



Linux KVM への Cisco ISE のインストール

- [KVM ハイパーバイザ サポート, 1 ページ](#)
- [Cisco ISE 評価版ソフトウェアの入手, 8 ページ](#)
- [KVM への Cisco ISE のインストール, 8 ページ](#)

KVM ハイパーバイザ サポート

Cisco ISE は、Red Hat Enterprise Linux (RHEL) 7.0 の KVM ハイパーバイザをサポートします。

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 sse3 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 ハードウェア要件

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、KVM に Cisco SNS 3515 および SNS 3595 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。

表 1: KVM システム要件

要件のタイプ	最小要件
CPU	<ul style="list-style-type: none"> • 評価 : <ul style="list-style-type: none"> ◦ クロック速度 : 2.0 GHz 以上 ◦ コア数 : 2 CPU コア • 実稼動 : <ul style="list-style-type: none"> ◦ クロック速度 : 2.0 GHz 以上 ◦ コア数 : 6 CPU コア (小規模) ~ 8 CPU コア (大規模) <p>6 コア、2.0 GHz 以上。</p> <p>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。</p> <p>(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。</p>
メモリ	<ul style="list-style-type: none"> • 評価 : <ul style="list-style-type: none"> ◦ 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 : <ul style="list-style-type: none"> ◦ 小規模 : 16 GB ◦ 大規模 : 64 GB

要件のタイプ	最小要件
ハードディスク	<ul style="list-style-type: none"> • 評価 : <ul style="list-style-type: none"> ◦ 最小 (ラボ テスト 限定、エンドポイント 数約 20) : 100 GB ◦ 推奨 : 200 GB • 実稼動 : <p>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)。</p> <p>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。</p> <p>(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。</p>
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 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	RHEL 7.0 の KVM

仮想マシンのアプライアンス サイズについての推奨事項

Cisco ISE の導入の規模を評価するとき、導入に必要なアプライアンスの数とサイズの詳細については、[配置の規模およびスケーリングについての推奨事項](#)の項を参照してください。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。次の表に、仮想アプライアンスのサイズ調整に最低限必要なリソースと SNS-3515 または SNS-3595 物理アプライアンスのリソースを比較できるように示します。

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。

- VM リソースを専用にし、複数の VM 間で共有したり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 사용하여 Cisco ISE 仮想アプライアンスを導入すると、十分なリソースが各 VM に割り当てられます。



(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。

- VM のポリシー サービス ノードは管理またはモニタリング ノードよりも少ないディスク領域で導入できます。すべての実稼働 Cisco ISE ノードの最小ディスク領域は 200 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、[ディスク領域に関する要件](#)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。

表 2: 実稼働環境向けの VM アプライアンスの最低仕様

プラットフォーム	小規模 VM アプライアンス (SNS-3515 ベース)	大規模 VM アプライアンス (SNS-3595 ベース)
プロセッサ	合計 6 コア (2.0 GHz 以上) または合計 12000 MHz の最小 CPU 割り当て。	合計 8 コア (2.0 GHz 以上) または合計 16000 MHz の最小 CPU 割り当て。
メモリ	16 GB	64 GB
合計ディスク領域	200 GB ～ 2 TB。詳細については、 ディスク領域に関する要件 を参照してください。	200 GB ～ 2 TB。詳細については、 ディスク領域に関する要件 を参照してください。
イーサネット NIC	最大 6 つのギガビットイーサネット NIC	最大 6 つのギガビットイーサネット NIC

ディスク領域に関する要件

次の表に、実稼働導入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。

表 3: 仮想マシンに推奨されるディスク領域

ISE ペルソナ	最小ディスク領域	最大ディスク領域	実稼働環境用に推奨されるディスク領域
スタンドアロン ISE	200 GB	2 TB	600 GB ～ 2 TB

ISE ペルソナ	最小ディスク領域	最大ディスク領域	実稼働環境用に推奨されるディスク領域
分散型 ISE : 管理のみ	200 GB	2 TB	250 ~ 300 GB
分散型 ISE : モニタリングのみ	200 GB	2 TB	600 GB ~ 2 TB
分散型 ISE : ポリシー サービスのみ	200 GB	2 TB	200 GB
分散型 ISE : 管理およびモニタリング	200 GB	2 TB	600 GB ~ 2 TB
分散 ISE : 管理、モニタリング、およびポリシー サービス	200 GB	2 TB	600 GB ~ 2 TB

ディスク領域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 VM に割り当てることができるディスク領域は最大で 2 TB のみです。
- 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 30 パーセントが RADIUS 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展開では、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リングノードがある場合、180 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、モニタリングノードのログを 38 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 30 GB が追加されます。要件に応じて、最大 2 TB のログストレージ分 VM ディスクサイズを増やすことができます。

仮想マシンのディスクサイズを増やす場合、アップグレードを実行する必要はありませんが、仮想マシン上で Cisco ISE の新規インストールを実行してください。

表 4-4 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、モニタリングノードでログを保持できる日数を示します。数値はログの抑制と異常クライアント検出が有効になっていることに基づいています。



(注) 次の表に、RADIUS ログストレージのデータを示します。モニタリングノードの VM ディスク領域の 30 パーセントが RADIUS ログの保存に割り当てられ、20 パーセントが TACACS ログ用に割り当てられます。

表 4: モニタリングノードに RADIUS ログが保存される日数

エンドポイント数	200 GB	400 GB	600 GB	1024 GB	2048 GB
10,000	126	252	378	645	1,289
20,000	63	126	189	323	645
30,000	54	84	126	215	430
40,000	32	63	95	162	323
50,000	26	51	76	129	258
100,000	13	26	38	65	129
150,000	9	17	26	43	86
200,000	7	13	19	33	65
250,000	6	11	16	26	52

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、インストールは中断されます。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。このパフォーマンス検証チェックは、ISO ベースおよび OVA (VMware) インストールに適用されます。

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。

show tech support コマンドを使用したオンデマンドの仮想マシンパフォーマンスチェック

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-vml23/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) (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: 322 Gigabyte
***** Physical RAM size detected: 40443664 Kbytes
***** Number of network interfaces detected: 1
***** Number of CPU cores: 2
```

```

***** CPU Mhz: 2300.00
***** Verifying CPU requirement...
***** Verifying RAM requirement...
***** Writing disk partition table...

```

Cisco ISE 評価版ソフトウェアの入手

Cisco ISE 評価版ソフトウェア (R-ISE-EVAL-K9=) を入手するには、シスコのアカウント チームまたは認定されたシスコ チャンネル パートナーにお問い合わせください。

評価システムから完全ライセンスを持つ実稼働環境のシステムに Cisco ISE 設定を移行するには、次のタスクを実行する必要があります。

- 評価版の設定をバックアップする。
- 実稼働 VM に必要なディスク領域があることを確認する。詳細については、[配置の規模およびスケーリングについての推奨事項](#)を参照してください。
- 実稼働の導入ライセンスをインストールする。
- 実稼働システムに設定を復元する。



(注) 評価の場合、VM に対するハードディスクの最小の割り当て要件は 200 GB です。より多くのユーザをサポートする実稼働環境に VM 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 TB）に再設定してください。

はじめる前に

評価目的で、VM 要件に準拠したサポート対象の VM に Cisco ISE をインストールできます。Cisco ISE を評価する場合は、VM のディスク領域を少なく設定できますが、最低 200 GB のディスク領域を割り当てることは必要です。

ステップ 1 <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。

ステップ 2 [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。ソフトウェア 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 サービスの評価を開始できます。

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-nohwcheck-2.1.0.381.x86_64.iso  
--disk=/home/libvirt-images/kvm-ise1.img,size=100  
--network type=direct,model=virtio,source=eth2,source_mode=bridge
```

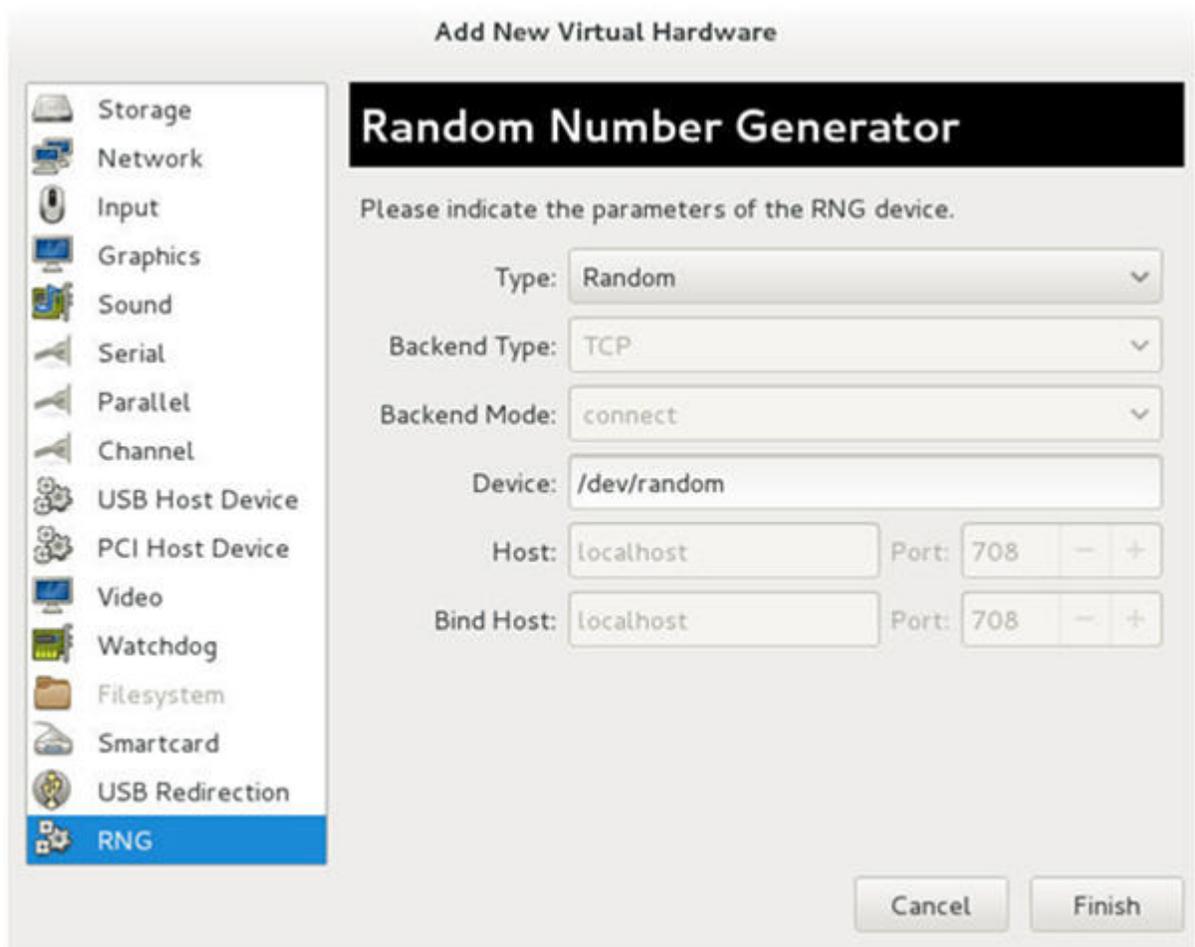
Ise-nohwcheck-2.1.0.381.x86_64.iso は Cisco ISE ISO イメージの名前です。

はじめる前に

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。
- [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]、バージョンとして [Red Hat Enterprise Linux 7.0] を選択して、[続行 (Forward)] をクリックします。
- 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。
- [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。
 - [参照 (Browse)] をクリックします。
 - 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。
 - [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。
 - ストレージ ボリュームの名前を入力します。
 - [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。
 - 最大キャパシティを入力します。
 - [終了 (Finish)] をクリックします。
 - 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。
 - [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。
- (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。
 - RHEL 7 をサポートするには、KVM 仮想マシンは乱数ジェネレータ (RNG) ハードウェアをサポートしている必要があります。RNG 設定については、次の図を参照してください。



CLI を使用して新しい VM を作成している場合は、次の設定を含めてください。

```
<rng model='virtio'
  <backend model='random'>/dev/random</backend>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0' />
</rng>
```

c) [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
Disk bus	VirtIO
Cache mode	none
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。

