

Implemente FTDv de escala automática en Azure en un entorno de confianza alta

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Azure ARM Template](#)

[APP de función](#)

[Aplicación lógica](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo implementar Cisco Firepower Threat Defense Virtual (FTDv) de escala automática en Azure en un entorno de alta confianza.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- NGFW y Firepower Management Center deben comunicarse a través de IP privada
- El equilibrador de carga externo no debe tener IP pública.
- La aplicación de la función debe poder comunicarse con IP privada

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Azure
- Centro de administración FirePOWER
- Conjunto de escalas de máquinas virtuales

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 tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

FTDv lleva la funcionalidad de firewall de última generación de Cisco Firepower a los entornos virtualizados, lo que permite aplicar políticas de seguridad coherentes para seguir las cargas de trabajo en los entornos físicos, virtuales y de nube, así como entre nubes.

Dado que estas implementaciones están disponibles en un entorno virtualizado, el NGFW no admite HA. Por lo tanto, para proporcionar una solución de alta disponibilidad, el firewall de última generación (NGFW) de Cisco utiliza las funciones nativas de Azure, como conjuntos de disponibilidad y Virtual Machine Scale Set (VMSS), con el fin de que NGFW esté altamente disponible y se adapte al aumento del tráfico a demanda.

Este documento se centra en la configuración del NGFW de Cisco para AutoScale en función de diferentes parámetros en los que el NGFW se amplía a petición o a medida. Esto cubre el caso práctico en el que el cliente necesita utilizar Firepower Management Center (FMC), que está disponible en el Data Center de ubicación y que se necesita para gestionar de forma centralizada todos los NGFW. Además, los clientes no desean que FMC y FTD se comuniquen a través de IP pública para el tráfico de gestión.

Antes de profundizar en la configuración y el diseño, a continuación se muestran los pocos conceptos que deberían entenderse bien para Azure:

- **Zona de disponibilidad:** Una zona de disponibilidad es una oferta de alta disponibilidad que protege sus aplicaciones y datos de las fallas del Data Center. Las zonas de disponibilidad son ubicaciones físicas únicas dentro de una región de Azure. Cada zona está formada por uno o más Data Centers equipados con alimentación, refrigeración y redes independientes.
- **VNET:** Azure Virtual Network (VNet) es el pilar fundamental de su red privada en Azure. VNet permite muchos tipos de recursos de Azure, como Azure Virtual Machines (VM), para comunicarse de forma segura entre sí, con Internet y con redes in situ. VNet es similar a una red tradicional que se utilizaría en su propio Data Center, pero ofrece ventajas adicionales de la infraestructura de Azure, como escalabilidad, disponibilidad y aislamiento. Cada subred dentro de una VNET es accesible entre sí de forma predeterminada, pero lo mismo no es válido para subredes en diferentes VNET.
- **Conjunto de disponibilidad:** Los conjuntos de disponibilidad son otra configuración del Data Center para proporcionar redundancia y disponibilidad de VM. Esta configuración dentro de un Data Center garantiza que durante un evento de mantenimiento planificado o no planificado, al menos una máquina virtual esté disponible y cumpla con el SLA de Azure del 99,95%.
- **VMSS:** Los conjuntos de escala de máquinas virtuales de Azure le permiten crear y administrar un grupo de VM con carga equilibrada. El número de instancias de VM puede aumentar o disminuir automáticamente en respuesta a la demanda o a una programación definida. Los conjuntos de ampliación proporcionan una alta disponibilidad a sus aplicaciones y le permiten administrar, configurar y actualizar de forma centralizada un gran número de

VM. Gracias a los conjuntos a escala de máquinas virtuales, puede crear servicios a gran escala para áreas como la informática, Big Data y cargas de trabajo de contenedores.

- **Aplicación Functions:** Azure Functions es un servicio en la nube disponible a demanda que proporciona toda la infraestructura y los recursos continuamente actualizados necesarios para ejecutar las aplicaciones. Se centra en los elementos de código que más le importan y Azure Functions se encarga del resto. Puede utilizar las funciones de Azure para crear API web, responder a los cambios de la base de datos, procesar flujos de IoT, administrar colas de mensajes, etc. En esta solución de escala automática, Azure Function son varias solicitudes API a FMC para crear objetos, registrar/anular el registro de FTDv, comprobar los parámetros, etc.
- **Aplicación lógica:** [Azure Logic Apps](#) es un servicio en la nube que le ayuda a programar, automatizar y organizar tareas, procesos empresariales y [flujos de trabajo](#) cuando necesita integrar aplicaciones, datos, sistemas y servicios en empresas u organizaciones. Logic Apps simplifica el diseño y la creación de soluciones escalables para la [integración de](#) aplicaciones, la integración de datos, la integración de sistemas, la integración de aplicaciones empresariales (EAI) y la comunicación interempresarial (B2B), ya sea en la nube, in situ o en ambos. Esta solución proporciona una secuencia lógica de las funciones que se van a ejecutar para el funcionamiento de la solución escalada automáticamente.

Actualmente, la solución AutoScale disponible para NGFW no proporciona un plan de administración para comunicarse con la IP privada local a VNet y requiere IP pública para intercambiar comunicación entre Firepower Management Center y NGFW.

Este artículo pretende resolver este problema hasta que la solución verificada esté disponible para la comunicación de Firepower Management Center y NGFW a través de IP privada.

Configurar

Para crear una solución de NGFW de escala automática, se utiliza esta guía de configuración:

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

con varias modificaciones para poder abordar los siguientes casos prácticos:

- La aplicación de la función debe poder comunicarse con el segmento IP interno del cliente
- El equilibrador de carga no debe tener IP pública
- El tráfico de administración entre NGFW y FMC se debe intercambiar por el segmento de IP privada.

Para crear una solución de NGFW AutoScaled, con los casos de uso mencionados anteriormente debe modificarlos en los pasos mencionados en la Guía oficial de Cisco:

1. Azure ARM Template

La plantilla ARM se utiliza para habilitar la automatización en Azure. Cisco ha proporcionado una plantilla ARM verificada que se puede aprovechar para crear una solución de ampliación automática. Pero esta plantilla ARM disponible en Public Github

<https://github.com/CiscoDevNet/cisco->

[fdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template](https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git) crea una aplicación de funciones que no se puede hacer para comunicarse con la red interna del cliente aunque se pueda acceder a ella a través de rutas Express. Por lo tanto, necesitamos modificarlo un poco para que Function App pueda ahora utilizar el modo Premium en lugar del Modo de consumo. Por lo tanto, la plantilla ARM necesaria está disponible en https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

2. APP de función

La aplicación Function es un conjunto de funciones de Azure. La funcionalidad básica incluye:

- Comunicar/Sondear las métricas de Azure periódicamente.
- Supervise la carga de FTDv y active las operaciones de ampliación y ampliación.
- Registre un nuevo FTDv con el FMC.
- Configure un nuevo FTDv a través de FMC.
- Anule el registro (elimine) de un FTDv escalado del FMC.

Como se menciona en el requisito, las distintas funciones que se crean para la creación o eliminación de NGFW bajo demanda se realizan en función de la IP pública del NGFW. Por lo tanto, necesitamos ajustar el código C# para obtener la IP privada en lugar de la IP pública. Después de tejer el código, el archivo zip para crear la aplicación Function está disponible en https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

con el nombre ASM_Function.zip. Esto permite que la aplicación Functions se comunique con Recursos Internos sin tener la IP pública.

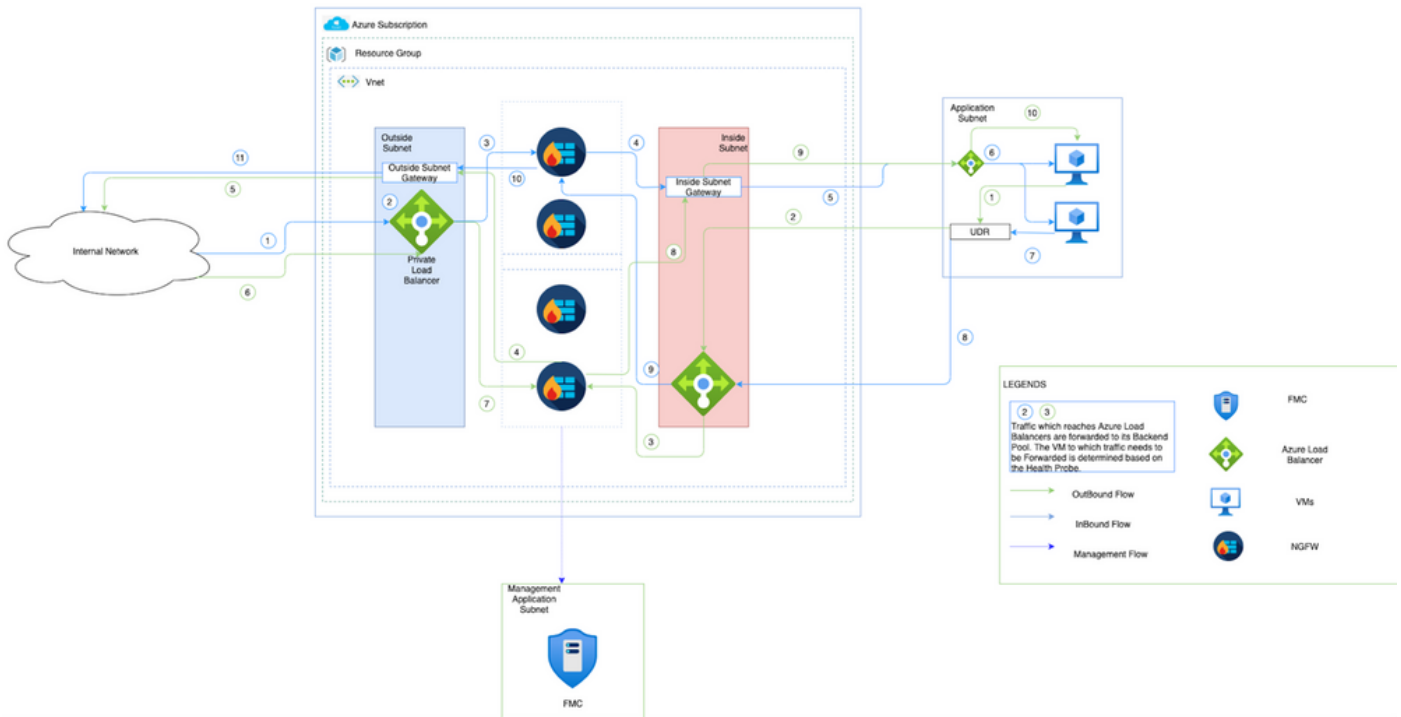
3. Aplicación lógica

La aplicación Auto Scale Logic es un flujo de trabajo, es decir, un conjunto de pasos en una secuencia. Las funciones de Azure son entidades independientes y no pueden comunicarse entre sí. Este orquestador secuenciará la ejecución de estas funciones e intercambiará información entre ellas.

- La aplicación lógica se utiliza para organizar y pasar información entre las funciones de Auto Scale Azure.
- Cada paso representa una función Auto Scale Azure o una lógica estándar integrada.
- La aplicación lógica se entrega como un archivo JSON.
- La aplicación lógica se puede personalizar mediante el archivo GUI o JSON.

Nota: El detalle de la aplicación lógica disponible en https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git debe modificarse cuidadosamente y los siguientes elementos deben sustituirse por detalles de implementación, nombre de FUNSTIONAPP, nombre del grupo de recursos, ID de SUSCRIPCIÓN.

Diagrama de la red



Esta imagen muestra cómo fluye el tráfico entrante y saliente dentro de un entorno de Azure a través de NGFW.

Configuraciones

Ahora, cree varios componentes necesarios para una solución escalada automáticamente.

1. Cree componentes de la lógica de escala automática.

Utilice la plantilla ARM y cree VMSS, Logic APP, Function APP, App Insight, Network Security Group.

Vaya a Inicio > Crear un recurso > Buscar plantilla y, a continuación, seleccione **Implementación de plantillas**. Ahora haga clic en **Crear** y crear su propia plantilla en el editor.

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. Haga clic en **Guardar**.

[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

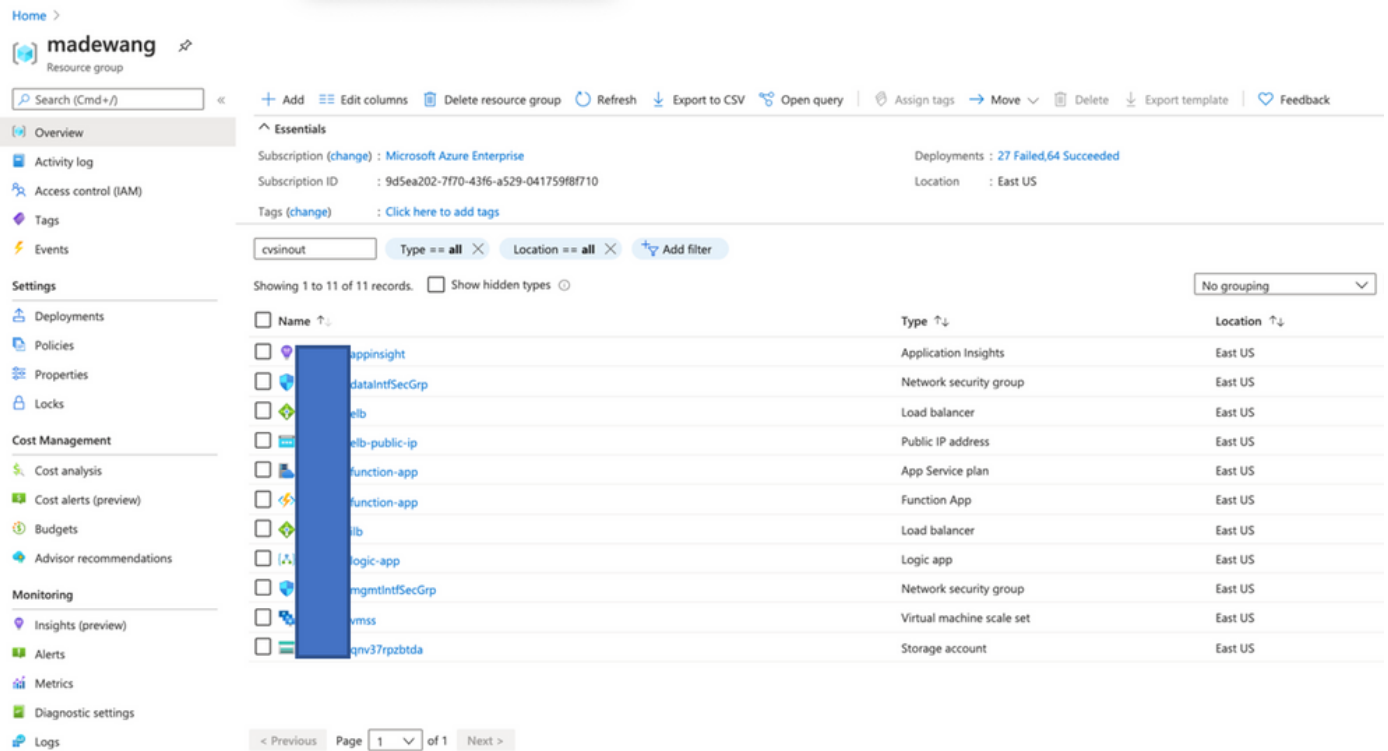
Review + create

< Previous

Next : Review + create >

Realice los cambios necesarios en esta plantilla y haga clic en **Revisar + Crear**.

3. Esto crea todos los componentes del grupo de recursos mencionado.

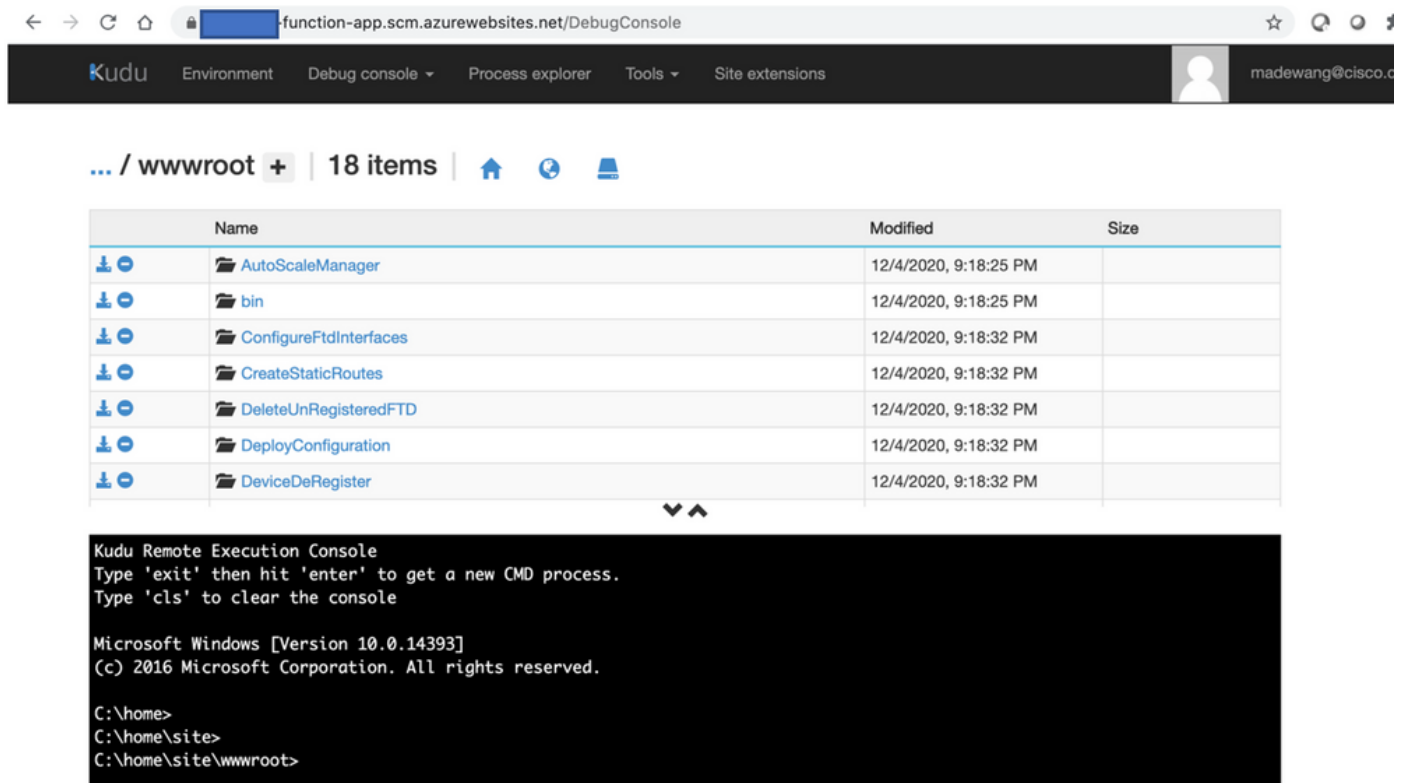


4. Inicie sesión en la url

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

Cargue el archivo **ASM_Function.zip** y **ftdssh.exe** en la carpeta **site/wwwroot/** (es obligatorio cargarlo en la ubicación especificada, de lo contrario la aplicación Function no identifica varias funciones).

Debería ser como esta imagen:



5. Active la aplicación **Function > Function**. Debería ver todas las funciones.

Home > madewang > [redacted] function-app

[fx] [redacted]-function-app | Functions
Function App

Search (Cmd+/) < + Add Refresh Delete

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events (preview)

Functions

[fx] Functions
App keys
App files
Proxies

Deployment
Deployment slots
Deployment Center
Deployment Center (Preview)

Settings
Configuration
Authentication / Authorization
Application Insights

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. Cambie el permiso de acceso para que VMSS pueda ejecutar las funciones dentro de la aplicación Function.

Vaya a <prefix>-vmss Access Control (IAM) > Add role assignment. Proporcione a este VMSS un acceso de colaborador a <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. Vaya a **Aplicación lógica > Vista Código lógico** y cambie el código lógico con el código disponible en

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

Aquí es necesario sustituir Azure Subscription, Resource Group Name y Function App Name antes de su uso; de lo contrario, no permite guardar correctamente.

8. Click **Save**. Vaya a Logic App Overview y Enable **Logic App**.

Verificación

Una vez habilitada la aplicación lógica, comienza inmediatamente a ejecutarse en el intervalo de 5 minutos.

Si todo está configurado correctamente, verá que las acciones de disparador se están realizando correctamente.

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	

Además, VM se crea bajo 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		Succeeded		Yes
out-vmss_2	out-vmss000002	Running		Succeeded		Yes

Inicie sesión en FMC y verifique que FMC y NGFW estén conectados a través de FTDv Private IP:

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

Mientras inicia sesión en la CLI de NGFW, verá lo siguiente:

```
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:~$
```

Por lo tanto, FMC se comunica con NGFW a través de Azure Private VNet Subnet.

Troubleshoot

A veces, Logic App falla mientras se crea un nuevo NGFW, para resolver tales problemas, se pueden realizar estos pasos:

1. Compruebe si la aplicación lógica se está ejecutando correctamente.

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

RECURRENCE 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	08585945096662968875411868431CU59	1.45 Seconds	
Failed	12/4/2020, 9:23 PM	08585945096748689653030909870CU58	1.74 Seconds	

2. Identifique la causa del error.
 Haga clic en el disparador que ha fallado.

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

Intente identificar el punto de falla del flujo de código. Del fragmento anterior, está claro que la lógica de ASM falló porque no pudo conectarse a FMC. A continuación, debe identificar por qué FMC no se pudo alcanzar según el flujo dentro de Azure.