

Déployer FTDv à mise à l'échelle automatique dans Azure dans un environnement de haute confiance

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Modèle ARM Azure](#)

[APP de fonction](#)

[Application logique](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment déployer Cisco Firepower Threat Defense Virtual (FTDv) à l'échelle automatique dans Azure dans un environnement de haute confiance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Les pare-feu de nouvelle génération et Firepower Management Center doivent communiquer sur IP privé
- L'équilibreur de charge externe ne doit pas avoir d'adresse IP publique.
- L'application de la fonction doit pouvoir communiquer avec une adresse IP privée

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Azure
- Centre de gestion Firepower

- Ensemble de l'échelle des machines virtuelles

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

FTDv intègre la fonctionnalité de pare-feu de nouvelle génération de Cisco Firepower aux environnements virtualisés, permettant ainsi des politiques de sécurité cohérentes pour suivre les charges de travail dans vos environnements physiques, virtuels et cloud, et entre les clouds.

Ces déploiements étant disponibles dans un environnement virtualisé, la prise en charge de la haute disponibilité n'est pas disponible pour les pare-feu de nouvelle génération. Par conséquent, pour fournir une solution hautement disponible, le pare-feu de nouvelle génération Cisco (NGFW) utilise les fonctionnalités natives d'Azure, telles que les ensembles de disponibilité et le Virtual Machine Scale Set (VMSS), pour rendre le pare-feu de nouvelle génération hautement disponible et répondre à l'augmentation du trafic à la demande.

Ce document se concentre sur la configuration de Cisco NGFW à AutoScale en fonction de différents paramètres dans lesquels le NGFW évolue à la demande ou évolue. Cela couvre le cas où le client a besoin d'utiliser Firepower Management Center (FMC), disponible dans le centre de données de colocation et nécessaire pour gérer de manière centralisée tous les pare-feu de nouvelle génération. De plus, les clients ne veulent pas que FMC et FTD communiquent sur IP public pour le trafic de gestion.

Avant d'approfondir la question de la configuration et de la conception, voici les quelques concepts qui doivent être bien compris dans Azure :

- **Zone de disponibilité** : Une zone de disponibilité est une offre de haute disponibilité qui protège vos applications et vos données des pannes de data center. Les zones de disponibilité sont des emplacements physiques uniques dans une région Azure. Chaque zone est composée d'un ou plusieurs data centers équipés d'une alimentation, d'un refroidissement et d'un réseau indépendants.
- **VNET** : Azure Virtual Network (VNet) est la pierre angulaire de votre réseau privé dans Azure. VNet permet à de nombreux types de ressources Azure, telles que les machines virtuelles Azure, de communiquer en toute sécurité entre elles, sur Internet et sur les réseaux locaux. VNet est similaire à un réseau traditionnel que vous utiliseriez dans votre propre centre de données, mais apporte avec lui des avantages supplémentaires de l'infrastructure d'Azure tels que l'évolutivité, la disponibilité et l'isolation. Chaque sous-réseau d'un réseau virtuel est accessible par défaut, mais ce n'est pas le cas pour les sous-réseaux de différents réseaux virtuels.
- **Jeu de disponibilité** : Les ensembles de disponibilité sont une autre configuration de centre de données pour fournir la redondance et la disponibilité des machines virtuelles. Cette configuration au sein d'un centre de données garantit qu'au cours d'un événement de maintenance planifié ou non, au moins une machine virtuelle est disponible et répond au contrat de niveau de service Azure à 99,95 %.

- **VMSS** : Les jeux d'échelle de machines virtuelles Azure vous permettent de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de VM peut augmenter ou diminuer automatiquement en réponse à la demande ou à un planning défini. Les jeux d'évolutivité offrent une haute disponibilité à vos applications et vous permettent de gérer, configurer et mettre à jour un grand nombre de machines virtuelles de manière centralisée. Avec des jeux d'échelle de machines virtuelles, vous pouvez créer des services à grande échelle pour des domaines tels que le calcul, le Big Data et les charges de travail de conteneur.
- **Fonctions App** : Azure Functions est un service cloud disponible à la demande qui fournit l'infrastructure et les ressources constamment mises à jour nécessaires pour exécuter vos applications. Vous vous concentrez sur les éléments de code qui vous importent le plus, et Azure Functions gère le reste. Vous pouvez utiliser Azure Functions pour créer des API Web, répondre aux modifications apportées à la base de données, traiter les flux IoT, gérer les files d'attente de messages, etc. Dans cette solution à mise à l'échelle automatique, Azure Function est diverses demandes d'API à FMC pour la création d'objets, l'enregistrement/désenregistrement de FTDv, la vérification des paramètres, etc.
- **Application logique** : [Azure Logic Apps](#) est un service cloud qui vous aide à planifier, automatiser et orchestrer des tâches, des processus commerciaux et des [workflows](#) lorsque vous avez besoin d'intégrer des applications, des données, des systèmes et des services dans les entreprises ou les organisations. Les applications logiques simplifient la façon dont vous concevez et construisez des solutions évolutives pour l'[intégration des](#) applications, l'intégration des données, l'intégration des systèmes, l'intégration des applications d'entreprise (EAI) et la communication entre entreprises (B2B), que ce soit dans le cloud, sur site ou les deux. Cette solution fournit le séquençage logique des fonctions à exécuter pour le fonctionnement de la solution à mise à l'échelle automatique.

Actuellement, la solution AutoScale disponible pour le pare-feu de nouvelle génération ne fournit pas de plan de gestion permettant de communiquer avec l'adresse IP privée locale au VPNet et nécessite l'échange d'adresses IP publiques entre Firepower Management Center et le pare-feu de nouvelle génération.

Cet article vise à résoudre ce problème jusqu'à ce que la solution vérifiée soit disponible pour les communications Firepower Management Center et NGFW sur IP privé.

Configuration

Afin de créer une solution de pare-feu de nouvelle génération à mise à l'échelle automatique, ce guide de configuration est utilisé :

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

avec plusieurs modifications afin de pouvoir traiter les cas d'utilisation suivants :

- L'application de la fonction doit pouvoir communiquer avec le segment IP interne du client
- L'équilibreur de charge ne doit pas avoir d'adresse IP publique

- Le trafic de gestion entre NGFW et FMC doit être échangé sur le segment IP privé.

Afin de créer une solution de pare-feu de nouvelle génération à évolutivité automatique, avec les cas d'utilisation mentionnés ci-dessus, vous devez les modifier dans les étapes mentionnées dans le Guide officiel de Cisco :

1. Modèle ARM Azure

Le modèle ARM est utilisé pour activer Automation dans Azure. Cisco a fourni un modèle ARM vérifié qui peut être utilisé pour créer une solution à évolutivité automatique. Mais ce modèle ARM disponible sur Public Github <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template> crée une application Fonctions qui ne peut pas être faite pour communiquer avec le réseau interne du Client s'ils sont accessibles via des routes express. Nous devons donc le modifier un peu afin que l'application de fonction puisse maintenant utiliser le mode Premium au lieu du mode Consommation. Le modèle ARM requis est donc disponible à l'adresse https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

2. APP de fonction

L'application de fonction est un ensemble de fonctions Azure. La fonctionnalité de base inclut :

- Communiquer/sonder régulièrement les mesures Azure.
- Surveillez la charge FTDv et déclenchez les opérations d'entrée/sortie d'échelle.
- Enregistrez un nouveau FTDv avec le FMC.
- Configurez un nouveau FTDv via FMC.
- Désenregistrez (supprimez) un FTDv évolutif du FMC.

Comme indiqué dans la condition requise, les différentes fonctions créées pour la création ou la suppression de pare-feu de nouvelle génération à la demande sont basées sur l'adresse IP publique du pare-feu de nouvelle génération. Par conséquent, nous devons modifier le code C# pour obtenir une adresse IP privée au lieu d'une adresse IP publique. Après avoir modifié le code, le fichier zip pour créer l'application de fonction est disponible à l'adresse https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

avec le nom ASM_Function.zip. Cela permet à l'application Fonctions de communiquer avec des ressources internes sans avoir l'adresse IP publique.

3. Application logique

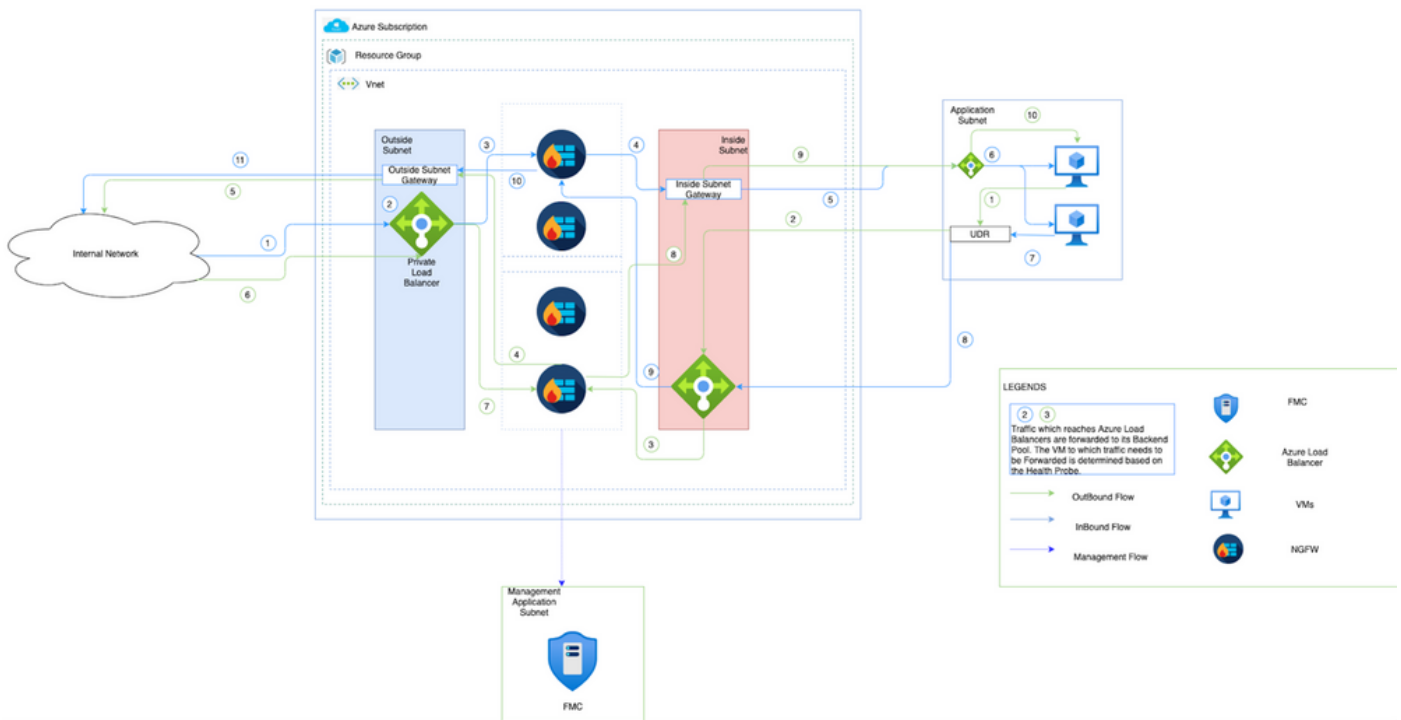
L'application logique de mise à l'échelle automatique est un workflow, c'est-à-dire un ensemble d'étapes dans une séquence. Les fonctions Azure sont des entités indépendantes et ne peuvent pas communiquer entre elles. Cet orchestrateur séquence l'exécution de ces fonctions et échange des informations entre elles.

- L'application logique est utilisée pour orchestrer et transmettre des informations entre les fonctions Auto Scale Azure.
- Chaque étape représente une fonction Auto Scale Azure ou une logique standard intégrée.
- L'application logique est livrée en tant que fichier JSON.
- L'application logique peut être personnalisée via l'interface utilisateur graphique ou le fichier JSON.

Note: Les détails de l'application logique disponibles à l'adresse https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git doivent être soigneusement modifiés et les éléments suivants doivent être remplacés par les détails du

déploiement, Nom FUNCTIONAPP, Nom du GROUPE DE RESSOURCES, ID D'ABONNEMENT.

Diagramme du réseau



Cette image montre comment le trafic entrant et sortant circule dans un environnement Azure via le pare-feu de nouvelle génération.

Configurations

Maintenant, créez différents composants nécessaires à une solution à mise à l'échelle automatique.

1. Créer des composants de la logique de mise à l'échelle automatique.

Utilisez le modèle ARM et créez VMSS, Logic APP, Function APP, App Insight, Network Security Group.

Accédez à **Accueil > Créer une ressource > Rechercher un modèle** puis sélectionnez **Déploiement de modèle**. Cliquez maintenant sur **Créer** et créer votre propre modèle dans l'éditeur.

Edit template

Edit your Azure Resource Manager template



+ Add resource ↑ Quickstart template ↑ Load file ↓ Download

<<	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. Cliquez sur **Enregistrer**.

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 * ⓘ

Resource group * ⓘ

[Create new](#)

Parameters

Region * ⓘ

Resource Name Prefix ⓘ

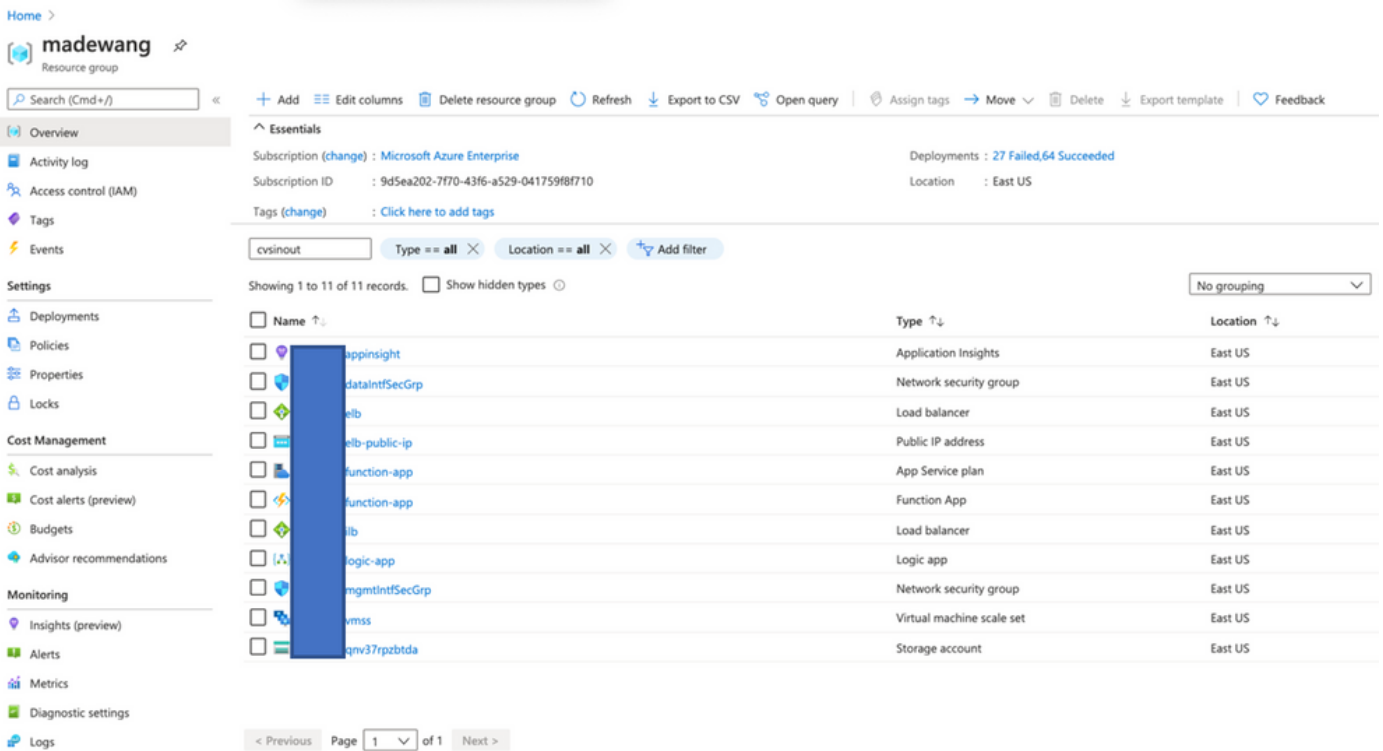
Virtual Network Rg ⓘ

Virtual Network Name ⓘ

Review + create < Previous Next : Review + create >

Apportez les modifications requises à ce modèle et cliquez sur **Vérifier +Créer**.

3. Ceci crée tous les composants sous le groupe de ressources mentionné.

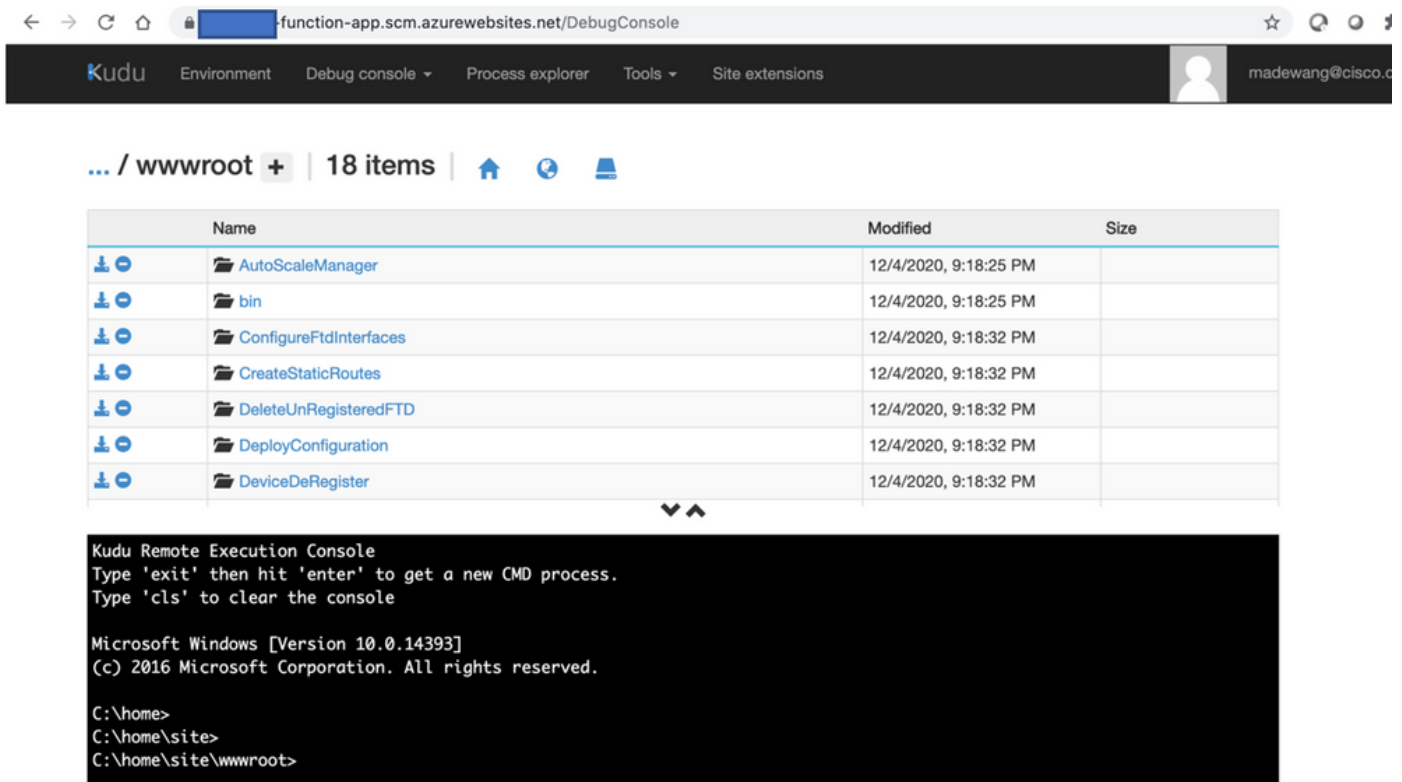


4. Se connecter à l'URL

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

Téléchargez le fichier **ASM_Function.zip** et **ftdssh.exe** vers **site/wwwroot/dossier** (il est obligatoire de le télécharger à l'emplacement spécifié, sinon l'application Fonction n'identifie pas différentes fonctions.)

Cette image devrait être la suivante :



5. Activez l'application Fonction > Fonction. Vous devriez voir toutes les fonctions.

Home > madewang > [redacted] function-app

[redacted]-function-app | Functions

Function App

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

Navigation menu:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Events (preview)
- Functions
 - Functions
 - App keys
 - App files
 - Proxies
- Deployment
 - Deployment slots
 - Deployment Center
 - Deployment Center (Preview)
- Settings
 - Configuration
 - Authentication / Authorization
 - Application Insights

6. Modifiez l'autorisation d'accès de sorte que VMSS puisse exécuter les Fonctions dans l'application de fonction.

Accédez à <prefix>-vmss Access Control (IAM) > Add role assignment. Fournir à ce VMSS un accès de contributeur à <prefix>-function-app





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... [Remove](#)

Click **Save**.

7. Accédez à **Application logique > Vue Code logique** et modifiez le code logique avec le code disponible à l'adresse

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

Ici, l'abonnement Azure, le nom du groupe de ressources et le nom de l'application de fonction doivent être remplacés avant d'être utilisés. Sinon, l'enregistrement n'est pas autorisé.

8. Cliquez **Save**. Accédez à Présentation de l'application logique et Activer l'**application logique**.

Vérification

Une fois que l'application logique est activée, elle commence immédiatement à s'exécuter dans l'intervalle de 5 minutes.

Si tout est configuré correctement, les actions de déclenchement s'affichent.

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	08585942397971652233385542405CU95	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	

En outre, la VM est créée sous VMSS.

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	Healthy	Succeeded	Yes	Yes
out-vmss_2	out-vmss000002	Running	Healthy	Succeeded	Yes	Yes

Connectez-vous à FMC et vérifiez que FMC et NGFW sont connectés via une adresse IP privée FTDv :

The screenshot displays the management interface for a Cisco Firepower Threat Defense for Azure device. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP Intelligence'. The 'Device Management' section is active, showing configuration for 'out-vmss_0'. The 'System' section lists details such as Model (Cisco Firepower Threat Defense for Azure), Serial (9ADMGX24KRE), Time (2020-12-08 14:06:09), and Version (6.6.0). The 'Health' section shows a green status and a policy named 'Initial_Health_Policy_2020-11-11_04:24:06'. The 'Management' section shows the Host IP address '10.6.0.9' highlighted with a red box. The 'Inventory Details' section shows CPU Type (CPU Xeon E5 series 2400 MHz), CPU Cores (1 CPU (16 cores)), and Memory (56832 MB RAM).

Lorsque vous vous connectez à l'interface de ligne de commande du pare-feu de nouvelle génération, vous voyez ceci :

```
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:~$
```

Par conséquent, FMC communique au pare-feu de nouvelle génération via le sous-réseau VPN privé Azure.

Dépannage

Parfois, l'application logique échoue lors de la création d'un nouveau pare-feu de nouvelle génération. Pour résoudre ce problème, ces étapes peuvent être effectuées :

1. Vérifiez si l'application logique fonctionne correctement.

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

RECURRENT
 Recurrence

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. Identifiez la cause de l'échec.
 Cliquez sur le déclencheur ayant échoué.

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	appId=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

Essayez d'identifier le point d'échec à partir du flux de code. À partir de l'extrait ci-dessus, il est clair que la logique ASM a échoué car elle n'a pas pu se connecter à FMC. Ensuite, vous devez identifier pourquoi FMC n'était pas accessible en fonction du flux dans Azure.