Distribuisci FTDv con scalabilità automatica in Azure in un ambiente con attendibilità elevata

Sommario

Introduzione

In questo documento viene descritto come distribuire Cisco Firepower Threat Defense Virtual (FTDv) con scalabilità automatica in Azure in un ambiente ad alta attendibilità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- NGFW e Firepower Management Center devono comunicare su IP privato
- Il servizio di bilanciamento del carico esterno non deve avere IP pubblico.
- L'app della funzione deve essere in grado di comunicare con IP privato

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Azure
- Firepower Management Center
- Set di scalabilità macchina virtuale

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FTDv introduce la funzionalità Cisco Firepower Next-Generation Firewall negli ambienti virtualizzati, consentendo policy di sicurezza coerenti per seguire i carichi di lavoro negli ambienti fisici, virtuali e cloud e tra cloud.

Poiché queste installazioni sono disponibili in un ambiente virtualizzato, attualmente il supporto per HA non è disponibile per NGFW. Pertanto, per fornire una soluzione a disponibilità elevata, Cisco Next-Generation Firewall (NGFW) utilizza le funzionalità native di Azure, ad esempio Set di disponibilità e Virtual Machine Scale Set (VMSS), per rendere NGFW altamente disponibile e gestire l'aumento del traffico su richiesta.

Questo documento è incentrato sulla configurazione di Cisco NGFW per AutoScale in base a diversi parametri in cui NGFW esegue la scalabilità su richiesta o in scalabilità orizzontale. In questo caso viene descritto il caso di utilizzo in cui il cliente ha la necessità di utilizzare Firepower Management Center (FMC), disponibile nel centro dati di co-locazione e necessario per gestire centralmente tutti i NGFW, anche i clienti non vogliono avere FMC e FTD per comunicare tramite IP pubblico per il traffico di gestione.

Prima di approfondire la configurazione e la progettazione, di seguito sono riportati alcuni concetti che dovrebbero essere ben compresi in Azure:

- Area di disponibilità: Un'area di disponibilità è un'offerta ad alta disponibilità che protegge le applicazioni e i dati dai guasti dei data center. Le aree di disponibilità sono posizioni fisiche univoche all'interno di un'area di Azure. Ogni zona è costituita da uno o più centri dati dotati di alimentazione, raffreddamento e reti indipendenti.

- RETE VIRTUALE: Rete virtuale di Azure è il blocco predefinito fondamentale per la rete privata in Azure. VNet consente a molti tipi di risorse di Azure, ad esempio Macchine virtuali di Azure, di comunicare tra loro in modo sicuro, tramite Internet e reti locali. VNet è simile a una rete tradizionale che viene gestita nel proprio centro dati ma offre ulteriori vantaggi dell'infrastruttura di Azure, ad esempio scalabilità, disponibilità e isolamento. Per impostazione predefinita, ogni subnet all'interno di una rete virtuale è raggiungibile, ma lo stesso non accade per le subnet in reti virtuali diverse.

- Set di disponibilità: I set di disponibilità rappresentano un'altra configurazione del centro dati per fornire ridondanza e disponibilità delle VM. Questa configurazione all'interno di un centro dati garantisce che durante un evento di manutenzione pianificato o non pianificato, almeno una macchina virtuale sia disponibile e soddisfi il 99,95% del contratto di servizio di Azure.

- VMSS: I set di scalabilità delle macchine virtuali di Azure consentono di creare e gestire un gruppo di macchine virtuali con carico bilanciato. Il numero di istanze di VM può aumentare o diminuire automaticamente in risposta a una richiesta o a una pianificazione definita. I set di scalabilità forniscono elevata disponibilità alle applicazioni e consentono di gestire, configurare e aggiornare centralmente un numero elevato di VM. Con i set di scalabilità delle

macchine virtuali è possibile creare servizi su larga scala per aree quali l'elaborazione, i big data e i carichi di lavoro dei contenitori.

- **App Funzioni:** Azure Functions è un servizio cloud disponibile su richiesta che fornisce tutte le risorse e l'infrastruttura costantemente aggiornate necessarie per eseguire le applicazioni. È possibile concentrarsi sulle parti di codice più importanti e le funzioni di Azure gestiscono il resto. È possibile utilizzare le funzioni di Azure per compilare API Web, rispondere alle modifiche del database, elaborare flussi IoT, gestire code di messaggi e altro ancora. In questa soluzione con scalabilità automatica, la funzione di Azure è costituita da varie richieste API inviate a FMC per la creazione di oggetti, la registrazione/annullamento della registrazione di FTDv, la verifica dei parametri e così via.

- **App per la logica:** App per la logica di Azure è un servizio cloud che consente di pianificare, automatizzare e orchestrare attività, processi aziendali e flussi di lavoro quando è necessario integrare app, dati, sistemi e servizi in aziende o organizzazioni. Le app per la logica semplificano la progettazione e la creazione di soluzioni scalabili per l'integrazione di app, dati, sistemi, applicazioni aziendali (EAI, Enterprise Application Integration) e comunicazioni business-to-business (B2B, Business-to-Business), sia nel cloud che on-premises o in entrambi. Questa soluzione fornisce la sequenza logica delle funzioni da eseguire per il funzionamento della soluzione con scalabilità automatica.

Attualmente, la soluzione AutoScale disponibile per NGFW non fornisce un piano di gestione per comunicare con l'IP privato locale alla rete virtuale e richiede l'IP pubblico per scambiare la comunicazione tra Firepower Management Center e NGFW.

Questo articolo mira a risolvere il problema finché la soluzione verificata non sarà disponibile per Firepower Management Center e la comunicazione NGFW su IP privato.

Configurazione

Per creare una soluzione NGFW con scalabilità automatica, utilizzare la presente guida alla configurazione:

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 varie modifiche, in modo da poter affrontare i seguenti casi di utilizzo:

- L'app della funzione deve essere in grado di comunicare con il segmento IP interno del cliente
- Il servizio di bilanciamento del carico non deve avere IP pubblico
- Il traffico di gestione tra NGFW e FMC deve essere scambiato sul segmento IP privato.

Per creare una soluzione AutoScaled NGFW, con i casi di utilizzo sopra menzionati è necessario modificare questi elementi nelle fasi indicate nella Guida ufficiale di Cisco:

1. **Modello di Azure ARM**

Il modello ARM viene utilizzato per abilitare l'automazione in Azure. Cisco ha fornito un modello ARM verificato che può essere utilizzato per creare una soluzione di scalabilità automatica. Ma questo modello ARM disponibile su Public Github https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template crea un'App Functions che non può essere resa disponibile per comunicare con la rete interna del Cliente anche se è

raggiungibile tramite Express Routes. Pertanto è necessario modificare leggermente questo elemento in modo che Function App possa ora utilizzare la modalità Premium anziché la modalità di consumo. Il modello ARM richiesto è disponibile all'indirizzo https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

2. Funzione APP

L'app per le funzioni è un insieme di funzioni di Azure. Le funzionalità di base includono:

- Comunica/esamina periodicamente le metriche di Azure.
- Monitoraggio del carico FTDv e attivazione delle operazioni di scalabilità in entrata/uscita.
- Registrare un nuovo FTDv presso il CCP.
- Configurare un nuovo FTDv tramite FMC.
- Annullare la registrazione (rimuovere) di un FTDv con ridimensionamento del CCP.

Come indicato nel requisito, la funzione che viene creata per la creazione o l'eliminazione di NGFW on-demand è basata sull'IP pubblico di NGFW. È quindi necessario modificare il codice C# per ottenere IP privato anziché pubblico. Dopo aver modificato il codice, il file zip per la creazione dell'applicazione Function è disponibile all'indirizzo https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

con il nome ASM_Function.zip. Ciò consente all'app Funzioni di comunicare con le risorse interne senza disporre dell'IP pubblico.

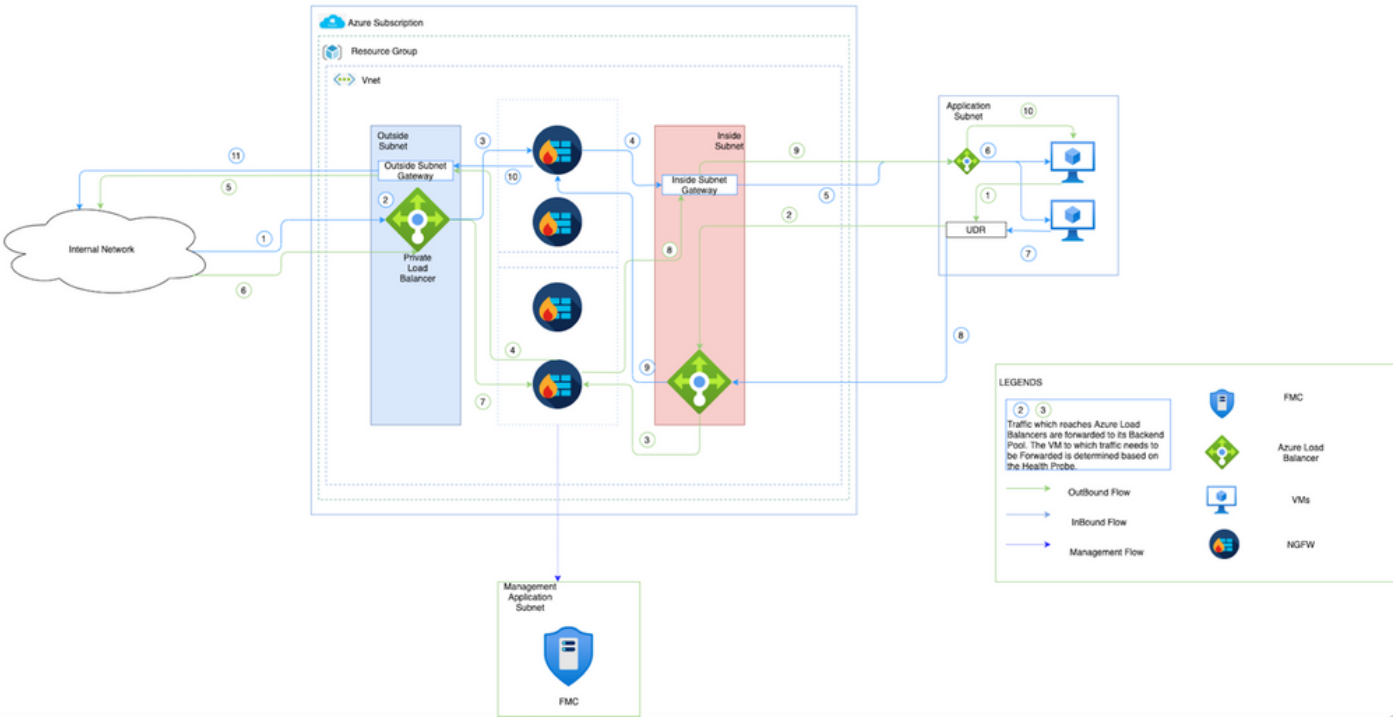
3. App per la logica

L'app per la logica di scalabilità automatica è un flusso di lavoro, ovvero un insieme di passaggi in una sequenza. Le funzioni di Azure sono entità indipendenti e non possono comunicare tra loro. Questo orchestrator sequenzia l'esecuzione di queste funzioni e scambia informazioni tra di esse.

- L'app per la logica viene utilizzata per orchestrare e passare informazioni tra le funzioni di scalabilità automatica di Azure.
- Ogni passaggio rappresenta una funzione di Azure con ridimensionamento automatico o una logica standard incorporata.
- L'app per la logica viene recapitata come file JSON.
- L'app per la logica può essere personalizzata tramite il file GUI o JSON.

> **Nota:** I dettagli dell'app per la logica disponibili all'indirizzo https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git devono essere modificati con attenzione e i seguenti elementi devono essere sostituiti con dettagli sulla distribuzione, nome FUNSTIONAPP, nome del GRUPPO DI RISORSE, ID SOTTOSCRIZIONE.

Esempio di rete



In questa immagine viene mostrato il flusso del traffico in entrata e in uscita all'interno di un ambiente Azure tramite NGFW.

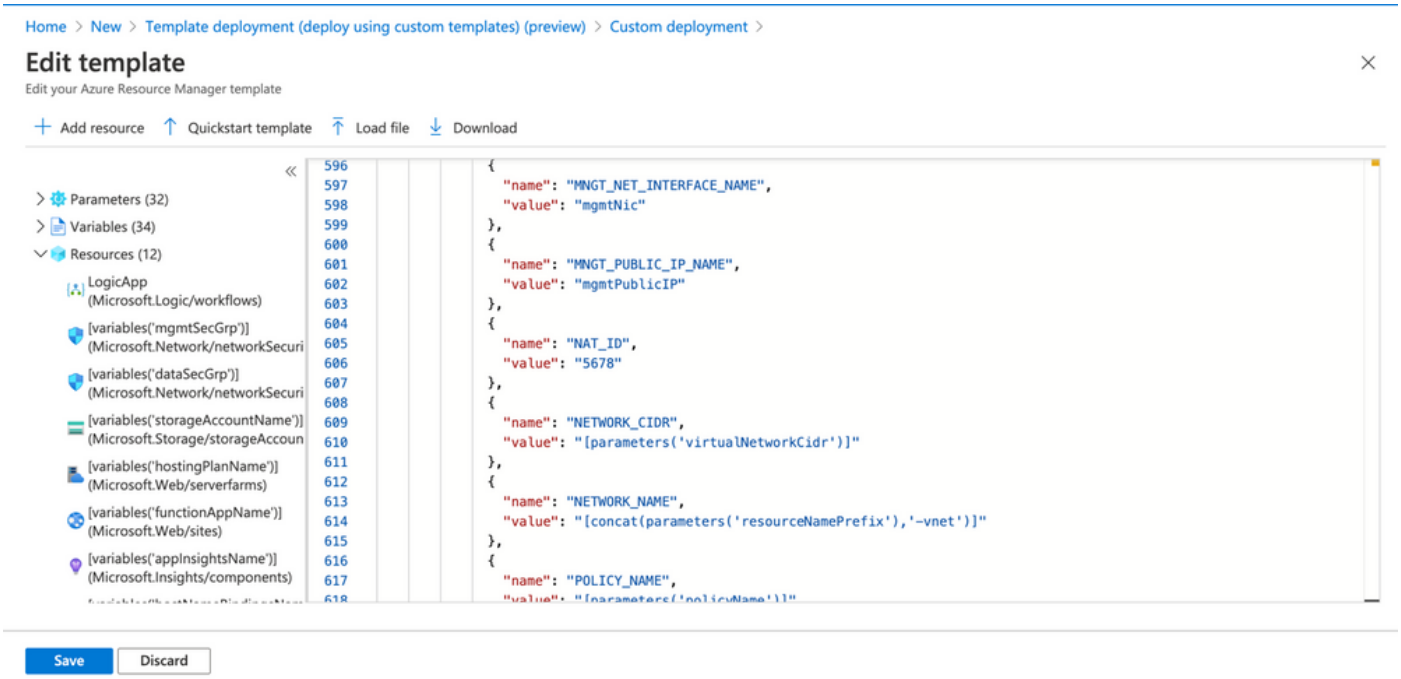
Configurazioni

Creare i vari componenti necessari per una soluzione con scalabilità automatica.

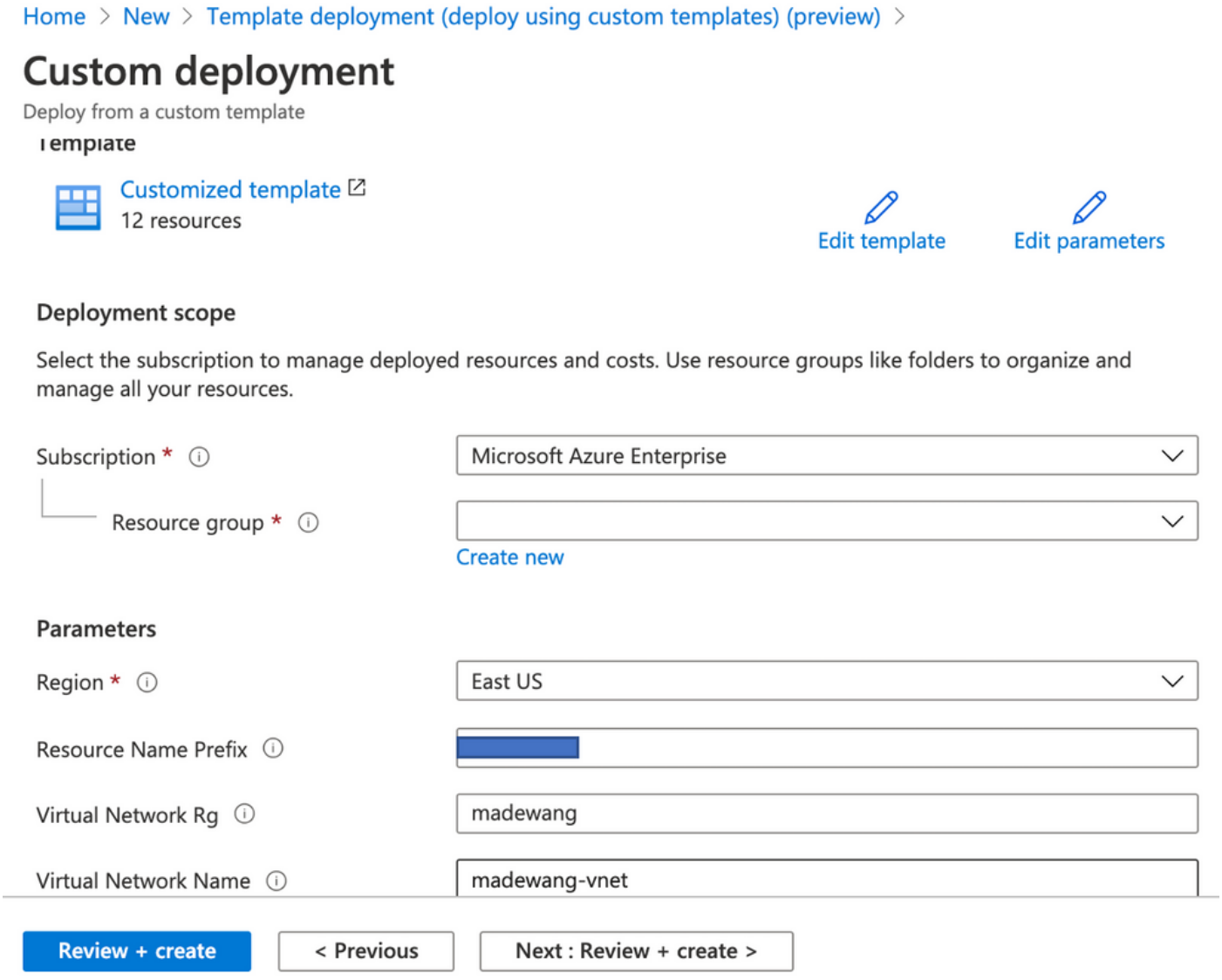
1. Creare i componenti della logica di scalabilità automatica.

Usare il modello ARM e creare VMSS, APP logica, APP funzioni, App Insight, Network Security Group.

Passare a **Home > Crea risorsa > Cerca modello** e quindi selezionare **Distribuzione modello**. Fare clic su **Create** and build your own template in the editor (Crea e crea un modello personalizzato nell'editor).

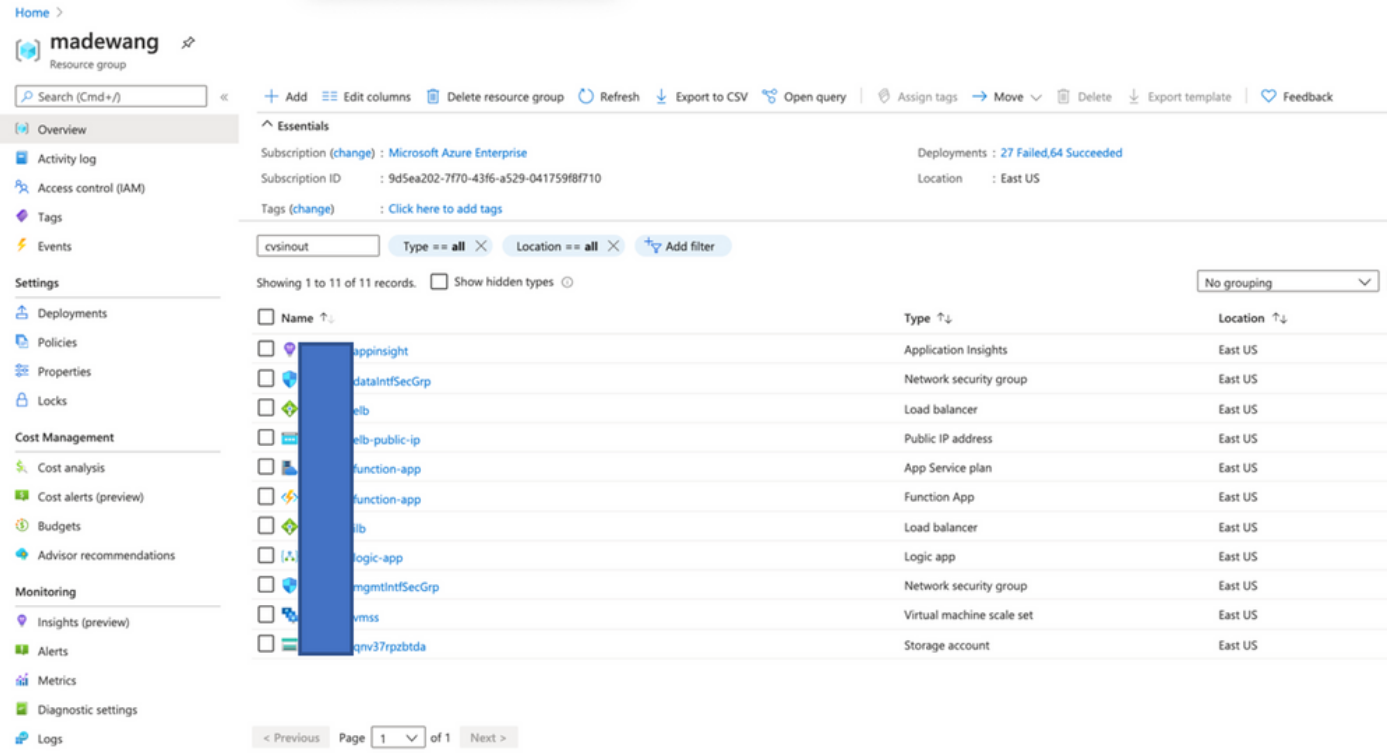


2. Fare clic su **Save** (Salva).



Apportare le modifiche necessarie al modello e fare clic su **Revisione +Crea**.

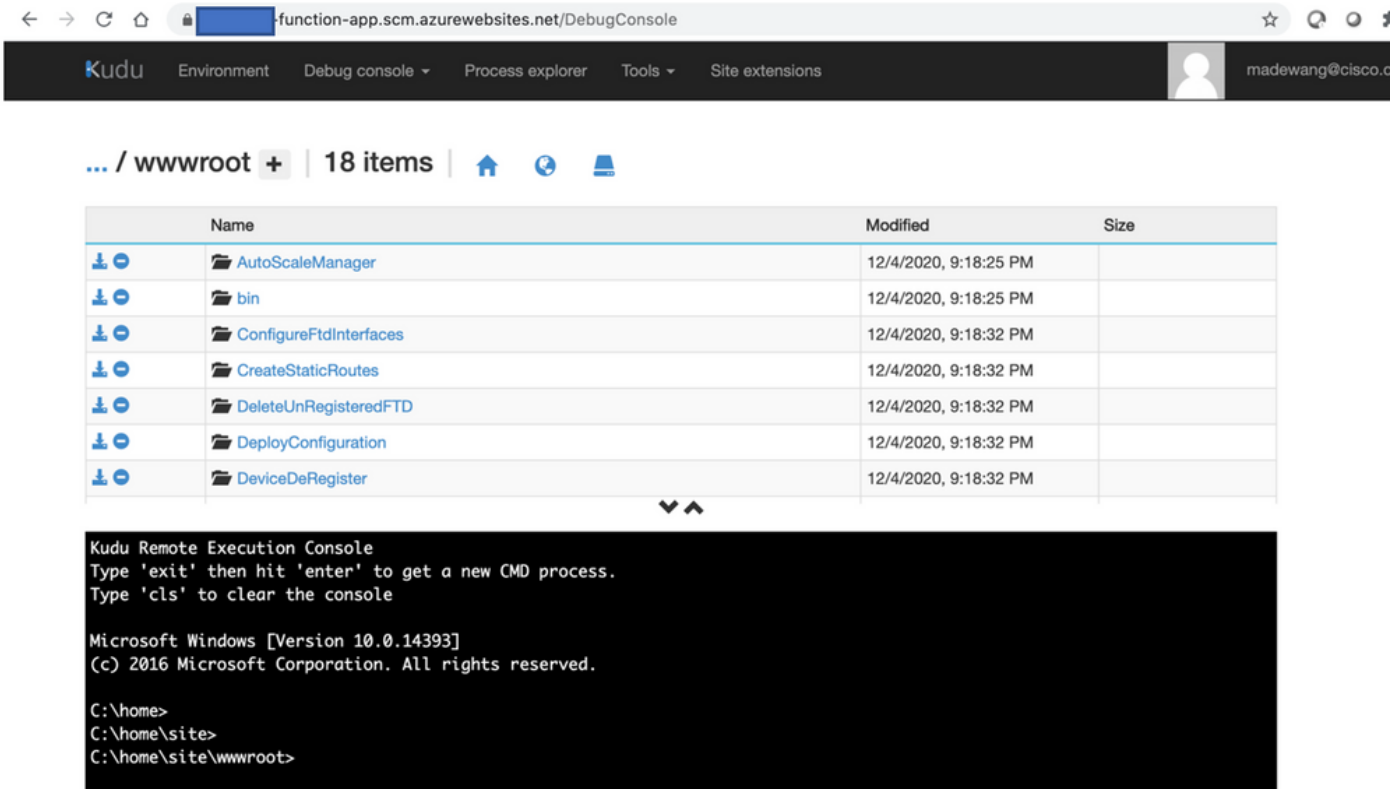
3. In questo modo vengono creati tutti i componenti del gruppo di risorse indicato.



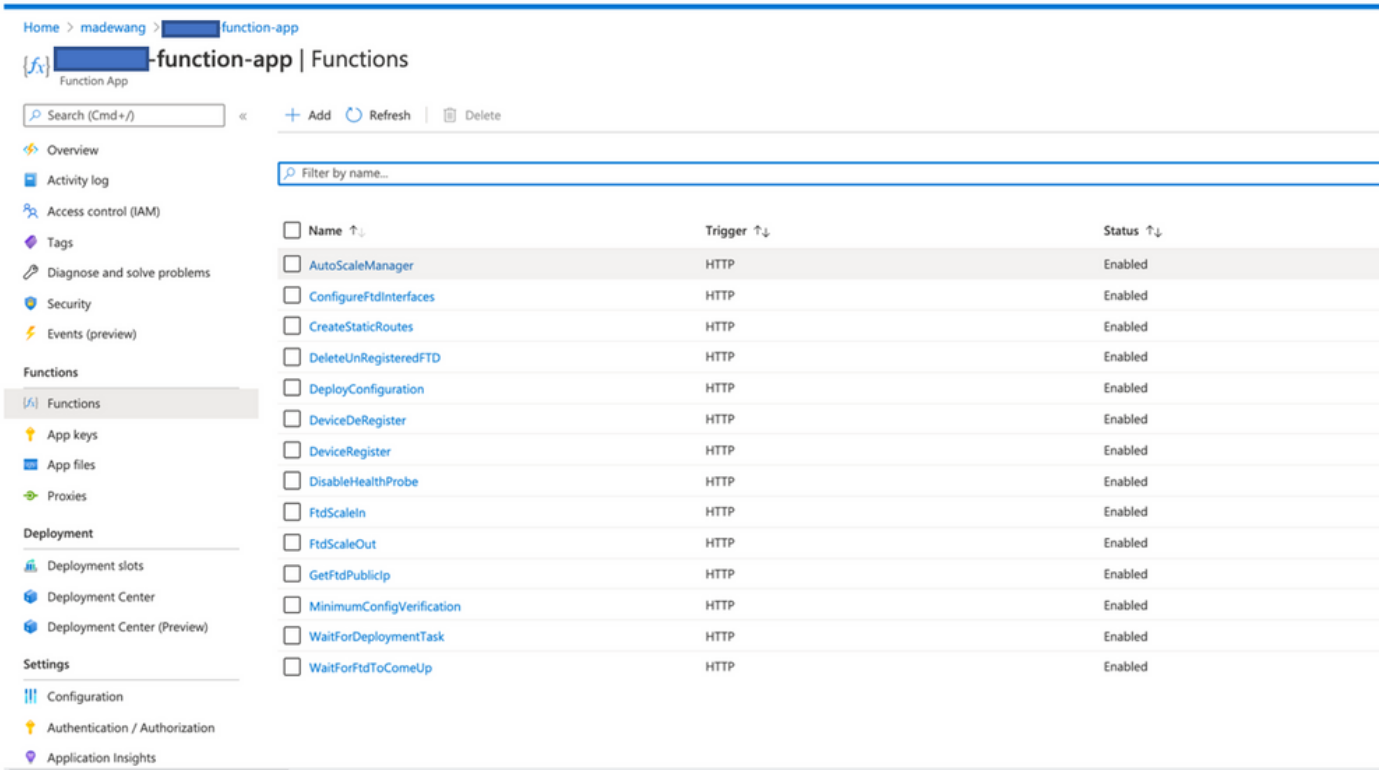
4. Accedere all'URL
https://<nome_app_funzione>.scm.azurewebsites.net/DebugConsole

Caricare il file **ASM_Function.zip** e **ftdssh.exe** nella cartella **site/wwwroot/** (è obbligatorio caricarlo nella posizione specificata, altrimenti l'applicazione Function non identifica diverse funzioni).

L'immagine dovrebbe essere simile alla seguente:

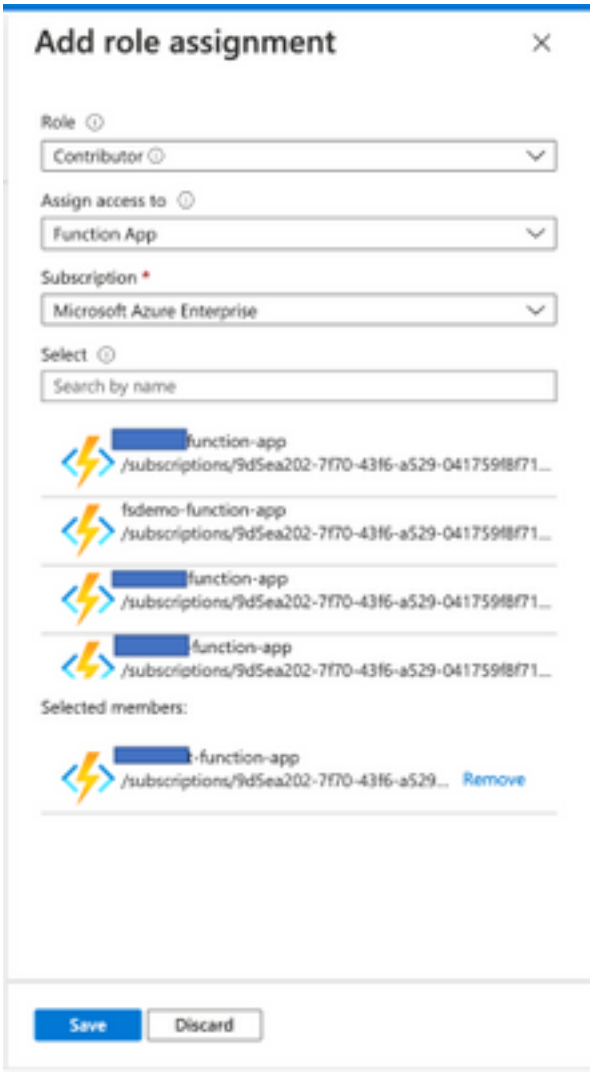


5. Archiviare l'**app Funzione > Funzione**. Verranno visualizzate tutte le funzioni.



6. Modificare l'autorizzazione di accesso in modo che VMSS possa eseguire le funzioni all'interno dell'app per le funzioni.

Passare a **<prefix>-vmss> Access Control (IAM) > Aggiungi assegnazione ruolo**. Fornire a questo servizio Copia Shadow del volume un accesso collaboratore a **<prefix>-function-app**



Fare clic su **Salva**.

7. Passare a **App per la logica > Vista codice logico** e modificare il codice logico con il codice disponibile in

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

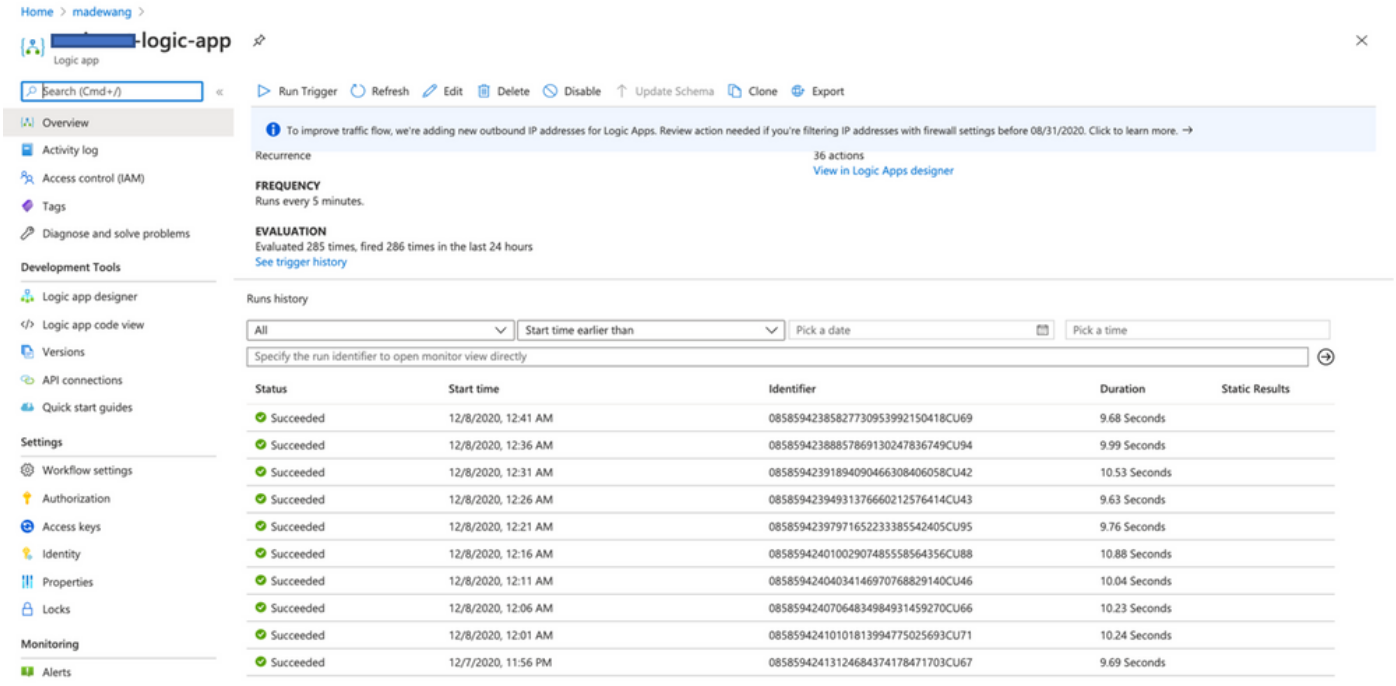
Ènecessario sostituire la sottoscrizione di Azure, il nome del gruppo di risorse e il nome dell'app per le funzioni prima dell'uso, altrimenti il salvataggio non verrà eseguito correttamente.

8. Fare clic su **Salva**. Passare a Panoramica app per la logica e Abilita **app per la logica**.

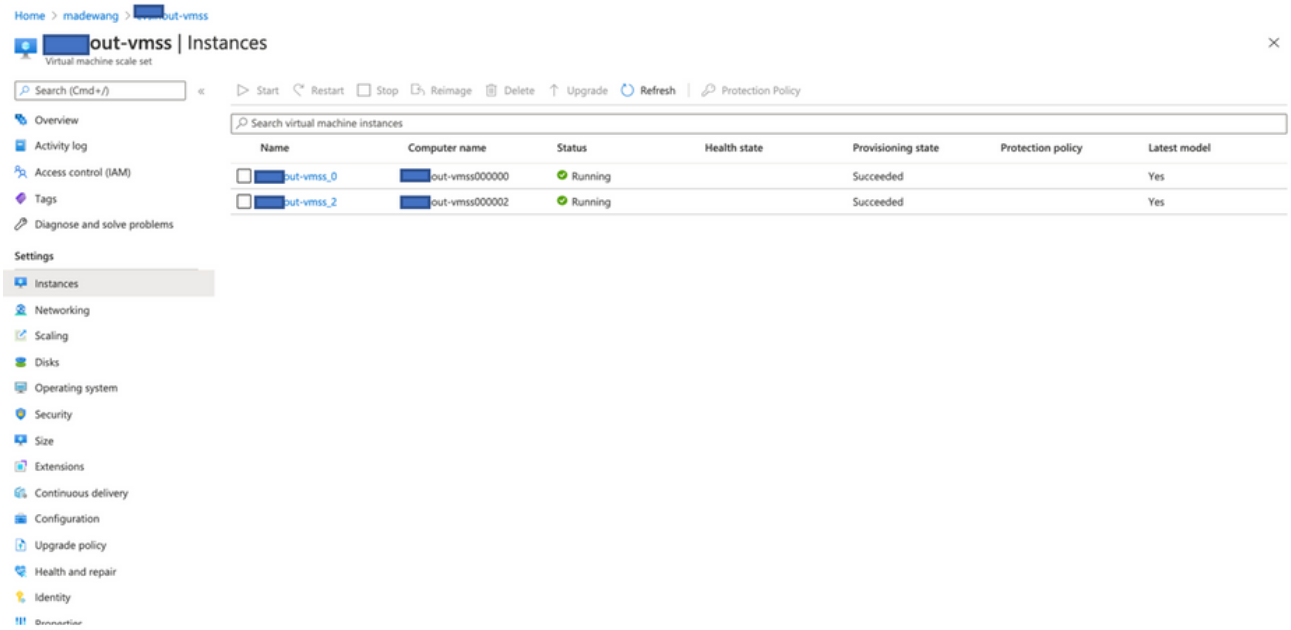
Verifica

Una volta abilitata l'app per la logica, l'esecuzione viene avviata immediatamente nell'intervallo di 5 minuti.

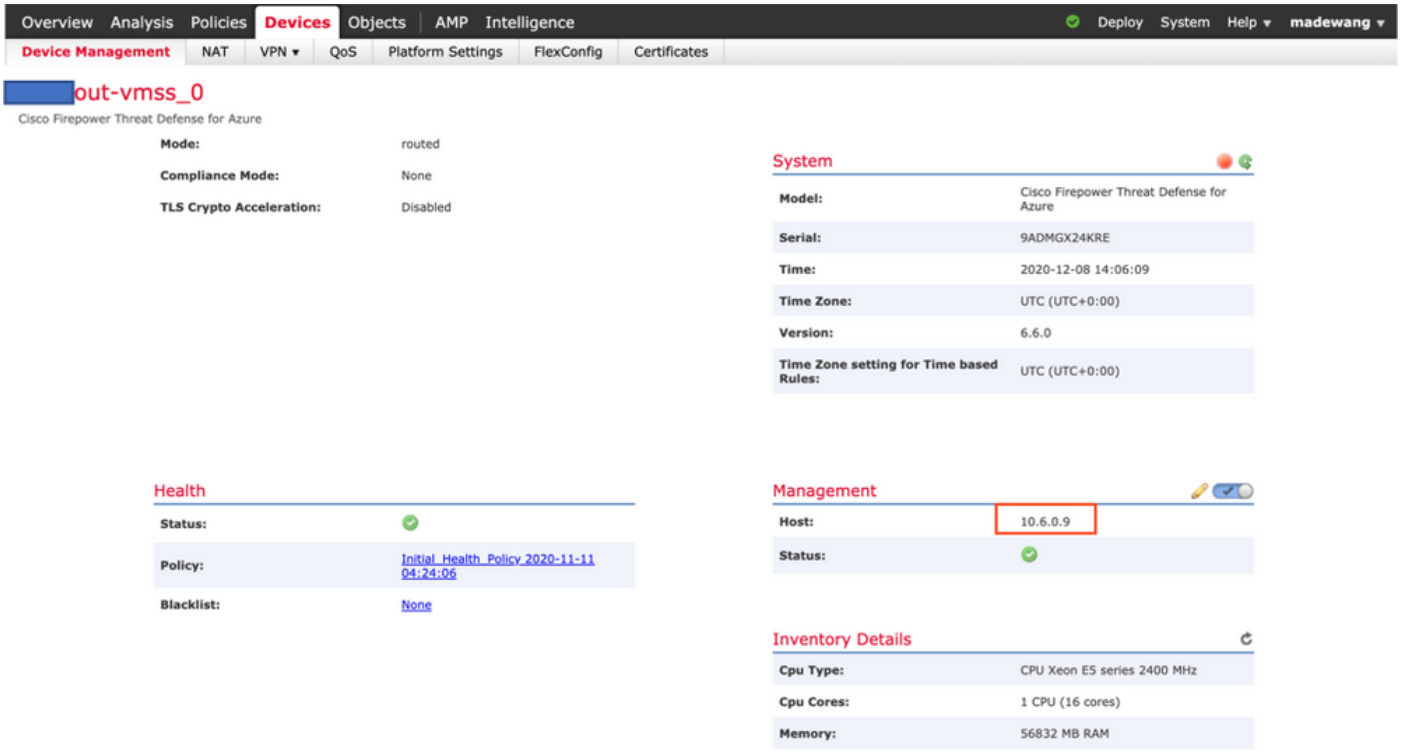
Se tutto è configurato correttamente, le azioni di attivazione avranno esito positivo.



Inoltre, la VM viene creata in VMSS.



Accedere al CCP e verificare che il CCP e il NGFW siano collegati tramite IP privato FTDv:



Quando si accede alla CLI di NGFW, vengono visualizzati i seguenti elementi:

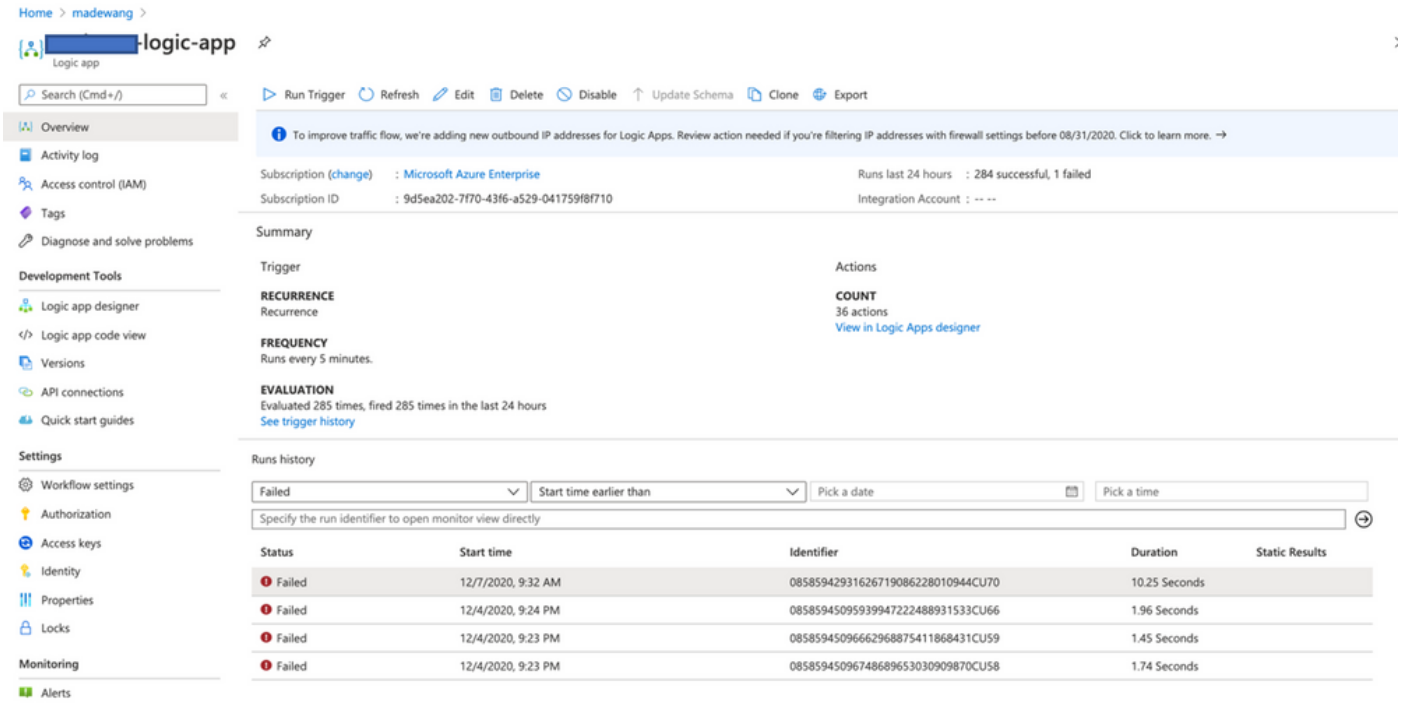
```
Cisco Fire Linux OS v6.6.0 (build 37)
Cisco Firepower Threat Defense for Azure v6.6.0 (build 90)

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

Pertanto FMC comunica a NGFW tramite la subnet VPN privata di Azure.

Risoluzione dei problemi

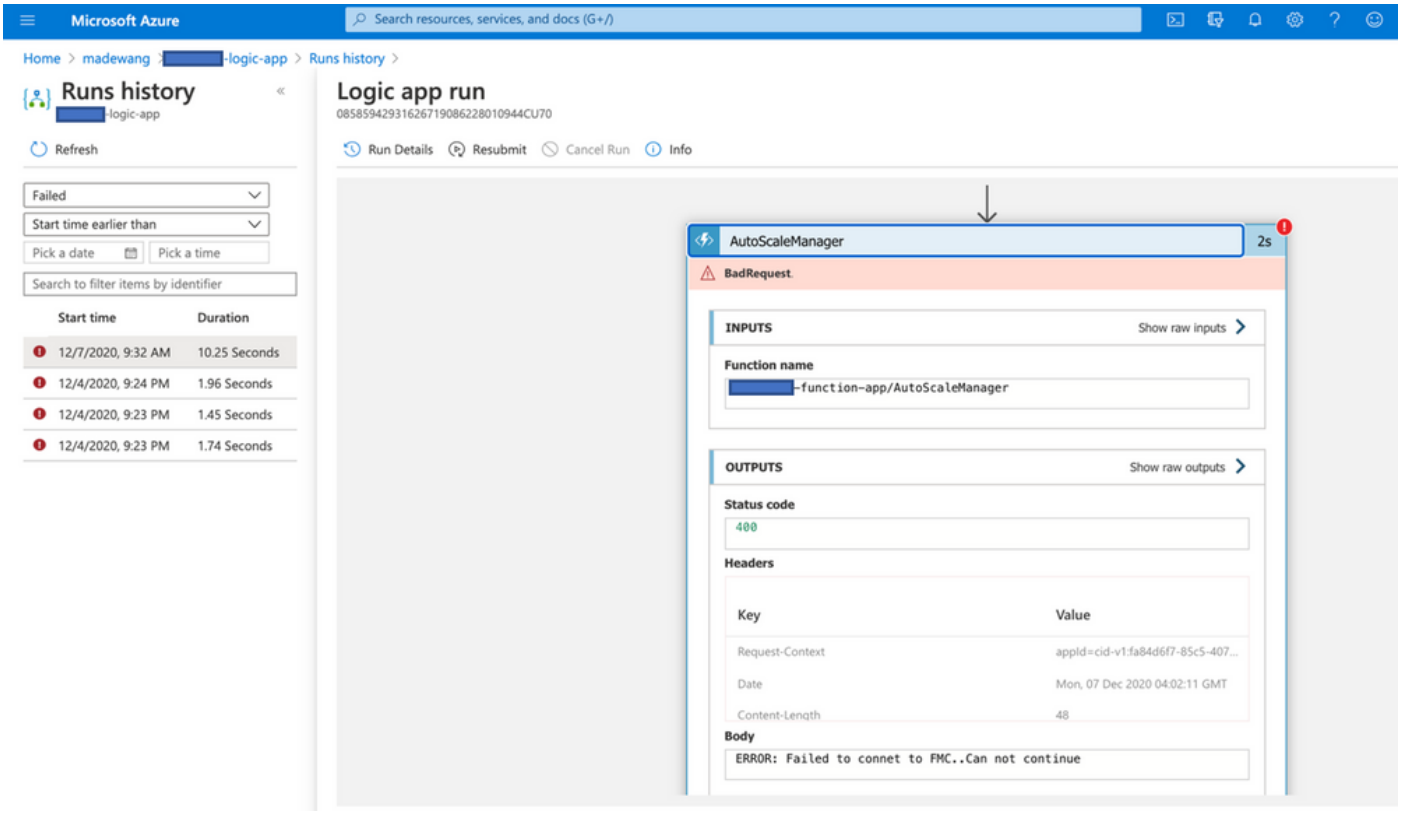
A volte l'app per la logica si interrompe durante la creazione di un nuovo NGFW. Per risolvere questo problema, è possibile eseguire le seguenti operazioni:

1. Verificare che l'app per la logica sia in esecuzione.



2. Identificare la causa del fallimento.

Fare clic sul trigger non riuscito.



Provare a identificare il punto di errore dal flusso di codice. Dal frammento di codice sopra riportato è evidente che la logica ASM non è riuscita in quanto non è stata in grado di connettersi a FMC. È quindi necessario identificare il motivo per cui FMC non è raggiungibile in base al flusso in Azure.