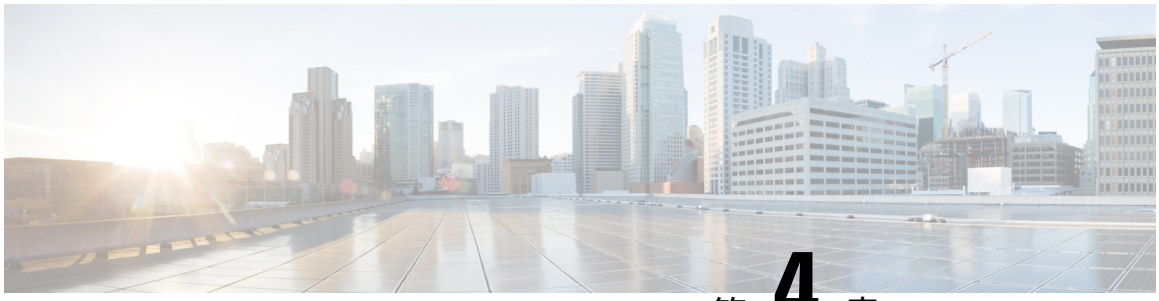
（注） このリリースの別のバージョンでは、バージョンと日付が変更されている場合があります。

ステップ 4 **show application status ise** コマンドを入力して ISE プロセスの状態を確認し、Enter を押します。
コンソールに次のメッセージが表示されます。

```
ise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
------------------------------------------------------------------
Database Listener                      running          14890
Database Server                        running          70 PROCESSES
Application Server                     running          19158
Profiler Database                      running          16293
ISE Indexing Engine                    running          20773
AD Connector                           running          22466
M&T Session Database                   running          16195
M&T Log Collector                      running          19294
M&T Log Processor                      running          19207
Certificate Authority Service          running          22237
EST Service                            running          29847
SXP Engine Service                     disabled
Docker Daemon                          running          21197
TC-NAC Service                         disabled
Wifi Setup Helper Container            not running
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled

ise/admin#
```



第 4 章

その他のインストール情報

SNS アプライアンス リファレンス

Cisco ISE をインストールするためのブート可能な USB デバイスの作成

LiveUSB-creator ツールを使用して、Cisco ISE のインストール ISO ファイルからのブート可能な USB デバイスを作成します。

始める前に

- https://github.com/lmacken/liveusb-creator/releases/tag/3.12.0 LiveUSB-creator をローカルシステムにダウンロードします。
- ローカル システムに Cisco ISE のインストール ISO ファイルをダウンロードします。
- 16 GB または 32 GB の USB デバイスを使用します。

ステップ 1 すべての領域を解放するには、FAT16 または FAT32 を使用して USB デバイスを再フォーマットします。

ステップ 2 ローカルシステムに USB デバイスを差し込み、**LiveUSB-creator** を起動します。

ステップ 3 [既存のLive CDを使用（Use Existing Live CD）] エリアの [参照（Browse）] をクリックし、Cisco ISE ISO ファイルを選択します。

ステップ 4 [ターゲットデバイス（Target Device）] ドロップダウンリストから USB デバイスを選択します。

ローカルシステムに接続された USB デバイスが 1 つだけの場合は、自動的に選択されます。

ステップ 5 [Live USBを作成（Create Live USB）] をクリックします。

経過表示バーに、ブート可能な USB 作成の進捗状況が表示されます。このプロセスが完了したら、USB ドライブの内容が、USB ツールを実行するために使用したローカルシステムで使用できます。Cisco ISE をインストールする前に、手動で更新する必要があるテキスト ファイルが 2 つあります。

ステップ 6 USB ドライブから、テキスト エディタで次のテキスト ファイルを開きます。

- isolinux/isolinux.cfg または syslinux/syslinux.cfg
- EFI/BOOT/grub.cfg

ステップ 7 両方のファイルの「**cdrom**」という記述を置き換えます。

- SNS 3515、3595、3615、3655、または 3695 アプライアンスがある場合、両方のファイルで「**cdrom**」という記述を「**hd:sdb1**」に置き換えます。

具体的には、「**cdrom**」という文字列のすべてのインスタンスを置き換えます。たとえば、

ks=*cdrom*/ks.cfg

これを次のように書き換えます。

ks=*hd:sdb1:*/ks.cfg

ステップ 8 ファイルを保存して終了します。

ステップ 9 安全に、ローカル システムから USB デバイスを削除します。

ステップ 10 ブート可能な USB デバイスを Cisco ISE アプライアンスに挿入し、アプライアンスを再起動して、USB ドライブから起動して Cisco ISE をインストールします。

Cisco SNS 3500/3600 シリーズ アプライアンスの再イメージ化

Cisco SNS 3500/3600 シリーズ アプライアンスには DVD ドライブがありません。したがって、Cisco ISE ソフトウェアを使用して Cisco ISE ハードウェア アプライアンスを再イメージ化するには、次のいずれかを実行します。

（注） SNS 3500 および 3600 シリーズ アプライアンスは Unified Extensible Firmware Interface（UEFI）のセキュア ブート機能をサポートしています。この機能は、Cisco ISE の署名付きイメージだけを SNS 3500 および 3600 シリーズ アプライアンスにインストールできるようにし、デバイスに物理アクセスしたとしても未署名のオペレーティング システムはインストールできないようにします。たとえば、Red Hat Enterprise Linux や Microsoft Windows などの一般的なオペレーティング システムは、このアプライアンスで起動できません。

SNS 3515 および SNS 3595 アプライアンスは、Cisco ISE 2.0.1 以降のリリースのみをサポートしています。SNS 3515 または SNS 3595 アプライアンスに、2.0.1 よりも前のリリースをインストールすることはできません。

- Cisco Integrated Management Controller（CIMC）インターフェイスを使用して、仮想 DVD デバイスにインストール .iso ファイルをマッピングします。詳細については、「#unique_52」を参照してください。

- インストール .iso ファイルを使用してインストール DVD を作成し、USB 外部 DVD ドライブを挿入して、DVD ドライブからアプライアンスを起動します。
- インストール .iso ファイルを使用してブート可能な USB デバイスを作成して、USB ドライブからアプライアンスを起動します。詳細については、「#unique_53」と「#unique_52」を参照してください。

VMware 仮想マシン

（注） このドキュメントに記載されている VMware フォームファクタの手順は、Cisco HyperFlex にインストールされている Cisco ISE にも適用されます。

仮想マシンのリソースおよびパフォーマンスのチェック

仮想マシンに Cisco ISE をインストールする前に、インストーラによって、仮想マシンの利用可能なハードウェアリソースと推奨される仕様を比較することで、ハードウェアの整合性チェックが行われます。

VM リソースのチェック中、インストーラは、ハードディスク領域、VM に割り当てられた CPU コアの数、CPU クロック速度、および VM に割り当てられた RAM をチェックします。VM リソースが基本評価仕様を満たさない場合、インストールは終了します。このリソースチェックは、ISO ベースのインストールにのみ適用されます。

セットアッププログラムを実行すると、VM パフォーマンスチェックが実行され、インストーラがディスク I/O パフォーマンスをチェックします。ディスク I/O パフォーマンスが推奨される仕様を満たさない場合、警告が画面に表示されますが、インストールを続行できます。

VM パフォーマンスチェックは定期的に（毎時）実行され、結果は 1 日で平均されます。ディスク I/O パフォーマンスが推奨される仕様を満たさない場合、アラームが生成されます。

VM パフォーマンス チェックは、**show tech-support** コマンドを使用して Cisco ISE CLI からオン デマンドで実行することもできます。

VM のリソースおよびパフォーマンスのチェックは Cisco ISE のインストールとは無関係に実行できます。このテストは Cisco ISE 起動メニューから実行できます。

ISO ファイルを使用した VMware 仮想マシンへの Cisco ISE のインストール

このセクションでは、ISO ファイルを使用して VMware 仮想マシンに Cisco ISE をインストールする方法について説明します。

VMware ESXi サーバーを設定するための前提条件

VMware ESXi サーバーを設定する前に、このセクションに記載されている次の設定の前提条件を確認してください。

- 管理者権限を持つユーザー（root ユーザー）として ESXi サーバーにログインする必要があります。
- Cisco ISE は 64 ビット システムです。64 ビット システムをインストールする前に、仮想化テクノロジー（VT）が ESXi サーバーで有効になっていることを確認してください。
- VMware 仮想マシンディスク領域の推奨量を割り当てていることを確認してください。詳細については、「#unique_31」を参照してください。
- VMware Virtual Machine File System（VMFS）を作成していない場合は、Cisco ISE 仮想アプライアンスをサポートするために作成する必要があります。VMFS は、VMware ホスト上に設定されたストレージボリュームごとに設定されます。VMFS5 では、1 MB のブロック サイズは最大で 1.999 TB の仮想ディスク サイズをサポートします。

仮想化テクノロジーのチェック

すでに ESXi サーバーをインストールしている場合は、マシンを再起動せずに、仮想化テクノロジーが有効かどうかを確認できます。これを行うには、**esxcfg-info**コマンドを使用します。次に例を示します。

```
~ # esxcfg-info |grep "HV Support"
|----HV Support.......................................3
|----World Command Line..............................grep HV Support
```

HV サポートの値が 3 の場合、VT は ESXi サーバーで有効であるため、インストールに進むことができます。

HV サポートの値が 2 の場合、VT はサポートされていますが、ESXi サーバーで有効になっていません。BIOS 設定を編集し、サーバーで VT を有効にする必要があります。

ESXi サーバーでの仮想化テクノロジーの有効化

Cisco ISE 仮想マシンの以前のバージョンをホストするために使用したものと同じハードウェアを再利用できます。ただし、最新のリリースをインストールする前に、ESXi サーバーで仮想化テクノロジー（VT）を有効にする必要があります。

ステップ 1 アプライアンスをリブートします。
ステップ 2 F2 を押して、セットアップを開始します。
ステップ 3 **[詳細設定（Advanced）]** > **[プロセッサの設定（Processor Configuration）]** を選択します。
ステップ 4 [Intel(R) VT] を選択して、有効にします。
ステップ 5 変更を保存し、終了するには、F10 を押します。

Cisco ISE プロファイラ サービスに対する VMware サーバー インターフェイスの設定

VMware サーバー インターフェイスを、スイッチ ポート アナライザ（SPAN）またはミラー化されたトラフィックの Cisco ISE プロファイラ サービスの専用プローブ インターフェイスへの収集をサポートするように設定します。

ステップ 1 **[設定（Configuration）]>[ネットワーキング（Networking）]>[プロパティ（Properties）]>[VMNetwork]**（VMware サーバーインスタンスの名前）> [VMswitch0]（VMware ESXi サーバーインターフェイスの 1 つ）> [プロパティ（Properties）] > [セキュリティ（Security）] の順に選択します。

ステップ 2 [セキュリティ（Security）] タブの [ポリシー例外（Policy Exceptions）] ペインで [プロミスキャスモード（Promiscuous Mode）] チェックボックスをオンにします。

ステップ 3 [プロミスキャスモード（Promiscuous Mode）] ドロップダウン リストで、[承認（Accept）] を選択し、[OK] をクリックします。

SPAN またはミラー化されたトラフィックのプロファイラ データ収集に使用する他の VMware ESXi サーバー インターフェイスで同じ手順を繰り返し行ってください。

シリアル コンソールを使用した VMware サーバーへの接続

ステップ 1 特定の VMware サーバー（たとえば ISE-120）の電源をオフにします。

ステップ 2 VMware サーバーを右クリックし、[編集（Edit）] を選択します。

ステップ 3 [ハードウェア（Hardware）] タブで [追加（Add）] をクリックします。

ステップ 4 [シリアルポート（Serial Port）] を選択し、[次へ（Next）] をクリックします。

ステップ 5 [シリアルポート出力（Serial Port Output）] 領域で、[ホストの物理シリアルポートを使用（Use physical serial port on the host）] または [ネットワーク経由で接続（Connect via Network）] オプション ボタンを使用して、[次へ（Next）] をクリックします。

- [ネットワーク経由で接続（Connect via Network）] オプションを選択した場合は、ESXi サーバー上のファイアウォール ポートを開く必要があります。
- [ホストの物理シリアルポートを使用（Use physical serial port on the host）] を選択する場合は、ポートを選択します。次の 2 つのいずれかのオプションを選択できます。
  - **/dev/ttyS0**（DOS または Windows オペレーティング システムで、これは COM1 として表示されます）。
  - **/dev/ttyS1**（DOS または Windows オペレーティング システムで、これは COM2 として表示されます）。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [デバイスステータス（Device Status）] 領域で、適切なチェックボックスをオンにします。デフォルトは [接続済み（Connected）] です。

ステップ 8 VMware サーバーに接続するには、[OK] をクリックします。

VMware サーバーの設定

始める前に

「VMware ESXi サーバーを設定するための前提条件」を必ず読みます。

ステップ 1 ESXi サーバーにログインします。

ステップ 2 VMware vSphere Client の左側のペインで、ホスト コンテナを右クリックして、[新規仮想マシン（New Virtual Machine）] を選択します。

ステップ 3 [設定（Configuration）] ダイアログボックスで、VMware 設定に [カスタム（Custom）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 VMware システムの名前を入力し、[次へ（Next）] をクリックします。

ヒント VMware ホストに使用するホスト名を使用します。

ステップ 5 推奨される使用可能な領域があるデータストアを選択し [次へ（Next）] をクリックします。

ステップ 6 （オプション）VM ホストまたはクラスタが複数の VMware 仮想マシン バージョンをサポートする場合は、[仮想マシンバージョン7（Virtual Machine Version 7）] などの仮想マシン バージョンを選択して、[次へ（Next）] をクリックします。

ステップ 7 [Linux] を選択し、[バージョン（Version）] ドロップダウンリストからサポートされている Red Hat Enterprise Linux バージョンを選択します。

ステップ 8 [仮想ソケット数（Number of virtual sockets）] および [仮想ソケットあたりのコア数（Number of cores per virtual socket）] ドロップダウン リストで、値を選択します。コアの総数は以下にする必要があります。

SNS 3600 シリーズ アプライアンス：

- 小規模：16
- 中規模：24
- 大規模：24

コアの数は、ハイパースレッディングにより、Cisco Secure Network Server 3600 シリーズのコア数の 2 倍です。たとえば、小規模ネットワーク展開の場合、8 個の CPU コアまたは 16 個のスレッドを持つ SNS 3615 の CPU 仕様を満たすために、16 個の vCPU コアを割り当てる必要があります。

（注） リソースの割り当てに合わせて CPU とメモリのリソースを予約することを強くお勧めします。これを行わない場合は ISE のパフォーマンスと安定性に大きく影響することがあります。

ステップ 9 メモリ容量を選択し、[次へ（Next）] をクリックします。

ステップ 10 [E1000] NIC ドライバを [アダプタ（Adapter）] ドロップダウンリストから選択し、[次へ（Next）] をクリックします。

（注） デフォルトで正しいアダプタ順序を確保するために、E1000 を選択することをお勧めします。VMXNET3 を選択した場合、ISE のアダプタ順序と同期させるために ESXi アダプタを再マップしなければならない場合があります。

ステップ 11 SCSI コントローラに [準仮想化（Paravirtual）] を選択し、[次へ（Next）] をクリックします。

ステップ 12 [新規仮想ディスクの作成（Create a new virtual disk）] を選択し、[次へ（Next）] をクリックします。

ステップ 13 [ディスクプロビジョニング（Disk Provisioning）] ダイアログボックスで、[シックプロビジョニング（eagerly zeroed）（Thick provisioned, eagerly zeroed）] オプションボタンをクリックし、[次へ（Next）] をクリックして続行します。

Cisco ISE は、シック プロビジョニングとシン プロビジョニングの両方をサポートします。ただし、特にモニターリングノードでは、パフォーマンスを高めるために、シックプロビジョニング（eagerly zeroed）を選択することをお勧めします。シン プロビジョニングを選択した場合は、最初のディスク拡張中に、より多くのディスク領域が必要なアップグレード、バックアップと復元、デバッグ ロギングなどの操作に影響が出ることがあります。

ステップ 14 [フォルトトレランスのようなクラスタリング機能をサポートする（Support clustering features such as Fault Tolerance）] チェックボックスの選択を解除します。

ステップ 15 詳細オプションを選択し、[次へ（Next）] をクリックします。

ステップ 16 新しく作成された VMware システムの名前、ゲスト OS、CPU、メモリ、およびディスク サイズなどの設定の詳細を確認します。

ステップ 17 [終了（Finish）] をクリックします。

これで、VMware システムがインストールされました。

次のタスク

新しく作成された VMware システムをアクティブにするには、VMware クライアントのユーザー インターフェイスの左側のペインで [VM] を右クリックして、[電源（Power）] > [電源オン（Power On）] を選択します。

仮想マシン電源オン起動遅延設定の延長

VMware 仮想マシンでは、起動遅延はデフォルトで 0 に設定されています。この起動遅延を変更して、起動オプション（例：管理者パスワードの再設定）を選択できます。

ステップ 1 vSphere Client から、VM を右クリックして [設定の編集（Edit Settings）] を選択します。

ステップ 2 [オプション（Options）] タブをクリックします。

ステップ 3 [詳細設定（Advanced）] > [起動オプション（Boot Options）] を選択します。

ステップ 4 [電源オン起動遅延（Power on Boot Delay）] 領域で、起動処理を遅延させる時間（ミリ秒）を選択します。

ステップ 5 [強制BIOS設定（Force BIOS Setup）] 領域のチェックボックスをオンにして、次回の VM 起動時に BIOS 設定画面を表示します。

ステップ 6 [OK] をクリックして変更を保存します。

VMware システムへの Cisco ISE ソフトウェアのインストール

始める前に

- インストール後に、永続ライセンスをインストールしない場合、Cisco ISE は自動的に最大 100 エンドポイントをサポートする 90 日間の評価ライセンスをインストールします。
- Cisco ISE ソフトウェアを Cisco ソフトウェアのダウンロード サイト（http://www.cisco.com/en/US/products/ps11640/index.html）からダウンロードし、DVD に書き込みます。Cisco.com クレデンシャルの提供が求められます。
- （オプション：VMware クラウドに Cisco ISE をインストールしている場合にのみ適用）VMware クラウドに Cisco ISE をインストールするプロセスは、VMware 仮想マシンに Cisco ISE をインストールするプロセスとまったく同じです。
  - Amazon Web サービス（AWS）の VMware クラウドに展開された Cisco ISE 仮想マシン：Cisco ISE は、AWS の VMware クラウドが提供するソフトウェア定義型データセンター（SDDC）でホストできます。オンプレミス展開、必要なデバイスとサービスへの到達可能性を有効にするために、セキュリティ グループ ポリシーが VMware クラウドで設定されていることを確認します（[ネットワーキングとセキュリティ（Networking and Security）] > [セキュリティ（Security）] > [ゲートウェイ ファイアウォール設定（Gateway Firewall Settings）]）。
  - Azure VMware ソリューション（AVS）に展開された Cisco ISE 仮想マシン：AVS は Microsoft Azure で VMware ワークロードをネイティブに実行します。Cisco ISE は VMware 仮想マシンとしてホストできます。

ステップ 1 VMware クライアントにログインします。

ステップ 2 仮想マシンを BIOS セットアップモードにするために、VM を右クリックして [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [オプション（Options）] タブをクリックします。

ステップ 4 [BIOSの強制設定（Force BIOS Setup）] 領域で [ブートオプション（Boot Options）] をクリックし、[BIOS] チェックボックスをオンにして、VM 起動時に BIOS 設定画面に入ります。

（注） 2 TB 以上の GPT パーティションをブートするには、VM 設定のブートモードでファームウェアを **BIOS** から **EFI** に変更する必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 協定世界時（UTC）および正しいブート順序が BIOS に設定されていることを確認します。

a) VM の電源がオンになっている場合は、システムの電源をオフにします。

b) VM をオンにします。

システムが BIOS セットアップ モードになります。

c) [BIOS] メニューで、矢印キーを使用して [日付と時刻（Date and Time）] フィールドに移動し、**Enter**を押します。

d) UTC/グリニッジ標準時（GMT）タイム ゾーンを入力します。

このタイム ゾーンの設定により、デプロイメント環境におけるさまざまなノードからのレポート、ログ、およびポスチャ エージェントのログ ファイルが、タイムスタンプで常に同期されるようになります。

e) 矢印キーを使用して [起動（Boot）] メニューに移動し、Enter を押します。

f) 矢印キーを押して、[CD-ROMドライブ（CD-ROM Drive）] を選択し、+ を押して CD-ROM ドライブを順序の先頭に移動します。

g) 矢印キーを使用して [終了（Exit）] メニューに移動し、[変更を保存して終了（Exit Saving Changes）] を選択します。

h) [はい（Yes）] を選択して変更を保存し、終了します。

ステップ 7 Cisco ISE ソフトウェア DVD を VMware ESXi ホストの CD/DVD ドライブに挿入して、仮想マシンをオンにします。

DVD の起動時、コンソールには次のように表示されます。

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

ステップ 8 矢印キーを使用して [Cisco ISEのインストール（シリアル コンソール）（Cisco ISE Installation (Serial Console)）] または [Cisco ISEのインストール（キーボード/モニター）（Cisco ISE Installation (Keyboard/Monitor)）] を選択して、Enter キーを押します。シリアル コンソール オプションを選択する場合は、仮想マシンでシリアル コンソールをセットアップしておく必要があります。コンソールの作成方法については、『VMware vSphere Documentation』を参照してください。
インストーラが、VMware システムへの Cisco ISE ソフトウェアのインストールを開始します。インストール プロセスが完了するまで、20 分かかります。インストール プロセスが終了すると、仮想マシンは自動的に再起動されます。VM の再起動時に、コンソールに次のように表示されます。

```
Type 'setup' to configure your appliance
localhost:
```

ステップ 9 システム プロンプトで、**setup** と入力し、Enter を押します。

（注） Cisco ISEリリース3.0以降、ISE仮想マシンをホストする仮想化プラットフォームのCPUは、（ストリーミングSIMD拡張）SSE 4.2命令セットをサポートする必要があります。そうしないと、特定のISEサービス（ISE APIゲートウェイなど）が機能せず、Cisco ISE GUIを起動できません。2011年以降は、Intel プロセッサと AMD プロセッサの両方が SSE 4.2 バージョンをサポートしています。

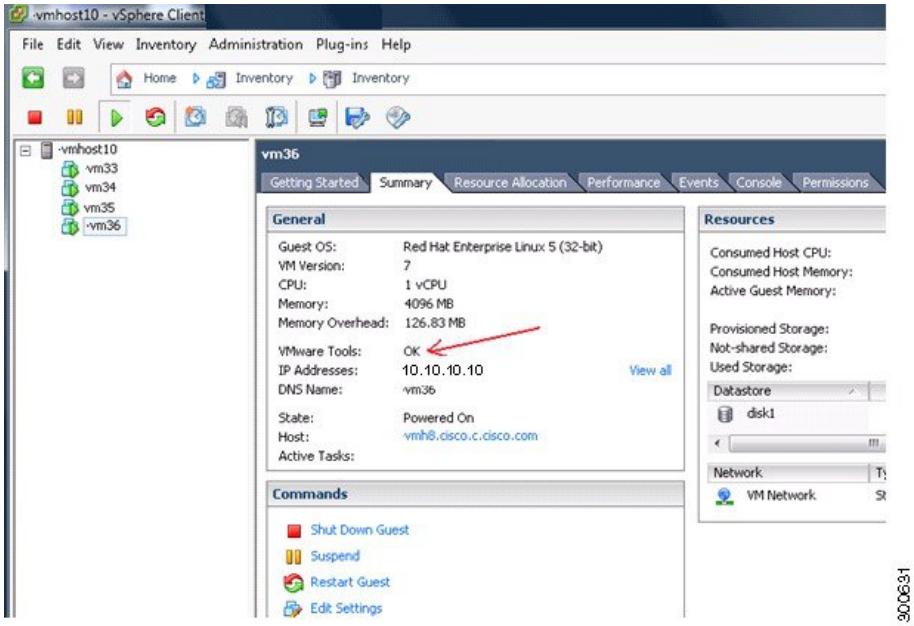
セットアップ ウィザードが表示され、ウィザードに従って初期設定を実行します。

VMware ツールのインストールの確認

vSphere Client の [概要（Summary）] タブを使用した VMware ツールのインストールの確認

vShpere Client で指定された VMware ホストの [概要（Summary）] タブに移動します。[VMware ツール（VMware Tools）] フィールドの値が OK である必要があります。

図 *7: vSphere Client* での *VMware* ツールの確認



CLI を使用した VMware ツールのインストールの確認

show inventory コマンドを使用して、VMware ツールがインストールされているかどうかを確認することもできます。このコマンドはNIC ドライバ情報をリストします。VMware ツールがインストールされている仮想マシンの [ドライバの説明（Driver Descr）] フィールドに、VMware Virtual Ethernet ドライバが表示されます。

```
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9       , VID: A0  , SN: FCH184X9XXX
Total RAM Memory: 65700380 kB
CPU Core Count: 16
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 4: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 5: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 6: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 7: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 8: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 9: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 10: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 11: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 12: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 13: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 14: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
```

```
CPU 15: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /xxx/abc
Disk 0: Capacity: 1198.00 GB
NIC Count: 6
NIC 0: Device Name: eth0:
NIC 0: HW Address: xx:xx:xx:xx:xx:xx
NIC 0: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 1: Device Name: eth1:
NIC 1: HW Address: xx:xx:xx:xx:xx:xx
NIC 1: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: HW Address: xx:xx:xx:xx:xx:xx
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: HW Address: xx:xx:xx:xx:xx:xx
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: HW Address: xx:xx:xx:xx:xx:xx
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
NIC 5: HW Address: xx:xx:xx:xx:xx:xx
NIC 5: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical.
```

VMware ツールのアップグレードのサポート

Cisco ISE ISO イメージ（通常、アップグレード、またはパッチ）には、サポートされる VMware ツールが含まれています。VMware クライアント ユーザー インターフェイスを使用した VMware ツールのアップグレードは、Cisco ISE ではサポートされていません。VMware ツールを新しいバージョンにアップグレードする場合、サポートは Cisco ISE の新しいバージョンで提供されます（通常、アップグレード、またはパッチ リリース）。

Cisco ISE 仮想マシンの複製

Cisco ISE VMware 仮想マシン（VM）を複製し、Cisco ISE ノードの厳密なレプリカを作成することができます。たとえば、複数のポリシー サービス ノード（PSN）を使用した分散デプロイメント環境で、VM の複製は PSN を迅速かつ効率的にデプロイするのに役立ちます。PSN をそれぞれ別個にインストールして設定する必要はありません。

テンプレートを使用して Cisco ISE VM を複製することもできます。

（注） 複製には VMware vCenter が必要です。セットアップ プログラムを実行する前に、複製を行う必要があります。

始める前に

- 複製する Cisco ISE VM を確実にシャットダウンします。vSphere Client で、複製する Cisco ISE VM を右クリックし、**[電源（Power）]**>**[ゲストをシャットダウン（Shut Down Guest）]** を選択します。

- 複製されたマシンの IP アドレスとホスト名を変更したことを確認してから、そのマシンの電源を入れて、ネットワークに接続します。

ステップ 1 管理者権限を持つユーザー（root ユーザー）として ESXi サーバーにログインします。

この手順を実行するには VMware vCenter が必要です。

ステップ 2 複製する Cisco ISE VM を右クリックし、[複製（Clone）] をクリックします。

ステップ 3 [名前とロケーション（Name and Location）] ダイアログボックスに作成する新しいマシンの名前を入力し、[次へ（Next）] をクリックします。

これは、新しく作成する Cisco ISE VM のホスト名ではなく、参照のための説明となる名前です。

ステップ 4 新しい Cisco ISE VM を実行するホストまたはクラスタを選択し、[次へ（Next）] をクリックします。

ステップ 5 作成している新しい Cisco ISE VM 用のデータストアを選択して、[次へ（Next）] をクリックします。

このデータストアは、ESXi サーバー上のローカル データストアまたはリモート ストレージの場合があります。データストアに十分なディスク領域があることを確認します。

ステップ 6 [ディスクフォーマット（Disk Format）] ダイアログボックスで [ソースと同じフォーマット（Same format as source）] オプション ボタンをクリックし、[次へ（Next）] をクリックします。

このオプションは、この新しいマシンの複製元である Cisco ISE VM で使用されているのと同じフォーマットをコピーします。

ステップ 7 [ゲストカスタマイズ（Guest Customization）] ダイアログボックスで [カスタマイズしない（Do not customize）] オプション ボタンをクリックし、[次へ（Next）] をクリックします。

ステップ 8 [終了（Finish）] をクリックします。

次のタスク

- 複製された仮想マシンの IP アドレスおよびホスト名の変更
- 複製された Cisco 仮想マシンのネットワークへの接続

テンプレートを使用した Cisco ISE 仮想マシンの複製

vCenter を使用している場合は、VMware テンプレートを使用して、Cisco ISE 仮想マシン（VM）を複製できます。テンプレートに Cisco ISE ノードを複製し、そのテンプレートを使用して、複数の新しい Cisco ISE ノードを作成できます。テンプレートを使用した仮想マシンの複製は、次の 2 つのステップで構成される手順です。

始める前に

（注） 複製には VMware vCenter が必要です。セットアップ プログラムを実行する前に、複製を行う必要があります。

ステップ 1 #unique_73

ステップ 2 #unique_74

仮想マシン テンプレートの作成

始める前に

- 複製する Cisco ISE VM を確実にシャットダウンします。vSphere Client で、複製する Cisco ISE VM を右クリックし、[電源（Power）]>[ゲストをシャットダウン（Shut Down Guest）] を選択します。
- テンプレートは、インストールしたばかりでセットアップ プログラムを実行していない Cisco ISE VM から作成することをお勧めします。これにより、IP アドレスおよびホスト名を個別に作成し、設定した Cisco ISE の各ノードでセットアップ プログラムをそれぞれ実行できるようになります。

ステップ 1 管理者権限を持つユーザー（root ユーザー）として ESXi サーバーにログインします。

この手順を実行するには VMware vCenter が必要です。

ステップ 2 複製する Cisco ISE VM を右クリックし、**[複製（Clone）]** > **[テンプレートに複製（Clone to Template）]** を選択します。

ステップ 3 テンプレートの名前を入力し、[名前とロケーション（Name and Location）] ダイアログボックスでテンプレートを保存する場所を選択して、[次へ（Next）] をクリックします。

ステップ 4 テンプレートを保存する ESXi ホストを選択して、[次へ（Next）] をクリックします。

ステップ 5 テンプレートを保存するデータストアを選択して、[次へ（Next）] をクリックします。

このデータストアに必要なディスク領域があることを確認します。

ステップ 6 [ディスクフォーマット（Disk Format）] ダイアログボックスで [ソースと同じフォーマット（Same format as source）] オプション ボタンをクリックし、[次へ（Next）] をクリックします。

[完了前の確認（Ready to Complete）] ダイアログボックスが表示されます。

ステップ 7 [終了（Finish）] をクリックします。

仮想マシン テンプレートのデプロイメント

仮想マシン テンプレートを作成したら、他の仮想マシン（VM）にデプロイできます。

ステップ 1 作成した Cisco ISE VM テンプレートを右クリックして、[このテンプレートから仮想マシンをデプロイ（Deploy Virtual Machine from this template）] を選択します。

ステップ 2 新しい Cisco ISE ノードの名前を入力し、[名前とロケーション（Name and Location）] ダイアログボックスでノードの場所を選択して、[次へ（Next）] をクリックします。

ステップ 3 新しい Cisco ISE ノードを保存する ESXi ホストを選択して、[次へ（Next）] をクリックします。

ステップ 4 新しい Cisco ISE に使用するデータストアを選択して、[次へ（Next）] をクリックします。

このデータストアに必要なディスク領域があることを確認します。

ステップ 5 [ディスクフォーマット（Disk Format）] ダイアログボックスで [ソースと同じフォーマット（Same format as source）] オプション ボタンをクリックし、[次へ（Next）] をクリックします。

ステップ 6 [ゲストカスタマイズ（Guest Customization）] ダイアログボックスの [カスタマイズしない（Do not customize）] オプション ボタンをクリックします。

[完了前の確認（Ready to Complete）] ダイアログボックスが表示されます。

ステップ 7 [仮想ハードウェアの編集（Edit Virtual Hardware）] チェックボックスをオンにして、[続行（Continue）] をクリックします。

[仮想マシンのプロパティ（Virtual Machine Properties）] ページが表示されます。

ステップ 8 [ネットワークアダプタ（Network Adapter）] を選択し、[接続済み（Connected）] チェックボックスおよび [電源投入時に接続（Connect at power on）] チェックボックスをオフにして、[OK] をクリックします。

ステップ 9 [終了（Finish）] をクリックします。

この Cisco ISE ノードの電源を投入し、IP アドレスとホスト名を設定し、ネットワークに接続できるようになりました。

次のタスク

- 複製された仮想マシンの IP アドレスおよびホスト名の変更
- 複製された Cisco 仮想マシンのネットワークへの接続

複製された仮想マシンの IP アドレスおよびホスト名の変更

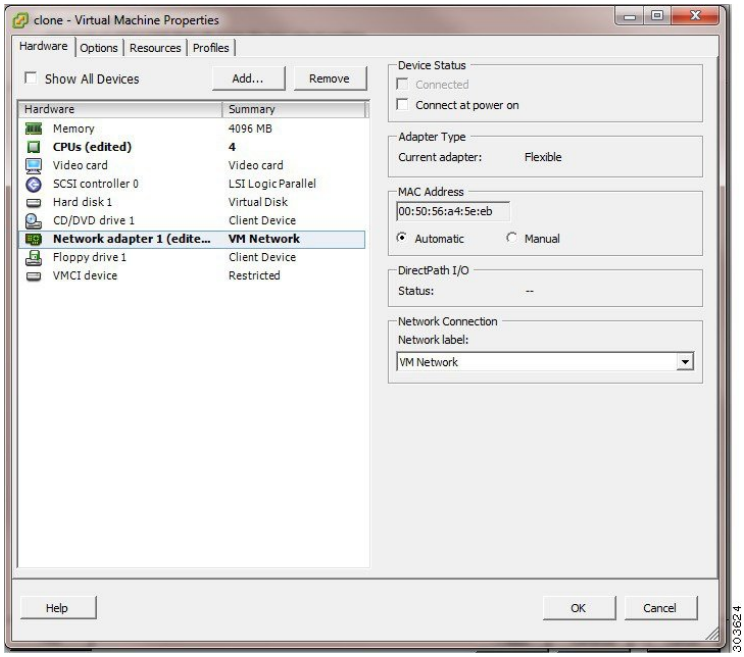
Cisco ISE 仮想マシン（VM）を複製したら、そのマシンの電源を入れて、IP アドレスとホスト名を変更する必要があります。

始める前に

- Cisco ISE ノードがスタンドアロン状態であることを確認します。

- 新しく複製された Cisco ISE VM に電源を入れるときに、このマシンにネットワーク アダプタが接続されていないことを確認します。[接続済み（Connected）] および [電源投入時に接続（Connect at power on）] チェックボックスをオフにします。オフにしない場合、このノードが起動すると、複製元のマシンと同じ IP アドレスが使用されます。

図 *8*：ネットワーク アダプタの接続解除



- 新しく複製された VM マシンの電源を入れたらすぐに、このマシン用に設定する IP アドレスとホスト名があることを確認します。この IP アドレスおよびホスト名のエントリは DNS サーバーにある必要があります。ノードのホスト名として「localhost」を使用することはできません。
- 新しい IP アドレスまたはホスト名に基づく Cisco ISE ノードの証明書があることを確認します。

手順

ステップ 1 新しく複製された Cisco ISE VM を右クリックして、**[電源（Power）] > [電源オン（Power On）]** を選択します。

ステップ 2 新しく複製された Cisco ISE VM を選択して、[コンソール（Console）] タブをクリックします。

ステップ 3 Cisco ISE CLI で、次のコマンドを入力します。

```
configure terminal
hostname hostname
```

hostname は、設定する新しいホスト名です。Cisco ISE サービスが再起動されます。

ステップ 4 次のコマンドを入力します。

```
interface gigabit 0
ip address ip_address netmask
```

ip_address は、ステップ 3 で入力したホスト名に対応するアドレスであり、netmask はその ip_address のサブネット マスクです。システムにより、Cisco ISE サービスを再起動するように求められます。ip address コマンドおよび hostname コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

ステップ 5 **Y** を入力して、Cisco ISE サービスを再起動します。

複製された Cisco 仮想マシンのネットワークへの接続

電源を入れ、IP アドレスおよびホスト名を変更したら、ネットワークに Cisco ISE ノードを接続する必要があります。

ステップ 1 新しく複製された Cisco ISE 仮想マシン（VM）を右クリックして、[設定の編集（Edit Settings）] をクリックします。

ステップ 2 [仮想マシンのプロパティ（Virtual Machine Properties）] ダイアログボックスで [ネットワークアダプタ（Network Adapter）] をクリックします。

ステップ 3 [デバイスステータス（Device Status）] 領域で、[接続済み（Connected）] チェックボックスおよび [電源投入時に接続（Connect at power on）] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

評価環境から実稼働環境への Cisco ISE VM の移行

Cisco ISE リリースを評価した後、評価システムから完全ライセンスを持つ実稼働システムに移行できます。

始める前に

- より多くのユーザーをサポートする実稼働環境に VMware サーバーを移動する場合は、Cisco ISE インストールを必ず推奨される最小ディスク サイズ以上（最大許容サイズは 2.4 TB）に再設定してください。
- 300 GB 未満のディスク容量を使用して作成された VM から実稼働 VM にはデータを移行できないことに注意してください。300 GB 以上のディスク容量を使用して作成された VM のデータのみ実稼働環境に移行できます。

ステップ 1 評価版の設定をバックアップします。

ステップ 2 実稼働 VM に必要なディスク領域があることを確認します。

ステップ 3 実稼働のデプロイメント ライセンスをインストールします。

ステップ 4 実稼働システムに設定を復元します。

仮想マシンパフォーマンスのオンデマンドでのチェック

CLI から **show tech-support** コマンドを実行して、VM のパフォーマンスをいつでもチェックできます。このコマンドの出力は次のようになります。

```
ise-vm123/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
**************************************
Average I/O bandwidth writing to disk device: 48 MB/second
Average I/O bandwidth reading from disk device: 193 MB/second
WARNING: VM I/O PERFORMANCE TESTS FAILED!
WARNING: The bandwidth writing to disk must be at least 50 MB/second,
WARNING: and bandwidth reading from disk must be at least 300 MB/second.
WARNING: This VM should not be used for production use until disk
WARNING: performance issue is addressed.
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 7.81502 s, 40.3 MB/s
Disk I/O bandwidth filesystem read test, reading 300 MB from /opt:
314572800 bytes (315 MB) copied, 0.416897 s, 755 MB/s
```

Cisco ISE 起動メニューからの仮想マシン リソースのチェック

Cisco ISE のインストールとは無関係に、起動メニューから仮想マシンのリソースをチェックできます。

次のように、CLI トランスクリプトが表示されます。

```
  Cisco ISE Installation (Serial Console)
  Cisco ISE Installation (Keyboard/Monitor)
  System Utilities (Serial Console)
  System Utilities (Keyboard/Monitor)
```

矢印キーを使用して [システムユーティリティ（シリアルコンソール）（System Utilities (Serial Console)）] または [システムユーティリティ（キーボード/モニター）（System Utilities (Keyboard/Monitor)）] を選択して、Enter キーを押します。次の画面が表示されます。

```
Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload

Enter option [1 - 3] q to Quit
```

VM リソースをチェックするには、**2** を入力します。次のような出力が表示されます。

```
*****
***** Virtual Machine host detected…
***** Hard disk(s) total size detected: 600 Gigabyte
***** Physical RAM size detected: 16267516 Kbytes
```

```
***** Number of network interfaces detected: 6
***** Number of CPU cores: 12
***** CPU Mhz: 2300.00
***** Verifying CPU requirement…
***** Verifying RAM requirement…
***** Writing disk partition table…
```

Linux KVM

KVM 仮想化チェック

KVM 仮想化には、ホストプロセッサ（Intel プロセッサの場合は Intel VT-x、AMD プロセッサの場合は AMD-V）からの仮想化サポートが必要です。ホストでターミナル ウィンドウを開き、**cat /proc/cpuinfo** コマンドを入力します。vmx または svm フラグが表示されます。

- Intel VT-x の場合：

```
# cat /proc/cpuinfo
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
 dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
nonstop_tsc aperfmperf eagerfpu pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer aes xsave avx lahf_lm arat epb xsaveopt
pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
```

- AMD-V の場合：

```
# cat /proc/cpuinfo
flags: fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush mmx fxsr sse
sse2 ht syscall nx mmxext fxsr_opt rdtscp lm 3dnowext 3dnow
 pni cx16 lahf_lm cmp_legacy svm cr8_legacy
```

KVM への Cisco ISE のインストール

この手順では、RHEL に KVM を作成し、そこに Virtual Machine Manager（virt-manager）を使用して Cisco ISE をインストールする方法について説明します。

CLI での Cisco ISE 導入を選択した場合は、次のようなコマンドを入力します。

#virt-install --name=*kvm-ise1* **--arch=x86_64 --cpu=host --vcpus=2 --ram=4096**
--os-type=linux --os-variant=rhel6 --hvm --virt-type=kvm
--cdrom=*/home/admin/Desktop/ise-3.0.0.x.SPA.x86_64.iso*
--disk=*/home/libvirt-images/kvm-ise1.img,size=100*
--network type=direct,model=virtio,source=*eth2***,source_mode=bridge**

ise-3.0.0.x.SPA.x86_64.iso は Cisco ISE ISO イメージの名前です。

始める前に

ローカル システムに Cisco ISE ISO イメージをダウンロードします。

ステップ 1 virt-manager で、[新規（New）] をクリックします。

[新規仮想マシンの作成（Create a new virtual machine）] ウィンドウが表示されます。

ステップ 2 [ローカルインストールメディア（ISO メディアまたは CDROM）（Local install media (ISO media or CDROM)）] をクリックし、[続行（Forward）] をクリックします。

ステップ 3 [ISOイメージを使用（Use ISO image）] オプション ボタンをクリックし、[参照（Browse）] をクリックして、ローカル システムから ISO イメージを選択します。

a) [インストールメディアに基づき OS を自動的に検出（Automatically detect operating system based on install media）] チェックボックスをオフにして OS タイプとして [Linux] を選択し、サポートされている Red Hat Enterprise Linux のバージョンを選択して、[続行（Forward）] をクリックします。

QEMU 1.5.3-160 でサポートされている KVM

ステップ 4 RAM と CPU の設定を選択し、[続行（Forward）] をクリックします。

ステップ 5 [この仮想マシンに対してストレージを有効にする（Enable storage for this virtual machine）] チェックボックスをオンにし、ストレージ設定を選択します。

a) [管理対象または他の既存ストレージを選択（Select managed or other existing storage）] オプションボタンをクリックします。
b) [参照（Browse）] をクリックします。
c) 左側の [ストレージプール（Storage Pools）] ナビゲーション ペインで、[ディスクファイルシステムディレクトリ（disk FileSystem Directory）] をクリックします。
d) [新規ボリューム（New Volume）] をクリックします。

[ストレージボリュームの作成（Create storage volume）] ウィンドウが表示されます。

e) ストレージ ボリュームの名前を入力します。
f) [フォーマット（Format）] ドロップダウン リストから [raw] を選択します。
g) 最大キャパシティを入力します。
h) [終了（Finish）] をクリックします。
i) 作成したボリュームを選択して [ボリュームの選択（Choose Volume）] を選択します。
j) [続行（Forward）] をクリックします。

[インストール開始前の確認（Ready to begin the installation）] 画面が表示されます。

ステップ 6 [インストール前に構成をカスタマイズ（Customize configuration before install）] チェックボックスをオンにします。

ステップ 7 [高度なオプション（Advanced Options）] で、インターフェイスのソースとして macvtap を選択し、[ソース モード（Source mode）] ドロップダウン リストで [ブリッジ（Bridge）] を選択し、[完了（Finish）] をクリックします。

a) （オプション）[ハードウェアを追加（Add Hardware）] をクリックして追加の NIC を追加します。

ネットワーク ソースとして macvtap、デバイス モデルとして virtio を選択します。

b) [終了（Finish）] をクリックします。

ステップ 8 [仮想マシン（Virtual Machine）] 画面でディスク デバイスを選択し、[高度なオプションおよびパフォーマンスオプション（Advanced and Performance Options）] の下で以下のオプションを選択して、[適用（Apply）] をクリックします。

フィールド	値
ディスク バス（Disk bus）	VirtIO
キャッシュ モード（Cache mode）	none
IO モード（IO mode）	native

ステップ 9 [インストール開始（Begin Installation）] をクリックして KVM に Cisco ISE をインストールします。Cisco ISE のインストール ブート メニューが表示されます。

ステップ 10 システム プロンプトで、1 と入力してモニターとキーボード ポートを選択するか、2 と入力してコンソール ポートを選択し、Enter を押します。

インストーラが、VM への Cisco ISE ソフトウェアのインストールを開始します。インストール プロセスが終了すると、コンソールに以下が表示されます。

```
Type 'setup' to configure your appliance
localhost:
```

ステップ 11 システム プロンプトで、**setup** と入力し、Enter を押します。
セットアップ ウィザードが表示され、ウィザードに従って初期設定を実行します。

Microsoft Hyper-V

Hyper-V での Cisco ISE 仮想マシンの作成

このセクションでは、新しい仮想マシンの作成、ローカル ディスクの ISO イメージの仮想 CD/DVD ドライブへのマッピング、CPU 設定の編集、および Hyper-V への Cisco ISE のインストールの方法を説明します。

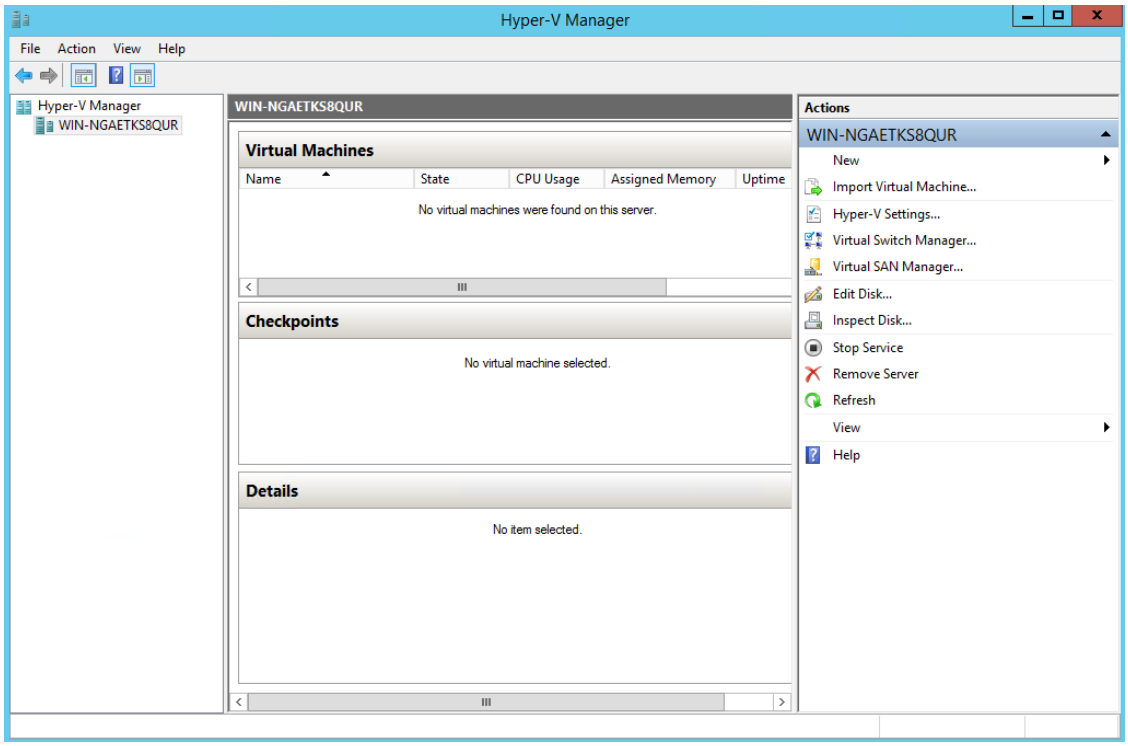
（注） Cisco ISE では、マルチパス I/O（MPIO）の使用はサポートされません。したがって、VM に MPIO を使用している場合、インストールは失敗します。

始める前に

Cisco ISE ISO イメージを、cisco.com からローカルシステムにダウンロードします。

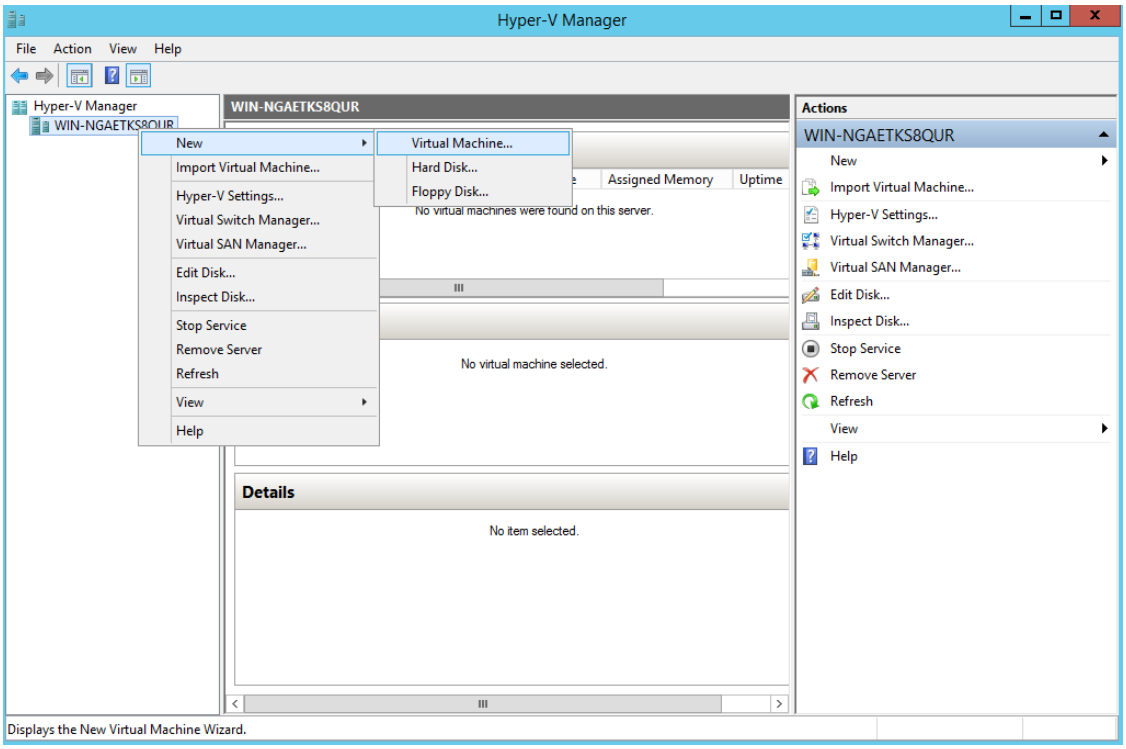
ステップ 1 サポートされている Windows サーバーの Hyper-V マネージャを起動します。

図 *9 : Hyper-V* マネージャ コンソール



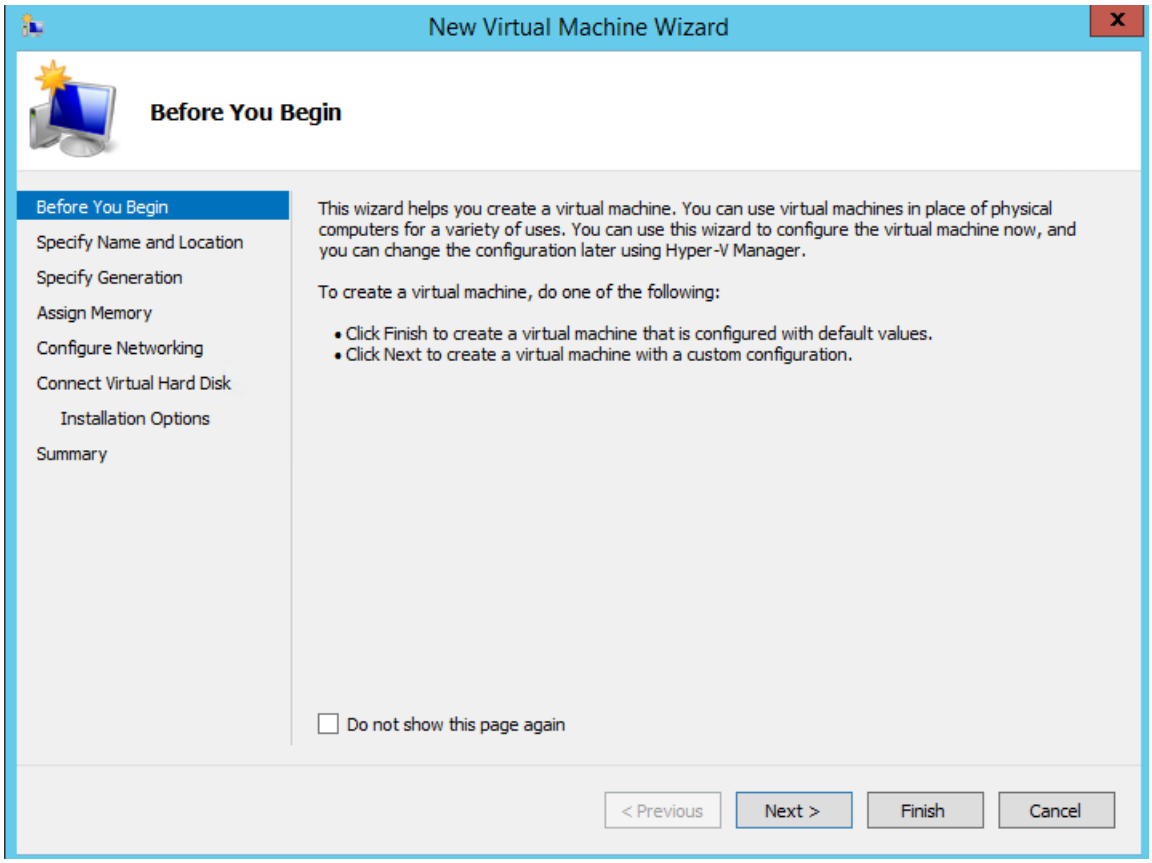
ステップ 2　VM ホストを右クリックし、[新規（New）] > [仮想マシン（Virtual Machine）] の順にクリックします。

図 *10* : 新しい仮想マシンの作成



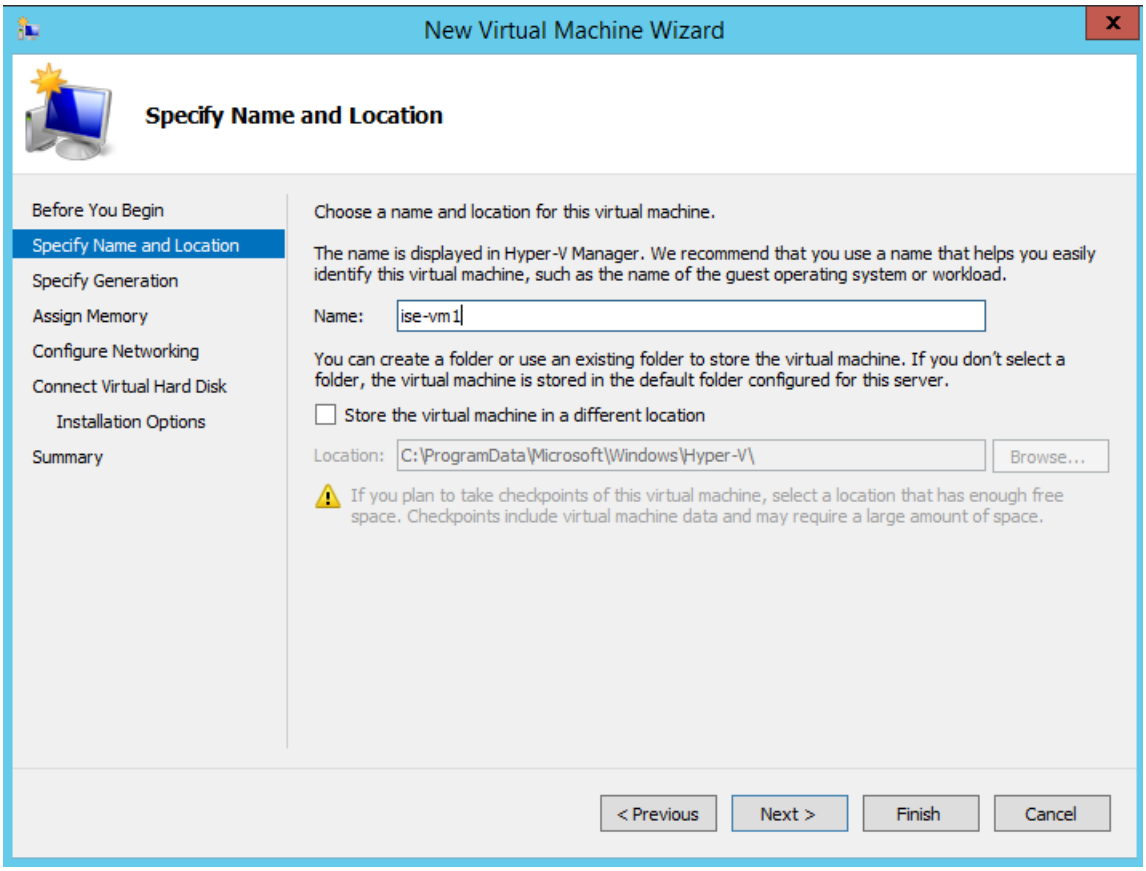
ステップ 3　[次へ（Next）] をクリックして VM 設定をカスタマイズします。

図 *11 : [New Virtual Machine]* ウィザード



ステップ 4 VM の名前を入力し、（オプションで）VM を保存する異なるパスを選択して、[次へ（Next）] をクリックします。

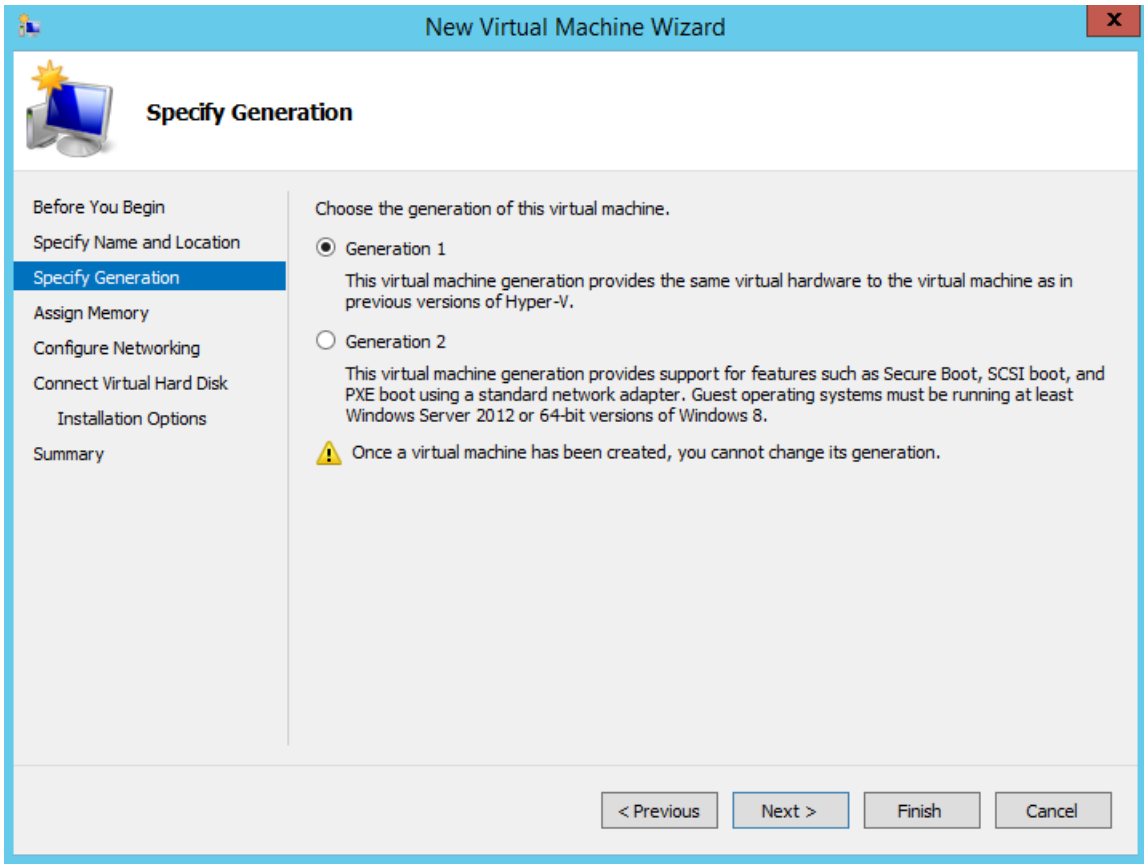
図 *12* : 名前と場所の指定



ステップ 5 [ジェネレーション1（Generation 1）] オプション ボタンをクリックし、[次へ（Next）] をクリックします。

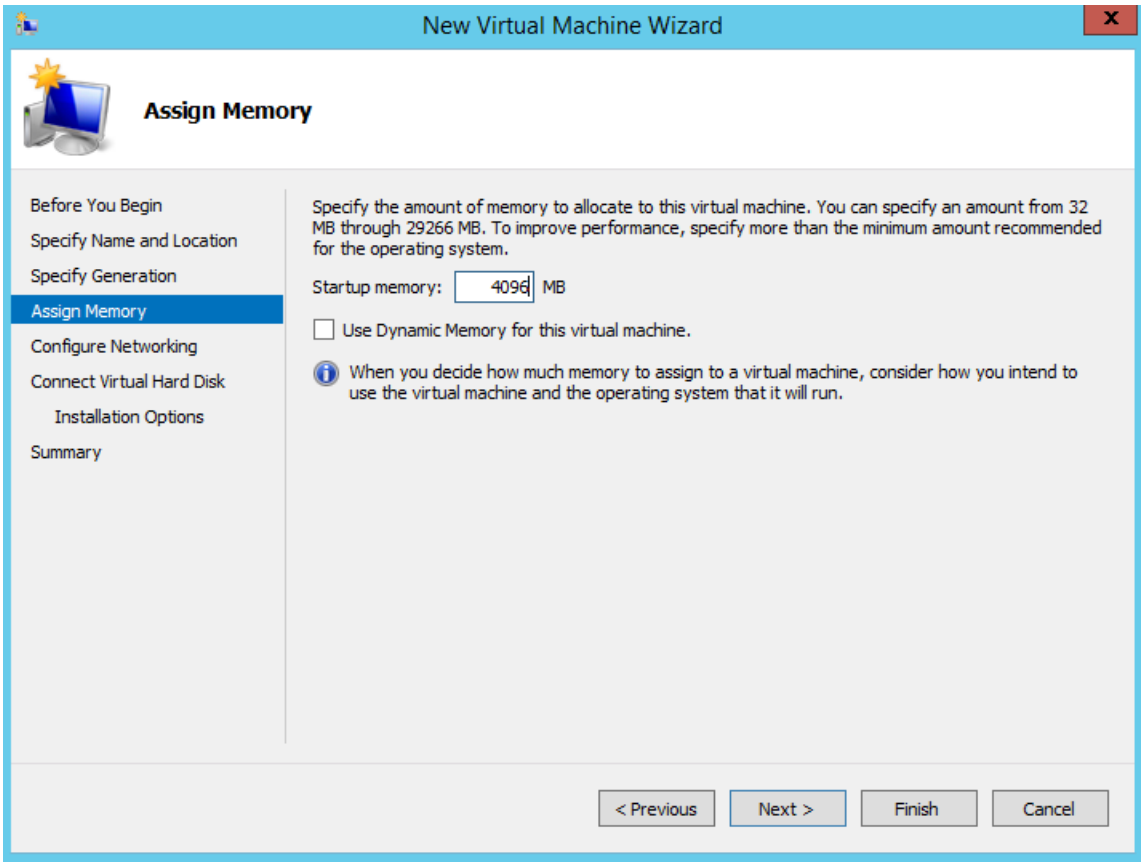
第 2 世代の ISE VM を作成する場合は、VM 設定の [セキュアブート（Secure Boot）] オプションを無効にします。

図 *13* : 生成の指定



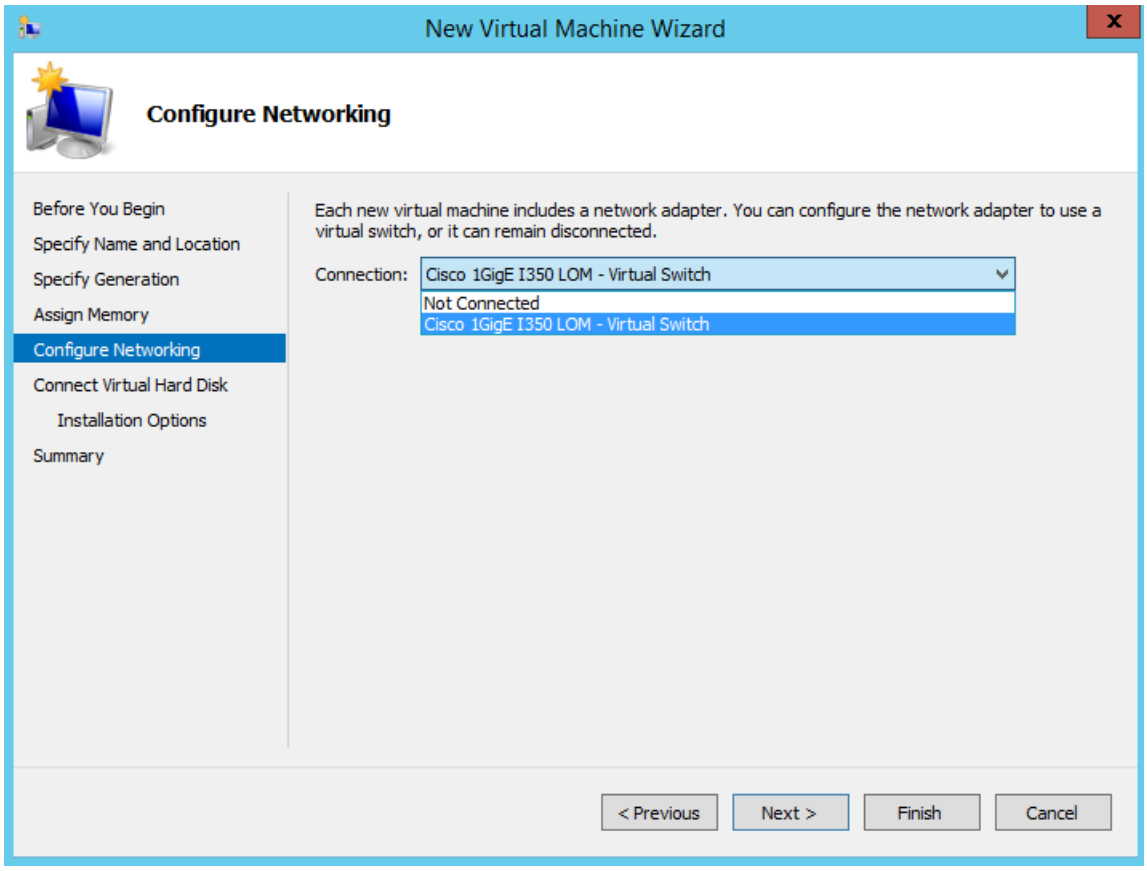
ステップ 6　この VM に割り当てるメモリの量を指定して（例：16000 MB）、[次へ（Next）] をクリックします。

図 *14* : メモリの割り当て



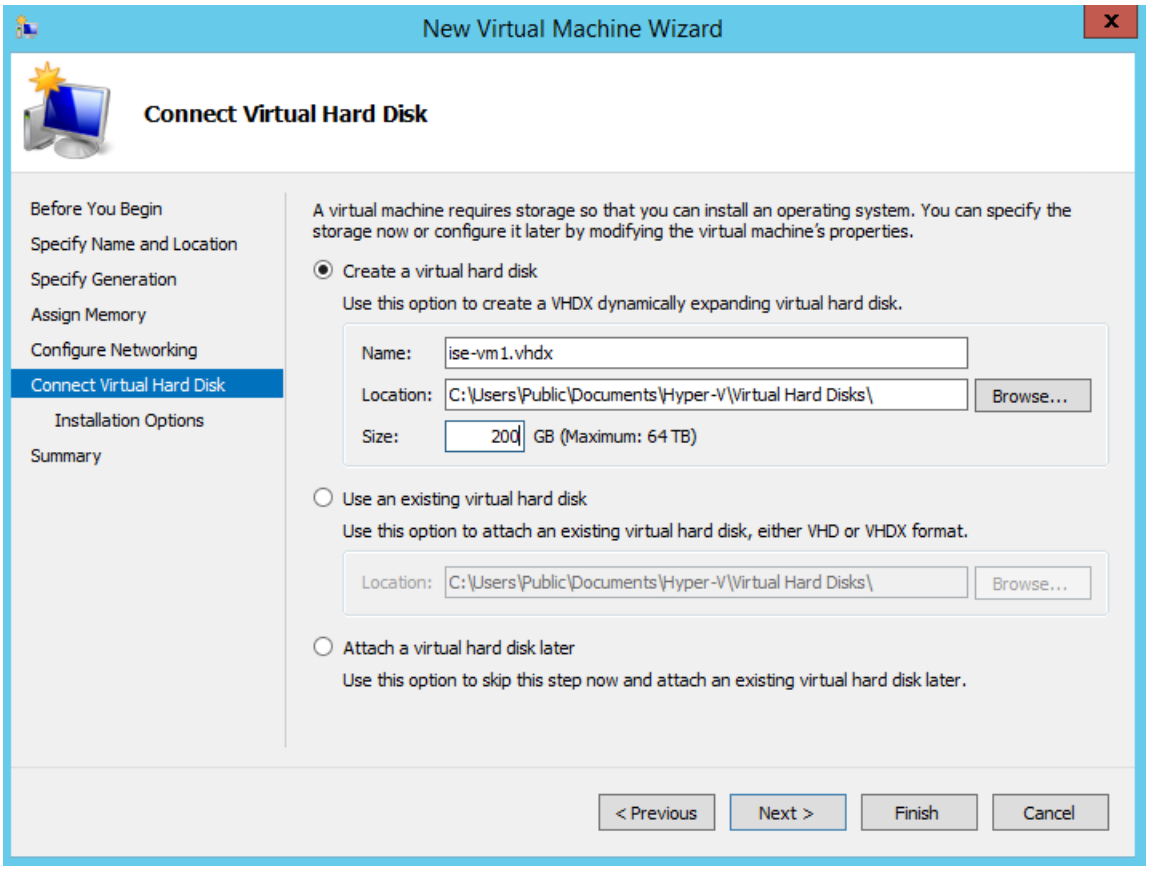
ステップ 7 ネットワーク アダプタを選択して、[次へ（Next）] をクリックします。

図 *15* : ネットワーキングの設定



ステップ 8 [仮想ディスクの作成（Create a virtual hard disk）] オプション ボタンをクリックして、[次へ（Next）] をクリックします。

図 *16* : 仮想ディスクの接続

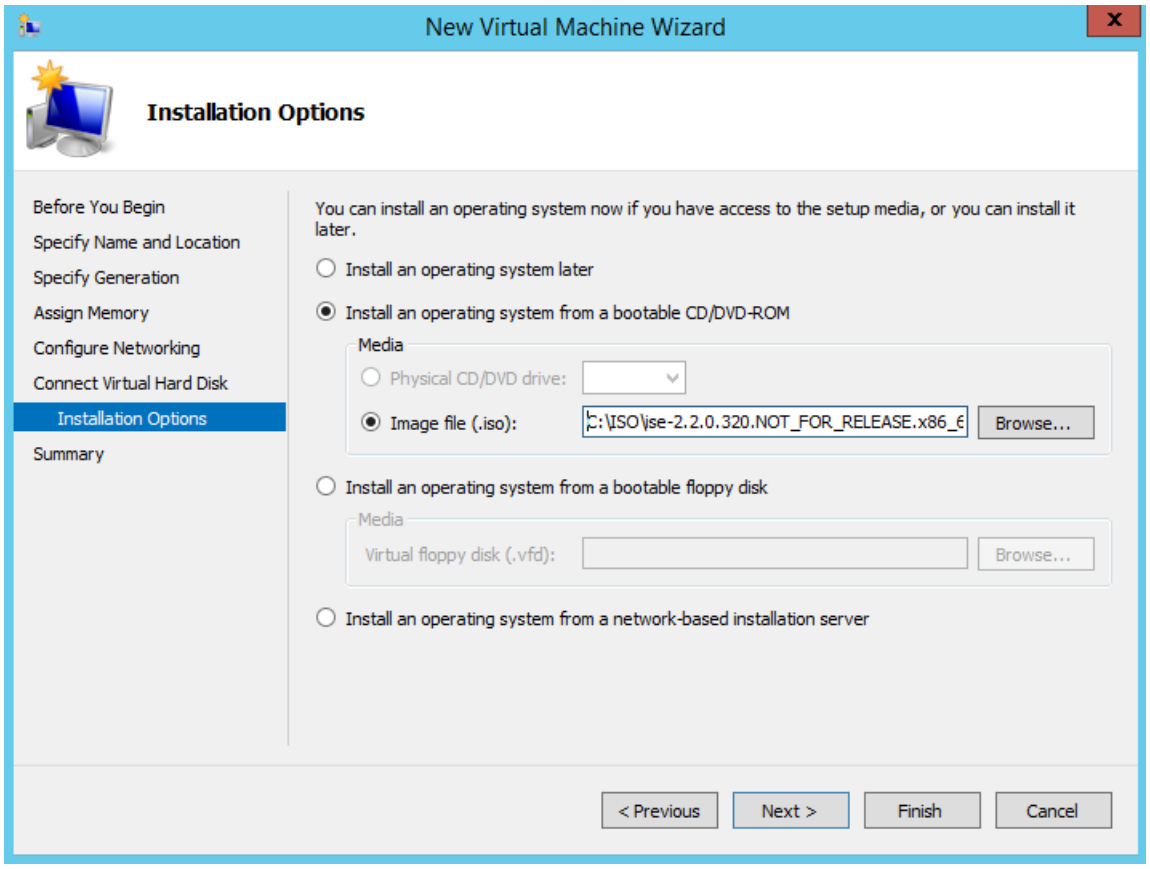


ステップ 9 [ブータブルCD/DVDからオペレーティングシステムをインストール（Install an operating system from a bootable CD/DVD-ROM）] をオプション ボタンをクリックします。

a) [メディア（Media）] エリアから、[イメージファイル（.iso）（Image file (.iso)）] オプション ボタンをクリックします。

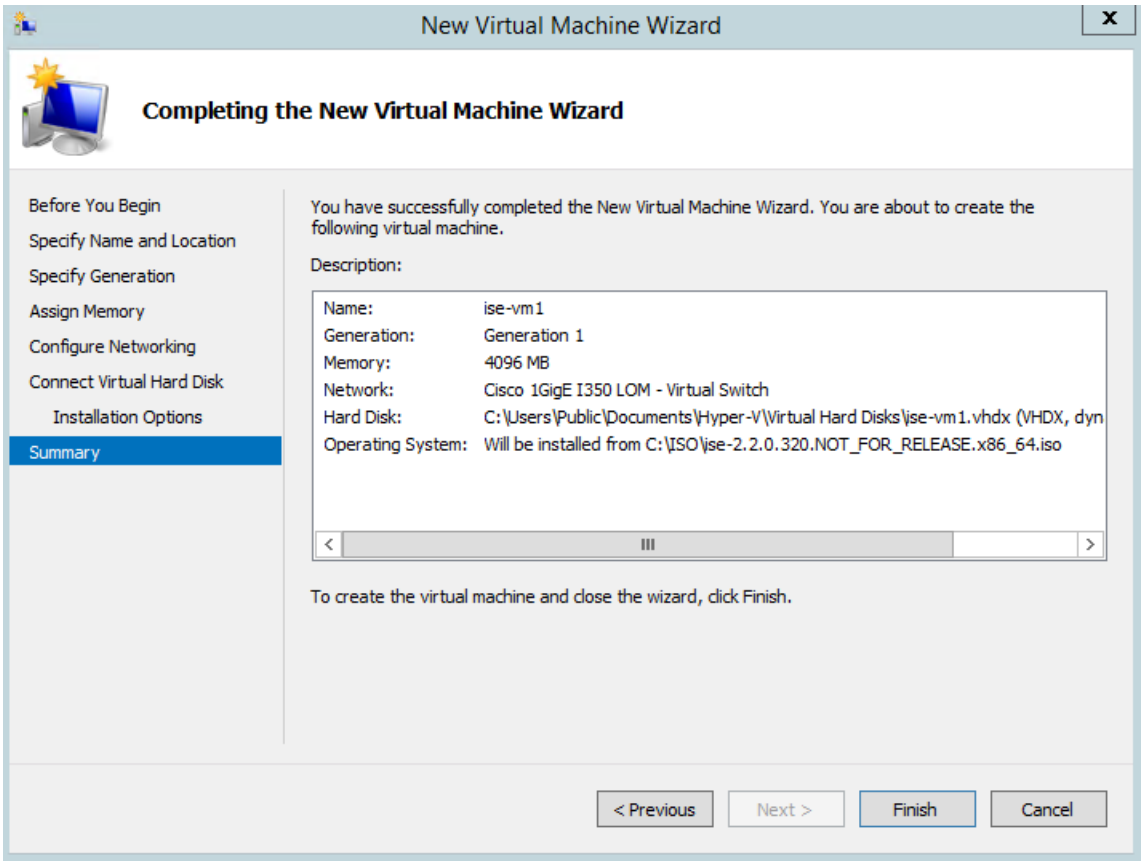
b) [参照（Browse）] をクリックして、ローカル システムから ISE ISO イメージを選択し、[次へ（Next）] をクリックします。

図 *17*: インストール オプション



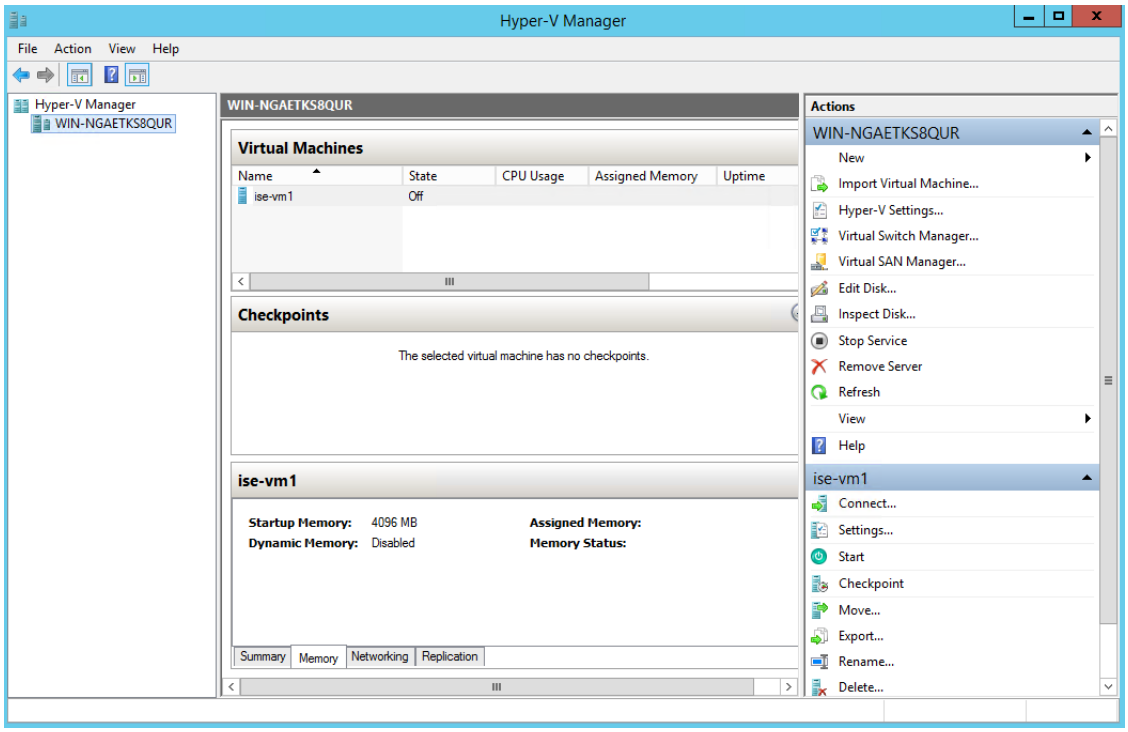
ステップ 10　[終了（Finish）] をクリックします。

図 *18 : [*新規仮想マシン（***New Virtual Machine***）*]* ウィザードの終了



Cisco ISE VM が Hyper-V に作成されます。

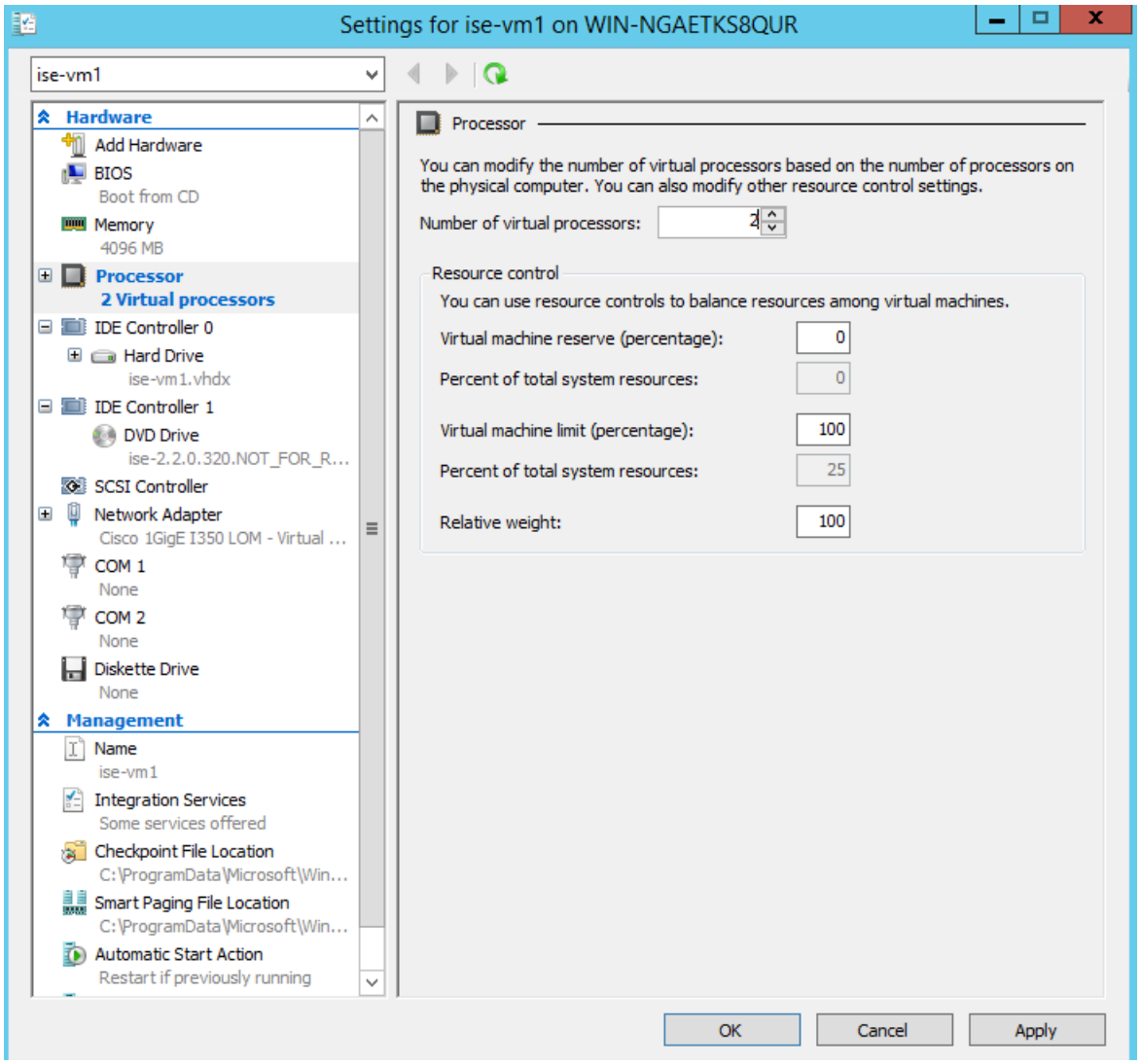
図 *19* : 新しい仮想マシンの作成完了



ステップ 11 VM を選択し、VM の設定を編集します。

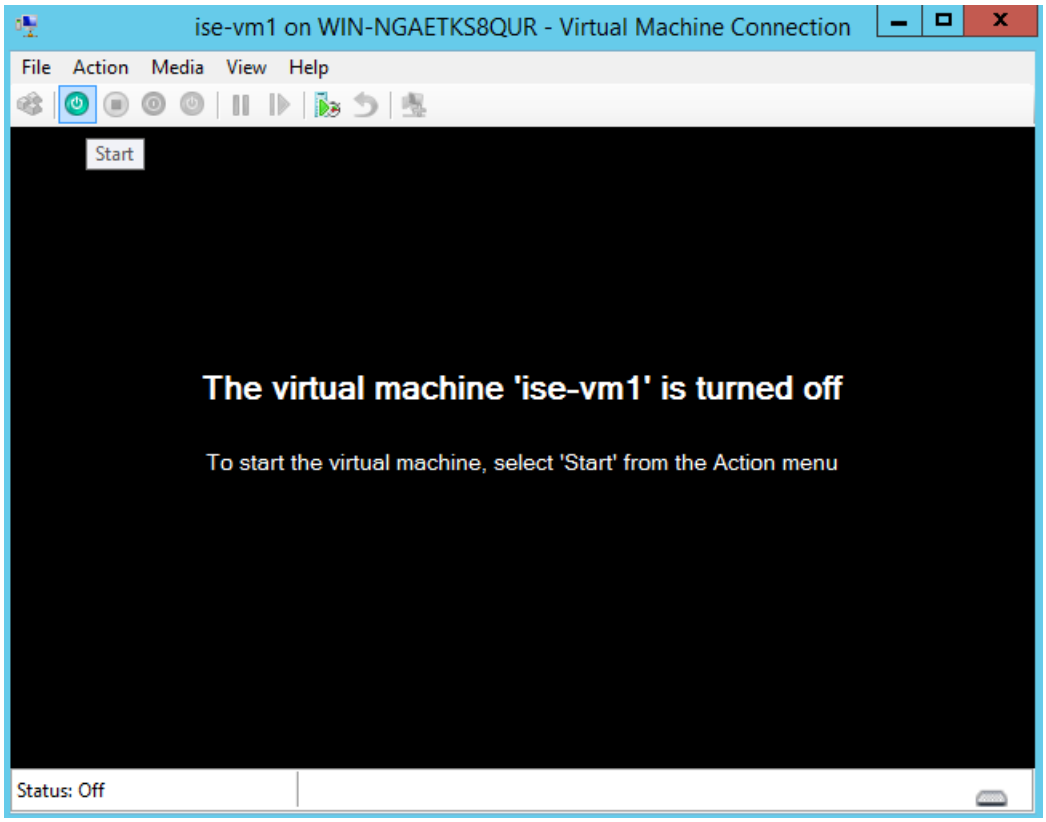
a) [プロセッサ（Processor）] を選択します。仮想プロセッサ数を入力し（例：6）、[OK] をクリックします。

図 *20 : VM* 設定の編集



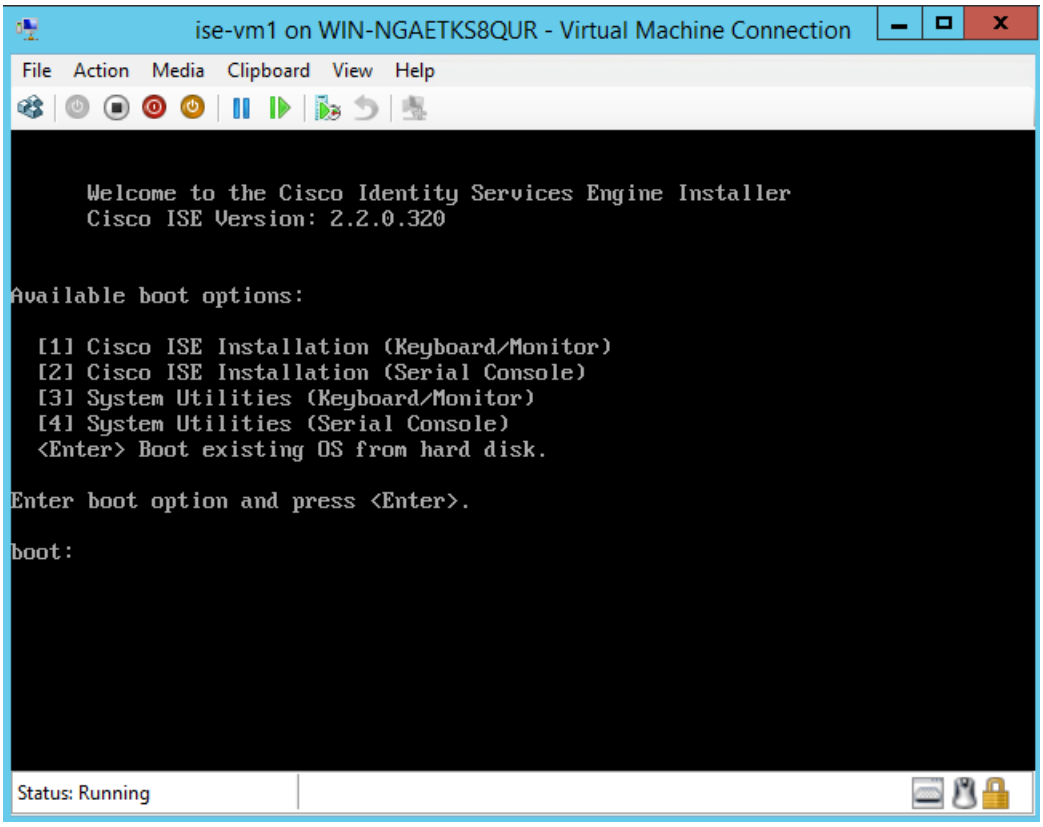
ステップ 12 VM を選択して [接続（Connect）] をクリックし、VM コンソールを起動します。[開始（start）] ボタンをクリックして、Cisco ISE VM をオンにします。

図 *21 : Cisco ISE VM* の起動

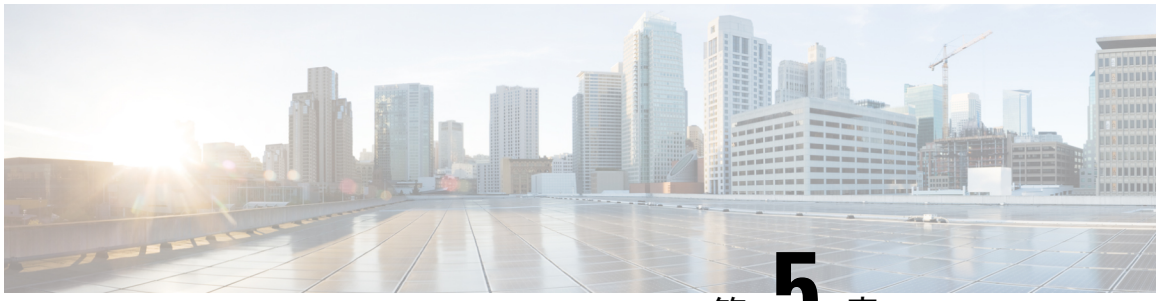


Cisco ISE のインストール メニューが表示されます。

図 *22 : Cisco ISE* のインストール メニュー



ステップ 13 キーボードとモニターを使用して Cisco ISE をインストールするには、**1** を入力します。



第 5 章

インストールの確認とインストール後のタスク

Cisco ISE の Web ベースのインターフェイスへのログイン

初めて Cisco ISE Web ベースのインターフェイスにログインするときは、事前にインストールされている評価ライセンスを使用します。

（注） Cisco ISE ユーザー インターフェイスを使用して、定期的に管理者ログイン パスワードをリセットすることをお勧めします。

注意 セキュリティ上の理由から、管理セッションの完了時には、ログアウトすることをお勧めします。ログアウトしない場合、30 分間何も操作しないと Cisco ISE の Web インターフェイスからログアウトされ、送信されていない設定データは保存されません。

検証済みブラウザの詳細については、『Cisco ISE リリースノート』の「検証済みブラウザ」のセクションを参照してください。

ステップ 1 Cisco ISE アプライアンスのリブートが完了したら、サポートされている Web ブラウザの 1 つを起動します。

ステップ 2 アドレス フィールドに、Cisco ISE アプライアンスの IP アドレス（またはホスト名）を次のフォーマットを使用して入力し、Enter を押します。

```
https://<IP address or host name>/admin/
```

ステップ 3 設定時に定義したユーザー名とパスワードを入力します。

ステップ 4 [ログイン（Login）] をクリックします。

CLI 管理と Web ベースの管理ユーザー タスクの違い

Cisco ISE セットアップ プログラムを使用して設定したユーザー名およびパスワードは、Cisco ISE CLI および Cisco ISE Web インターフェイスでの管理アクセスで使用するためのものです。Cisco ISE CLI にアクセスできる管理者を CLI 管理ユーザーといいます。デフォルトでは、CLI 管理ユーザーのユーザー名は admin、パスワードはセットアップ プロセスでユーザーが定義したパスワードです。デフォルトのパスワードはありません。

Cisco ISE Web インターフェイスへの最初のアクセスは、セットアップ プロセスで定義した CLI 管理ユーザーのユーザー名、およびパスワードを使用して行うことができます。Web ベース admin のデフォルトのユーザー名およびパスワードはありません。

CLI 管理ユーザーは、Cisco ISE の Web ベースの管理ユーザー データベースにコピーされます。最初の CLI 管理ユーザーのみが Web ベースの管理ユーザーとしてコピーされます。両方の管理ロールで同じユーザー名とパスワードを使用できるように、CLI と Web ベースの管理ユーザー ストアは同期を保持する必要があります。

Cisco ISE CLI 管理ユーザーは、Cisco ISE Web ベースの管理ユーザーとは異なる権限と機能を持ち、他の管理タスクを実行できます。

表 *13 : CLI* 管理ユーザーおよび *Web* ベース管理ユーザーによって実行されるタスク

管理ユーザー タイプ	タスク
CLI 管理および Web ベース管理の両方	• Cisco ISE アプリケーション データをバックアップする。 • Cisco ISE アプライアンス上でシステム、アプリケーション、または診断ログを表示する。 • Cisco ISE ソフトウェア パッチ、メンテナンス リリース、およびアップグレードを適用する。 • NTP サーバー コンフィギュレーションを設定する。

管理ユーザー タイプ	タスク
CLI 管理のみ	• Cisco ISE アプリケーション ソフトウェアを起動および停止する。 • Cisco ISE アプライアンスをリロードまたはシャットダウンする。 • ロックアウトした場合、Web ベースの管理ユーザーをリセットする。 • ISE CLI にアクセスする。

CLI 管理者の作成

Cisco ISE では、セットアップ プロセスで作成した CLI 管理ユーザー アカウントに加え、追加の CLI 管理ユーザー アカウントを作成することができます。CLI 管理ユーザーのクレデンシャルを保護するために、Cisco ISE CLI アクセスに必要な CLI 管理ユーザーの作成数は最低限にします。

CLI 管理者ユーザーを追加するには、次のコマンドをコンフィギュレーションモードで使用します。

```
username <username> password [plain/hash] <password> role admin
```

Web ベースの管理者の作成

Cisco ISE システムに初めて Web によるアクセスを行う場合、管理者のユーザー名とパスワードはセットアップ時に設定した CLI ベースのアクセスと同じです。

管理者ユーザーを追加するには、次の手順を実行します。

1. [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）] の順に選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、
2. [追加（Add）] > [管理者ユーザーの作成（Create an Admin User）] を選択します。
3. 名前、パスワード、管理者グループ、およびその他の必要な詳細情報を入力します。
4. **[送信（Submit）]** をクリックします。

管理者のロックアウトにより無効化されたパスワードのリセット

管理者が、誤ったパスワードをアカウントが無効になる所定の回数入力する場合があります。デフォルトの最小試行回数は 5 です。

次の手順によって、Cisco ISE CLI で **application reset-passwd ise** コマンドを使用して、管理者ユーザー インターフェイス パスワードをリセットします。このコマンドは、管理者の CLI の

パスワードには影響を与えません。正常に管理者パスワードをリセットすると、クレデンシャルはただちにアクティブになり、システムをリブートせずにログインできます。。

Cisco ISE により、[管理者ログイン（Administrator Logins）] ウィンドウにログエントリが追加されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[運用（Operations）]**>**[レポート（Reports）]**>**[レポート（Reports）]**>**[監査（Audit）]**>**[管理者ログイン（Administrator Logins）]** です。その管理者 ID に関連付けられたパスワードがリセットされるまで、管理者 ID のログイン情報は一時的に停止されます。

ステップ 1 ダイレクト コンソール CLI にアクセスして、次を入力します。

application reset-passwd ise administrator_ID

ステップ 2 この管理者 ID に使用されていた前の 2 つのパスワードと異なる新しいパスワードを指定して、確認します。

```
Enter new password:
Confirm new password:

Password reset successfully
```

Cisco ISE の設定の確認

Web ブラウザおよび CLI を使用して Cisco ISE 設定を確認するための、それぞれ異なるユーザー名およびパスワード クレデンシャルのセットを使用する 2 通りの方法があります。

（注） CLI 管理ユーザーと Web ベースの管理ユーザーのクレデンシャルは、Cisco ISE では異なります。

Web ブラウザを使用した設定の確認

ステップ 1 Cisco ISE アプライアンスのリブートが完了したら、サポートされている Web ブラウザの 1 つを起動します。

ステップ 2 アドレス フィールドに、Cisco ISE アプライアンスの IP アドレス（またはホスト名）を次のフォーマットを使用して入力し、Enter を押します。

ステップ 3 Cisco ISE のログイン ページで、セットアップ時に定義したユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

たとえば、https://10.10.10.10/admin/ と入力すると Cisco ISE のログイン ページが表示されます。

```
https://<IP address or host name>/admin/
```

（注） Cisco ISE システムに初めて Web によるアクセスを行う場合、管理者のユーザー名とパスワードはセットアップ時に設定した CLI ベースのアクセスと同じです。

ステップ 4 アプライアンスが正しく動作していることを確認するには、Cisco ISE ダッシュボードを使用します。

次のタスク

Cisco ISE の Web ベースのユーザー インターフェイス メニューを使用して、Cisco ISE システムをニーズに合わせて設定できます。Cisco ISE の設定の詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

CLI を使用した設定の確認

始める前に

最新の Cisco ISE パッチをダウンロードしてインストールし、Cisco ISE を最新の状態に保ちます。

ステップ 1 Cisco ISE アプライアンスのリブートが完了したら、PuTTY などのサポートされる製品を起動して、Cisco ISE アプライアンスへの Secure Shell（SSH）接続を確立します。

ステップ 2 [ホスト名（Host Name）]（または [IPアドレス（IP Address）]）フィールドにホスト名（または Cisco ISE アプライアンスのドット付き 10 進表記の IP アドレス）を入力し、[開く（Open）] をクリックします。

ステップ 3 ログインプロンプトで、セットアップ時に設定した CLI 管理ユーザー名（admin がデフォルト）を入力し、Enter を押します。

ステップ 4 パスワードプロンプトで、セットアップ時に設定した CLI 管理パスワード（これはユーザー定義でデフォルトはありません）を入力し、Enter を押します。

ステップ 5 システム プロンプトで **show application version ise** と入力し、Enter を押します。

ステップ 6 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。

コンソール出力は次のように表示されます。

```
ise-server/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4930
Database Server                        running          66 PROCESSES
Application Server                     running          8231
Profiler Database                      running          6022
ISE Indexing Engine                    running          8634
AD Connector                           running          9485
M&T Session Database                   running          3059
M&T Log Collector                      running          9271
M&T Log Processor                      running          9129
Certificate Authority Service          running          8968
EST Service                            running          18887
SXP Engine Service                     disabled
TC-NAC Docker Service                  disabled
TC-NAC MongoDB Container               disabled
```

```
TC-NAC RabbitMQ Container               disabled
TC-NAC Core Engine Container            disabled
VA Database                             disabled
VA Service                              disabled
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID Service                       disabled
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled
```

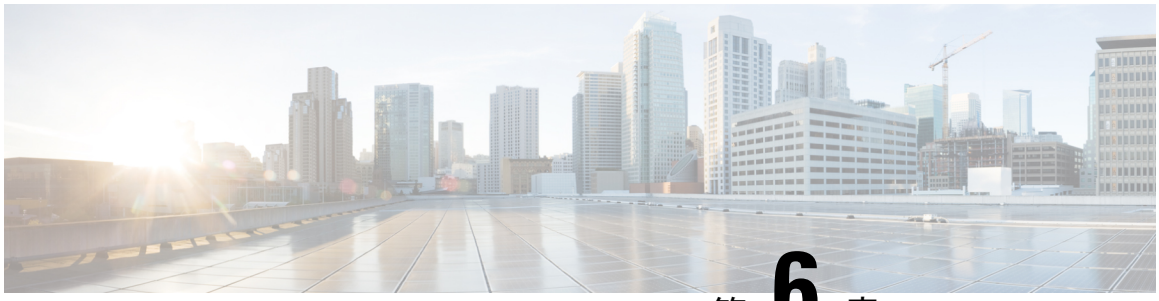
インストール後のタスクの一覧

Cisco ISE をインストールした後、次の必須タスクを実行する必要があります。

表 *14*：インストール後の必須タスク

タスク	アドミニストレーション ガイドのリンク
最新のパッチの適用（存在する場合）	ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Maintain and Monitor」の章にある「Software Patch Installation Guideline」の項を参照してください。
ライセンスのインストール	詳細については、Cisco ISE 発注ガイド [英語] を参照してください。ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Licensing」の章を参照してください。
証明書のインストール	ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Basic Setup」の章にある「Certificate Management in Cisco ISE」の項を参照してください。
バックアップのリポジトリの作成	ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Maintain and Monitor」の章にある「Create Repositories」の項を参照してください。
バックアップ スケジュールの設定	ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Maintain and Monitor」の章にある「Schedule a Backup」の項を参照してください。

タスク	アドミニストレーション ガイドのリンク
Cisco ISE ペルソナのデプロイメント	ご使用のリリースの *Cisco ISE* 管理者ガイド [英語] の「Deployment」の章にある「Cisco ISE Distributed Deployment」の項を参照してください。



第 6 章

共通システム メンテナンス タスク

高可用性のためのイーサネットインターフェイスのボンディング

Cisco ISE は、物理インターフェイスに高可用性を提供するために、1 つの仮想インターフェイスへの 2 つのイーサネットインターフェイスのボンディングをサポートします。この機能は、ネットワーク インターフェイス カード（NIC）のボンディングまたは NIC チーミングと呼ばれます。2 つのインターフェイスをボンディングすると、2 つの NIC は 1 つの MAC アドレスを持つ単一のデバイスとして認識されます。

Cisco ISE の NIC ボンディング機能は、ロード バランシングまたはリンク アグリゲーション機能をサポートしていません。Cisco ISE は、NIC ボンディングの高可用性機能だけをサポートします。

インターフェイスのボンディングでは、次の状況でも Cisco ISE サービスが影響を受けないことを保証します。

- 物理インタフェースの障害
- スイッチ ポート接続の喪失（シャットダウンまたは障害）
- スイッチ ラインカードの障害

2 つのインターフェイスをボンディングすると、インターフェイスの一方がプライマリ インターフェイスになり、もう一方はバックアップインターフェイスになります。2 つのインターフェイスをボンディングすると、すべてのトラフィックは通常、プライマリ インターフェイス

を通過します。プライマリ インターフェイスが何らかの理由で失敗すると、バックアップ インターフェイスがすべてのトラフィックを引き継いで処理します。ボンディングにはプライマリ インターフェイスの IP アドレスと MAC アドレスが必要です。

NIC ボンディング機能を設定する際に、Cisco ISE は固定物理 NIC を組み合わせて NIC のボンディングを形成します。ボンディング インターフェイスを形成するためにボンディングすることができる NIC について、次の表に概要を示します。

表 *15*：ボンディングしてインターフェイスを形成する物理 *NIC*

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 0	Eth0	プライマリ	ボンド 0
ギガビットイーサネット 1	Eth1	バックアップ	
ギガビットイーサネット 2	Eth2	プライマリ	ボンド 1
ギガビットイーサネット 3	Eth3	バックアップ	
ギガビットイーサネット 4	Eth4	プライマリ	ボンド 2
ギガビットイーサネット 5	Eth5	バックアップ	

対応プラットフォーム

NIC ボンディング機能は、サポートされているすべてのプラットフォームとノードペルソナでサポートされています。サポートされるプラットフォームは次のとおりです。

- SNS 3500 および 3600 シリーズ アプライアンス：ボンド 0、1、および 2
- VMware 仮想マシン：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）
- Linux KVM ノード：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）

イーサネットインターフェイスのボンディングに関するガイドライン

- Cisco ISE は最大 6 つのイーサネット インターフェイスをサポートするので、ボンドは 3 つ（ボンド 0、ボンド 1、ボンド 2）のみ設定できます。

- ボンドに含まれるインターフェイスを変更したり、ボンドのインターフェイスのロールを変更したりすることはできません。ボンディングできるNICとボンドでのロールについての情報は、上記の表を参照してください。
- Eth0 インターフェイスは、管理インターフェイスとランタイム インターフェイスの両方として機能します。その他のインターフェイスは、ランタイムインターフェイスとして機能します。
- ボンドを作成する前に、プライマリ インターフェイス（プライマリ NIC）に IP アドレスを割り当てる必要があります。ボンド 0 を作成する前は、Eth0 インターフェイスに IPv4 アドレスを割り当てる必要があります。同様に、ボンド 1 と 2 を作成する前は、Eth2 と Eth4 インターフェイスに IPv4 または IPv6 アドレスをそれぞれ割り当てる必要があります。
- ボンドを作成する前に、バックアップ インターフェイス（Eth1、Eth3、および Eth5）に IP アドレスが割り当てられている場合は、バックアップ インターフェイスからその IP アドレスを削除します。バックアップ インターフェイスには IP アドレスを割り当てないでください。
- ボンドを 1 つのみ（ボンド 0）作成し、残りのインターフェイスをそのままにすることもできます。この場合、ボンド0は管理インターフェイスとランタイムインターフェイスとして機能し、残りのインターフェイスはランタイムインターフェイスとして機能します。
- ボンドでは、プライマリ インターフェイスの IP アドレスを変更できます。プライマリ インターフェイスの IP アドレスと想定されるので、新しい IP アドレスがボンディングされたインターフェイスに割り当てられます。
- 2 つのインターフェイス間のボンドを削除すると、ボンディングされたインターフェイスに割り当てられていた IP アドレスは、プライマリ インターフェイスに再び割り当てられます。
- デプロイメントに含まれる Cisco ISE ノードで NIC ボンディング機能を設定するには、そのノードをデプロイメントから登録解除し、NICボンディングを設定して、デプロイメントに再度登録する必要があります。
- ボンド（Eth0、Eth2、または Eth4 インターフェイス）のプライマリ インターフェイスとして機能する物理インターフェイスにスタティック ルートが設定されている場合は、物理インターフェイスではなくボンディングされたインターフェイスで動作するようにスタティック ルートが自動的に更新されます。

NIC ボンディングの設定

NIC ボンディングは Cisco ISE CLI から設定できます。次の手順では、Eth0 と Eth1 インターフェイス間にボンド 0 を設定する方法を説明します。

始める前に

バックアップインターフェイスとして動作する物理インターフェイス（Eth1、Eth3、Eth5インターフェイスなど）に IP アドレスが設定されている場合は、バックアップ インターフェイスからその IP アドレスを削除する必要があります。バックアップ インターフェイスには IP アドレスを割り当てないでください。

ステップ 1 管理者アカウントを使用して Cisco ISE CLI にログインします。

ステップ 2 **configure terminal** と入力して、コンフィギュレーション モードを開始します。

ステップ 3 **interface GigabitEthernet 0** コマンドを入力します。

ステップ 4 backup interface GigabitEthernet 1 コマンドを入力します。
コンソールに次のメッセージが表示されます。

```
% Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure
you want to proceed? Y/N [N]:
```

ステップ 5 Y を入力して、Enter を押します。

ボンド 0 が設定されました。Cisco ISE が自動的に再起動します。しばらく待ってから、すべてのサービスが正常に稼働していることを確認します。すべてのサービスが実行していることを確認するために、CLI から **show application status ise** コマンドを入力します。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

```
ise/admin(config-GigabitEthernet)#
```

NIC ボンディング設定の確認

NIC ボンディング機能が設定されているかどうかを確認するには、Cisco ISE CLI から **show running-config** コマンドを実行します。次のような出力が表示されます。

```
!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
```

上記の出力では、「backup interface GigabitEthernet 1」は、ギガビット イーサネット 0 に NIC ボンディングが設定されていて、ギガビットイーサネット 0 がプライマリ インターフェイス、ギガビット イーサネット 1 がバックアップ インターフェイスとされていることを示します。また、ADE-OS 設定では、プライマリおよびバックアップのインターフェイスに効果的に同じ IP アドレスを設定していても、running config でバックアップ インターフェイスの IP アドレスは表示されません。

また、**show interfaces** コマンドを実行して、ボンディングされたインターフェイスを表示できます。

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::8a5a:92ff:fe88:4aea  prefixlen 64  scopeid 0x20<link>
        ether 88:5a:92:88:4a:ea  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfab00000-fabfffff

GigabitEthernet 1
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfaa00000-faafffff
```

NIC ボンディングの削除

backup interface コマンドの **no** 形式を使用して、NIC ボンドを削除します。

始める前に

ステップ 1 管理者アカウントを使用して Cisco ISE CLI にログインします。

ステップ 2 **configure terminal** と入力して、コンフィギュレーション モードを開始します。

ステップ 3 **interface GigabitEthernet 0** コマンドを入力します。

ステップ 4 **no backup interface GigabitEthernet 1** コマンドを入力します。

```
% Notice: Bonded Interface bond 0 has been removed.
```

ステップ 5 **Y** を入力して Enter キーを押します。

ボンド 0 が削除されました。Cisco ISE が自動的に再起動します。しばらく待ってから、すべてのサービスが正常に稼働していることを確認します。すべてのサービスが実行していることを確認するために、CLI から **show application status ise** コマンドを入力します。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

紛失、失念、または侵害されたパスワードの DVD を使用したリセット

始める前に

次の接続関連の状態が原因で、Cisco ISE ソフトウェア DVD を使用して Cisco ISE アプライアンスを起動しようとしたときに問題が発生する場合があることを理解しておいてください。

- ターミナル サーバーにシリアル コンソールから Cisco ISE アプライアンスへの exec に設定された接続が関連付けられている。これを *no exec* に設定すると、キーボードとビデオ モニター接続およびシリアル コンソール接続を使用できるようになります。
- Cisco ISE アプライアンスへのキーボードおよびビデオ モニター接続がある（これはリモート キーボードおよびビデオ モニター接続または VMware vSphere Client コンソール接続のいずれかになります）。
- Cisco ISE アプライアンスへのシリアル コンソール接続がある。

ステップ 1 Cisco ISE アプライアンスの電源がオンになっていることを確認します。

ステップ 2 Cisco ISE ソフトウェア DVD を挿入します。

たとえば、Cisco ISE 3515 コンソールに次のメッセージが表示されます。

```
Cisco ISE Installation (Serial Console)
  Cisco ISE Installation (Keyboard/Monitor)
  System Utilities (Serial Console)
  System Utilities (Keyboard/Monitor)
```

ステップ 3 矢印キーを使用して、ローカル シリアル コンソール ポート接続を使用する場合は [システムユーティリティ（シリアル コンソール）（System Utilities (Serial Console)）] を選択し、アプライアンスに対してキーボードとビデオモニター接続を使用する場合は[システムユーティリティ（キーボード/モニター）（System Utilities (Keyboard/Monitor)）] を選択して、Enter を押します。

次に示すような ISO ユーティリティ メニューが表示されます。

```
Available System Utilities:
  [1] Recover Administrator Password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload
Enter option [1 - 3] q to Quit:
```

ステップ 4 管理者パスワードを回復するには、**1** を入力します。

コンソールに次のメッセージが表示されます。

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.
```

```
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4

Enter choice between [1 - 4] or q to Quit: 2

Password:
Verify password:

Save change and reboot? [Y/N]:
```

ステップ 5 パスワードをリセットする管理者ユーザーに対応する番号を入力します。

ステップ 6 新しいパスワードを入力して確認します。

ステップ 7 変更を保存するには **Y** と入力します。

管理者のロックアウトにより無効化されたパスワードのリセット

管理者が、誤ったパスワードをアカウントが無効になる所定の回数入力する場合があります。デフォルトの最小試行回数は 5 です。

次の手順によって、Cisco ISE CLI で **application reset-passwd ise** コマンドを使用して、管理者ユーザー インターフェイス パスワードをリセットします。このコマンドは、管理者の CLI のパスワードには影響を与えません。正常に管理者パスワードをリセットすると、クレデンシャルはただちにアクティブになり、システムをリブートせずにログインできます。。

Cisco ISE により、[管理者ログイン（Administrator Logins）] ウィンドウにログエントリが追加されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[運用（Operations）]**>**[レポート（Reports）]**>**[レポート（Reports）]**>**[監査（Audit）]**>**[管理者ログイン（Administrator Logins）]** です。その管理者 ID に関連付けられたパスワードがリセットされるまで、管理者 ID のログイン情報は一時的に停止されます。

ステップ 1 ダイレクト コンソール CLI にアクセスして、次を入力します。

application reset-passwd ise administrator_ID

ステップ 2 この管理者 ID に使用されていた前の 2 つのパスワードと異なる新しいパスワードを指定して、確認します。

```
Enter new password:
Confirm new password:

Password reset successfully
```

Return Material Authorization（RMA）

Return Material Authorization（RMA）の場合、SNS サーバー上の個々のコンポーネントを交換する場合は、Cisco ISE をインストールする前に必ずアプライアンスを再イメージ化してください。Cisco TAC に連絡して、サポートを受けてください。

Cisco ISE アプライアンスの IP アドレスの変更

始める前に

- IP アドレスを変更する前に、Cisco ISE ノードがスタンドアロン状態であることを確認します。ノードが分散デプロイメント環境の一部である場合は、その環境からノードを登録解除して、スタンドアロン ノードにします。
- Cisco ISE アプライアンスの IP アドレスを変更する場合は、**no ip address** コマンドを使用しないでください。

ステップ 1 Cisco ISE CLI にログインします。

ステップ 2 次のコマンドを入力します。

a) **configure terminal**
b) **interface GigabitEthernet 0**
c) **ip address new_ip_address new_subnet_mask**

システムにより、IP アドレスを変更するように求められます。**Y** を入力します。次のような画面が表示されます。

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0

% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
```

```
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
```

Cisco ISE により、システムを再起動するように求められます。

ステップ 3 システムを再起動する場合は **Y** と入力します。

インストールおよびアップグレード履歴の表示

Cisco ISE は Cisco ISE リリースおよびパッチのインストール、アップグレード、およびアンインストールの詳細を表示するコマンドライン インターフェイス（CLI）コマンドを提供します。**show version history** コマンドでは次の詳細が提供されます。

- 日付：インストールまたはアンインストールが実行された日時
- アプリケーション：Cisco ISE アプリケーション
- バージョン：インストールまたは削除されたバージョン
- 操作：インストール、アンインストール、パッチのインストール、パッチのアンインストール
- バンドル ファイル名：インストールまたは削除されたバンドルの名前
- リポジトリ：Cisco ISE アプリケーション バンドルがインストールされたリポジトリアンインストールには適用されません。

ステップ 1 Cisco ISE CLI にログインします。

ステップ 2 コマンド **show version history** を入力します。

次の出力が表示されます。

```
ise/admin# show version history
--------------------------------------------
Install Date: Fri Nov 30 21:48:58 UTC 2018
Application: ise
Version: 3.0.0.xxx
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

システムの消去の実行

Cisco ISE アプライアンスまたは VM からすべての情報を安全に消去するために、システムの消去を実行できます。システムの消去を実行するこのオプションは、Cisco ISE が NIST Special Publication 800-88 データ破壊に関する標準を確実に準拠するようにします。

始める前に

次の接続関連の状態が原因で、Cisco ISE ソフトウェア DVD を使用して Cisco ISE アプライアンスを起動しようとしたときに問題が発生する場合があることを理解しておいてください。

- ターミナル サーバーにシリアル コンソールから Cisco ISE アプライアンスへの exec に設定された接続が関連付けられている。これを *no exec* に設定すると、KVM 接続およびシリアル コンソール接続を使用できるようになります。
- Cisco ISE アプライアンスへのキーボードおよびビデオ モニター（KVM）接続がある（これはリモート KVM または VMware vSphere クライアント コンソール接続のいずれかになります）。
- Cisco ISE アプライアンスへのシリアル コンソール接続がある。

ステップ 1 Cisco ISE アプライアンスの電源がオンになっていることを確認します。

ステップ 2 Cisco ISE ソフトウェア DVD を挿入します。

たとえば、Cisco ISE 3515 コンソールに次のメッセージが表示されます。

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

ステップ 3 矢印キーを使用して [システムユーティリティ（シリアルコンソール）（System Utilities (Serial Console)）] を選択して、Enter キーを押します。

次に示すような ISO ユーティリティ メニューが表示されます。

```
Available System Utilities:

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reload

Enter option [1 - 3] q to Quit:
```

ステップ 4 **3** を入力してシステムの消去を実行します。

コンソールに次のメッセージが表示されます。

```
 **********   W A R N I N G   **********
THIS UTILITY WILL PERFORM A SYSTEM ERASE ON THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS
 TO COMPLETE. THE RESULT WILL BE COMPLETE
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL
 MEDIA TO RESTORE TO FACTORY DEFAULT STATE.

ARE YOU SURE YOU WANT TO CONTINUE? [Y/N] Y
```

ステップ 5 **Y** と入力します。

コンソール プロンプトで、別の警告が表示されます。

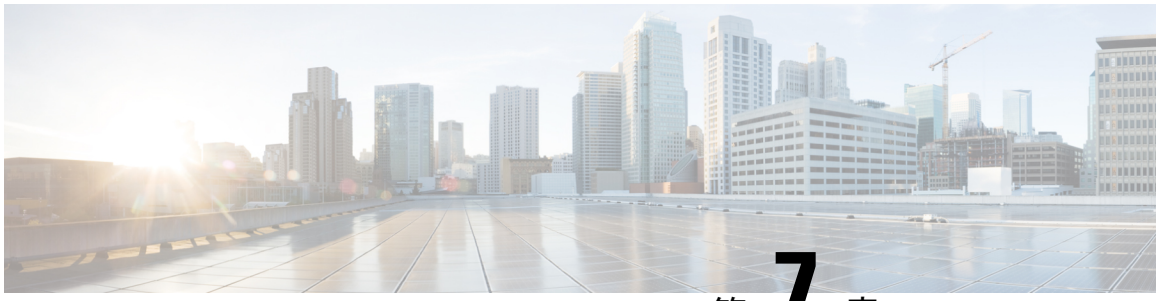
```
THIS IS YOUR LAST CHANGE TO CANCEL. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

ステップ 6 **Y** を入力してシステムの消去を実行します。

コンソールに次のメッセージが表示されます。

```
Deleting system disk, please wait…
Writing random data to all sectors of disk device (/dev/sda)…
Writing zeros to all sectors of disk device (/dev/sda)…
Completed!  System is now erased.
Press <Enter> to reboot.
```

システムの消去を実行した後、アプライアンスを再利用する場合は、Cisco ISE DVD を使用してシステムを起動し、起動メニューからインストール オプションを選択します。



第 7 章

Cisco ISE ポート リファレンス

Cisco ISE すべてのペルソナ ノード ポート

表 *16* : すべてのノードで使用されるポート

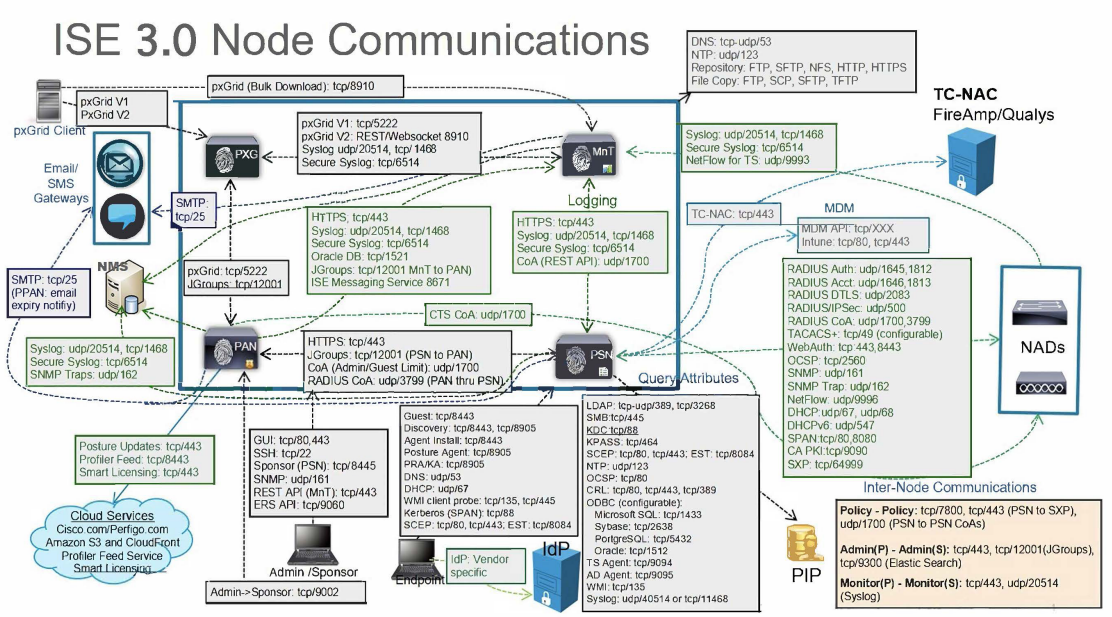
Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
複製および同期	• HTTPS（SOAP）：TCP/443 • データの同期/レプリケーション（JGroups）：TCP/12001（グローバル） • ISE メッセージング サービス：SSL：TCP/8671 • プロファイラエンドポイント所有権の同期/レプリケーション：TCP/6379	—

Cisco ISE インフラストラクチャ

この付録では、Cisco ISE が外部アプリケーションやデバイスとのイントラネットワーク通信に使用する、TCP および User Datagram Protocol（UDP）のポートの一覧を示します。この付録に示される Cisco ISE ポートが、対応するファイアウォールでオープンになっている必要があります。

Cisco ISE ネットワークでサービスを設定する場合は、次の情報に注意してください。

- ポートは、展開で有効になっているサービスに基づいて有効になります。ISE で実行中のサービスによって開かれるポートは別として、Cisco ISE は他のすべてのポートへのアクセスを拒否します。
- Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。
- RADIUS はすべてのネットワーク インターフェイス カード（NIC）でリッスンします。
- Cisco ISE サーバー インターフェイスは VLAN タギングをサポートしていません。ハードウェア アプライアンス上にインストールする場合は、Cisco ISE ノードへの接続に使用するスイッチ ポートの VLAN トランキングを無効にし、アクセス レイヤ ポートとして設定してください。
- 一時ポート範囲は 10000 ー 65500 です。これは、Cisco ISE リリース 2.1 以降でも同じです。
- VMware on Cloud は、サイト間 VPN ネットワーク構成でサポートされます。したがって、ネットワーク アクセス デバイスおよびクライアントから Cisco ISE への IP アドレスまたはポートの到達可能性は、NAT またはポートフィルタリングを使用せずに確立する必要があります。
- すべての NIC が IP アドレスを使用して設定できます。
- ポリシー情報ポイントは、外部の情報がポリシー サービス ペルソナに伝送されるポイントを表します。たとえば、外部情報は Lightweight Directory Access Protocol（LDAP）属性になります。



関連コンセプト

分散デプロイメント環境のノード タイプおよびペルソナ （3 ページ）

（注） ISE の TCP キープアライブ時間は 60 分です。ISE ノード間にファイアウォールが存在する場合は、そのファイアウォールに応じて TCP タイムアウト値を調整します。

Cisco ISE 管理ノードのポート

次の表に、管理ノードが使用するポートを示します。

表 *17 :* 管理ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット **0** またはボンド **0** のポート	その他のイーサネット インターフェイス（ギガビット イーサネット **1** ～ **5**、またはボンド **1** および **2**）のポート
管理		—

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
	• HTTP：TCP/80、HTTPS：TCP/443（TCP/443 にリダイレクトされた TCP/80。設定不可） • SSH サーバー：TCP/22 • CoA • 外部 RESTful サービス（ERS）REST API：TCP/9060 • • 管理者 GUI からのゲストアカウントの管理：TCP/9002 • ElasticSearch（コンテキストの可視性、プライマリからセカンダリ管理者ノードへのデータのレプリケート）：TCP/9300 （注） ポート 80 および 443 は、管理 Web アプリケーションをサポートしていて、デフォルトで有効になっています。 ギガビット イーサネット 0 では、Cisco ISE への HTTPS および SSH アクセスは制限されています。 TCP/9300 は、着信トラフィックに対しプライマリとセカンダリ両方の管理ノードで開いている必要があります。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
モニターリング	• SNMP クエリー：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • ICMP	
ロギング（アウトバウンド）	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SNMP トラップ：UDP/162	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザー インターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268、UDP/389 • SMB：TCP/445 • KDC：TCP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521、 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
電子メール	ゲスト アカウントおよびユーザー パスワードの有効期限の電子メール通知：SMTP：TCP/25	
スマート ライセンス	TCP/443 経由のシスコのクラウドへの接続 TCP/443 と ICMP を介した SSM オンプレミス サーバーへの接続	

Cisco ISE モニターリング ノードのポート

次の表に、モニターリング ノードが使用するポートを示します。

表 *18 :* モニターリング ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
管理	• HTTP：TCP/80、HTTPS：TCP/443 • SSH サーバー：TCP/22	—
モニターリング	Simple Network Management Protocol [SNMP]：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • ICMP	
ログ	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SMTP：アラームの電子メール用の TCP/25 • SNMP トラップ：UDP/162	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザー インターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268、UDP/389 • SMB：TCP/445 • KDC：TCP/88、UDP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521、15723、16820 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
インバウンド通信に使用されるポート	• MnT REST API のルーティングのために有効になっている ISE API ゲートウェイを持つ ISE ノードからの MnT インバウンド通信：TCP/9443 • PAN からのグローバル検索：TCP/1521 （注） これらのポートは、オンプレミスかクラウドかに関係なく、すべてのタイプの展開で必要です。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
pxGrid の一括ダウンロード	SSL：TCP/8910	

Cisco ISE ポリシー サービス ノードのポート

Cisco ISE はセキュリティを強化するために HTTP Strict Transport Security（HSTS）をサポートしています。Cisco ISE は、HTTPS を使用してのみアクセスできるブラウザを示す HTTPS 応答を送信します。ユーザーが HTTPS ではなく HTTP を使用して ISE にアクセスしようとすると、ブラウザはネットワーク トラフィックを生成する前に接続を HTTPS に変更します。この機能により、ブラウザが暗号化されていない HTTP を使用して要求を Cisco ISE に送信することがなくなり、サーバーは暗号化された要求をリダイレクトできるようになります。

次の表に、ポリシー サービス ノードが使用するポートを示します。

表 *19*：ポリシー サービス ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
管理	• HTTP：TCP/80、HTTPS：TCP/443 • SSH サーバー：TCP/22 • OCSP：TCP/2560	Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。
クラスタリング（ノード グループ）	ノード グループ/JGroups：TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
デバイス管理	TACACS+：TCP/49 （注） このポートは、リリース 2.1 以降のリリースで設定できます。	
TrustSec	HTTP と Cisco ISE REST API を使用して、ポート 9063 を介して TrustSec データをネットワークデバイスに転送します。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
SXP	• PSN（SXP ノード）から NAD：TCP/64999 • PSN から SXP へ（ノード間通信）： TCP/9644	
TC-NAC	TCP/443	
モニターリング	Simple Network Management Protocol [SNMP]：UDP/161 （注） このポートは、ルート テーブルによって異なります。	
ロギング（アウトバウンド）	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SNMP トラップ：UDP/162	
セッション	• RADIUS 認証：UDP/1645、1812 • RADIUS アカウンティング：UDP/1646、1813 • RADIUS DTLS 認証/アカウンティング：UDP/2083 • RADIUS 許可変更（CoA）送信：UDP/1700 • RADIUS 許可変更（CoA）リッスン/リレー：UDP/1700、3799 （注） UDP ポート 3799 は、設定できません。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザーインターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268 • SMB：TCP/445 • KDC：TCP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
パッシブ ID（インバウンド）	• TS エージェント：TCP/9094 • AD エージェント：TCP/9095 • syslog：UDP/40514、TCP/11468	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
Web ポータル サービス： - ゲスト/Web 認証 - ゲスト スポンサー ポータル - デバイス ポータル - クライアントのプロビジョニング - 証明書のプロビジョニング - ブロックリストポータル	HTTPS（インターフェイスは Cisco ISE のサービスに対して有効にする必要があります）： • ブロックリストポータル：TCP/8000-8999（デフォルトポートは TCP/8444 ） • ゲストポータルおよびクライアントのプロビジョニング：TCP/8000-8999（デフォルトポートは TCP/8443） • 証明書のプロビジョニングポータル：TCP/8000-8999（デフォルトポートは TCP/8443 ） • デバイスポータル：TCP/8000-8999（デフォルトポートは TCP/8443） • スポンサーポータル：TCP/8000-8999（デフォルトポートは TCP/8443） • ゲストとスポンサーのポータルからの SMTP ゲストの通知：TCP/25	
ポスチャ - 検出 - プロビジョニング - アセスメント/ハートビート	• 検出（クライアント側）：TCP/80（HTTP）、TCP/8905（HTTPS） （注） デフォルトでは、TCP/80 は TCP/8443 にリダイレクトされます。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 Cisco ISE は、TCP ポート 8905 のポスチャおよびクライアント プロビジョニングの管理証明書を提示します。 Cisco ISE は、TCP ポート 8443（またはポータルで使用するために設定したポート）のポータル証明書を提示します。 • 検出（ポリシー サービス ノード側）：TCP/8443、8905（HTTPS） AnyConnect リリース 4.4 以降が搭載された Cisco ISE リリース 2.2 以降から、このポートは設定可能です。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
個人所有デバイスの持ち込み（BYOD）/ネットワーク サービス プロトコル（NSP） - リダイレクト - プロビジョニング - SCEP	• プロビジョニング - URL リダイレクト：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • EST 認証付きの Android デバイスの場合：TCP/8084 Android デバイスの場合、ポート 8084 を リダイレクト ACL に追加する必要があります。 • プロビジョニング - ActiveX と Java アプレットのインストール（ウィザードのインストールの開始を含む）：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • プロビジョニング - Cisco ISE からのウィザードのインストール（Windows および Mac OS）：TCP/8443 • プロビジョニング - Google Play（Android）からのウィザードのインストール：TCP/443 • プロビジョニング - サプリカントのプロビジョニング プロセス：TCP/8905 • CA への SCEP プロキシ：TCP/80 または TCP/443（SCEP RA URL の設定に基づく）	
モバイル デバイス管理（MDM）API の統合	• URL リダイレクト：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • API：ベンダー固有 • エージェントのインストールおよびデバイスの登録：ベンダー固有	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
プロファイリング	• NetFlow：UDP/9996 （注） このポートは、設定可能です。 • DHCP：UDP/67 （注） このポートは、設定可能です。 • DHCP SPAN プローブ：UDP/68 • HTTP：TCP/80、8080 • DNS：UDP/53（ルックアップ） （注） このポートは、ルート テーブルによって異なります。 • SNMP クエリー：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • SNMP トラップ：UDP/162 （注） このポートは、設定可能です。	

Cisco ISE pxGrid サービス ポート

次の表に、pxGrid サービス ノードが使用するポートを示します。

表 *20 : pxGrid* サービス ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
管理	• SSL：TCP/5222（ノード間通信） • SSL：TCP/7400（ノード グループ通信）	—

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
pxGrid 登録者数	TCP/8910	

OCSP および CRL サービス ポート

Cisco ISE サービスおよびポートへの参照には Cisco ISE 管理ノード、ポリシー サービス ノード、モニターリング ノードで個別に使用される基本ポートが表示されますが、Online Certificate Status Protocol（OCSP）サービスおよび証明書失効リスト（CRL）の場合、ポートは CA サーバーまたは OCSP/CRL をホストするサービスによって異なります。

OCSP の場合、使用可能なデフォルト ポートは TCP 80 または TCP 443 です。Cisco ISE 管理者ポータルでは、OCSP サービス用の HTTP ベースの URL が予期されるため、TCP 80 がデフォルトです。デフォルト以外のポートも使用できます。

CRL の場合、デフォルトのプロトコルには、HTTP、HTTPS、および LDAP が含まれており、それぞれのデフォルト ポートは 80、443、および 389 になります。実際のポートは CRL サーバーで設定されます。

Cisco ISE プロセス

次の表に、Cisco ISE プロセスとそのサービスへの影響を示します。

プロセス名	説明	サービスへの影響
データベース リスナー	Oracle Enterprise データベース リスナー（Oracle Enterprise Database Listener）	すべてのサービスが正常に動作するには実行状態でなければならない
データベース サーバー	Oracle Enterprise データベース サーバー（Oracle Enterprise Database Server）。設定と処理データの両方を格納する	すべてのサービスが正常に動作するには実行状態でなければならない
アプリケーション サーバー（Application Server）	ISE 用メイン Tomcat サーバー	すべてのサービスが正常に動作するには実行状態でなければならない
Profiler データベース	ISE プロファイリング サービス用の Redis データベース	ISE プロファイリング サービスが正常に動作するには実行状態でなければならない

AD コネクタ	アクティブ ディレクトリ ランタイム	ISEがアクティブディレクトリ認証を実行するには実行状態でなければならない
MnT セッション データベース	MnT サービス用 Oracle TimesTen データベース	すべてのサービスが正常に動作するには実行状態でなければならない
MnT ログ コレクタ	MnT サービスのログ コレクタ	MnT 運用データのため実行状態でなければならない
MnT ログ プロセッサ	MnT サービスのログ プロセッサ	MnT 運用データのため実行状態でなければならない
証明書認証局サービス	ISE 内部 CA サービス	ISE 内部 CA が有効になっている場合は実行状態でなければならない

必要なインターネット URL

次の表に、特定の URL を使用する機能を示します。IP トラフィックが Cisco ISE とこれらのリソース間を移動できるように、ネットワークファイアウォールまたはプロキシサーバーのいずれかを設定する必要があります。リストされている URL にこのアクセスを提供できない場合は、関連付けられている機能が損なわれるか、または動作不能になります。

表 *21* : 必要な *URL* アクセス

機能	URL
ポスチャの更新	https://www.cisco.com/ https://iseservice.cisco.com
フィードサービスのプロファイリング	https://ise.cisco.com
スマート ライセンス	https://tools.cisco.com
インタラクティブヘルプ	*.walkme.com *.walkmeusercontent.com