Cisco Secure Email and Web 仮想アプライアンス設置ガイド

公開日：2023 年 5 月 4 日

改訂日：2023 年 6 月 7 日

目次

Cisco Systems, Inc.
www.cisco.com

Cisco Secure 仮想アプライアンスについて

Cisco Secure 仮想アプライアンスは、Cisco Secure 仮想アプライアンスの管理（30 ページ）に記載されているわずかな変更を除き、Cisco Secure Email Gateway、Cisco Secure Web Appliance、または Cisco Secure Email and Web Manager の各物理ハードウェアアプライアンスと同じように機能します。

HYPER-V の導入でサポートされる仮想アプライアンスモデルおよび AsyncOS リリース

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスクサイズ	メモリ	プロセッサコア数
Cisco Secure Web 仮想アプライアンス	AsyncOS 14.5	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24
	AsyncOS 12.5 以降	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスクサイズ	メモリ	プロセッサコア数
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 11.7 以降	**S100V**	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 11.0 以降	**S100V**	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4
		S600V	1024 GB	-	24 GB	12

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	メモリ	プロセッサコア数
Cisco Secure Email Virtual Gateway	AsyncOS 15.0 以降	**C600V**	500 GB	16 GB	8

製品	AsyncOS リリース	モデル	推奨ディスクサイズ（Disk Size）	メモリ	プロセッサコア数
Cisco Secure Email and Web Manager Virtual	AsyncOS 15.0 以降	**M600V**	2032 GB	16 GB	8

KVM の導入でサポートされる仮想アプライアンス モデルおよび AsyncOS リリース

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	メモリ	プロセッサコア数
Cisco Secure Email Virtual Gateway	AsyncOS 15.0 以降	**C600V**	500 GB	16 GB	8

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	メモリ	プロセッサコア数
Cisco Secure Email Virtual Gateway	AsyncOS 13.0 以降 AsyncOS 12.0 以降 AsyncOS 11.0 以降 AsyncOS 10.0.1 以降 AsyncOS 14.0 以降	**C100V**	200 GB	6 GB	2
		C300V	500 GB	8 GB	4
		C600V	500 GB	8 GB	8

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスクサイズ	メモリ	プロセッサコア数
Cisco Secure Web 仮想アプライアンス	AsyncOS 14.5	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスクサイズ	メモリ	プロセッサコア数
	AsyncOS 12.5 以降	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 11.7 以降	**S100V**	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 10.1 以降	**S600V**	1024 GB	-	24 GB	12
	AsyncOS 8.6 以降	**S100V**	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

製品	AsyncOS リリース	モデル	ディスク サイズ（Disk Size）	メモリ	最大メモリ	プロセッサコア数
Cisco Secure Email and Web Manager Virtual	AsyncOS 15.0 以降	**M600V**	2032 GB	16 GB	16 GB	8
	AsyncOS 14.1.0 以降	**M600V**	2032 GB	8 GB	16 GB	8

VMWare ESXi の導入でサポートされる仮想アプライアンスモデル

（注） **AsyncOS ドキュメントで明示的に記載されている場合を除き、OVF で定義された ESXi 構成に対する変更はサポートされていません。**

[AsyncOS 15.0 以降]

[アップグレードのシナリオ]：Cisco Content Security 仮想アプライアンスの OVF イメージで、アップグレード時に以前のバージョンの AsyncOS の事前設定されたメモリの値から新しい値に次のように切り替えることができます。

- C100v モデル：8 GB
- C300v および C600v モデル：16 GB
- M600v モデル：16 GB

[新規インストールのシナリオ]：Cisco Content Security 仮想アプライアンスの OVF イメージで、次の事前設定されたメモリの値を使用できます。

- C100v モデル：8 GB
- C300v および C600v モデル：16 GB
- M600v モデル：16 GB

製品	モデル	ディスク容量	メモリ	プロセッサコア数
Cisco Secure Email Virtual Gateway	**C100V**	200 GB	8 GB	2
	C300V	500 GB	16 GB	4
	C600V	500 GB	16 GB	8

製品	モデル	ディスク容量	メモリ	最大メモリ	プロセッサコア数
Cisco Secure Email and Web Manager Virtual	**M100V**	250 GB	6 GB	8 GB	2
	M300V	1024 GB	8 GB	16 GB	4
	M600V	2032 GB	16 GB	16 GB	8

[**AsyncOS 15.0 より前**] Cisco Content Security 仮想アプライアンスの OVF イメージで、事前設定されたメモリの値から新しい最大値に次のように切り替えることができます。

- M100v/C100v モデル：6 ～ 8 GB
- M300v/M600v/C300v/C600v モデル：8 ～ 16 GB

製品	モデル	ディスク容量	メモリ	最大メモリ*	プロセッサコア数
Cisco Secure Email Virtual Gateway	**C100V**	200 GB	6 GB	8 GB	2
	C300V	500 GB	8 GB	16 GB	4
	C600V	500 GB	8 GB	16 GB	8

製品	モデル	ディスク容量	メモリ	最大メモリ*	プロセッサコア数
Cisco Secure Email and Web Manager Virtual	**M100V**	250 GB	6 GB	8 GB	2
	M300V	1024 GB	8 GB	16 GB	4
	M600V	2032 GB	8 GB	16 GB	8

* 最大メモリの列は、テストで認定された最大メモリ構成を示しています。

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスク サイズ	メモリ	プロセッサコア数
Cisco Secure Web 仮想アプライアンス	AsyncOS 14.5	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24
	AsyncOS 12.5 以降	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12

製品	AsyncOS リリース	モデル	推奨ディスクサイズ	サポートされるディスク サイズ	メモリ	プロセッサコア数
	AsyncOS 11.7 以降	**S100V**	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 10.1 以降	**S600V**	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 8.6 以降	**S100V**	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

AsyncOS バージョンの要件は、サポートされる VMWare ESXi Hypervisor（13 ページ）に記載されています。

システム要件

Microsoft Hyper-V の導入

サポートされる Microsoft Hyper-V およびホスト オペレーティング システム

AsyncOS バージョン	Hyper-V バージョン
AsyncOS 11.0（Web）以降	Hyper-V バージョン 5.0
AsyncOS 15.0（Email）以降	Microsoft Hyper-V Server 2019
AsyncOS 15.0（Management）以降	Microsoft Hyper-V Server 2019

Microsoft Hyper-V 導入のハードウェア要件

[Secure Email Virtual Gateway]

ハードウェア:

- Cisco UCS C シリーズ 220/240 M5 でサポート
- Cisco Secure Email Virtual パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® Gold 6126 CPU @ 2.60GHz プロセッサを搭載した Cisco Unified Computing System™（Cisco UCS®）C シリーズ M5 サーバーを最低限使用しています。

（注） AsyncOS 15.0 以降では、Secure Email Virtual Gateway で第 2 世代の展開がサポートされます。

[Secure Email and Web Manager Virtual]

ハードウェア:

- Cisco UCS C シリーズ 220/240 M5 でサポート
- Cisco Secure Email and Web Manager Virtual パフォーマンステストラボでは、Intel® Xeon® Gold 6140 CPU @ 2.30GHz を搭載した Cisco Unified Computing System™（Cisco UCS®）C シリーズ M5 サーバーを最低限使用しています。

（注） AsyncOS 15.0 以降では、Secure Email and Web Manager Virtual で第 2 世代の展開がサポートされます。

KVM の導入

KVM の導入に適した環境を次に示します。すべての導入で、ディスクストレージのシンプロビジョニングを使用します。

Red Hat Enterprise Linux Server

ホスト OS:

- Red Hat Enterprise Linux Server 8.6（Redhat にはリリースのコード名のサポートはない）

バージョン情報:

- Linux：4.18.0-372.9.1.el8.x86_64
- libvirt/QEMU：

  ライブラリにコンパイル済み：libvirt 8.0.0

  ライブラリ使用時：libvirt 8.0.0

  API の使用：QEMU 8.0.0

  ハイパーバイザの実行時：QEMU 6.2.0

ハードウェア:

- Cisco UCS C シリーズ 220/240 M4 または M5 でサポート
- Cisco Secure Email Virtual パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® Gold 6126 CPU @ 2.60GHz プロセッサを搭載した Cisco Unified Computing System™（Cisco UCS®）C シリーズ M5 サーバーを最低限使用しています。

KVM ドライバ

サポートされている KVM ドライバ:

- ネットワーク：E1000、Virtio
- ディスク：VirtIO

KVM パッケージ

ホストへのインストールに必要な/関連する KVM パッケージ

- qemu-kvm
- qemu-img
- libvirt
- libvirt-python
- libvirt-client
- virt-manager（X-windows が必要）
- virt-install

VMware ESXi の導入

サポートされる VMWare ESXi Hypervisor

AsyncOS バージョン	VMware ESXi のバージョン
AsyncOS（電子メール）	
AsyncOS 15.0.x	6.7 および 7.0
AsyncOS 14.x	6.7 および 7.0
AsyncOS 13.x	6.5 および 6.7
AsyncOS 12.0	6.5 および 6.7
AsyncOS 11.1	6.5
AsyncOS 11.0	6.5
AsyncOS（管理）	
AsyncOS 15.0.x	6.7 および 7.0
AsyncOS 14.2.x	6.7 および 7.0
AsyncOS 14.1.x	6.7 および 7.0
AsyncOS 14.0.x	6.7
AsyncOS 13.8.x	6.7
AsyncOS 13.6.2	6.7
AsyncOS 13.5.x	6.5
AsyncOS 13.x	6.5
AsyncOS 12.x	6.5
AsyncOS 11.5.1	6.5
AsyncOS 11.x	6.5
AsyncOS（Web）	
AsyncOS 14.5.x	6.5、6.7、および 7.0
AsyncOS 14.0.x	6.5、6.7、および 7.0
AsyncOS 12.7.x	6.5 および 6.7
AsyncOS 12.5.x	6.5 および 6.7
AsyncOS 12.0.x	6.5 および 6.7
AsyncOS 11.8.1 以降	6.5 および 6.7
AsyncOS 11.8.0	6.5
AsyncOS 11.7.x	6.5
AsyncOS 11.5.x	6.5
AsyncOS 10.x	6.5

他の VMware ハイパーバイザについては「ベストエフォート」ベースでサポートされます。つまり、シスコで支援を試みますが、一部の問題を再現できない、または解決策を保証できない場合があります。

VMWare ESXi 導入時のハードウェア要件

Cisco UCS サーバ（ブレードまたはラックマウント）が、サポートされている唯一のハードウェアプラットフォームです。

ご使用の仮想アプライアンスをホスティングするサーバの最小要件は以下のとおりです。

ハイパーバイザの詳細：

- VMware ESXi 6.7/7.0（詳細については サポートされる VMWare ESXi Hypervisor（13 ページ）を参照）

ハードウェア：

- Cisco UCS C シリーズ 220/240 M4 または M5 でサポート

他のハードウェア プラットフォームについては「ベストエフォート」ベースでサポートされます。つまり、シスコで支援を試みますが、一部の問題を再現できない、または解決策を保証できない場合があります。

（注） ドキュメントに明示的に記載されている場合を除き、シスコは、IP インターフェイスの削除、アプライアンスの CPU コアや RAM サイズの変更など、Cisco コンテンツ セキュリティ仮想アプライアンスのハードウェア構成の変更をサポートしていません。このような変更が行われると、アプライアンスがアラートを送信することがあります。

（注） VMWare ESXi 6.7 の導入は、AsyncOS 11.8.1-023 以降（Web セキュリティアプライアンス用）を搭載した Cisco UCS M4 および M5 シャーシサーバでサポートされています。

（注） VMWare ESXi 7.0 の導入は、AsyncOS 14.0.1-053 以降（Cisco Secure Web Appliance 用）を搭載した Cisco UCS M4 および M5 シャーシサーバーでサポートされています。

ESXi ドライバ

サポートされている ESXi ドライバ：

- ネットワークアダプタタイプ：E1000

（Hosted Email Security のみ）FlexPod ソリューションでの導入

AsyncOS for Email リリース 8.5 以降の場合：

FlexPod ソリューションの一部としての Cisco Secure Email Virtual Gateway の導入の詳細については、http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/white-paper-c11-731731.pdf を参照してください。CCO ログインにより、このマニュアルにアクセスできるかどうかが決まります。

FlexPod の全般的な情報については、https://www.cisco.com/c/ja_jp/solutions/data-center-virtualization/flexpod/index.html を参照してください。

FlexPod は、仮想 Cisco Secure Web Appliance または仮想 Cisco Secure Email and Web Manager アプライアンス の導入には適用されません。

Content Secure イメージとファイルの準備

導入環境に最適なサイズの仮想アプライアンスイメージの決定

ニーズを満たす最適なサイズの仮想アプライアンスイメージを決定します。次の場所から入手できる製品のデータシートを参照してください。

アプライアンス	データシートへのリンク
Cisco Secure Email ゲートウェイ	「Cisco Secure Email Gateway アプライアンスデータシート」へのリンクは、次のページから検索してください。 https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html データシートで「Cisco Secure Email Virtual Gateway Specifications」という名前の表を検索します。
Cisco Secure Web Appliance	「Cisco Secure Web Appliance データ シート」へのリンクは、次のページから検索してください。 https://www.cisco.com/c/ja_jp/products/security/web-security-appliance/datasheet-listing.html データシートで、「Cisco WSAV」という名前の表を検索します。
Cisco Secure Email and Web Manager	「Cisco Secure Email and Web Manager アプライアンスデータシート」へのリンクは、次のページから検索してください。 https://www.cisco.com/c/dam/en/us/products/se/2019/4/Collateral/security-management-app-ds.pdf データシートで「Cisco Secure Email and Web Manager Virtual」という名前の表を検索します。

Cisco コンテンツ セキュリティ仮想アプライアンスのイメージのダウンロード

はじめる前に

- シスコからご使用の仮想アプライアンスのライセンスを取得します。
- 導入環境に最適なサイズの仮想アプライアンスイメージの決定（15 ページ）を参照してください。

ステップ 1 ご使用の仮想アプライアンスの [シスコダウンロードソフトウェア（Cisco Download Software）] ページに移動します。

- Cisco Secure Email Virtual Gateway の場合：
  https://software.cisco.com/download/home/284900944/type/282975113/release
- Cisco Secure Web Appliance の場合：
  https://software.cisco.com/download/home/284806698/type/282975114/release
- Cisco Secure Email and Web Manager Virtual の場合：
  https://software.cisco.com/download/home/286283259/type/286283388/release

ステップ 2 左側のナビゲーションウィンドウで、AsyncOS のバージョンを選択します。

ステップ 3 ダウンロードする仮想アプライアンス モデル イメージの [ダウンロード（Download）] をクリックします。

ステップ 4 ローカルマシンにイメージを保存します。

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）

起動時にロードするライセンスおよびコンフィギュレーション ファイルの準備（KVM の導入）

この機能は、Cisco Secure Web Appliance の AsyncOS 8.6 で導入されました。その他のコンテンツ セキュリティ アプライアンスやその他の AsyncOS リリースでは使用できません。

Cisco コンテンツ セキュリティ仮想アプライアンスのライセンスおよびコンフィギュレーション ファイルは、Cisco アプライアンスの最初の起動時に自動的にロードできます（初回起動後はロードされません）。

ステップ 1 次のライセンスおよびコンフィギュレーション ファイルを取得し、名前を付けます。

- コンフィギュレーション ファイル：`config.xml`
- ライセンス ファイル：`license.xml`

ステップ 2 これらのファイルのいずれか、または両方が含まれる ISO イメージを作成します。

次の作業

AsyncOS.QCOW イメージを導入する場合は、ISO を仮想 CD-ROM ドライブとして仮想マシンインスタンスに接続します。

起動後は、お使いのシスコ仮想アプライアンスでステータスログを確認できます。この機能に関連するエラーメッセージには「**0**」というキーワードが含まれています。アプライアンスにログインし、CLI から `tail` コマンドを実行する必要があります。詳細についてはユーザーガイドの「コマンド ライン インターフェイス」の章で「Cisco Secure Web Appliance CLI Commands」を参照してください。

関連項目

- KVM での導入（19 ページ）

Microsoft Hyper-V への導入

	操作	詳細情報
1.	ご使用の AsyncOS リリースのリリースノートを確認します。	リリースノートは、その他の情報（38 ページ）から入手できます。
2.	シスコから仮想アプライアンスのイメージと MD5 ハッシュをダウンロードします。	MD5 ハッシュでアプライアンスイメージのデータ整合性を確認する必要があります。 Content Secure イメージとファイルの準備（15 ページ）。
3.	Hyper-V に仮想アプライアンスを導入します。	a. Windows サーバ オペレーティング システムを設定します。必要な Hyper-V の役割がインストールされていることを確認します。詳細については、システム要件（10 ページ）を参照してください。 b. Content Secure イメージとファイルの準備（15 ページ）に示すように、イメージをダウンロードします。 c. Hyper-V マネージャの [新しい仮想マシンウィザード（New Virtual Machine Wizard）] を使用して、仮想アプライアンスイメージをインストールします。 d. ウィザードを完了します。 e. Hyper-V マネージャでプロセッサの設定を編集します。必要なプロセッサおよび NIC の数を確認するには、導入環境に最適なサイズの仮想アプライアンスイメージの決定（15 ページ）を参照してください。
4.	DHCP が無効の場合は、ネットワーク上にアプライアンスをセットアップします。	DHCP が無効の場合に実行するネットワーク上でのアプライアンスの設定（Microsoft Hyper-V）（18 ページ）
5.	ライセンスファイルをインストールします。	仮想アプライアンスのライセンスファイルのインストール（28 ページ）。
6.	アプライアンスの Web UI にログインし、物理アプライアンスの場合と同様にアプライアンスソフトウェアを設定します。 たとえば、以下を行うことができます。 • System Setup ウィザードの実行 • コンフィギュレーションファイルのアップロード • 手動による機能の設定	• アプライアンスのアクセスと設定の手順の詳細については（必要な情報の収集を含む）、その他の情報（38 ページ）の関連する場所から入手可能なオンラインヘルプ、またはお使いの AsyncOS リリースのユーザガイドを参照してください。 • 物理アプライアンスから設定を移行するには、お使いの AsyncOS リリースのリリースノートを参照してください。 機能キーはそれぞれの機能を有効にするまでアクティブ化されません。

（注） 次に、Microsoft Hyper-V generation 1 プラットフォームに導入された仮想 Cisco Secure Web Appliance（FreeBSD 10.x）の制限事項を示します。

- `etherconfig` CLI コマンドを使用して、仮想アプライアンス インターフェイスを変更することはできません。
- `ifconfig` CLI コマンドは、デュプレックスモードで動作している場合でも、仮想アプライアンス インターフェイスのステータスを Unknown またはシンプレックスとして表示します。

ただし、上記の制限により、アプライアンスのパフォーマンスに影響はありません。

（注） AsyncOS 15.0 以降では、Secure Email Gateway で第 2 世代の展開がサポートされます。

AsyncOS 15.0 以降では、Secure Email and Web Manager で第 2 世代の展開がサポートされます。

現在、第 2 世代の展開の「セキュアブート」および「トラステッド プラットフォーム モジュール（TPM）」テクノロジーはサポートされていません。

DHCP が無効の場合に実行するネットワーク上でのアプライアンスの設定（Microsoft Hyper-V）

（注） 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

ステップ 1 Hyper-V マネージャコンソールから、`interfaceconfig` を実行します。

ステップ 2 仮想アプライアンス管理ポートの IP アドレスを書き留めます。

（注） 管理ポートは DHCP サーバから IP アドレスを取得します。アプライアンスが DHCP サーバにアクセスできない場合は、デフォルトで `192.168.42.42` が使用されます。

（注） `setgateway` コマンドを使用して、デフォルトゲートウェイを設定します。

ステップ 3 変更を確定します。

（注） ホスト名は、セットアップウィザードが完了するまで更新されません。

KVM での導入

	操作	詳細情報
ステップ 1	機器とソフトウェアが、すべてのシステム要件を満たしていることを確認します。	システム要件（10 ページ）、および使用する製品とツールのマニュアルを参照してください。
ステップ 2	ご使用の AsyncOS リリースのリリースノートを確認します。	リリースノートは、その他の情報（38 ページ）から入手できます。
ステップ 3	UCS サーバ、ホスト OS、および KVM を設定します。	使用する製品およびツールのマニュアルを参照してください。
ステップ 4	仮想コンテンツ セキュリティ アプライアンスイメージをダウンロードします。	Cisco コンテンツ セキュリティ仮想アプライアンスのイメージのダウンロード（15 ページ）を参照してください。
ステップ 5	シスコのイメージがこの導入と互換性があることを確認します。	KVM の導入と仮想アプライアンスイメージの互換性の確認（20 ページ）を参照してください
ステップ 6	（オプション）起動時に自動的にロードするライセンスおよびコンフィギュレーション ファイルが含まれる ISO ファイルを用意します。	起動時にロードするライセンスおよびコンフィギュレーション ファイルの準備（KVM の導入）（16 ページ）を参照してください。
ステップ 7	RAM の容量とお使いの仮想アプライアンスモデルに割り当てる CPU コアの数を決定します。	3 ページを参照してください。
ステップ 8	仮想コンテンツ セキュリティ アプライアンスイメージを展開します。	次のいずれかの方法を使用します。 • Virtual Machine Manager を使用した仮想アプライアンスの導入（20 ページ） • virt-install を使用した仮想アプライアンスの導入：例（21 ページ）
ステップ 9	Cisco Web セキュリティ アプライアンスの AsyncOS 8.5 で導入された高可用性機能を展開する場合は、ホストを設定してこの機能をサポートします。	（オプション）高可用性をサポートする仮想インターフェイスの構成（22 ページ）を参照してください。

	操作	詳細情報
ステップ 10	最初の起動時にライセンスとコンフィギュレーション ファイルをロードするようにシステムを設定していなかった場合は、次の操作を実行します。 • 仮想アプライアンスのライセンス ファイルをインストールする • 機能ライセンスをインストールする • Cisco コンテンツ セキュリティ仮想アプライアンスを構成する	• 仮想アプライアンスのライセンス ファイルをインストールするには、Amazon Web Services（AWS）EC2/VPC の導入（27 ページ）を参照してください。 • 機能ライセンスをインストールしてアプライアンスを構成するには、お使いの AsyncOS リリースのユーザガイドまたはオンラインヘルプを参照してください。
ステップ 11	ライセンスの有効期限に近い場合は、アプライアンスを構成してアラートを送信します。	オンラインヘルプまたはご使用の AsyncOS リリースのユーザガイドを参照してください。

KVM の導入と仮想アプライアンスイメージの互換性の確認

シスコのイメージの qcow バージョンは、1.1 よりも低い QEMU バージョンとの互換性がありません。QEMU バージョンが 1.1 よりも低い場合は、イメージを変換して導入との互換性を持たせる必要があります。

Virtual Machine Manager を使用した仮想アプライアンスの導入

ステップ 1 virt-manager アプリケーションを起動します。

ステップ 2 [新規（New）] を選択します。

ステップ 3 仮想アプライアンスに付ける一意の名前を入力します。

ステップ 4 [既存のイメージをインポート（Import existing image）] を選択します。

ステップ 5 [転送（Forward）] を選択します。

ステップ 6 オプションを次のように入力します。

- OS タイプ：**UNIX**
- バージョン：**FreeBSD 13**

ステップ 7 ダウンロードする仮想アプライアンスイメージを参照し、選択します。

ステップ 8 [転送（Forward）] を選択します。

ステップ 9 導入する仮想アプライアンスモデルの RAM および CPU の値を入力します。

3 ページを参照してください。

ステップ 10 [転送（Forward）] を選択します。

ステップ 11 [カスタマイズ（Customize）] チェックボックスをオンにします。

ステップ 12 [完了（Finish）] を選択します。

ステップ 13 ディスク ドライブを次のように構成します。

a. 左ペインで、ドライブを選択します。

b. [詳細設定(Advanced)] オプションで、次のオプションを選択します。

- ディスクバス:**Virtio**
- ストレージ形式:qcow2

c. [適用(Apply)] を選択します。

ステップ 14 管理インターフェイスのネットワーク デバイスを構成します。

a. 左ペインで、[NIC] を選択します。

b. 次のオプションを選択します。

- 送信元デバイス:お使いの管理 VLAN
- デバイス モデル:virtIO
- 送信元モード:VEPA

c. [適用(Apply)] を選択します。

ステップ 15 4 つの追加インターフェイスのネットワークデバイスを構成します。

使用する各インターフェイスで、以前のサブステップのセットを繰り返します。

ステップ 16 起動時にロードされるライセンスおよびコンフィギュレーション ファイルを使用して ISO イメージを用意した場合は、

仮想マシン インスタンスに仮想 CD-ROM ドライブとして ISO イメージを接続します。

ステップ 17 [インストールを開始(Begin Installation)] をクリックします。

関連項目

- KVM での導入(19 ページ)

virt-install を使用した仮想アプライアンスの導入:例

はじめる前に

RAM の容量と、アプライアンスに必要な CPU コアの数を決定します。3 ページを参照してください。

手順

ステップ 1 仮想アプライアンスに配置するストレージプールを作成します。

```
virsh pool-define-as --name vm-pool --type dir --target /home/username/vm-pool
virsh pool-start vm-pool
```

ステップ 2 ストレージプールに仮想アプライアンスイメージをコピーします。

```
cd /home/yusername/vm-pool
tar xvf ~/asyncos-8-6-0-007-S100V.qcow2.tar.gz
```

ステップ 3 仮想アプライアンスをインストールします。

```
virt-install \
--virt-type kvm \
--os-type=unix \
--os-variant=freebsd13 \
--name test-dut \(この名前は一意でなければなりません)
--ram 8192 \(お使いの仮想アプライアンスモデルに適切な値を使用します)
--vcpus 2 \(お使いの仮想アプライアンスモデルに適切な値を使用します)
--noreboot \
--import \
--disk
path=/home/username/vm-pool/asyncos-8-6-0-007-S100V.qcow2,format=qcow2,bus=virtio \
--disk path=/home/username/vm-pool/wsa.iso,bus=ide,device=cdrom \(起動時にロードするライセンスおよびコンフィギュレーション ファイルを使用して ISO を作成した場合)
--network type=direct,source=enp6s0.483,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.484,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.485,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.486,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.487,source_mode=vepa,model=virtio \
```

ステップ 4 仮想アプライアンスの再起動:

```
virsh start test-dut
virsh --connect qemu:///system start test-dut
```

ステップ 5 仮想アプライアンスの開始/停止:

```
--virsh shutdown test-dut
--virsh start test-dut
```

関連項目

- KVM での導入(19 ページ)

(オプション)高可用性をサポートする仮想インターフェイスの構成

高可用性機能は Cisco Web セキュリティ アプライアンスの AsyncOS 8.5 で導入されました。詳細については、ユーザガイドおよびオンラインヘルプに記載されています。

お使いの Cisco Secure Web Appliance が高可用性のフェールオーバー グループに追加される場合は、仮想インターフェイスを構成して無差別モードを使用します。これにより、フェールオーバー グループ内のアプライアンスがマルチキャストを使用して相互に通信できるようになります。

これは、いつでも変更することができます。

ステップ 1 ホスト OS で、マルチキャスト トラフィックが関連付けられるインターフェイスに関連する `macvtap` インターフェイスを検索します。

ステップ 2 `macvtap` インターフェイスを設定し、無差別モードを使用します。

```
Enter on the host: ifconfig macvtapX promisc
```

関連項目

- KVM での導入（19 ページ）

VMWare ESXi での導入

	操作	詳細情報
1.	ご使用の AsyncOS リリースのリリースノートを確認します。	リリースノートは、その他の情報（38 ページ）から入手できます。
2.	シスコから仮想アプライアンスのイメージと MD5 ハッシュをダウンロードします。	MD5 ハッシュでアプライアンスイメージのデータ整合性を確認する必要があります。 Content Secure イメージとファイルの準備（15 ページ）。
3.	ESXi ホストまたはクラスタ上に仮想アプライアンスを配置します。	仮想アプライアンスの導入（25 ページ）。
4.	（オプション）ネットワークで複数の仮想アプライアンスを実行する場合は、イメージのクローンを作成します。	Cisco Web セキュリティアプライアンスの AsyncOS 8.5 で導入された高可用性機能を展開する場合は、ホストを設定してこの機能をサポートします。詳細については、（オプション）高可用性をサポートする仮想インターフェイスの構成（24 ページ）を参照してください。（24 ページ）。
5.	断続的な接続の問題を防止します。	仮想マシンでの未使用のネットワーク インターフェイス カード（NIC）の無効化。
6.	Cisco コンテンツ セキュリティ仮想アプライアンスでランダム故障を避けるために仮想マシンの同期を設定します。	重要：ランダム故障の防止（26 ページ）
7.	DHCP が無効の場合は、ネットワーク上にアプライアンスをセットアップします。	DHCP が無効の場合のネットワーク上でのアプライアンスの設定（VMware vSphere）（27 ページ）
8.	ライセンスファイルをインストールします。	仮想アプライアンスのライセンスファイルのインストール（28 ページ）。

	操作	詳細情報
9.	アプライアンスの Web UI にログインし、物理アプライアンスの場合と同様にアプライアンスソフトウェアを設定します。 たとえば、以下を行うことができます。 • System Setup ウィザードの実行 • コンフィギュレーション ファイルのアップロード • 手動による機能の設定	• アプライアンスのアクセスと設定の手順の詳細については(必要な情報の収集を含む)、その他の情報(38 ページ)の関連する場所から入手可能なオンラインヘルプ、またはお使いの AsyncOS リリースのユーザガイドを参照してください。 • 物理アプライアンスから設定を移行するには、お使いの AsyncOS リリースのリリースノートを参照してください。 機能キーはそれぞれの機能を有効にするまでアクティブ化されません。
10.	ライセンスの有効期限に近い場合は、アプライアンスを構成してアラートを送信します。	その他の情報(38 ページ)の関連する場所から入手可能なオンラインヘルプ、またはお使いの AsyncOS リリースのユーザガイドを参照してください。

Cisco Web セキュリティアプライアンスの AsyncOS 8.5 で導入された高可用性機能を展開する場合は、ホストを設定してこの機能をサポートします。詳細については、(オプション)高可用性をサポートする仮想インターフェイスの構成(24 ページ)を参照してください。

(オプション)高可用性をサポートする仮想インターフェイスの構成

高可用性機能は Cisco Web セキュリティ アプライアンスの AsyncOS 8.5 で導入されました。詳細については、ユーザガイドおよびオンラインヘルプに記載されています。

お使いの Cisco Secure Web Appliance が高可用性のフェールオーバー グループに追加される場合は、仮想インターフェイスを構成して無差別モードを使用します。これにより、フェールオーバー グループ内のアプライアンスがマルチキャストを使用して相互に通信できるようになります。

これは、いつでも変更することができます。

アプライアンスの仮想インターフェイスに関連付けられた **VLAN ポートグループ/分散ポートグループ**について、[無差別モード(Promiscuous mode)] を [承諾(Accept)] 状態に設定します。

(オプション)仮想アプライアンスのクローン作成

環境内で複数の仮想セキュリティアプライアンスを実行する場合は、次の手順に従います。

- シスコは、仮想セキュリティアプライアンスを初めて実行する前に、そのアプライアンスのクローンを作成することを推奨します。
- 仮想アプライアンスのライセンスが強制的にインストールされた後に仮想セキュリティアプライアンスのクローンを作成するとライセンスが失効します。ライセンスを再インストールする必要があります。
- クローンを作成する前に仮想アプライアンスをシャットダウンする必要があります。
- すでに使用されている仮想アプライアンスのクローンを作成する場合は、詳細について、すでに使用中の仮想アプライアンスのクローン作成(29 ページ)を参照してください。

仮想マシンのクローンを作成する手順の詳細については、http://www.vmware.com/support/ws55/doc/ws_clone.html [英語] にある VMware の技術文書を参照してください。

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）

仮想アプライアンスの導入

はじめる前に

- 仮想アプライアンスを導入する ESXi ホストまたはクラスタを設定します。詳細については、システム要件（10 ページ）を参照してください。
- ローカルマシンに VMware vSphere クライアントをインストールします。
- Content Secure イメージとファイルの準備（15 ページ）に示すように、イメージをダウンロードします。

ステップ 1 固有のディレクトリで仮想アプライアンスの .zip ファイルを解凍します（例：`C:\vESA\C100V` または `:\vWSA\S300V`）。

ステップ 2 ローカルマシンの VMware vSphere クライアントを開きます。

ステップ 3 仮想アプライアンスを配置する ESXi ホストまたはクラスタを選択します。

ステップ 4 [ファイル（File）] > [OVF テンプレートを導入（Deploy OVF Template）] を選択します。

ステップ 5 作成したディレクトリ内の OVF ファイルへのパスを入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 ウィザードを完了します。

- ディスクストレージのシンプロビジョニングは、ハイパーバイザ層でサポートされています。このオプションを選択すると、ディスク容量を消費し、パフォーマンスが低下する可能性があります。

（注） **AsyncOS ドキュメントで明示的に記載されている場合を除き、OVF で定義された ESXi 構成に対する変更はサポートされていません。**

（注） 仮想アプライアンスのバックアップ（スナップショット）を作成するために、またはスナップショットから仮想アプライアンスを復元するために、VMware などのサードパーティ製ツールを使用しないでください。代わりにユーザインターフェイスの [システム管理（System Administration）] > [設定ファイル（Configuration File）] メニューを使用するか、CLI コマンド `saveconfig` を使用して、設定のバックアップを作成できます。バックアップした設定は生成された別の仮想アプライアンスにロードできます。

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）

重要：ランダム故障の防止

注意 シスコテクニカルサポートから指示された場合を除き、仮想アプライアンスをシャットダウンまたは再起動するために vSphere クライアントまたは Web クライアントを使用しないでください。CLI から shutdown コマンドまたは reboot コマンドを使用するか、アプライアンス GUI の [システム管理（System Administration）] タブにある [シャットダウン/再起動（Shutdown/Reboot）] オプションを使用することをお推めします。アプライアンスの電源を再投入する（または仮想インフラストラクチャへの停電が発生する）と、メッセージの消失、データベースの破損、ログデータの損失が発生する可能性があります。ファイルシステムのマウント解除に失敗すると、ファイルシステムが破損するため、システムが破損状態になります。

Cisco コンテンツ セキュリティ仮想アプライアンスでのランダムな故障を回避するために、仮想マシン固有のタイミングの特異性に対処する必要があります。これらの問題を回避するには、仮想マシンで正確なタイムスタンプカウンタの同期を有効にします。

はじめる前に

- 計時の基礎、仮想タイムスタンプカウンタ、および正確な同期の詳細については、http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf [英語] にある VMWare の『Timekeeping in Virtual Machines PDF』を参照してください。
- ご使用のバージョンの vSphere クライアントの手順は、次の手順とは異なる場合があります。これを汎用ガイドとして使用し、必要に応じてご使用のクライアントのマニュアルを参照してください。

ステップ 1 vSphere Client で、マシンのリストから仮想アプライアンスを選択します。

ステップ 2 CLI にログインして `shutdown` コマンドを入力し、仮想アプライアンスの電源をオフにします。

ステップ 3 アプライアンスを右クリックし、[設定を編集（Edit Settings）] を選択します。

ステップ 4 [オプション（Options）] タブをクリックし、[詳細設定（Advanced）] > [全般（General）] を選択します。

ステップ 5 [設定パラメータ（Configuration Parameters）] をクリックします。

ステップ 6 次のパラメータを編集または追加します。

```
monitor_control.disable_tsc_offsetting=TRUE
monitor_control.disable_rdtscopt_bt=TRUE
timeTracker.forceMonotonicTTAT=TRUE
```

ステップ 7 設定ウィンドウを閉じ、アプライアンスを実行します。

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）

DHCP が無効の場合のネットワーク上でのアプライアンスの設定（VMware vSphere）

（注） 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

ステップ 1 vSphere クライアントコンソールから、`interfaceconfig` を実行します。

ステップ 2 仮想アプライアンス管理ポートの IP アドレスを書き留めます。

（注） 管理ポートは DHCP サーバから IP アドレスを取得します。アプライアンスが DHCP サーバにアクセスできない場合は、デフォルトで `192.168.42.42` が使用されます。

ステップ 3 `setgateway` コマンドを使用して、デフォルトゲートウェイを設定します。

ステップ 4 変更を確定します。

（注） ホスト名は、セットアップウィザードが完了するまで更新されません。

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）

Microsoft Azure の展開

Microsoft Azure の展開については、『Microsoft Azure クラウドプットフォームへの Cisco Secure Email Virtual Gateway および Cisco Secure Email and Web Manager Virtual の展開』ガイドを参照してください。

Amazon Web Services（AWS）EC2/VPC の導入

Amazon Web Services（AWS）EC2 の展開については、『Amazon Web Services の Amazon Elastic Compute Cloud に Cisco Secure Email ゲートウェイ、Secure Web、および Cisco Secure Email and Web Manager 仮想アプライアンスを展開する』ガイドを参照してください。

仮想アプライアンスのライセンスファイルのインストール

（注） 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

はじめる前に

（任意）ライセンスファイルをアップロードする仮想アプライアンスへの FTP 接続を実行します。端末にライセンスを貼り付ける場合は、この作業を行う必要はありません。

手順

ステップ 1 端末アプリケーションの SSH または Telnet を使用して、admin/ironport ユーザとしてアプライアンスの CLI にログインします。

（注） vSphere クライアントコンソールを使用して CLI にライセンスファイルの内容を貼り付けることはできません。

ステップ 2 `loadlicense` コマンドを実行します。

ステップ 3 次のいずれかのオプションを使用してライセンスファイルをインストールします。

- オプション 1 を選択して、端末にライセンスファイルの内容を貼り付けます。
- すでに FTP を使用してライセンスファイルをアプライアンスの `configuration` ディレクトリにアップロードした場合は、オプション 2 を選択して、ライセンスファイルを `configuration` ディレクトリにロードします。

ステップ 4 ライセンス契約を読み、同意します。

ステップ 5 （任意）`showlicense` を実行して、ライセンスの詳細を見直します。

次の作業

Microsoft Hyper-V の導入の場合

- Microsoft Hyper-V への導入（17 ページ）に戻ります。

KVM の導入の場合

- KVM での導入（19 ページ）に戻ります。

ESXi の導入の場合

- 管理インターフェイスの IP アドレスの詳細については、VMWare ESXi での導入（23 ページ）を参照してください。
- 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとにこのトピックの手順を繰り返します。
- 残りのセットアップ手順については、VMWare ESXi での導入（23 ページ）を参照してください。

別の物理ホストへの仮想アプライアンスの移行

VMware® VMotion™ を使用して、実行中の仮想アプライアンスを別の物理ホストに移行できます。

要件:

- 両方の物理ホストのネットワーク構成が同じである必要があります。
- 両方の物理ホストに、仮想アプライアンスのインターフェイスがマップされているものと同じ定義済みのネットワークへのアクセス権がなければなりません。
- 両方の物理ホストに、仮想アプライアンスで使用するデータストアへのアクセス権がなければなりません。このデータストアには、ストレージ エリア ネットワーク（SAN）またはネットワーク接続ストレージ（NAS）が有効です。
- Cisco Secure Email Virtual Gateway のキューにはメールが含まれていない必要があります。

（注） VMotion のマニュアルを参考にして、仮想マシンを移行します。現在、自動 VMotion は Secure Web Appliance ではサポートされていません。

すでに使用中の仮想アプライアンスのクローン作成

はじめる前に

- 仮想マシンのクローンを作成する手順の詳細については、http://www.vmware.com/support/ws55/doc/ws_clone.html [英語] にある VMware の技術文書を参照してください。
- ご使用のアプライアンスのネットワーク設定およびセキュリティ機能の管理方法については、Cisco Secure 製品およびリリースのユーザーガイドを参照してください。

ステップ 1 Cisco Secure Email Virtual Gateway のクローンを作成する場合:
CLI で `suspend` コマンドを使用してアプライアンスを一時停止し、アプライアンスがキュー内のすべてのメッセージを配信するのに十分な遅延期間を入力します。

ステップ 2 セキュリティ管理仮想アプライアンスのクローンを作成する場合:
管理対象となる E メールおよび Web セキュリティアプライアンスの集約管理サービスを無効にします。

ステップ 3 CLI で `shutdown` コマンドを実行して、仮想アプライアンスをシャットダウンします。

ステップ 4 仮想アプライアンスイメージのクローンを作成します。

ステップ 5 VMware vSphere Client を使用してクローンを作成したアプライアンスを起動し、次を実行します。

a. Cisco.com からダウンロードした未変更の .OVF イメージファイルではなく、構成済みのイメージのクローンを作成した場合:

- クローン作成された仮想アプライアンスにライセンスファイルをインストールします。
- クローン作成された仮想アプライアンスのネットワーク設定を変更します。

電源投入時に、ネットワーク アダプタは自動的に接続しません。IP アドレス、ホスト名、および IP アドレスを再設定します。次に、ネットワークアダプタの電源を入れます。

設定は、機能キーをインストールするまで完了しません。

b. クローン作成された Cisco Secure Email Virtual Gateway アプライアンスの場合:
   - 隔離されたすべてのメッセージを削除します。
   - メッセージトラッキングおよびレポーティングのデータを削除します。

c. クローン作成された Web セキュリティ仮想アプライアンスの場合:
   - プロキシキャッシュを消去します。
   - CLI で `authcache` > `flushall` コマンドを使用してプロキシ認証キャッシュを消去します。
   - CLI で `diagnostic` > `reporting` > `flushall` > `deletedb` コマンドを使用して、レポーティングおよびトラッキングのデータを削除します。
   - システム セットアップ ウィザード(SSW)を実行します。ライセンスが使用可能になっている必要があります。
   - 認証領域の場合は、ドメインに再参加します。
   - 認証の設定の場合は、リダイレクトホスト名を変更します。
   - 元の仮想アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、クローン作成されたアプライアンスをセキュリティ管理アプライアンスに追加します。

ステップ 6 VMware vSphere クライアントを使用して元の仮想アプライアンスを起動して、動作を再開します。正常に動作していることを確認します。

ステップ 7 クローン作成されたアプライアンスで動作を再開します。

Cisco Secure 仮想アプライアンスの管理

IP アドレス

仮想アプライアンスに最初に電源を入れると、管理ポートは DHCP ホストから IP アドレスを取得します。仮想アプライアンスが DHCP サーバから IP アドレスを取得できない場合は、管理インターフェイスの IP アドレスとして `192.168.42.42` が使用されます。仮想アプライアンスで [システム設定(System Setup)] ウィザードを実行すると、CLI によって管理インターフェイスの IP アドレスが表示されます。

仮想アプライアンスのライセンス

(注) 仮想アプライアンスのライセンスをインストールする前に、テクニカルサポートのトンネルを開くことはできません。テクニカルサポートのトンネルに関する情報は、AsyncOS リリースのユーザガイドにあります。

Cisco Secure 仮想アプライアンスには、ホスト上で仮想アプライアンスを実行するための追加ライセンスが必要です。このライセンスは複数のクローン作成された仮想アプライアンスに使用できます。ライセンスは、ハイパーバイザに依存しません。

Web セキュリティ 8.5 以降の AsyncOS、E メール セキュリティ 8.5.x 以降の AsyncOS、およびセキュリティ管理 8.4 以降の AsyncOS の場合:

- 個々の機能の機能キーごとに有効期限が異なる可能性があります。
- 仮想アプライアンスのライセンスの有効期限が切れた後も、180 日間のセキュリティサービスを使用せずにアプライアンスは引き続き Web プロキシ(Web セキュリティ アプライアンス)として機能し、電子メールを配信し(E メール セキュリティ アプライアンス)、または隔離済みメッセージを自動的に処理(セキュリティ管理アプライアンス)します。この期間中、セキュリティサービスは更新されません。Cisco Secure Email and Web Manager アプライアンス では、管理者とエンド ユーザが隔離を管理することはできませんが、管理対象アプライアンスでは引き続き管理対象 Cisco Secure Email Gateway アプライアンス からの隔離済みメッセージを受け入れ、スケジュールされた隔離済みメッセージの削除が実行されます。

E メール セキュリティ 8.0 の AsyncOS および Web セキュリティ 7.7.5 と 8.0 の AsyncOS の場合:

- 機能キーは仮想アプライアンスのライセンスに含まれています。機能キーは、該当の機能がアクティブ化されてない場合でも、ライセンスと同時に失効します。新しい機能キーを購入する場合は、新しい仮想アプライアンスのライセンス ファイルをダウンロードしてインストールする必要があります。
- 機能キーが仮想アプライアンスのライセンスに含まれているため、AsyncOS 機能の評価ライセンスはありません。

(注) AsyncOS バージョンを復帰させた場合の影響については、ご使用の AsyncOS のリリースのオンラインヘルプまたはユーザガイドを参照してください。

関連項目

- 仮想アプライアンスのライセンスファイルのインストール(28 ページ)

強制リセット、電源オフ、およびリセットの各オプションが完全にサポートされていない

以下の操作は、ハードウェア アプライアンスのプラグを抜くことと同等であり、特に AsyncOS の起動中ではサポートされていません。

- KVM の強制リセットオプション
- VMWare の [電源オフ(Power Off)] と [リセット(Reset)] オプション

仮想アプライアンスの CLI コマンド

Cisco Secure 仮想アプライアンスには既存の CLI コマンドに対する更新、および仮想アプライアンス専用のコマンドである `loadlicense` が含まれています。次の CLI コマンドが変更されています。

コマンド	仮想 SMA でのサポートの有無	情報
loadlicense	対応	このコマンドを使うと、仮想アプライアンスにライセンスをインストールすることができます。最初にこのコマンドを使用してライセンスをインストールしないと、仮想アプライアンスの System Setup ウィザードは実行できません。
etherconfig	—	仮想アプライアンスにペアリングのオプションは含まれていません。
version	—	このコマンドは、UDI、RAID および BMC 情報を除き、仮想アプライアンスに関するすべての情報を返します。
resetconfig	—	このコマンドを実行すると、アプライアンス上に仮想アプライアンス ライセンスおよび機能キーが残ります。
revert	—	AsyncOS 8.5 for Email Security からは、ご使用のアプライアンスのオンラインヘルプおよびユーザガイドのシステム管理の章で動作が説明されています。
reload	—	このコマンドを実行すると、アプライアンスで仮想アプライアンス ライセンスおよびすべての機能キーが削除されます。このコマンドは、Web セキュリティ アプライアンスでのみ使用可能です。
diagnostic	—	次の `diagnostic` > `raid` のサブメニューオプションでは、情報は返されません。 1. `Run disk verify` 2. `実行中のタスクのモニタ` 3. `Display disk verify verdict` このコマンドは、E メール セキュリティ アプライアンスでのみ使用可能です。
showlicense	対応	ライセンスの詳細を表示します。 仮想 E メールおよび Web セキュリティ アプライアンスでは、`featurekey` コマンドを使用して追加情報を入手できます。

仮想アプライアンスの SNMP

仮想アプライアンスの AsyncOS はハードウェア関連の情報については報告せず、ハードウェア関連のトラップは生成されません。次の情報は、クエリーから除外されます。

- `powerSupplyTable`
- `temperatureTable`
- `fanTable`
- `raidEvents`
- `raidTable`

トラブルシューティングとサポート

トラブルシューティング：KVM の導入

再起動時の仮想アプライアンスの停止

問題 仮想アプライアンスは、再起動すると停止します。

ソリューション これは KVM の問題です。ホストを再起動するたびに、次の回避策を実行してください。

ステップ 1 次の点をチェックします。

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

ステップ 2 上記の値が Y に設定されている場合：

a. 仮想アプライアンスを停止し、KVM カーネルモジュールを再インストールします。

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b. 仮想アプライアンスを再起動します。

詳細については、https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html [英語] および https://bugs.launchpad.net/qemu/+bug/1329956 [英語] を参照してください。

ネットワーク接続が最初に成功した後で失敗する

問題 前回の作業後にネットワーク接続が失われる。

ソリューション これは KVM の問題です。OpenStack ドキュメントの「KVM: Network connectivity works initially, then fails」の項を参照してください。このドキュメントは、http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html [英語] にあります。

パフォーマンスの低下、ウォッチドッグ問題、および高 CPU 使用率

問題 Red Hat™ Enterprise Linux 上で KVM を使用して仮想アプライアンスを実行しているときに、アプライアンスのパフォーマンスが低下して、ウォッチドッグの問題が発生し、アプライアンスが異常に高い CPU 使用率を示す。

ソリューション Red Hat™ Enterprise Linux から最新の Host OS アップデートをインストールしてください。

トラブルシューティング：VMWare ESXi の導入

断続的な接続の問題

問題 断続的な接続の問題。

ソリューション 未使用のすべての NIC が ESXi で無効になっていることを確認します。

ランダム故障

問題 原因が明らかでないランダムな故障が発生します。

ソリューション 重要：ランダム故障の防止（26 ページ）を参照してください。

仮想アプライアンスのサポートの取得

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco Secure 仮想アプライアンスのサポートケースを報告する場合は、契約番号と製品 ID コード（PID）を提供する必要があります。

発注書を参照するか以下の一覧を参照すると、仮想アプライアンスで動作中のソフトウェアライセンスに基づく PID を特定できます。

- Cisco Secure Email Virtual Gateway アプライアンスの製品 ID コード（PID）（34 ページ）
- Cisco Secure Web 仮想プライアンスの製品 ID コード（PID）（36 ページ）
- Cisco Secure Email and Web Manager Virtual の製品 ID コード（PID）（37 ページ）

Cisco Secure Email Virtual Gateway アプライアンスの製品 ID コード（PID）

Cisco Secure Email Unified SKU の概要

Cisco Secure Email Unified SKU の注文には、次の 4 つの SKU タイプが含まれます。

- サブスクリプション SKU は、サブスクリプション期間と開始日を定義するために使用されます。
- 製品 SKU は、サブスクリプションを構成する製品と数量を定義するために使用されます。
- 製品アドオン SKU は、他の製品 SKU にのみ追加できます。
- サポート SKU では、サブスクリプションのサポートレベルを定義します。

注文は、E メール セキュリティ サブスクリプション SKU の選択から始まります。次にサブスクリプションを構成する製品 SKU、アドオン SKU、サポート SKU を選択してサブスクリプションを設定します。

サブスクリプション SKU

Email Security-CSEMAIL-SEC-SUB のサブスクリプション SKU は 1 つだけです。サブスクリプションの期間と支払いオプションは、サブスクリプションに含まれるすべての製品に適用されます。

機能	PID	説明
Cisco Secure Email Gateway Essentials	ESA-ESS-LIC	内容: • スパム対策 • ウイルス対策 • アウトブレイク フィルタ • Cisco Secure Malware Defense（AMP）制限サンプル
Cisco Secure Email Gateway Advantage	ESA-ADV-LIC	内容: • スパム対策 • ウイルス対策 • アウトブレイク フィルタ • Cisco Secure Malware Defense（AMP）無制限サンプル • Graymail Safe の登録解除 • データ損失防止 • 暗号化
Cisco Secure Email Gateway Premier	ESA-PRE-LIC	内容: • スパム対策 • ウイルス対策 • アウトブレイク フィルタ • Cisco Secure Malware Defense（AMP）無制限サンプル • Graymail Safe の登録解除 • データ損失防止 • 暗号化 • Cisco Secure Awareness トレーニング
Cisco Secure Email and Web Manager アプライアンス（SMA）	SMA-EMGT-LIC	すべての中央集中型電子メールセキュリティ機能
イメージアナライザ	ESA-IA-LIC	アドオンとして利用可能
インテリジェント マルチスキャン	ESA-IMS-LIC	アドオンとして利用可能
McAfee Anti-Malware	ESA-MFE-LIC	アドオンとして利用可能

機能	PID	説明
Graymail Safe の登録解除	ESA-GSU-LIC	アドオンとして利用可能（Advantage および Premier バンドルの一部）
データ損失防止	ESA-DLP-LIC	アドオンとして利用可能（Advantage および Premier バンドルの一部）
暗号化	ESA-ENC-LIC	アドオンとして利用可能（Advantage および Premier バンドルの一部）

Cisco Secure Web 仮想プライアンスの製品 ID コード（PID）

Cisco Secure Web Appliance Unified SKU の概要

Cisco Secure Web Appliance Unified SKU の注文には、次の 4 つの SKU タイプが含まれます。

- サブスクリプション SKU は、サブスクリプション期間と開始日を定義するために使用されます。
- 製品 SKU は、サブスクリプションを構成する製品と数量を定義するために使用されます。
- 製品アドオン SKU は、他の製品 SKU にのみ追加できます。
- サポート SKU では、サブスクリプションのサポートレベルを定義します。

注文は、Cisco Secure Web Appliance サブスクリプション SKU の選択から始まります。次にサブスクリプションを構成する製品 SKU、アドオン SKU、サポート SKU を選択してサブスクリプションを設定します。

サブスクリプション SKU

Cisco Secure Web Appliance のサブスクリプション SKU は 1 つだけです（WEB-SEC-SUB）。サブスクリプションの期間と支払いオプションは、サブスクリプションに含まれるすべての製品に適用されます。

機能	PID	説明
Cisco Secure Web Essentials	WSA-WSE-LIC	内容: • Web Usage Controls • Web レピュテーション
Cisco Secure Web Advantage	WSA-WSP-LIC	内容: • Web Usage Controls • Web レピュテーション • Sophos および Webroot Anti-Malware シグネチャ

機能	PID	説明
Cisco Secure Web Premier	WSA-WSS-LIC	内容: • Web Usage Controls • Web レピュテーション • Sophos および Webroot Anti-Malware シグネチャ • Cisco Secure Malware Analytics • Cisco Cognitive Intelligence
Cisco Secure Malware Analytics	WSA-AMP-LIC	内容: • Cisco Secure Malware Analytics
Cisco Secure Web Anti-Virus McAfee	WSA-AMM-LIC	内容: • McAfee Anti-Malware シグネチャ
Cisco Secure Web Sophos Anti-Malware	WSA-AMS-LIC	内容: • Sophos Anti-Malware シグネチャ
Cisco Secure Web Webroot Anti-Malware	WSA-AMW-LIC	内容: • Webroot Anti-Malware シグネチャ

Cisco Secure Email and Web Manager Virtual の製品 ID コード（PID）

機能	PID	説明
Cisco Secure Email and Web Manager アプライアンス（SMA）	SMA-EMGT-LIC	すべての中央集中型電子メールセキュリティ機能

Cisco TAC

Cisco TAC の連絡先情報（電話番号を含む）:
https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

その他の情報

サポートオプションに関する情報などの詳細については、ご使用の AsyncOS リリースのリリースノートとユーザガイドまたはオンラインヘルプを参照してください。

Cisco Content Security 製品のマニュアル:	入手場所
Content Cisco Secure Email and Web Manager アプライアンス	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliances	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email Gateway アプライアンス	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html

関連項目

- Microsoft Hyper-V への導入（17 ページ）
- KVM での導入（19 ページ）
- VMWare ESXi での導入（23 ページ）
