

Azureでの自動拡張FTDvの高信頼環境への導入

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[Azure ARMテンプレート](#)

[機能APP](#)

[ロジックアプリ](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Azureの自動拡張Cisco Firepower Threat Defense Virtual(FTDv)を高い信頼環境に導入する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- NGFWとFirepower Management CenterはプライベートIP経由で通信する必要があります
- 外部ロードバランサにはパブリックIPを設定しないでください。
- 機能のアプリはプライベートIPと通信できる必要があります

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Azure
- Firepower Management Center
- 仮想マシンスケールセット

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FTDvは、シスコのFirepower Next-Generation Firewall機能を仮想化環境に提供し、一貫したセキュリティポリシーを使用して、物理環境、仮想環境、クラウド環境、クラウド環境のワークロードに対応します。

これらの導入は仮想化環境で利用できるため、現在NGFWではHAをサポートしていません。したがって、可用性の高いソリューションを提供するために、Cisco Next-Generation Firewall(NGFW)は、可用性セットや仮想マシンスケールセット(VMSS)などのAzureのネイティブ機能を使用して、NGFWの可用性を高め、オンデマンドでトラフィックを増加させます。

このドキュメントでは、NGFWがオンデマンドで拡張または拡張するさまざまなパラメータに基づいて、Cisco NGFWをAutoScaleに設定する方法について説明します。これは、コロケーションデータセンターで使用可能で、すべてのNGFWを一元管理するために必要なFirepower Management Center(FMC)を使用する必要がある場合の使用例をカバーします。また、FMCとFTDが管理トラフィック用にパブリックIPで通信することを希望しません。

構成と設計の考慮事項について詳しく説明する前に、Azureに関する十分な理解が必要な概念を次に示します。

- **可用性ゾーン:** アベイラビリティゾーンは、データセンターの障害からアプリケーションとデータを保護するハイアベイラビリティサービスです。可用性ゾーンは、Azureリージョン内の一意の物理的な場所です。各ゾーンは、独立した電力、冷却、およびネットワーキングを備えた1つ以上のデータセンターで構成されます。
- **VNET:** Azure Virtual Network (VNet)は、Azureのプライベートネットワークの基本的な構成要素です。VNetを使用すると、Azure Virtual Machines (VM)など、さまざまな種類のAzureリソースが、相互、インターネット、およびオンプレミスネットワークと安全に通信できるようになります。VNetは、独自のデータセンターで運用する従来のネットワークに似ていますが、スケール、アベイラビリティ、分離など、Azureのインフラストラクチャの利点が追加されています。VNET内のすべてのサブネットは、デフォルトで相互に到達可能ですが、異なるVNET内のサブネットに対しても同じではありません。
- **可用性セット:** 可用性セットは、VMの冗長性と可用性を提供するためのもう1つのデータセンター構成です。データセンター内のこの構成により、計画されたメンテナンスイベントまたは予期しないメンテナンスイベントの間に、少なくとも1つの仮想マシンが利用可能になり、99.95% Azure SLAを満たすことができます。
- **VMSS:** Azure仮想マシンのスケールセットを使用すると、負荷分散されたVMのグループを作成および管理できます。VMインスタンスの数は、需要または定義されたスケジュールに応じて自動的に増減します。スケールセットは、アプリケーションに高可用性を提供し、多数のVMを一元的に管理、構成、更新できます。仮想マシンのスケールセットを使用すると、コンピューティング、ビッグデータ、コンテナワークロードなどの領域に大規模なサービスを構築できます。
- **機能アプリ:** Azure Functionsは、アプリケーションの実行に必要な継続的に更新されるすべてのインフラストラクチャとリソースをオンデマンドで提供するクラウドサービスです。最も重要なコードの部分に焦点を当て、Azure Functionsが残りを処理します。Azure

Functionsを使用すると、Web APIの構築、データベースの変更への応答、IoTストリームの処理、メッセージキューの管理などを行うことができます。この自動スケールソリューションでは、Azure Functionは、オブジェクトの作成、FTDvの登録/登録解除、パラメータの確認などのさまざまなAPI要求です。

- **Logic App:**[Azure Logic Apps](#)は、企業または組織間でアプリケーション、データ、システム、およびサービスを統合する必要がある場合に、タスク、ビジネスプロセス、ワークフローのスケジュール、自動化、オーケストレーションを支援するクラウドサービスです。Logic Appsは、クラウド、オンプレミス、または両方で、アプリ統合、データ統合、システム統合、エンタープライズアプリケーション統合(EAI)、およびBusiness-to-Business(B2B)通信のためのスケラブルなソリューションの設計と構築を簡素化します。このソリューションは、自動スケールソリューションの機能に対して実行される機能の論理的なシーケンスを提供します。

現在、NGFWで使用可能なAutoScaleソリューションは、VNetにローカルなプライベートIPと通信するための管理計画を提供しておらず、Firepower Management CenterとNGFW間で通信を交換するためにパブリックIPが必要です。

この記事では、検証済みのソリューションがプライベートIP経由のFirepower Management Center(FMC)およびNGFW通信で使用できるようになるまで、この問題を解決することを目的としています。

設定

自動スケールNGFWソリューションを作成するには、次のコンフィギュレーションガイドを使用します。

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/azure/ftdv-azure-gsg/ftdv-azure-autoscale.html#Cisco_Concept.dita_c0b3cf0d-9690-4342-8cba-e66730e70c47

次の使用例に対処できるように、いくつかの修正を加えます。

- 機能のアプリは、お客様の内部IPセグメントと通信できる必要があります
- ロードバランサにパブリックIPを設定しないでください
- NGFWとFMC間の管理トラフィックは、プライベートIPセグメントを介して交換する必要があります。

上記の使用例を使用してAutoScaled NGFWソリューションを作成するには、シスコの公式ガイドに記載されている手順で次の項目を変更する必要があります。

1. Azure ARMテンプレート

ARMテンプレートは、Azureで自動化を有効にするために使用されます。シスコは、自動スケールソリューションの作成に利用できる検証済みのARMテンプレートを提供しています。ただし、このARMテンプレートはPublic Github <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template>で利用できるため、Expressルートを通じて到達可能であるにもかかわらず、お客様の内部ネットワークと通信できない機能アプリケーションを作成します。したがって、Function AppがConsumption Modeの代わりにPremiumモードを使用できるように、これを少し変更する必要があります。したがって、必要なARMテンプレートは、https://github.com/Madhuri150791/FunctionApp_with_Premium_Plan.gitから入手できます

2. 機能APP

関数アプリは、Azure関数のセットです。基本機能には次のものがあります。

- Azureメトリックを定期的に通信/プローブします。
- FTDvの負荷を監視し、スケールイン/スケールアウト操作をトリガーします。
- 新しいFTDvをFMCに登録します。
- FMC経由で新しいFTDvを設定します。
- スケールインFTDvをFMCから登録解除（削除）します。

要件で述べたように、オンデマンドNGFWの作成または削除のために作成されるさまざまな機能は、NGFWのパブリックIPに基づいて実行されます。したがって、パブリックIPではなくプライベートIPを取得するためにC#コードを調整する必要があります。コードを微調整した後、関数アプリケーションを作成するためのzipファイルは

https://github.com/Madhuri150791/FunctionApp_with_Premiiium_Plan.gitで入手 [できます](#)

ASM_Function.zipという名前のASM_Function.zipこれにより、FunctionsアプリはパブリックIPを持たずに内部リソースと通信できます。

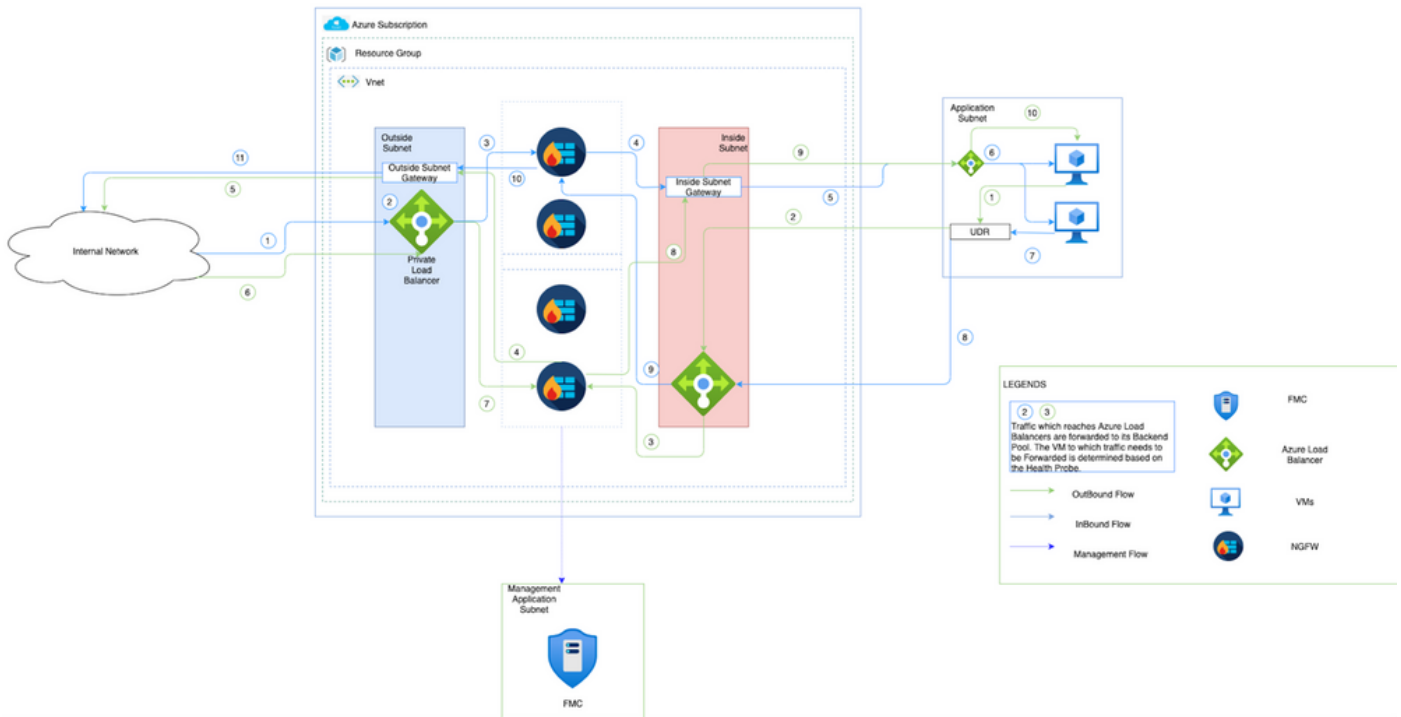
3. ロジックアプリ

Auto Scale Logic Appはワークフロー、つまり一連のステップの集合です。Azure関数は独立したエンティティであり、互いに通信できません。このオーケストレータは、これらの関数の実行をシーケンスし、それらの間で情報を交換します。

- Logic Appは、Auto Scale Azure機能間で情報をオーケストレーションおよび渡すために使用されます。
- 各ステップは、自動スケールAzure機能または組み込みの標準ロジックを表します。
- ロジックアプリケーションはJSONファイルとして提供されます。
- ロジックアプリケーションは、GUIまたはJSONファイルを使用してカスタマイズできます。

注：https://github.com/Madhuri150791/FunctionApp_with_Premiiium_Plan.gitで入手できるロジックアプリの詳細は慎重に変更する必要があります。次の項目は、展開の詳細、FUNCTIONAPP名、リソースグループ名、サブスクリプションIDに置き換える必要があります。

ネットワーク図



この図は、NGFWを介してAzure環境内でインバウンドおよびアウトバウンドトラフィックがどのように流れるかを示しています。

設定

次に、自動スケールソリューションに必要なさまざまなコンポーネントを作成します。

1. Autoscale Logicのコンポーネントを作成します。

ARMテンプレートを使用して、VMSS、Logic APP、Function APP、App Insight、Network Security Groupを作成します。

[ホーム] > [リソースの作成] > [テンプレートの検索]に移動し、[テンプレート配置]を選択します。次に、エディタで[Create and build your own template]をクリックします。

Home > New > Template deployment (deploy using custom templates) (preview) > Custom deployment >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↕ Load file ↓ Download

- Parameters (32)
- Variables (34)
- Resources (12)
 - LogicApp (Microsoft.Logic/workflows)
 - [variables('mgmtSecGrp')] (Microsoft.Network/networkSecurityGroups)
 - [variables('dataSecGrp')] (Microsoft.Network/networkSecurityGroups)
 - [variables('storageAccountName')] (Microsoft.Storage/storageAccounts)
 - [variables('hostingPlanName')] (Microsoft.Web/serverfarms)
 - [variables('functionAppName')] (Microsoft.Web/sites)
 - [variables('appInsightsName')] (Microsoft.Insights/components)

```

596 {
597   "name": "MNGT_NET_INTERFACE_NAME",
598   "value": "mgmtNic"
599 },
600 {
601   "name": "MNGT_PUBLIC_IP_NAME",
602   "value": "mgmtPublicIP"
603 },
604 {
605   "name": "NAT_ID",
606   "value": "5678"
607 },
608 {
609   "name": "NETWORK_CIDR",
610   "value": "[parameters('virtualNetworkCidr')]"
611 },
612 {
613   "name": "NETWORK_NAME",
614   "value": "[concat(parameters('resourceNamePrefix'), '-vnet')]"
615 },
616 {
617   "name": "POLICY_NAME",
618   "value": "[parameters('policyName')]"

```

Save Discard

2. [Save] をクリックします。

[Home](#) > [New](#) > [Template deployment \(deploy using custom templates\) \(preview\)](#) >

Custom deployment

Deploy from a custom template

Template



Customized template [↗](#)

12 resources

 Edit template

 Edit parameters

Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [i](#)

Microsoft Azure Enterprise [v](#)



Resource group * [i](#)

[Create new](#)

Parameters

Region * [i](#)

East US [v](#)

Resource Name Prefix [i](#)

Virtual Network Rg [i](#)

madewang

Virtual Network Name [i](#)

madewang-vnet

[Review + create](#)

[< Previous](#)

[Next : Review + create >](#)

このテンプレートに必要な変更を加え、[Review +Create]をクリックします。

3. これにより、前述のリソースグループの下にすべてのコンポーネントが作成されます。

Home > madewang Resource group

Search (Cmd+/) Add Edit columns Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Feedback

Overview

Activity log

Access control (IAM)

Tags

Events

Settings

Deployments

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Advisor recommendations

Monitoring

Insights (preview)

Alerts

Metrics

Diagnostic settings

Logs

Essentials

Subscription (change) : Microsoft Azure Enterprise

Subscription ID : 9d5ea202-7f70-43f6-a529-041759f8f710

Deployments : 27 Failed,64 Succeeded

Location : East US

Tags (change) : Click here to add tags

Filter: cvsinout Type == all Location == all Add filter

Showing 1 to 11 of 11 records. Show hidden types

Name	Type	Location
appinsight	Application Insights	East US
dataIntSecGrp	Network security group	East US
alb	Load balancer	East US
alb-public-ip	Public IP address	East US
function-app	App Service plan	East US
function-app	Function App	East US
alb	Load balancer	East US
logic-app	Logic app	East US
mgmtIntSecGrp	Network security group	East US
vmss	Virtual machine scale set	East US
storage37rpzbtida	Storage account	East US

< Previous Page 1 of 1 Next >

4. URLにログインします

https://<function_app_name>.scm.azurewebsites.net/DebugConsole

ファイルASM_Function.zipおよびftdssh.exeをsite/wwwroot/folderにアップロードします(指定した場所にアップロードする必要があります。指定しない場所では、Function Appが各種機能を識別できません)。

次の図のようになります。

function-app.scm.azurewebsites.net/DebugConsole

Kudu Environment Debug console Process explorer Tools Site extensions madewang@cisco.c

... / wwwroot + | 18 items | Home Refresh Download

Name	Modified	Size
AutoScaleManager	12/4/2020, 9:18:25 PM	
bin	12/4/2020, 9:18:25 PM	
ConfigureFtdInterfaces	12/4/2020, 9:18:32 PM	
CreateStaticRoutes	12/4/2020, 9:18:32 PM	
DeleteUnRegisteredFTD	12/4/2020, 9:18:32 PM	
DeployConfiguration	12/4/2020, 9:18:32 PM	
DeviceDeRegister	12/4/2020, 9:18:32 PM	

```

Kudu Remote Execution Console
Type 'exit' then hit 'enter' to get a new CMD process.
Type 'cls' to clear the console

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\home>
C:\home\site>
C:\home\site\wwwroot>

```

5. [Function app] > [Function]をオンにします。すべての機能が表示されます。

Home > madewang > <prefix>-function-app

<prefix>-function-app | Functions

Search (Cmd+/) < Add Refresh Delete

Filter by name...

<input type="checkbox"/>	Name ↑↓	Trigger ↑↓	Status ↑↓
<input type="checkbox"/>	AutoScaleManager	HTTP	Enabled
<input type="checkbox"/>	ConfigureFtdInterfaces	HTTP	Enabled
<input type="checkbox"/>	CreateStaticRoutes	HTTP	Enabled
<input type="checkbox"/>	DeleteUnRegisteredFTD	HTTP	Enabled
<input type="checkbox"/>	DeployConfiguration	HTTP	Enabled
<input type="checkbox"/>	DeviceDeRegister	HTTP	Enabled
<input type="checkbox"/>	DeviceRegister	HTTP	Enabled
<input type="checkbox"/>	DisableHealthProbe	HTTP	Enabled
<input type="checkbox"/>	FtdScaleIn	HTTP	Enabled
<input type="checkbox"/>	FtdScaleOut	HTTP	Enabled
<input type="checkbox"/>	GetFtdPublicIp	HTTP	Enabled
<input type="checkbox"/>	MinimumConfigVerification	HTTP	Enabled
<input type="checkbox"/>	WaitForDeploymentTask	HTTP	Enabled
<input type="checkbox"/>	WaitForFtdToComeUp	HTTP	Enabled

6. VMSSが機能アプリケーション内の機能を実行できるように、アクセス権限を変更します。
 <prefix>-vmss [Access Control (IAM)] > [Add role assignment]に移動します。このVMSSに
 <prefix>-function-appへのコントリビュータアクセスを提供します





Add role assignment ×

Role ⌵
Contributor ⌵


Assign access to ⌵
Function App ⌵

Subscription *
Microsoft Azure Enterprise ⌵

Select ⌵
Search by name

-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  fsdemo-function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...

Selected members:

-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71... Remove

Save Discard

[Save] をクリックします。

7. 「ロジックアプリ」> 「ロジックコード」ビューに移動し、次の場所で使用可能なコードを使用してロジックコードを変更します。

<https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/Logic%20App>

ここでは、使用する前にAzureサブスクリプション、リソースグループ名、および機能アプリ名を置き換える必要があります。そうしないと、は正常に保存できません。

8. [Save] をクリックします。「論理アプリケーションの概要」および「論理アプリケーションの有効化」に移動します。

確認

ロジックアプリが有効になると、直ちに5分の間隔で実行が開始されます。

すべてが正しく設定されている場合は、トリガーアクションが成功します。

Home > madewang > logic-app

Logic app

Search (Cmd+/) <<

Run Trigger Refresh Edit Delete Disable Update Schema Clone Export

To improve traffic flow, we're adding new outbound IP addresses for Logic Apps. Review action needed if you're filtering IP addresses with firewall settings before 08/31/2020. Click to learn more. →

Recurrence 36 actions
View in Logic Apps designer

FREQUENCY
Runs every 5 minutes.

EVALUATION
Evaluated 285 times, fired 286 times in the last 24 hours
See trigger history

Runs history

All Start time earlier than Pick a date Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
✓ Succeeded	12/8/2020, 12:41 AM	08585942385827730953992150418CU69	9.68 Seconds	
✓ Succeeded	12/8/2020, 12:36 AM	08585942388857869130247836749CU94	9.99 Seconds	
✓ Succeeded	12/8/2020, 12:31 AM	08585942391894090466308406058CU42	10.53 Seconds	
✓ Succeeded	12/8/2020, 12:26 AM	08585942394931376660212576414CU43	9.63 Seconds	
✓ Succeeded	12/8/2020, 12:21 AM	0858594239797165223385542405CU95	9.76 Seconds	
✓ Succeeded	12/8/2020, 12:16 AM	08585942401002907485558564356CU88	10.88 Seconds	
✓ Succeeded	12/8/2020, 12:11 AM	08585942404034146970768829140CU46	10.04 Seconds	
✓ Succeeded	12/8/2020, 12:06 AM	08585942407064834984931459270CU66	10.23 Seconds	
✓ Succeeded	12/8/2020, 12:01 AM	08585942410101813994775025693CU71	10.24 Seconds	
✓ Succeeded	12/7/2020, 11:56 PM	08585942413124684374178471703CU67	9.69 Seconds	

また、VMはVMSSの下に作成されます。

Home > madewang > out-vmss

out-vmss | Instances

Virtual machine scale set

Search (Cmd+/) <<

Start Restart Stop Reimage Delete Upgrade Refresh Protection Policy

Search virtual machine instances

Name	Computer name	Status	Health state	Provisioning state	Protection policy	Latest model
out-vmss_0	out-vmss000000	Running	✓	Succeeded		Yes
out-vmss_2	out-vmss000002	Running	✓	Succeeded		Yes

FMCにログインし、FMCとNGFWがFTDvプライベートIP経由で接続されていることを確認します。

The screenshot displays the management console for a Cisco Firepower Threat Defense for Azure device. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' section is active, showing 'out-vmss_0'. The main content area is divided into several sections:

- Mode:** routed
- Compliance Mode:** None
- TLS Crypto Acceleration:** Disabled
- System:**
 - Model: Cisco Firepower Threat Defense for Azure
 - Serial: 9ADMGX24KRE
 - Time: 2020-12-08 14:06:09
 - Time Zone: UTC (UTC+0:00)
 - Version: 6.6.0
 - Time Zone setting for Time based Rules: UTC (UTC+0:00)
- Health:**
 - Status: ✔
 - Policy: [Initial_Health_Policy_2020-11-11_04:24:06](#)
 - Blacklist: [None](#)
- Management:**
 - Host: 10.6.0.9
 - Status: ✔
- Inventory Details:**
 - Cpu Type: CPU Xeon E5 series 2400 MHz
 - Cpu Cores: 1 CPU (16 cores)
 - Memory: 56832 MB RAM

NGFW CLIにログインすると、次のように表示されます。

```
Cisco Fire Linux OS v6.6.0 (build 37)
Cisco Firepower Threat Defense for Azure v6.6.0 (build 90)

> ex
exit expert
> expert
admin@inout-vmss-0:~$ netstat | grep 8305
tcp        0      0 inout-vmss-0:8305    madewangfmc.inter:41997 ESTABLISHED
tcp        0      0 inout-vmss-0:8305    madewangfmc.inter:54513 ESTABLISHED
admin@inout-vmss-0:~$
```

したがって、FMCはAzure Private VNet Subnet経由でNGFWと通信します。

トラブルシューティング

新しいNGFWの構築中にLogic Appが失敗する場合があります。このような状況をトラブルシューティングするには、次の手順を実行します。

1. ロジックアプリが正常に実行されているかどうかを確認します。

Home > madewang > logic-app

Search (Cmd+V)

Run Trigger Refresh Edit Delete Disable Update Schema Clone Export

To improve traffic flow, we're adding new outbound IP addresses for Logic Apps. Review action needed if you're filtering IP addresses with firewall settings before 08/31/2020. Click to learn more. →

Subscription (change) : Microsoft Azure Enterprise Runs last 24 hours : 284 successful, 1 failed
 Subscription ID : 9d5ea202-7170-4316-a529-041759f8f710 Integration Account : -- --

Summary

Trigger Actions

RECURRENTCE COUNT
 Recurrence 36 actions
[View in Logic Apps designer](#)

FREQUENCY
 Runs every 5 minutes.

EVALUATION
 Evaluated 285 times, fired 285 times in the last 24 hours
[See trigger history](#)

Runs history

Failed Start time earlier than Pick a date Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
Failed	12/7/2020, 9:32 AM	08585942931626719086228010944CU70	10.25 Seconds	
Failed	12/4/2020, 9:24 PM	08585945095939947222488931533CU66	1.96 Seconds	
Failed	12/4/2020, 9:23 PM	0858594509662968875411868431CU59	1.45 Seconds	
Failed	12/4/2020, 9:23 PM	08585945096748689653030909870CU58	1.74 Seconds	

2. 障害の原因を特定します。
 失敗したトリガーをクリックします。

Microsoft Azure Search resources, services, and docs (G+)

Home > madewang > logic-app > Runs history

Runs history

Refresh

Failed Start time earlier than Pick a date Pick a time Search to filter items by identifier

Start time	Duration
12/7/2020, 9:32 AM	10.25 Seconds
12/4/2020, 9:24 PM	1.96 Seconds
12/4/2020, 9:23 PM	1.45 Seconds
12/4/2020, 9:23 PM	1.74 Seconds

Logic app run
 08585942931626719086228010944CU70

Run Details Resubmit Cancel Run Info

AutoScaleManager 2s

BadRequest

INPUTS Show raw inputs >

Function name
 -function-app/AutoScaleManager

OUTPUTS Show raw outputs >

Status code
 400

Headers

Key	Value
Request-Context	appld=cid-v1.fa84d6f7-85c5-407...
Date	Mon, 07 Dec 2020 04:02:11 GMT
Content-Length	48

Body
 ERROR: Failed to connet to FMC..Can not continue

コードフローからエラーポイントを特定してみます。上記のスニペットから、ASMロジックがFMCに接続できなかったため失敗していることは明らかです。次に、Azure内のフローごとにFMCに到達できなかった理由を特定する必要があります。