



Nutanix 上で ASAav を展開する

この章では、ASAav を Nutanix 環境に展開する手順について説明します。

- [Nutanix で ASAav を使い始める \(1 ページ\)](#)
- [Nutanix に ASAav を展開する方法 \(5 ページ\)](#)

Nutanix で ASAav を使い始める

Cisco 適応型セキュリティ仮想アプライアンス (ASAav) は、仮想化環境に包括的なファイアウォール機能を提供し、データセンタートラフィックとマルチテナント環境のセキュリティを強化します。

Nutanix 上で ASAav を展開します。

Nutanix での ASAav のガイドラインと制限



重要 ASAav は、8GB のディスクストレージサイズで展開されます。ディスク容量のリソース割り当てを変更することはできません。

ASAav を展開する前に、次のガイドラインと制限事項を確認します。

推奨される vNIC

最適なパフォーマンスを得るには、次の vNIC をお勧めします。

VirtIO : 10 Gbps の動作をサポートしますが、CPU サイクルも必要な準仮想化ネットワークドライバです。

CPU ピニング

Nutanix 環境で ASAav を機能させるには、CPU ピニングが必要です。「[CPU ピンニングの有効化](#)」を参照します。

ハイ アベイラビリティのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じライセンス権限付与を備えていることを確認してください（たとえば、両方の装置が 2 Gbps の権限付与であることなど）。



重要 ハイアベイラビリティペアを作成するときは、同じ順序で各 ASAv にデータインターフェイスを追加する必要があります。完全に同じインターフェイスが各 ASAv に追加されているが、順序が異なる場合、ASAv コンソールにエラーが表示され、フェールオーバー機能に影響を与える可能性があります。

一般的な注意事項

- サポートされるインターフェイスの最大数は 10 です。10 を超える数のインターフェイスを追加しようとすると、エラーメッセージが表示されます。



- (注)
- デフォルトでは、ASAv は同じサブネット上に管理インターフェイスと内部インターフェイスを設定します。
 - ネットワーク インターフェイスを変更するときは、ASAv デバイスをオフにする必要があります。
-
- デフォルトでは、ASAv は、異なるサブネット上に管理インターフェイスと内部インターフェイスの両方を設定したことを前提としています。管理インターフェイスには「IP address DHCP setroute」があり、デフォルトゲートウェイは DHCP によって提供されます。
 - ASAv は、3 つ以上のインターフェイスを使用して最初の起動時にパワーアップする必要があります。システムは、3 つのインターフェイスなしでは展開されません。
 - ASAv は、データトラフィック用に 1 つの管理インターフェイス (nic0) と最大 9 つのネットワーク インターフェイス (nic1-9) の合計 10 のインターフェイスをサポートします。データトラフィックのネットワークインターフェイスは、任意の順序に従うことができます。



- (注)
- ASAv のネットワーク インターフェイスの最小数は、3 つのデータインターフェイスです。
-
- コンソールアクセスの場合、ターミナルサーバーは telnet を介してサポートされます。
 - サポートされている vCPU とメモリのパラメータは次のとおりです。

| CPU | メモリ | ASAv プラットフォームのサイズ | ライセンスのタイプ |
|-----|-------|--------------------|---------------|
| 1 | 2 GB | 1vCPU/2 GB (デフォルト) | 1G (ASAv10) |
| 4 | 8 GB | 4 vCPU/8 GB | 2G (ASAv30) |
| 8 | 16 GB | 8 vCPU/16 GB | 10G (ASAv50) |
| 16 | 32 GB | 16vCPU/32GB | 20G (ASAv100) |

サポートされる機能

- ルーテッドモード (デフォルト)
- トランスペアレント モード



(注) マルチノードクラスタのサービスチェーンは、トランスペアレントモードではサポートされていません。

インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークに関する以下の用語索引を参照してください。

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|------------|--------------------|---------------------|---------|
| vnic0 | Management0-0 | Management0/0 | 管理 |
| vnic1 | GigabitEthernet0-1 | GigabitEthernet 0/1 | Outside |
| vnic2 | GigabitEthernet0-2 | GigabitEthernet 0/2 | 内側 |
| vnic3-9 | データ | データ | データ |

Proxmox VE 上の ASAv

Proxmox Virtual Environment (VE) は、Nutanix 仮想マシンを管理できるオープンソースのサーバー仮想化プラットフォームです。Proxmox VE は、Web ベースの管理インターフェイスも提供します。

Proxmox VE に ASAv を導入する場合は、エミュレートされたシリアルポートを持つように VM を設定する必要があります。シリアルポートがないと、スタートアッププロセス中に ASAv がループ状態になります。すべての管理タスクは、Proxmox VE Web ベース管理インターフェイスを使用して実行できます。



- (注) Unix シェルまたは Windows Powershell に慣れている上級ユーザー向けに、Proxmox VE は仮想環境のすべてのコンポーネントを管理するコマンドラインインターフェイスを提供します。このコマンドラインインターフェイスには、インテリジェントなタブ補完機能と UNIX の man ページ形式の完全なドキュメントがあります。

ASAv を正しく開始するには、VM にシリアルデバイスを設定する必要があります。

1. メイン Management Center の左側のナビゲーションツリーで ASAv VM を選択します。
2. 仮想マシンの電源をオフにします。
3. **Hardware > Add > Network Device** を選択して、シリアルポートを追加します。
4. 仮想マシンの電源をオンにします。
5. Xterm.js を使用して ASAv VM にアクセスします。

ゲスト/サーバーで端末をセットアップしてアクティブ化する方法については、[Proxmox シリアル端末](#)のページを参照してください。

サポートされない機能

- Nutanix AHV 上の ASAv は、インターフェイスのホットプラグをサポートしていません。ASAv の電源がオンになっているときに、インターフェイスを追加または削除しないでください。
- Nutanix AHV は、Single Root I/O Virtualization (SR-IOV) または Data Plane Development Kit-Open vSwitch (DPDK-OVS) をサポートしていません。



- (注) Nutanix AHV は、VirtIO を使用したゲスト内 DPDK をサポートします。詳細については、[AHV での DPDK サポート](#)を参照してください。

関連資料

- [Nutanix Release Notes](#)
- [Nutanix Field Installation Guide](#)
- [Nutanix でのハードウェアのサポート](#)
- [Nutanix AHV での Virtio-Net Multi-Queue サポート](#)

ASAv と Nutanix のシステム要件

ASA のバージョン

9.16.2

ASAv メモリ、vCPU、およびディスクのサイジング

ASAv の導入に使用される特定のハードウェアは、導入されるインスタンスの数と使用要件によって異なります。ASAv の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

ASAv ライセンス

- ASAv CLI からセキュリティサービスのすべてのライセンス資格を設定します。
- ライセンスの管理方法の詳細については、『[Cisco ASA コンフィギュレーションガイド](#)』の「ASAv のスマート ソフトウェア ライセンシングの設定」を参照してください。

Nutanix のコンポーネントとバージョン

| コンポーネント | バージョン |
|----------------------------|----------------|
| Nutanix Acropolis OS (AOS) | 5.15.5 LTS 以降 |
| Nutanix クラスタチェック (NCC) | 4.0.0.1 |
| Nutanix AHV | 20201105.12 以降 |

Nutanix に ASAv を展開する方法

| ステップ | タスク | 詳細情報 |
|------|---|---|
| 1 | 前提条件を確認します。 | ASAv と Nutanix を展開するための前提条件 (6 ページ) |
| 2 | ASAv qcow2 ファイルを Nutanix 環境にアップロードします。 | QCOW2 ファイルを Nutanix にアップロード (6 ページ) |
| 3 | 仮想マシンの展開時に適用される初期構成データを使用して、第 0 日の構成ファイルを準備します。 | 第 0 日のコンフィギュレーションファイルの準備 (7 ページ) |
| 4 | Nutanix に ASAv を展開します。 | ASAv を Nutanix に展開する (9 ページ) |
| 5 | ASAv を起動します。 | ASAv の起動 (10 ページ) |

ASAv と Nutanix を展開するための前提条件

- Cisco.com から ASAv qcow2 ファイルをダウンロードし、Linux ホストに格納します。
<http://www.cisco.com/go/asa-software>



(注) Cisco.com のログインおよびシスコ サービス契約が必要です。

- ASA ソフトウェアおよび HyperFlex ハイパーバイザの互換性については、「[Cisco Asa Compatibility](#)」を参照してください。

QCOW2 ファイルを Nutanix にアップロード

ASAv を Nutanix 環境に展開するには、Prism Web コンソールで ASAv qcow2 ディスクファイルからイメージを作成する必要があります。

始める前に

Cisco.com から qcow2 ディスクファイルをダウンロードします：<https://software.cisco.com/download/navigator.html>)

-
- ステップ 1 Nutanix Prism Web コンソールにログインします。
- ステップ 2 歯車アイコンをクリックして [設定 (Settings)] ページを開きます。
- ステップ 3 左側のペインで [イメージの設定 (Image Configuration)] をクリックします。
- ステップ 4 [Upload Image] をクリックします。
- ステップ 5 イメージを作成します。
1. イメージの名前を入力します。
 2. [イメージタイプ (Image Type)] ドロップダウンリストから、[ディスク (DISK)] を選択します。
 3. [ストレージコンテナ (Storage Container)] ドロップダウンリストから、目的のコンテナを選択します。
 4. ASAv qcow2 ディスクファイルの場所を指定します。
URL を指定して Web サーバーからファイルをインポートすることも、ワークステーションからファイルをアップロードすることもできます。
 5. [保存 (Save)] をクリックします。
- ステップ 6 [イメージの設定 (Image Configuration)] ページに新しいイメージが表示されるまで待ちます。
-

第 0 日のコンフィギュレーション ファイルの準備

ASAv を展開する前に、第 0 日の構成ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキスト ファイルです。

第 0 日のコンフィギュレーション ファイルを使用して展開する場合、プロセスで、ASAv アプライアンスの初期設定全体を実行できます。

ファイルでは、以下を指定できます。

- システムのホスト名。
- 管理者アカウントの新しい管理者ユーザー名とパスワード。
- 最初のファイアウォール モード。最初のファイアウォール モード（ルーテッドまたはトランスパレント）を設定します。

ローカルを使用して展開を管理する予定の場合は、ファイアウォールモードにルーテッドのみ入力できます。ASAv デバイスマネージャを使用して透過ファイアウォールモードインターフェイスを設定することはできません。

- 有効にする ASDM :
 - **http server enable**
 - **access-group all global**
 - **http 0.0.0.0 0.0.0.0 management**
- アクセス リスト (Access List)
- Name-Server
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。



(注) 第 0 日の構成ファイルをアップロードするか、表示されたテキストボックスにコンテンツをコピーして貼り付けることができます。

ステップ 1 任意のテキストエディタを使用して、新しいテキストファイルを作成します。

ステップ 2 次の例に示すように、テキストファイルに構成の詳細を入力します。

例 :

```
ASA Version 9.16.2
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
```

```
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

最初の行は ASA のバージョンで始める必要があります。day0-config は、有効な ASA 構成である必要があります。day0-config を生成する最適な方法は、既存の ASA または ASA v から実行コンフィギュレーションの関連部分をコピーすることです。day0-config 内の行の順序は重要で、既存の `show running-config` コマンド出力の順序と一致している必要があります。

Day0-config 可能な構成：

- ホスト名
- ドメイン名
- Administrative Password
- インターフェイス
- IP アドレス
- スタティック ルート
- DHCP サーバー
- ネットワーク アドレス変換規則

(注) 第 0 日の構成ファイルの内容は、JSON 形式である必要があります。JSON 検証ツールを使用してテキストを検証する必要があります。

ステップ 3 ファイルを day0-config.txt として保存します。

ステップ 4 [Custom Script] オプションを選択します。

ステップ 5 day0-config.txt ファイルをアップロードするか、表示されたテキストボックスにファイルをコピーして貼り付けます。

ステップ 6 ステップ 1～3 を繰り返して、展開する ASA v ごとに一意のデフォルト構成ファイルを作成します。

ASAv を Nutanix に展開する

始める前に

展開する FMCv のイメージが [Image Configuration] ページに表示されていることを確認します。

-
- ステップ 1** Nutanix Prism Web コンソールにログインします。
- ステップ 2** メインメニューバーで、[View] ドロップダウンリストをクリックし、[VM] を選択します。
- ステップ 3** VM ダッシュボードで、[VM の作成 (Create VM)] をクリックします。
- ステップ 4** 次の手順を実行します。
1. ASAv インスタンスの名前を入力します。
 2. (オプション) ASAv インスタンスの説明を入力します。
 3. ASAv インスタンスで使用するタイムゾーンを選択します。
- ステップ 5** コンピューティングの詳細を入力します。
1. ASAv インスタンスに割り当てる仮想 CPU の数を入力します。
 2. 各仮想 CPU に割り当てる必要があるコアの数を入力します。
 3. ASAv インスタンスに割り当てるメモリの量 (GB) を入力します。
- ステップ 6** ASAv インスタンスにディスクを接続します。
1. [Disks] で、[Add New Disk] をクリックします。
 2. [タイプ (Type)] ドロップダウンリストから、[ディスク (DISK)] を選択します。
 3. [操作 (Operation)] ドロップダウンリストから、[イメージサービスから複製 (Clone from Image Service)] を選択します。
 4. [Bus Type] ドロップダウンリストから [SATA] を選択します。
 5. [イメージ (Image)] ドロップダウンリストから、使用するイメージを選択します。
 6. [追加 (Add)] をクリックします。
- ステップ 7** 3 つ以上の仮想ネットワーク インターフェイスを設定します。
- [ネットワークアダプタ (NIC) (Network Adapters (NIC))] で、[新しい NIC の追加 (Add New NIC)] をクリックし、ネットワークを選択して、[追加 (Add)] をクリックします。
- このプロセスを繰り返して、ネットワーク インターフェイスをさらに追加します。
- Nutanix 上の ASAv は、データトラフィック用に 1 つの管理インターフェイスと最大 9 つのネットワーク インターフェイスの合計 10 のインターフェイスをサポートします。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- vnic0 : 管理インターフェイス (必須)
- vnic1 : 外部インターフェイス (必須)
- vnic2 : 内部インターフェイス (必須)
- vnic3-9 : データインターフェイス (オプション)

ステップ 8 ASAv のアフィニティポリシーを設定します。

[VM Host Affinity] で、[Set Affinity] をクリックし、ホストを選択して、[Save] をクリックします。

ノードに障害が発生した場合でも VM を実行できるようにするには、1 つ以上のホストを選択します。

ステップ 9 第 0 日の構成ファイルを準備済みの場合は、次の手順を実行します。

1. [カスタムスクリプト (Custom Script)] を選択します。
2. [Upload A File] をクリックし、第 0 日の構成ファイル (day0-config.txt) を選択するか、もしくはコンテンツをコピーしてペーストします。

(注) 他のすべてのカスタム スクリプト オプションは、リリースではサポートされていません。

ステップ 10 [Save] をクリックして、ASAv インスタンスを展開します。VM テーブルビューにインスタンスが表示されます。

ステップ 11 VM テーブルビューで、新しく作成したインスタンスを選択し、[Power On] をクリックします。

ASAv の起動

VM の電源がオンになったら、day0-config ファイルを使用して事前定義されたユーザー名とパスワードで [ASAv-VM] > [Launch Console] を選択してアクセスします。



(注) 初期設定の完了後の仮想デバイスのこれらの設定を変更するには、CLI を使用します。

ステップ 1 [Launch Console] をクリックして、展開された ASAv にアクセスします。

ステップ 2 asav ログインプロンプトで、day0-config ユーザー名とパスワードを使用してログインします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。